



Your reliable networking solutions partner

User's Guide

Dray Tek

VigorAP 800 Wireless Access Point User's Guide

Version: 1.12 Firmware Version: V1.0.2 Date: 13/11/2012



Copyright Information

Copyright Declarations	Copyright 2012 All rights reserved. This publication contains information that is protected by copyright. No part may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language without written permission from the copyright holders.	
Trademarks	 The following trademarks are used in this document: Microsoft is a registered trademark of Microsoft Corp. Windows, Windows 95, 98, Me, NT, 2000, XP, Vista and Explorer are trademarks of Microsoft Corp. Apple and Mac OS are registered trademarks of Apple Inc. Other products may be trademarks or registered trademarks of their respective manufacturers. 	

Safety Instructions and Approval

Safety Instructions	 Read the installation guide thoroughly before you set up the modem. The modem is a complicated electronic unit that may be repaired only be authorized and qualified personnel. Do not try to open or repair the modem yourself. Do not place the modem in a damp or humid place, e.g. a bathroom. The modem should be used in a sheltered area, within a temperature range of +5 to +40 Celsius. Do not expose the modem to direct sunlight or other heat sources. The housing and electronic components may be damaged by direct sunlight or heat sources. Do not deploy the cable for LAN connection outdoor to prevent electronic shock hazards. Keep the package out of reach of children. When you want to dispose of the modem, please follow local regulations on conservation of the environment.
Warranty	We warrant to the original end user (purchaser) that the modem will be free from any defects in workmanship or materials for a period of one (1) year from the date of purchase from the dealer. Please keep your purchase receipt in a safe place as it serves as proof of date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, we will, at our discretion, repair or replace the defective products or components, without charge for either parts or labor, to whatever extent we deem necessary 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 Owner	Web registration is preferred. You can register your Vigor modem via http://www.draytek.com.
Firmware & Tools Updates	Due to the continuous evolution of DrayTek technology, all modems will be regularly upgraded. Please consult the DrayTek web site for more information on newest firmware, tools and documents.
	http://www.draytek.com



European Community Declarations

Manufacturer: DrayTek Corp.

Address:No. 26, Fu Shing Road, Hukou Township, Hsinchu Industrial Park, Hsinchu County, Taiwan 303Product:VigorAP 800

DrayTek Corp. declares that VigorAP 800 is in compliance with the following essential requirements and other relevant provisions of R&TTE Directive 1999/5/EEC.

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.

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



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.



Dray Tek

Table of Contents



Preface	.1
1.1 Introduction	
1.2 LED Indicators and Connectors	2
1.3 Hardware Installation	4
 1.3.1 Wired Connection for PC in LAN 1.3.2 Wired Connection for Notebook in WLAN 1.3.2 Wireless Connection 1.3.3 POE Connection 	5 6



Network Configuration	9
2.1 Windows 95/98/Me IP Address Setup	9
2.2 Windows 2000 IP Address Setup	11
2.3 Windows XP IP Address Setup	12
2.4 Windows Vista IP Address Setup	13
2.5 Accessing to Web User Interface	14
2.6 Changing Password	15
2.7 Quick Start Wizard	16
 2.7.1 Configuring 2.4G Wireless Settings – General 2.7.2 Configuring 2.4G Wireless Settings based on the Operation Mode 2.7.3 Configuring 5G Wireless Settings 2.7.4 Finishing the Wireless Settings Wizard 	17 20
2.8 Online Status	22



Web Configuration	23
3.1 Operation Mode	
3.2 LAN	25
3.3 General Concepts for Wireless LAN	
3.4 Wireless LAN Settings for AP Mode	29
 3.4.1 General Setup	
3.5 Wireless LAN Settings for Station-Infrastructure Mode	



 3.5.1 General Setup 3.5.2 Site Survey 3.5.3 Statistics	45 45
3.6 Wireless LAN Settings for AP Bridge-Point to Point/AP Bridge-Point to Multi-Point Mode	48
3.6.1 General Setup 3.6.2 AP Discovery 3.6.3 WDS AP Status	51
3.7 Wireless LAN Settings for AP Bridge-WDS Mode	53
 3.7.1 General Setup	58 60 62 62 64
3.8 Wireless LAN Settings for Universal Repeater Mode	65
 3.8.1 General Setup	69 73 74 75 76
3.9 Wireless LAN (5G) Settings for AP Mode	79
 3.9.1 General Setup	80 83 84
3.10 RADIUS Server	87
3.11 System Maintenance	88
 3.11.1 System Status	89 90 91 92
3.12 Diagnostics	93
3.13 Support Area	94



Application and Examples	97
4.1 Upgrade Firmware for Your Modem	97
4.2 How to set different segments for different SSIDs in VigorAP 800	100



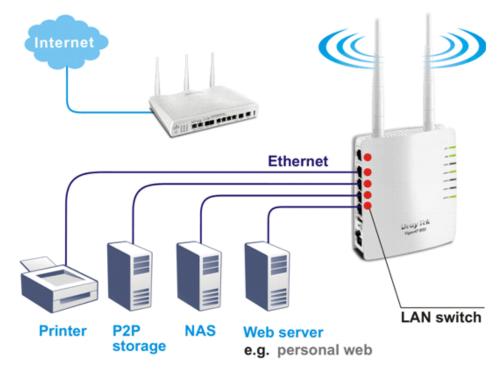
Trouble Shooting	103
5.1 Checking If the Hardware Status Is OK or Not	. 103
5.2 Checking If the Network Connection Settings on Your Computer Is OK or Not	. 104
5.3 Pinging the Modem from Your Computer	. 106
5.4 Backing to Factory Default Setting If Necessary	. 107
5.5 Contacting Your Dealer	. 108



1.1 Introduction

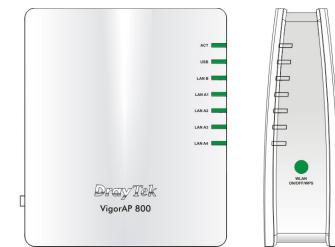
Thank you for purchasing this VigorAP 800! With this high cost-efficiency VigorAP 800, computers and wireless devices which are compatible with 802.11n can connect to existing wired Ethernet network via this VigorAP 800, at the speed of 300Mbps.

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.	
USB	On	A USB device is connected and active.	
	Blinking	The data is transmitting.	
LAN B	On	A normal connection is through its corresponding port.	
	Off	LAN is disconnected.	
	Blinking	Data is transmitting (sending/receiving).	
LAN A1 - A4	On	A normal connection is through its corresponding port.	
	Off	LAN is disconnected.	
WLAN	On	Wireless function is ready.	
(Green LED) on	Off	Wireless function is not ready.	
WLAN button	Blinking	Data is transmitting (sending/receiving).	
WPS	Off	The WPS is off.	
(Orange LED) on WLAN button	Blinking (Orange)	Blink with 1 second cycle for 2 minutes WPS is enabled and waiting for wireless client to connect with it.	
	Blinking (Orange)	Data is transmitting (sending/receiving).	
WPS Button	Press this button for 2 seconds to wait for client device making network connection through WPS. When the orange LED lights up, the WPS will be on.		

	Interface	Description
	LAN B	Connecter for xDSL / Cable modem or router.
	LAN A1 (PoE) -	Connecter for xDSL / Cable modem or router.
	A4	
	USB	Connector for future use.
	Factory Reset	Restore the default settings. Usage: Turn on VigorAP 800. Press the button and keep for more than 10 seconds. Then VigorAP 800 will restart with the
Ar - LAN US	ON OFF PWR	factory default configuration. ON/OFF: Power switch. PWR: Connecter for a power adapter.

1.3 Hardware Installation

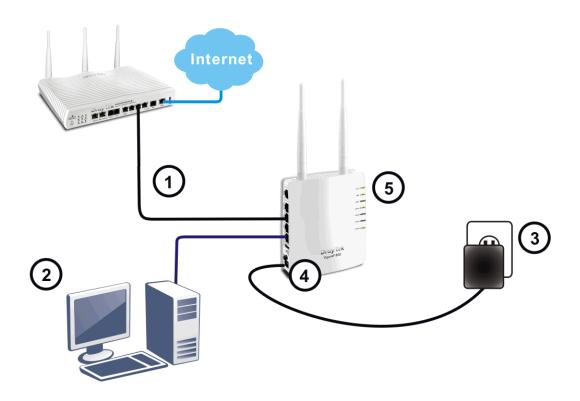
This section will guide you to install the modem through hardware connection and configure the modem's settings through web browser.

Before starting to configure the modem, you have to connect your devices correctly.

1.3.1 Wired Connection for PC in LAN

- 1. Connect VigorAP 800 to ADSL modem, router, or switch/hub in your network through the LAN A port of the access point by Ethernet cable.
- 2. Connect a computer to other available LAN A port. Make sure the subnet IP address of the PC is the same as VigorAP 800 management IP, e.g., **192.168.1.X**.
- 3. Connect the A/C power adapter to the wall socket, and then connect it to the PWR connector of the access point.
- 4. Power on VigorAP 800.
- 5. Check all LEDs on the front panel. **ACT** LED should be steadily on, **LAN** LEDs should be on if the access point is correctly connected to the ADSL modem or router.

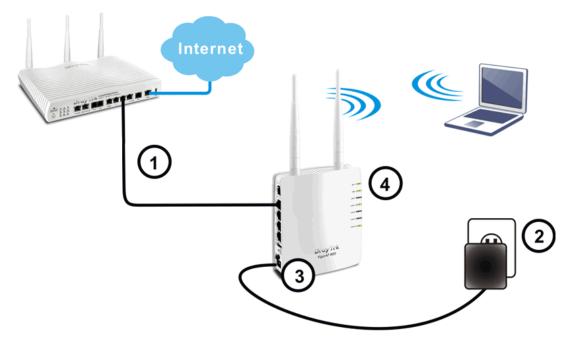
(For the detailed information of LED status, please refer to section 1.2.)



1.3.2 Wired Connection for Notebook in WLAN

- 1. Connect VigorAP 800 to ADSL modem or router in your network through the LAN A port of the access point by Ethernet cable.
- 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 800.
- 4. Check all LEDs on the front panel. **ACT** LED should be steadily on, **LAN** LEDs should be on if the access point is correctly connected to the ADSL modem or router.

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



1.3.2 Wireless Connection

VigorAP 800 can access Internet via an ADSL modem, router, or switch/hub in your network through wireless connection.

- 1. Connect VigorAP 800 to ADSL modem or router via wireless network.
- 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 800.
- 4. Check all LEDs on the front panel. **ACT** LED should be steadily on, **LAN** LEDs should be on if VigorAP 800 is correctly connected to the ADSL modem, router or switch/hub.

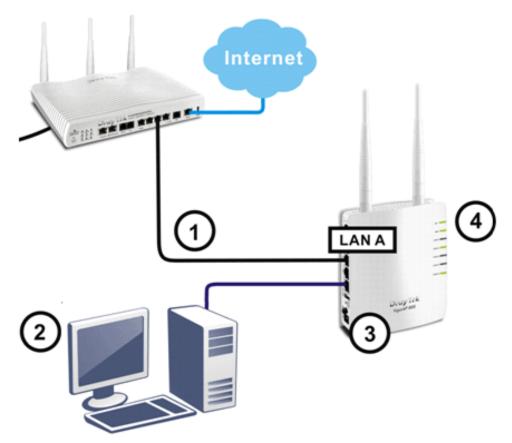
(For the detailed information of LED status, please refer to section 1.2.)



1.3.3 POE Connection

VigorAP 800 can gain the power from the connected switch, e.g., VigorSwitch P2260. PoE (Power over Ethernet) can break the install limitation caused by the fixed power supply.

- 1. Connect VigorAP 800 to a switch in your network through the LAN A1 port of the access point by Ethernet cable.
- 2. Connect a computer to LAN A2 A4. Make sure the subnet IP address of the PC is the same as VigorAP 800 management IP, e.g., **192.168.1.X**.
- 3. Power on VigorAP 800.
- 4. Check all LEDs on the front panel. **ACT** LED should be steadily on, **LAN** LEDs should be on if the access point is correctly connected to the ADSL modem, router or switch/hub.



This page is left blank.

VigorAP 800 User's Guide

Dray Tek



After the network connection is built, the next step you should do is setup VigorAP 800 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 95/98/Me	- 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 95/98/Me IP Address Setup

Click **Start** button (it should be located at lower-left corner of your computer), then click control panel. Double-click **Network** icon, and the **Network** window will appear. Select **TCP/IP**, then click 'Properties'.

Network	? ×
Configuration Identification Access Control	
The following network components are installed: Client for Microsoft Networks Client for NetWare Networks MC EtherPower Adapter (SMC8432) FIX/SPX sompatible Protocol TCP/IP	
Add <u>R</u> emove <u>Properties</u>	.
Primary Network Logon:	
Client for Microsoft Networks	-
<u>File and Print Sharing</u> Description TCP/IP is the protocol you use to connect to the Internet and wide-area networks.	
	-
OK Can	cel



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

IP address: 192.168.1.9

TCP/IP Propertie	es	? ×
Bindings Gateway	Advanced WINS Configuration	DNS Configuration IP Address
by a DHCP ser	can be automatically assig ver. If your network does ir network administrator for ace below.	not have a DHCP
O <u>O</u> btain an -⊙ <u>Specify</u> a	IP address from a DHCP n IP address:	server
<u>I</u> P Addre	ss:	
S <u>u</u> bnet M	Mask: .	· ·
		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	n Properties	?×
General		
Connect using:		
🗒 Realtek RTL8	029(AS) PCI Ethernet Ad	apter
,		Configure
Components checke	ed are used by this conne	ction:
File and Print	ter Sharing for Microsoft N	Vetworks

Install	<u>U</u> ninstall	Properties
Description	**	
wide area network	trol Protocol/Internet Prot < protocol that provides c erconnected networks.	
Sho <u>w</u> icon in tasl	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

nternet Protocol (TCP/IP) Pro	perties	? ×
General		
	d automatically if your network supp sed to ask your network administrate	
Obtain an IP address autor	matically.	
$\square \bigcirc \bigcirc$ Use the following IP addre	\$:	
[P address:		
S <u>u</u> bnet mask:		
Default gateway:		
Obtain DNS server addres	sautomatically	
C Use the following DNS ser	ver addresses:	
Preferred DNS server:		
Alternate DNS server:		
		xed
	ОК	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:
Elient for Microsoft Networks End Painter Sharing for Microsoft Networks
QoS Packet Scheduler
☑ 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

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

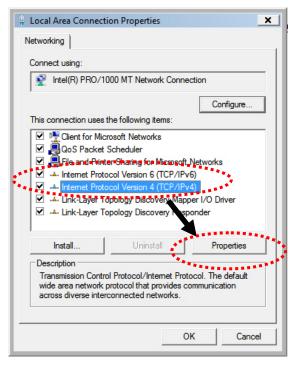
IP address: 192.168.1.9

Subnet Mask: 255.255.255.0.

Internet	Protocol (TCP/IP) Pr	operties	? 🛛
General			
this cap		automatically if your network support d to ask your network administrator f	
00	otain an IP address autom	atically	
- 💽 U <u>s</u>	e the following IP address		
<u>I</u> P ad	ldress:	666 192.168.1.9	
Subr	iet mas	255 . 255 . 255 . 0	
Defa	ult gateway:	· · ·	
OOL	tain DNS server address	automatically	
- O Us	e the following DNS serve	er addresses:	
<u>P</u> refe	rred DNS server:		
Alterr	nate DNS server:		
		Advanced	i
		OK C	ncel

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.

neral	
	ed automatically if your network supports
or the appropriate IP settings	i need to ask your network administrator s.
 Obtain an IP address aut Obtain the following IP address 	
IP at s:	192.168.1.9
onet mask:	255.255.255.0
Default gateway:	Te este
	n seine de la companya
Obtain DNS server addre	
Output the following DNS set	rver addresses:
Preferred DNS server:	Grah relacted Region
Alternate DNS server:	
	Advanced

Dray Tek

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).

1. Make sure your PC connects to the VigorAP 800 correctly.



Notice: You may either simply set up your computer to get IP dynamically from the modem or set up the IP address of the computer to be the same subnet as **the default IP address of VigorAP 800 192.168.1.2**. For the detailed information, please refer to the later section - Trouble Shooting of the guide.

2. Open a web browser on your PC and type http://192.168.1.2. A pop-up window will open to ask for username and password. Pease type "admin/admin" on Username/Password and click OK.

Connect to 192.1	68.1.2 🛛 🛛 🔀
	G S
VigorAP800	
User name:	🔮 admin 🔽
Password:	****
	Remember my password
	OK Cancel

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

	System Status		
< Start Wizard le Status ation Mode	Model : VigorAP 800 Firmware Version : 1.0.2 Build Date/Time : 1509 Fri Feb 25 10:26:12 CST 2 System Uptime : 0d 00:00:36	011	
ess LAN	Operation Mode : Universal Repeater		
ess LAN (5G)	System		I AN-A
US Server	Memory total : 30268 kB	MAC Address	: 00:50:7F:C9:1E:24
m Maintenance	Memory left : 13472 kB	IP Address	: 192.168.1.2
stics		IP Mask	: 255.255.255.0
rt Area	Wireless		LAN-B
ation Note	MAC Address : 00:50:7F:C9:1E:24	MAC Address	: 00:50:7F:C9:1E:24
	SSID : R1_AP800	IP Address	: 192.168.2.2
Registration	Channel : 2	IP Mask	: 255.255.255.0

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

2.6 Changing Password

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

System Maintenance >> Admi	nistration Password	
Adminstrator Settings		
Account	admin	
Password	••••	
	OK	

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

Connect to 192.1	68.1.1 ? 🔀
	GR
Login to the Router \	Web Configurator
User name:	2
Password:	
	Remember my password
	OK Cancel

2.7 Quick Start Wizard

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

2.7.1 Configuring 2.4G Wireless Settings – General

This page displays general settings for the operation mode selected.

Quick Start Wizard >>	2.4G Wireless
Operation Mode :	Universal Repeater AP 800 can act as a wireless repeater; it can be Station and AP at the same time.
Wireless Mode : Main SSID :	Mixed(11b+11g+11n) V R1_AP800 V Enable 2 Subnet (Simulate 2 APs)
Channel : Extension Channel : Station List : AP Discovery :	Multiple SSID 2417MHz (Channel 2) 2437MHz (Channel 6) Display Display
Ai biscovery.	Next > Cancel
Operation Mode	There are six operation modes for wireless connection. Settings for each mode are different.
	AP Bridge-WDS AP Station-Infrastructure AP Bridge-Point to Point AP Bridge-Point to Multi-Point AP Bridge-WDS Universal Repeater
Wireless Mode	At present, VigorAP 800 can connect to 11b only, 11g only, 11n only, Mixed (11b+11g) 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)
Main SSID	Mixed(11b+11g+11n) Set a name for VigorAP 800 to be identified.
	Enable 2 Subnet (Simulate 2 APs) - Check the box to enable the function for two independent subnets. Once you enable this function, LAN-A and LAN-B would be independent. Next, you can connect one router in LAN-A, and another router in LAN-B. Such mechanism can make you feeling that you have two independent AP/subnet functions in one VigorAP 800.
	If you disable this function, LAN-A and LAN-B ports are in the same domain. You could only connect one router (no matter



connecting to LAN-A or LAN-B) in this environment.

Multiple SSID - When **Enable 2 Subnet** is enabled, you can specify subnet interface (LAN-A or LAN-B) for each SSID by using the drop down menu.

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.

2417MHz (Channel 2)	۷
AutoSelect	
2412MHz (Channel 1)	
2417MHz (Channel 2)	
2422MHz (Channel 3)	
2427MHz (Channel 4)	
2432MHz (Channel 5)	
2437MHz (Channel 6)	
2442MHz (Channel 7)	

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.
Station List	Click this 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 800 can scan all regulatory channels and find working APs in the neighborhood.

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

2.7.2 Configuring 2.4G 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 Station-Infrastructure

When you choose Station-Infrastructure, you will need to configure the following page to connect to one AP.

System Configura	onnect to AP :				
Profile Name	1001	- PPC	NE001		
			DF001		
SSID		123	4		
Network Type		Infr	rastructure 💌		
Power Saving Mode			CAM (Constantly Awake Mode) Yower Saving Mode		
RTS Threshold		Πu	Jsed 2347		
Fragment Thresh	nold	Πu	Ised 2346		
Security Policy					
Security Mode OPE		OPE	EN		
WEP					
WEP Key Length			64 bit (10 hex digits / 5 ascii keys) 💙		
WEP Key Entry M	/lethod		Hexadecimal 💌		
	WEP Key 1 :				
	WEP Key 2 :				
WEP Keys	WEP Key 3 :				
	WEP Key 4 :				
Default Key			Кеу 1 🗸		

Advanced Settings for AP Bridge-Point to Point

Quick Start Wizard >> 2.4G Wireless

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

Phy Mode :	ССК
Security :	
◯Disabled ◯WEP ◯TKIP ◯AES	
Key :	
Peer MAC Address :	

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 :	ССК 💌
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 :

Advanced Settings for AP Bridge-WDS

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

Quick Start	Wizard	>> 2.4G	Wireless
Source Start		L.T.	11101033

Quick Start Wizard >> 2.4G Wireless

Note : Enter the configuration of APs which AP Remote AP should always set LAN-A MA	
Phy Mode :	ССК
1. Subnet LAN-A 💌 Security :	3. Subnet LAN-A 💌 Security :
◯ Disabled ◯ WEP ◯ TKIP ◯ AES	◯ Disabled ◯ WEP ◯ TKIP ◯ AES
Key :	Кеу :
Peer MAC Address :	Peer MAC Address :
2. Subnet LAN-A 💌 Security :	4. Subnet LAN-A 🛩 Security :
◯ Disabled ◯ WEP ◯ TKIP ◯ AES	◯ Disabled ◯ WEP ◯ TKIP ◯ AES
Кеу :	Key :
Peer MAC Address :	Peer MAC Address :
	<pre>< Back Next > Cancel</pre>

Dray Tek

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 >> 2.4G Wireless				
Please input the SSID you want to connect to : Universal Repeater Parameters				
SSID	R1			
MAC Address (Optional)				
Security Mode	WPA/PSK 💌			
Encryption Type	ТКІР 💌			
Pass Phrase	•••••			
	<pre>< Back Next > Cancel</pre>			

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

2.7.3 Configuring 5G Wireless Settings

VigorAP 800 offers 5G wireless connection capability. You can setup 5G features in Quick Start Wizard first. Once the USB 5G wireless dongle connects to VigorAP 800, it can work immediately.

Quick Start Wizard >>	5G Wireless
Wireless Mode : Main SSID :	11n only(5G) DrayTek-5G Multiple SSID
Channel :	5240MHz (Channel 48) 💌
Extension Channel :	5220MHz (Channel 44) 💌
Station List :	Display
Wireless Mode	<pre>< Back Next > Cancel At present, VigorAP 800 can connect to 11a only, 11n only (5G),</pre>
	Mixed (11a+11n) stations simultaneously. Simply choose Mixed (11a+11n) mode. 11n only(5G) 11a only 11n only(5G) Mixed (11a+11n)
Main SSID	Set a name for VigorAP 800 to be identified.
	Multiple SSID – Set the SSIDs and specify subnet interface (LAN-A or LAN-B) for each SSID by click Multiple SSID.
Channel	Means the channel of frequency of the wireless LAN. The default channel is 48. 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.



	5240MHz (Channel 48) 🛛 👻	
	AutoSelect 5180MHz (Channel 36) 5200MHz (Channel 40) 5220MHz (Channel 44)	
	5240MHz (Channel 48) 5260MHz (Channel 52) 5280MHz (Channel 56) 5300MHz (Channel 60) 5320MHz (Channel 64)	
Extension Channel	5500MHz (Channel 100) 5520MHz (Channel 104) With 802.11n, there is one option t	o double the bandwidth
	channel. The available extension c	

channel. The available extension channel options will be varied
according to the **Channel** selected above.Station ListClick this button to open the Station List dialog. It provides the

n List Click this button to open the Station List dialog. It provides the knowledge of connecting wireless clients now along with its status code.

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



2.8 Online Status

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

Online Status

System	Status				System Uptime: ()d 00:55:
LAN-A S	tatus					
IP Addre	ess	TX Packets	RX Packets	TX Bytes	RX Bytes	
192.16	58.1.2	5053	10099	1776825	572711	
LAN-B S	tatus					
IP Addre	ess	TX Packets	RX Packets	TX Bytes	RX Bytes	
192.16	58.2.2	112	0	4704	0	
Universa	al Repeate	erStatus				
IP	Gatew	/ay	SSID		Channel	
			R1		2	
Mac	Secur	ity Mode	TX Pac	kets	RX Packets	
	WPAP	SK	43026		16287	

Detailed explanation is shown below:

LAN-A/LAN-B Status

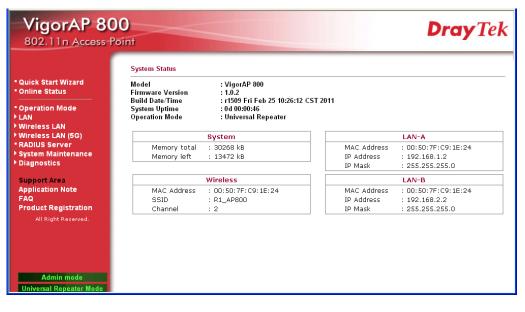
IP Address	Displays the IP address of the LAN interface.
TX Packets	Displays the total transmitted packets at the LAN interface.
RX Packets	Displays the total number of received packets at the LAN interface.
TX Bytes	Displays the total transmitted size at the LAN interface.
RX Bytes	Displays the total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



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.

۲	AP :
	AP 800 acts as a bridge between wireless devices and wired Ethernet network, and exchanges data between them.
$^{\circ}$	Station-Infrastructure :
	Enable the Ethernet device as a wireless station and join a wireless network through an AP.
\circ	AP Bridge-Point to Point :
	AP 800 will connect to another AP 800 which uses the same mode, and all wired Ethernet client of both AP 800s will be connected together.
\circ	AP Bridge-Point to Multi-Point :
	AP 800 will connect to up to four AP 800s which uses the same mode, and all wired Ethernet clients of every AP 800s will be connected together.
\bigcirc	AP Bridge-WDS :
	AP 800 will connect to up to four AP 800s which uses the same mode, and all wired Ethernet clients of every AP 800s will be connected together. This mode is still able to accept wireless clients.
\bigcirc	Universal Repeater :
	AP 800 can act as a wireless repeater; it can be Station and AP at the same time.

AP	This mode allows wireless clients to connect to access point and exchange data with the devices connected to the wired network.
Station-Infrastructure	Enable the Ethernet device such as TV and Game player connected to the VigorAP 800 to an access point.
AP Bridge-Point to Point	This mode can establish wireless connection with another VigorAP 800 using the same mode, and link the wired network which these two VigorAP 800s 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 800s using the same mode, and link the wired network which these VigorAP 800s 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-A IP Network Configu	ration	DHCP Server Configuration			
For NAT Usage		●Enable Server ○Disable Server			
IP Address	192.168.1.2	Start IP Address	192.168.1.6		
Subnet Mask	255.255.255.0	End IP Address	192.168.1.9		
		Subnet Mask	255.255.255.0		
		Default Gateway	192.168.1.1		
		Lease Time	86400		
		Primary DNS Server			
		Secondary DNS Server			
LAN-B IP Network Configu	ration	DHCP Server Configuration			
For NAT Usage		◯Enable Server ⊙Disable Server			
IP Address	192.168.2.2	Start IP Address			
Subnet Mask	255.255.255.0	End IP Address			
		Subnet Mask			
		Default Gateway			
		Lease Time	86400		
		Primary DNS Server			
		Secondary DNS Server			

OK	Cancel

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)
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.

Dray Tek

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.
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.

3.3 General Concepts for Wireless LAN

The VigorAP 800 is equipped with a wireless LAN interface compliant with the standard IEEE 802.11n draft 2 protocol. To boost its performance further, the VigorAP 800 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 800 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 800. 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.

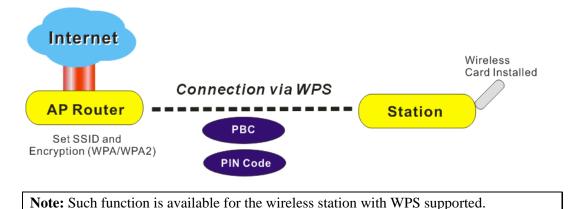
Since WEP has been proved vulnerable, you may consider using WPA for the most secure connection. You should select the appropriate security mechanism according to your needs. No matter which security suite you select, they all will enhance the over-the-air data protection and /or privacy on your wireless network. The VigorAP 800 is very flexible and can support multiple secure connections with both WEP and WPA at the same time.



WPS Introduction

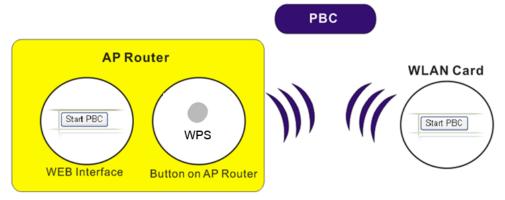
WPS (Wi-Fi Protected Setup) provides easy procedure to make network connection between wireless station and wireless access point (VigorAP 800) with the encryption of WPA and WPA2.

It is the simplest way to build connection between wireless network clients and VigorAP 800. 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 800 automatically.

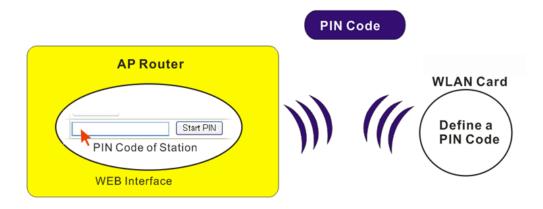


There are two methods to do network connection through WPS between AP and Stations: pressing the *Start PBC* button or using *PIN Code*.

On the side of VigorAP 800 series which served as an AP, press **WPS** button once on the front panel of VigorAP 800 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 800.



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	
 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
```

eral Setting (IEEE 802.	.11)		
Enable Wireless LAN			
Mode :	Mixed(11b+11g+11n) 💌		
Hide SSID I R1_AP800 C DrayTek-LAI G Hide SSID: Isolate Member: MAC Clone:			
Channel : Extension Channel	2417MHz (Channel 2)		
Packet-OVERDRIV	Ε		
🗹 Tx Burst			
Nete i			
Note :	norte 11a mada		
1.Tx Burst only su			
1.Tx Burst only su	pports 11g mode. ology must also be supported in clients to boost WLAN performance.		
1.Tx Burst only su			
1.Tx Burst only su 2.The same techn	ology must also be supported in clients to boost WLAN performance.		



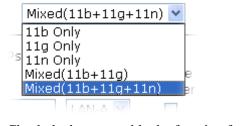
Cancel

OK

Enable Wireless LAN Check the box to enable wireless function.

Mode

At present, VigorAP 800 can connect to 11b only, 11g only, 11n only, Mixed (11b+11g) and Mixed (11b+11g+11n) stations simultaneously. Simply choose Mixed (11b+11g+11n) mode.



Enable 2 Subnet (Simulate 2 APs)	Check the box to enable the function for two independent subnets. Once you enable this function, LAN-A and LAN-B would be independent. Next, you can connect one router in LAN-A, and another router in LAN-B. Such mechanism can make you feeling that you have two independent AP/subnet functions in one VigorAP 800.
	If you disable this function, LAN-A and LAN-B ports are in the same domain. You could only connect one router (no matter connecting to LAN-A or LAN-B) in this environment.
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 800 while site surveying. The system allows you to set three sets of SSID for different usage.
SSID	Set a name for VigorAP 800 to be identified. Default settings are DrayTek-LAN-A and DrayTek-LAN-B. When Enable 2 Subnet is enabled, you can specify subnet interface (LAN-A or LAN-B) for each SSID by using the drop down menu.
Subnet	Choose LAN-A or LAN-B for each SSID. If you choose LAN-A, the wireless clients connecting to this SSID could only communicate with LAN-A.
Isolate LAN	Check this box to make the wireless clients (stations) with the same SSID not accessing for wired PC in LAN.
	Note: If Isolate LAN is checked, do not type any value for VLAN ID.
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. 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.
	2437MHz (Channel 6) AutoSelect 2412MHz (Channel 1) 2417MHz (Channel 2) 2422MHz (Channel 3) 2427MHz (Channel 4) 2432MHz (Channel 5) 2437MHz (Channel 5) 2442MHz (Channel 7) 2442MHz (Channel 7) 2452MHz (Channel 8) 2452MHz (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.
	the Wireless client will also change based on this MAC address. SSID4: Reserved for Universal Repeater mode so it's not listed.
	Channel : 2462MHz (Channel 11) ▼ Rate : Auto ▼ Packet-OVERDRIVE 1 Mbps 2 Mbps 2 Mbps 5.5 Mbps 11 Mbps Note :
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	~ Advance Setting		_
Auto launch when Windows start up	Disable <u>R</u> adio		
Remember mini status position	Fragmentation Threshold :	234	6
🗌 Auto hide mini status	RTS Threshold :	234	7
Set mini status always on top	Frequency :	802.11b/g/n - 2.4GH	*
Enable IP Setting and Proxy Setting in Profile	Ad-hoc <u>C</u> hannel:	1	-
Group Roaming Ad-hoc	Power Save Mode:	Disable	~
	Tx <u>B</u> urst :	Disable	1
WLAN type to connect Infrastructure and Ad-hoc network Infrastructure network only Ad-hoc network only			
Automatically connect to non-preferred networks			
	OK	Cancel	ply

WMM CapableTo apply WMM parameters for wireless data transmission, please
click the Enable radio button.

VigorAP 800 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

Antenna

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%	

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 >> Security Settings

SSID 1	SSID 2	SSID 3	SSID 4			
Mo	de	Disab	e	~		
-	DADING C	·				
WPA	t up <u>RADIUS Server</u>	IT 802.1x IS 6	enabled.			
WF	A Algorithms	○ ткі	P 🔿 AES 🔿	TKIP/AES		
Pas	ss Phrase					
Key	y Renewal Interval	3600	seconds			
PM	K Cache Period	10	minutes			
	-Authentication	🖲 Disa	able 🔾 Enable			
WEP						
۲	Кеу 1 :				Hex 💌	
	Key 2 :				Hex 💟	
	Кеу 3:				Hex 💌	
	Кеу 4 :				Hex 🔽	
80:	2.1× WEP	🔿 Disa	able 🔿 Enable			

ОК

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	

Cancel

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 800 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.
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 ','. Such feature is available for WEP mode.
	Hex ASCII Hex
802.1x WEP	Disable - Disable the WEP Encryption. Data sent to the AP

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 Serve			
IP Address			
Port	1812		
Shared Secret			
Session Timeout	0		
	ОК		
Use internal RADIUS Server	There is a RADIUS server built in VigorAP 800 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, 3.10 RADIUS Server to configure settings for internal server of VigorAP 800.		
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.)		

3.4.3 Access Control

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

Wireless LAN >> Access Control

SSID 1	SSID 2	SSID 3	SSID 4		
	P	olicy: Disable		~	
		МАС	Address Filter		
	Index		MAC A	\ddress	_
	Client's MA	C Address :]:[]:[
	ſ	Add D	elete Edit	Cancel	

ОК

Cancel

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 WLAN from LAN will separate all the WLAN stations from LAN based on the MAC Address list.
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.
ОК	Click it to save the access control list.
Cancel	Clean all entries in the MAC address list.

3.4.4 WPS

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

🗹 Enable WPS 📍		
Wi-Fi Protected Setup Informa	ion	
WPS Configured	Yes	
WPS SSID	DrayTek-LAN-A	
WPS Auth Mode	Open	
WPS Encryp Type	None	
AP PIN	22413482 Generate	

Configure via Push Button	Start PBC
Configure via Client PinCode	Start PIN
Status: The Authentication Mode is NOT V	VPA/WPA2 PSK!!

Note: WPS can help your wireless client automatically connect to the $\ensuremath{\mathsf{Access}}$ point.

Q: WPS is Enabled. ♂: Waiting for WPS requests from wireless clients.

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 800 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 800r. Only WPA2/PSK and WPA/PSK support WPS.
WPS Encryp Type	Display encryption mode (None, WEP, TKIP, AES, etc.) of VigorAP 800.
AP PIN	The number displayed here is used for remote client entering the registrar's PIN code in remote station to make a network connection.
Configure via Push Button	Click Start PBC to invoke Push-Button style WPS setup procedure. VigorAP 800 will wait for WPS requests from wireless clients about two minutes. The WPS LED on VigorAP 800 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 VigorAP 800 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).

 $[\]mathbb{Q}$: WPS is Disabled.

3.4.5 AP Discovery

VigorAP 800 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 >> Access Point Discovery	1
----------------------------------------	---

SSID	BSSID	RSSI	Channel	Encryption	Authentication
Default_SS	00:12:34:54:34:20	39%	1	NONE	
2920	00:50:7f:ce:06:c0	0%	1	TKIP	WPA/PSK
2920	00:50:7f:9d:1d:98	0%	1	TKIP	WPA/PSK
Vigor2710	00:50:7f:a0:51:50	0%	2	NONE	
FAE-292222	00:50:7f:c9:3b:24	34%	4	AES	WPA2/PSK
DrayTek	00:50:7f:ca:8e:9c	65%	6	TKIP	Mixed(WPA+WPA2)/PSK
mike	00:1d:7d:34:e0:0e	15%	6	NONE	
DrayTek	00:50:7f:00:00:00	55%	6	NONE	
Dennis_Tes	00:50:7f:c3:59:f8	96%	6	NONE	
T-Com-f498	00:50:7f:92:f4:98	0%	6	AES	WPA2/PSK
Vigor2820	00:50:7f:a6:3b:98	39%	9	AES	WPA2/PSK
DrayTek	00:50:7f:c9:76:0c	100%	11	NONE	
PM	00:0e:2e:44:84:38	44%	11	AES	WPA2/PSK
FAE_AP700	00:50:7f:9e:60:d8	34%	11	TKIP/AES	Mixed(WPA+WPA2)/PSK
Setlla	00:50:7f:cc:08:64	76%	11	AES	WPA2/PSK
0024A57217	00:24:a5:72:17:a8	0%	11	NONE	
0024A57217	00:24:a5:72:17:ac	0%	11	NONE	
DrayTek	00:50:7f:66:66:64	39%	11	NONE	
DrayTek	00:50:7f:c8:42:fc	0%	11	NONE	

See Channel Statistics

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

Scan

SSID	Display the SSID of the AP scanned by VigorAP 800.
BSSID	Display the MAC address of the AP scanned by VigorAP 800.
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 800.
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.

3.4.6 Station List

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

MAC Address	SSID	Auth	Encrypt
	Refresh		
dd to <u>Access Control</u> :			
lient's MAC Address : :			

Add

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.
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 .

3.5 Wireless LAN Settings for Station-Infrastructure Mode

When you choose **Station-Infrastructure** as the operation mode, the Wireless LAN menu items will include General Setup, Site Survey, Statistics and WPS.

▶ Wireless LAN
 General Setup
 Site Survey
 Statistics
• WPS

Wireless LAN >> General Setup

3.5.1 General Setup

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

ble Wireless LAN				
Node :		Mixed	l(11b+11g+11n) 🔽	
ofile List				
Profile	SSID	Channel	Authentication	Encryption
acket-OVERDRIV	Add	Delete	Edit C	onnect
ote:				
Tx Burst only su	pports 11g	mode.		
.The same techn	iology must	: also be supp	orted in AP to boost WI	.AN performance
Mac Clone				
ote :				

Enable Wireless LAN

Check the box to enable wireless function.

Mode

At present, VigorAP 800 can connect to 11 b only, 11 g only, 11 n only, Mixed (11b+11g), Mixed (11b+11g+11n) and Mixed (11g+11n) stations simultaneously. Simply choose Mixed (11b+11g+11n) mode.

Mixed(11b+11g+11n)	*
11b Only	
11g Only	
11n Only	
Mixed(11b+11g)	- i c
Mixed(11b+11g+11n)	
Mixed(11g+11n)	

Click this button to add new wireless profiles.

Delete	Click this button to delete the selected wireless profile.
Edit	Click this button to modify the existing wireless profile.
Connect	Click this button to connect the wireless station to AP with the selected profile.

Packet-OVERDRIVEThis 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**).

Vigor N61 802.11n Wireless USB Adapter Utility			×
Configuration Status Option About			
General Setting Auto launch when Windows gtart up	Advance Setting Disable <u>R</u> adio		
Remember mini status position	Fragmentation Threshold :	23	46
🗌 Auto hide mini status	RTS Threshold :	23	47
Set <u>m</u> ini status always on top	Frequency :	802.11b/g/n - 2.4GH	*
Enable IP Setting and Proxy Setting in Profile	Ad-hoc <u>C</u> hannel:	1	~
Group Roaming Ad-hoc	Po <u>w</u> er Save Mode:	Disable	~
	Tx Burst :	Disable	~
WLAN type to connect			
Infrastructure and Ad-hoc network			
 Infrastructure network only 			
○ Ad-hoc network only			
Automatically connect to non-preferred networks			
	OK	Cancel A ₁	oply

Mac Clone

Check this box and manually enter the MAC address for Station mode driver.

Add a New Wireless Profile

To add a new wireless profile for the stations, click **Add.** The following dialog box will appear.

System Configu	ration						1	
Profile Name		PROF001						
SSID								
Network Type		Infrastru	ucture 💌					
Power Saving N	/lode		(Constantly Av r Saving Mode	vake Mode)				
RTS Threshold		Used	2347					
Fragment Three	shold	Used	2346					
Security Policy								
Security Mode		OPEN	*					
WEP								
WEP Key Lengt	h	64 b	oit (10 hex digit	s / 5 ascii keys)	*			
WEP Key Entry	Method	Hex	adecimal 💌					
	WEP Key 1 :							
	WEP Key 2 :							
WEP Keys	WEP Key 3 :							
	WEP Key 4 :						J	
Default Key		Key	1 💙					
	ОК		Cancel					
Profile Name				new profile			>	
✓Profile NameSSID	1	Гуре a п Гуре the	ame for the name for s	e new profile puch access p		t can be	used for	
	e I t E n	Type a m Type the connection infrastr o Ethernet Ethernet network	name for the e name for s on by the st ucture - In net device s device as a through an	this mode, y uch as TV and wireless stations	you can o nd Gam ation and t or AP 1	connect e player l join to a couter.	the acces to enable a wireles	ss point e the ss
SSID	7 c t t E n 8	Type a m Type the connection infrastr o Ethernet hetwork 802.11	name for the e name for s on by the st ucture - In net device s device as a through an Ad Hoc – A	uch access p tations. this mode, y uch as TV an wireless sta	you can o nd Gam ation and t or AP i twork is	connect t e player l join to a router. a netwo	the acces to enable a wireles rk where	ss point e the ss
SSID	e I E F N 8 V	Type a m Type the connection o Ethernet Dethernet Detwork B02.11 A vireless Infrast	aame for the e name for s on by the st ucture - In net device s device as a through an Ad Hoc – A stations can ructure Ad Hoc	this mode, y uch as TV an uch as TV an wireless sta access point n ad-hoc net	you can o nd Gam ation and t or AP i twork is	connect t e player l join to a router. a netwo	the acces to enable a wireles rk where	ss point e the ss
SSID	e I t E N 8 V	Type a m Type the connection o Ethernet betwork 302.11 wireless Infrast 102.11	aame for the e name for s on by the st ucture - In net device s device as a through an Ad Hoc – A stations can ructure Ad Hoc ucture	this mode, y uch as TV an uch as TV an wireless sta access point n ad-hoc net	you can o nd Gam ation and t or AP i twork is ate with	connect e player l join to a couter. a netwo peer to p	the acces to enable a wireles rk where	ss point e the ss
SSID Network Type	e I t E Mode C	Type a m Type the connection o Ethernet Detwork 802.11 Avireless Infrastr B02.11 Infrastr Choose m	aame for the e name for s on by the st ucture - In net device s device as a through an Ad Hoc – A stations can ructure Ad Hoc ucture	this mode, y this mode, y uch as TV an wireless sta access point n ad-hoc net communica	point tha you can o nd Gam tion and t or AP i twork is ate with	connect e player l join to a couter. a netwo peer to p	the acces to enable a wireles rk where peer (P2F	e the ss P).
SSID Network Type	e I tt F m 8 v V Mode C S S S S	Fype a m Fype the connection o Ethernet betwork 302.11 A vireless Infrastr Choose for CAM – aving jo Power S	aame for the e name for s on by the st ucture - In net device s device as a through an Ad Hoc – A stations can ructure Ad Hoc ucture the power s Choose this ob. Saving Mod	aving mode	ooint tha you can o nd Gamo tion and tor AP n twork is ate with for such not neco this iten	connect e player l join to a couter. a netwo peer to p device. essary to n to get i	the acces to enable a wireles rk where peer (P2F perform nto the p	ss point e the ss P).
SSID Network Type	e I E Mode C S I I I I I I I I I I I I I I I I I I	Type a m Type the connection o Ethernet betwork 302.11 A wireless Infrast B02.11 Choose m CAM – aving jo Power S aving st point.	aame for the e name for so on by the so net device so device as a through an Ad Hoc – A stations can ructure Ad Hoc ucture the power so Choose this ob. Saving Mod tatus when the RTS threshop	aving mode a sitem if it is le – Choose	point tha you can o nd Gamo tion and t or AP i twork is ate with for such not neco this iten ata passi	connect f e player l join to a couter. a netwo peer to p device. essary to n to get i ing throu Do not f	the acces to enable a wireles rk where peer (P2F peer (P2F peer of the p of the p of the accession of the p of t	ss point e the ss P). n power ccess lefault



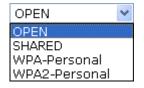
default value if you don't know what it is, default value is 2346.

Security Mode 802.11 standard defines two mechanisms for authentication of wireless LAN clients: Open Authentication and Shared Key Authentication.

Choose one of the security modes from the drop down list. If you choose OPEN or SHARED, you have to type WEP information.

OPEN – Open authentication is basically null authentication algorithm, which means that there is no verification of the user.

SHARED – It works similar to Open authentication with only one major difference. If you choose OPEN with WEP encryption key, the WEP keys is used to encrypt and decrypt the data but not for authentication. In Shared key authentication, WEP encryption will be used for authentication.



If you choose **WPA-Personal** or **WPA2-Personal**, the corresponding WPA settings will be listed as follows. You have to choose the WPA algorithms and type the pass phrase for such security mode.

Security Policy	
Security Mode	WPA-Personal 💌
	JL
WPA	

WPA Algorithms	⊙ TKIP ○ AES				
Pass Phrase					

WPA Algorithms – Choose Temporal Key Integrity Protocol (TKIP) or AES for data encryption.

Pass Phrase – Please type 8 to 63 alphanumerical characters here.

WEP Key LengthWEP (Wired Equivalent Privacy) is a common encryption
mode. It is safe enough for home and personal use. However, if
you need higher level of security, please consider using WPA
encryption (see next section).

Some wireless clients do not support WPA, but support WEP. Therefore WEP is still a good choice for you if you have such kind of client in your network environment.

64 bi	t (10 hex digits / 5 ascii keys) 👘	*
	: (10 hex digits / 5 ascii keys)	
128 Ł	oit (26 hex digits / 13 ascii keys)	

There are two types of WEP key length: 64-bit and 128-bit. Using 128-bit is safer than 64-bit, but it will reduce some data

	transfer performance.
WEP Key Entry Method	There are two types of key method: ASCII and Hex. When you select a key format, the number of characters of key will be displayed. For example, if you select 64-bit as key length, and Hex as key format, you'll see the message at the right of Key Format is 'Hex (10 characters) which means the length of WEP key is 10 characters.
	Hexadecimal 💙 Hexadecimal Ascii Text
WEP Keys (Key 1 – Key 4)	Input WEP key characters here, the number of characters must be the same as the number displayed at Key Format field. You can use any alphanumerical characters (0-9, a-z, and A-Z) if you select ASCII key format, and if you select Hex as key format, you can use characters 0-9, a-f, and A-F. You must enter at least one encryption key here. If you entered multiple WEP keys, they should not be the same with each other.
Default Key	You can set up to four sets of WEP key, and you can decide which key is being used as default here. If you don't know

which one you should use, select 'Key 1'.

Below shows an example for a wireless profile created.

Wireless LAN >> General Setup

General Setting (IEEE 802.11) 🗹 Enable Wireless LAN Mode : Mixed(11b+11g+11n) 🔽 Pofile List Encryption Profile SSID Channel Authentication \bigcirc PROF001 vigor-1 Auto OPEN NONE Connect Add Packet-OVERDRIVE 🗹 Tx Burst Note : 1.Tx Burst only supports 11g mode. 2. The same technology must also be supported in AP to boost WLAN performance. Mac Clone Note : 1. Please notice that the last byte of this MAC address must be a multiple of 8.

Cancel

Dray Tek

ОK

3.5.2 Site Survey

The page will list the access points nearby as VigorAP800 is set to Station mode. You can select one of the access points to associate.

Wireless LAN >> Station	Site Survey			
Site Survey				
SSID BSSID	RSSI Channel	Encryption	Authentication	
	Connect	Scan Add Profile		
SSID	Display the SS	ID name of the acce	ss point.	
BSSID	Display the BS	SID (MAC Address	s) of the access point.	
RSSI	1,000	nal strength of the a Receive Signal Stre	ccess point. RSSI is the ength Indication.	
Channel	Display the cha	nnel number of the	access point.	
Encryption Display the encryption setting of the access points. If you have to g 2-7 Wireless Security to set the same security with the access point you want to associate.				
Authentication	Display the aut	hentication type of t	the access point.	
Connect	Connect to the	wireless AP that yo	u choose.	
Scan	Search the stati	ons connected to su	ch access point.	
Add Profile	•	l add a profile autor ss AP that you choo	natically for you to connect se.	

3.5.3 Statistics

This page displays the statistics for data transmission and receiving between the access point and the stations.

Wireless LAN >> Station Statistics

Transmit Statistics

Frames Transmitted Successfully	4256
Frames Transmitted Successfully Without Retry	4256
Frames Transmitted Successfully After Retry(s)	0
Frames Fail To Receive ACK After All Retries	0
RTS Frames Sucessfully Receive CTS	0
RTS Frames Fail To Receive CTS	0

Receive Statistics

Frames Received Successfully	49
Frames Received With CRC Error	11
Frames Dropped Due To Out-of-Resource	0
Duplicate Frames Received	0

Reset Counters



Click Rest Counters if required.

3.5.4 WPS (Wi-Fi Protected Setup)

Wi-Fi Protected Setup (WPS) is the simplest way to build connection between wireless network clients and the access point. You don't have to select encryption mode and input a long encryption passphrase every time when you need to setup a wireless client. You only have to press a button on wireless client and the access point, and the WPS will do the setup for you.

VigorAP800 supports two types of WPS: Push-Button Configuration (PBC), and PIN code. If you want to use PBC, you have to switch VigorAP800 to WPS mode and push a specific button on the wireless client to start WPS mode. You can push Reset/WPS button of this VigorAP800, or click **PBC Start** button in the web configuration interface to do this; if you want to use PIN code, you have to provide the PIN code of the wireless client you wish to connect to this access point and then switch the wireless client to WPS mode.

Note: WPS function of VigorAP800 will not work for those wireless AP/clients do not support WPS.

To use WPS function to set encrypted connection between VigorAP800 and WPS-enabled wireless AP, please open **Wireless LAN** >>**WPS**. The following information will be displayed:

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

WPS	AP :	site	survey
-----	------	------	--------

No.	SSID	BSSID	RSSI	Ch.	Auth.	Encrypt	Ver.	Status
۲	Amanda	00507F223344	0%	1	WPA/PSK	ТКІР	1.0	Conf.

Refresh

Device Configure

Configure via Push Button	Start PBC
Configure via Client PinCode	Start PIN Renew PIN
	Cancel

Status: Idle

SSID	Display the SSID name of the access point.
BSSID	Display the BSSID (MAC Address) of the access point.
RSSI	Display the signal strength of the access point. RSSI is the abbreviation of Receive Signal Strength Indication.
Ch. (Channel)	Display the channel number of the access point.
Auth. (Authentication)	Display the authentication type of the access point.
Encrypt (Encryption)	Display the encryption setting of the access points. If you have selected the access point with security setting, you have to go to 2-7 Wireless Security to set the same security with the access point you want to associate.
Ver. (Version)	Display the version of WPS.

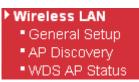


Status	Display the status of WPS access point.
Refresh	Click this button to refresh the AP site survey.
Start PBC	Click Start PBC to make a WPS connection within 2 minutes.
PIN Start	When using PinCode method, it is required to enter PIN Code (Personal Identification Number Code, 8-digit numbers) into Registrar. When the wireless station is Enrollee, the users can use Renew PIN to re-generate a new PIN code.
Renew PIN	Click this button to re-generate a new PIN code.

Note: When you're using PBC type WPS setup, you must press **PBC** button (hardware or software) of wireless client within 2 minutes. If you didn't press **PBC** button of wireless client within this time period, please press **PBC** button (hardware or software) of this access point again.

3.6 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.



Wireless LAN >> General Setup

AP Bridge-Point to Point allows VigorAP 800 to connect to **another** VigorAP 800 which uses the same mode. All wired Ethernet clients of both VigorAP 800s will be connected together.

Point-to Multi-Point Mode allows AP 800 to connect up to **four** AP 800s which uses the same mode. All wired Ethernet clients of every VigorAP 800 will be connected together.

3.6.1 General Setup

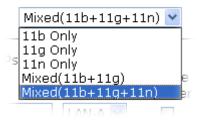
By clicking the **General Setup**, a new web page will appear so that you could configure the Phy mode, security, Tx Burst and choose proper mode. Please refer to the following figure for more information.

able Wireless LAN	
Mode :	Mixed(11b+11g+11n) 💌
Channel : 2417MHz (Channel 2) 💌	
Extension Channel :	2437MHz (Channel 6) 💌
Note : Enter the configuration	on of APs which AP 800 want to connect.
Phy Mode:	ССК
Key : Peer Mac Address: 	
Peer Mac Address:	mode.
Peer Mac Address:	mode. : also be supported in clients to boost WLAN performance.

OK Cancel

Enable Wireless LAN Mode Check the box to enable wireless function.

At present, VigorAP 800 can connect to 11b only, 11g only, 11n only, Mixed (11b+11g) and Mixed (11b+11g+11n) stations simultaneously. Simply choose Mixed (11b+11g+11n) mode.



Channel

Rate

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 11) 💌	
	AutoSelect	\vdash
AE	2412MHz (Channel 1)	0
	2417MHz (Channel 2)	
	2422MHz (Channel 3)	
	2427MHz (Channel 4)	
	2432MHz (Channel 5)	
	2437MHz (Channel 6)	
	2442MHz (Channel 7)	
Э.	2447MHz (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.

If you choose 11g Only, 11b Only or 11n Only, such feature will be available for you to set data transmission rate.

Mode :	11g Only	
Channel :	2462MHz (C	hannel
Rate :	Auto 🛛 🚩	
Note : Enter the configuration of AF	Auto 1 Mbps 2 Mbps	300 wa
Phy Mode:	5.5 Mbps 11 Mbps	K 🚩

Phy ModeSelect CCK (11b mode), OFDM (11g mode), or HTMIX
(11b/g/n mixed mode) from the drop down menu for the access
point that VigorAP 800 wants to connect. Each access point

should be setup to the same **Phy** mode for connecting with each other.

ССК	*
ССК	
OFDM	
HTMIX	

Select WEP, TKIP or AES as the encryption algorithm. Type the Security key number if required. Type the peer MAC address for the access point that VigorAP **Peer Mac Address** 800 connects to. **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**).

General Setting	Advance Setting	
🗹 Auto launch when Windows start up	Disable <u>R</u> adio	
Remember mini status position	\underline{F} ragmentation Threshold :	23
🗌 Auto <u>h</u> ide mini status	RTS Threshold :	23
Set <u>m</u> ini status always on top	Frequency :	802.11b/g/n - 2.4GH
Enable IP Setting and Proxy Setting in Profile	Ad-hoc <u>C</u> hannel:	1
Group Roaming Ad-hoc	Po <u>w</u> er Save Mode:	Disable
	Tx <u>B</u> urst :	Disable
WLAN type to connect		
 Infrastructure and Ad-hoc <u>n</u>etwork 		
 Infrastructure network only 		
O Ad-hoc network only		
Automatically connect to non-preferred networks		
	OK	Cancel

VigorAP 800 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	۷
2T2R	
1T1R	

Tx Power

Antenna

WMM Capable

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%	

3.6.2 AP Discovery

VigorAP 800 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 800.

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 800 can be found. Please click **Scan** to discover all the connected APs.

Access Point List					
Select SSID	BSSID	RSSI	Channel	Encryption	Authentication
			Sc	an	
See <u>Channel</u> !	Statistics				
Note: During th	ie scanning p	orocess (ał	bout 5 seconds	s), no station is allo	wed to connect with the router.
AP's MAC Addr		: .]:[]]:[]	: AP's	
]: AP's :	5510
Add to <u>WDS Se</u>	aangs: OBrid	dge Ad	a		
SSID		Displ	ov the SSID	of the AD scenne	d by VigorAP 800r.
		•	2		
BSSID		Displa	ay the MAC	address of the Al	P scanned by VigorAP 800.
RSSI		-		strength of the acceive Signal Stre	ccess point. RSSI is the ength Indication.
Channel		-	ay the wirele AP 800.	ss channel used f	or the AP that is scanned by
Encryption		Displa	ay the encry	otion mode for the	e scanned AP.
Authenticati	on	Displa	ay the auther	ntication type that	the scanned AP applied.
Scan				ver all the connec above this button	ted AP. The results will be
Statistics		It disp	plays the stat	istics for the char	nnels used by APs.
AP's MAC A	ddress	•		und AP applying IAC address.	the WDS settings, please
AP's SSID		specif	y MAC addı	* *	n WDS settings, you can he AP. Here is the place tha
Add			0	•	Next, click Add . Later, the led and be shown on WDS

Wireless LAN >> Access Point Discovery



settings page.

3.6.3 WDS AP Status

VigorAP 800 can display the status such as MAC address, physical mode, power save and bandwidth for the working AP connected with WDS. Click **Refresh** to get the newest information.

Wireless LAN >> WDS AP Status

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

Refresh

3.7 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 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 Phy mode, security, Tx Burst and choose proper mode. Please refer to the following figure for more information.

Wireless LAN >> General Setup

General Setting (IEEE 802.11)

Mode	:			Mixed(1	1b+11g+:	11n) 🚩			
Hide SSID 1 2 2 3 3 4 3 Hide S	R1_AP800 DrayTek-L	AN-B Prevent 1	Subnet	Isolate LAN	Canned	VLAN ID (0:Untagge 0 0 0 0 same SSID			Clone
MACC	lone:	the Wirel	ess client	will also	change	e MAC addr based on tł .C address r	nis MAC	C addre	ss. Please
Chanr	nel :			2417MH	z (Chann	el 2) 💌			
Exten	sion Chann	el :		2437MH	z (Chann	el 6) 🔽			
1. Su	bnet LAN-4		-			et LAN-A V	-	-	
● C Key Peer I 2. Su ● C Key	bnet LAN-4 visabled Mac Addres :	S:	TKIP • A		3. Subn The Disa Key Peer Ma The Subn Subn Subn Key	et LAN-A v abled O W : c Address: : et LAN-A v abled O W : c Address:	EP O	TKIP	
1. Su © C Key Peer I 2. Su © C Key Peer I Packe	bnet LAN-4 visabled Mac Addres Mac Addres bnet LAN-4 visabled Mac Addres Mac Addres t-OVERDRI	WEP S: : 	TKIP • A		3. Subn The Disa Key Peer Ma The Subn Subn Subn Key	abled	EP 0	TKIP :; inity: TKIP	
1. Su	bnet LAN-4 Disabled () Mac Address Mac Address bnet LAN-4 Disabled () Mac Address Mac Address LOVERDRI' Burst	WEP S: : 	TKIP • A		3. Subn The Disa Key Peer Ma The Subn Subn Subn Key	abled	: Secul	TKIP :; inity: TKIP	• AES
1. Su © C Key Peer I 2. Su © C Key Peer I Packe V Tx Note :	bnet LAN-4 bisabled () Mac Addres is () : () bnet LAN-4 bisabled () Mac Addres is () : () Mac Addres t-OVERDRI' Burst	WEP S: : 	TKIP • A		3. Subn The Disa Key Peer Ma The Subn Subn Subn Key	abled	: Secul	TKIP :; inity: TKIP	• AES
1. Su © C Key Peer I © C Key Peer I Packe V Tx Note : 1.Tx B	bnet LAN-4 visabled Mac Addres is : : : : : : : : : : : : : : : : : : :	WEP s: : WEP WEP s: : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : </td <td>TKIP A</td> <td></td> <td>3. Subn</td> <td>abled</td> <td>: : :</td> <td>TKIP :: rity: TKIP ::</td> <td>• AES</td>	TKIP A		3. Subn	abled	: : :	TKIP :: rity: TKIP ::	• AES
Su Example 2. Su Tx Note : I.Tx B Example 2. The	bnet LAN-4 visabled Mac Addres is : : : : : : : : : : : : : : : : : : :	WEP s: : WEP WEP s: : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : </td <td>TKIP A</td> <td>ES</td> <td>3. Subn</td> <td>abled O W : Control Co</td> <td>: : :</td> <td>TKIP :: rity: TKIP ::</td> <td>• AES</td>	TKIP A	ES	3. Subn	abled O W : Control Co	: : :	TKIP :: rity: TKIP ::	• AES
Su Example 2. Su Tx Note : I.Tx B Example 2. The	bnet LAN-4 Disabled () Mac Address Mac Address bnet LAN-4 Disabled () Mac Address Mac Address t-OVERDRI' Burst turst only s same tech Capable	WEP s: : WEP WEP s: : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : </td <td>TKIP A</td> <td>ES</td> <td>3. Subn</td> <td>abled O W : Control Co</td> <td>: : :</td> <td>TKIP :: rity: TKIP ::</td> <td>• AES</td>	TKIP A	ES	3. Subn	abled O W : Control Co	: : :	TKIP :: rity: TKIP ::	• AES

Enable Wireless LAN

Check the box to enable wireless function.

Mode

At present, VigorAP 800 can connect to 11b only, 11g only, 11n only, Mixed (11b+11g) and Mixed (11b+11g+11n) stations simultaneously. Simply choose Mixed (11b+11g+11n) mode.

	Mixed(11b+11g+11n) 🔽	
	11b Only	
	11g Only	
PS	11n Only	
	Mixed(11b+11g)	e
	Mixed(11b+11g+11n)	er
	LAN-A 🗸	_

Enable 2 Subnet (Simulate 2 APs)	Check the box to enable the function for two independent subnets. Once you enable this function, LAN-A and LAN-B would be independent. Next, you can connect one router in LAN-A, and another router in LAN-B. Such mechanism can make you feeling that you have two independent AP/subnet functions in one VigorAP 800.
	If you disable this function, LAN-A and LAN-B ports are in the same domain. You could only connect one router (no matter connecting to LAN-A or LAN-B) in this environment.
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 800 while site surveying. The system allows you to set three sets of SSID for different usage.
SSID	Set a name for VigorAP 800 to be identified. Default settings are DrayTek-LAN-A and DrayTek-LAN-B. When Enable 2 Subnet is enabled, you can specify subnet interface (LAN-A or LAN-B) for each SSID by using the drop down menu.
Subnet	Choose LAN-A or LAN-B for each SSID.
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. 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.

	2437MHz (Channel 6) AutoSelect 2412MHz (Channel 1)	
	2417MHz (Channel 2)	
	2422MHz (Channel 3)	
	2427MHz (Channel 4)	
	2432MHz (Channel 5) 2437MHz (Channel 6)	
	2442MHz (Channel 7)	
	2447MHz (Channel 8)	
	2452MHz (Channel 9) 2457MHz (Channel 10)	
	2462MHz (Channel 11)	
	2467MHz (Channel 12)	
	2472MHz (Channel 13)	
Extension Channel		e option to double the bandwidth per tension channel options will be varied
D-4-	e	
Rate	will be available for you t	1b Only or 11n Only, such feature o set data transmission rate.
		versal Repeater mode so it's not listed.
	Channel : Rate :	2462MHz (Channel 11) 🔽 Auto 🔽
	Packet-OVERDRIVE	1 Mbps 2 Mbps
	V Tx Burst	5.5 Mbps 11 Mbps
Phy Mode	• •	ansmission rates developed by hy Mode . Data will be transmitted via
	CCK	
Subnet	Choose LAN-A or LAN-I	B for each SSID.
Security	Select WEP, TKIP or AES	s as the encryption algorithm.
Peer Mac Address	Four peer MAC addresses at one time.	s are allowed to be entered in this page
Packet-OVERDRIVE	about 40%* more (by che when both sides of Acces	the performance in data transmission cking Tx Burs t). It is active only s Point and Station (in wireless client)
		e same time. That is, the wireless client and invoke the function, too.

VigorAP 800 User's Guide

Vigor N61 802.11n Wireless USB Adapter Utility			×
Configuration Status Option About			
General Setting	- Advance Setting		
🗹 Auto launch when Windows start up	📃 Disable <u>R</u> adio		
Remember mini status position	\underline{F} ragmentation Threshold :	23	46
Auto hide mini status	RTS Threshold :	23	47
Set <u>m</u> ini status always on top	Frequency :	802.11b/g/n - 2.4GH	~
Enable IP Setting and Proxy Setting in Profile	Ad-hoc <u>C</u> hannel:	1	~
Group Roaming Ad-hoc	Po <u>w</u> er Save Mode:	Disable	~
	Tx Burst :	Disable	~
WLAN type to connect			
Infrastructure and Ad-hoc <u>n</u> etwork			
 Infrastructure network only 			
Ad-hoc network only			
Automatically connect to non-preferred networks			
	OK (Cancel Ap	ply

To apply WMM parameters for wireless data transmission, please click the **Enable** radio button.

VigorAP 800 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

Antenna

WMM Capable

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%	

3.7.2 Security

Wireless LAN >> Security Settings

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.

SSID 1	SSID 2	SSID	3	SSID 4		
Mo	ode	[Disable		~	
	et up <u>RADIUS Sen</u>	<u>/er</u> if 802.	1x is ena	abled.		
WPA						
W	PA Algorithms		○ ткір	O AES – C	TKIP/AES	
Pa	ss Phrase					
Ke	y Renewal Interv	al	3600 se	econds		
PM	PMK Cache Period		10 m	inutes		
Pri	Pre-Authentication		🖲 Disabl	e 🔾 Enable		
WEP						
۲	Key 1 :	[Hex 🔽
	○ Key 2 :					Hex 💌
	🔾 Кеу 3 :					Hex 💌
С	🔾 Кеу 4 :					Hex 💌
80	2.1x WEP		O Disabl	e O Enable	9	

Mode

There are several modes provided for you to choose.

Cancel

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	

ОК

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 800 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.
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.
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.
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.
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.
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.
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

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

ОK

Use internal RADIUS Server	There is a RADIUS server built in VigorAP 800 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, 3.10 RADIUS Server to configure settings for internal server of VigorAP 800.
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.)

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).



Wireless LAN >> Access Control

SSID 1	SSID 2 SSID 3 SSID 4			
	Policy: Disable			
MAC Address Filter				
	Index MAC Address			
	Client's MAC Address : : : : : :			
	Add Delete Edit Cancel			

Cancel

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 WLAN from LAN will separate all the WLAN stations from LAN based on the MAC Address list. Activate MAC address filter Disable Activate 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.
ОК	Click it to save the access control list.
Cancel	Clean all entries in the MAC address list.

ОК

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	on			
WPS Configured	Yes			
WPS SSID	DrayTek-LAN-A			
WPS Auth Mode	Open			
WPS Encryp Type	None			
AP PIN	22413482 Generate			
Device Configure				
Configure via Push Button	Start PBC			

Configure via Client PinCode Start PBC

Status: The Authentication Mode is NOT WPA/WPA2 PSK!!

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

Q: WPS is Enabled.

℃: Waiting for WPS requests from wireless clients.

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 800 is properly configured, you can see 'Yes' message here.
WPS SSID	Display current selected SSID.
WPS Auth Mode	Display current authentication mode of VigorAP 800. Only WPA2/PSK and WPA/PSK support WPS.
WPS Encryp Type	Display encryption mode (None, WEP, TKIP, AES, etc.) of VigorAP 800.
AP PIN	The number displayed here is used for remote client entering the registrar's PIN code in remote station to make a network connection.
Configure via Push Button	Click Start PBC to make a WPS connection within 2 minutes.
Configure via Client PinCode	When using PinCode method, it is required to enter PIN Code (Personal Identification Number Code, 8-digit numbers) into Registrar.

3.7.5 AP Discovery

VigorAP 800 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 800 can be found. Please click **Scan** to discover all the connected APs.



 $[\]ensuremath{\mathbb{Q}}$: WPS is Disabled.

Wireless LAN >> Access Point Discovery						
Access Point List						
Select SSID	BSSID	RSSI	Channel	Encryption	Authentication	
			Sc	an		
See <u>Channel</u>	Statistics					
Note: During th	ne scanning	process (a	bout 5 seconds), no station is allo	wed to connect with the router.	
AP's MAC Add	ress	:::	:	: AP's	SSID	
Add to <u>WDS Se</u>	ettings: 💿 Re	peater 📃	Add			

SSID	Display the SSID of the AP scanned by VigorAP 800.	
BSSID	Display the MAC address of the AP scanned by VigorAP 800.	
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 800.	
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	
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 Repeater for the specified AP. Next, click Add . Later, the MAC address of the AP will be added and be shown on WDS settings page.	

3.7.6 WDS AP Status

VigorAP 800 can display the status such as MAC address, physical mode, power save and bandwidth for the working AP connected with WDS. Click **Refresh** to get the newest information.

Wireless LAN >> WDS AP Status WDS AP List					
1	00:50:7F:C9:76:0C	ССК	OFF	20M	

Refresh

3.7.7 Station List

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

Wire	ess	LAN	>>	Station	List
				0.001011	

Station List			
MAC Address	SSID	Auth	Encrypt
v	Refresh	1	
Add to Access Control :			
Client's MAC Address : : :	:		

Add

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.
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.



3.8 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, WPS, AP Discovery, Universal Repeater and Station List.



3.8.1 General Setup

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

Please refer to the following figure for more information.

Wireless LAN >> General Setup

General Setting	IEEE 802.11)	
-----------------	--------------	--

Enable Wireless LAI Mode :	N Mixed(11b+11g+11n)
Hido	
Channel : Extension Chann	2417MHz (Channel 2) 🔽 nel : 2437MHz (Channel 6) 🔽
	VE supports 11g mode. mology must also be supported in clients to boost WLAN performance.
WMM Capable	⊙ Enable 🔿 Disable
Antenna : Tx Power :	2T2R 💌 100% 💌
	OK Cancel

Enable Wireless LAN

Check the box to enable wireless function.

Mode

At present, VigorAP 800 can connect to 11b only, 11g only, 11n only, Mixed (11b+11g) and Mixed (11b+11g+11n) stations simultaneously. Simply choose Mixed (11b+11g+11n) mode.

	Mixed(11b+11g+11n) 🔽	
_	11b Only	
	11g Only	
S	11n Only	
	Mixed(11b+11g)	e
	Mixed(11b+11g+11n)	þr

Enable 2 Subnet (Simulate 2 APs) Check the box to enable the function for two independent subnets. Once you enable this function, LAN-A and LAN-B would be independent. Next, you can connect one router in LAN-A, and another router in LAN-B. Such mechanism can make you feeling that you have two independent AP/subnet

	functions in one VigorAP 800.
	If you disable this function, LAN-A and LAN-B ports are in the same domain. You could only connect one router (no matter connecting to LAN-A or LAN-B) in this environment.
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 800 while site surveying. The system allows you to set three sets of SSID for different usage.
SSID	Set a name for VigorAP 800 to be identified. Default settings are DrayTek-LAN-A and DrayTek-LAN-B. When Enable 2 Subnet is enabled, you can specify subnet interface (LAN-A or LAN-B) for each SSID by using the drop down menu.
Subnet	Choose LAN-A or LAN-B for each SSID. If you choose LAN-A, the wireless clients connecting to this SSID could only communicate with LAN-A.
Isolate LAN	Check this box to make the wireless clients (stations) with the same SSID not accessing for wired PC in LAN.
	Note: If Isolate LAN is checked, do not type any value for VLAN ID.
Isolate Member	Check this box to make the wireless clients (stations) with the same SSID not accessing for each other.
Isolate Member VLAN ID	Check this box to make the wireless clients (stations) with the
	Check this box to make the wireless clients (stations) with the same SSID not accessing for each other. Type the value for such SSID. Packets transferred from such
	Check this box to make the wireless clients (stations) with the same SSID not accessing for each other. 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

2437MHz (Channel 6)
AutoSelect
2412MHz (Channel 1)
2417MHz (Channel 2)
2422MHz (Channel 3)
2427MHz (Channel 4)
2432MHz (Channel 5)
2437MHz (Channel 6)
2442MHz (Channel 7)
2447MHz (Channel 8)
2452MHz (Channel 9)
0457MU = (01 1.40)
2457MHz (Channel 10)
2457MHz (Channel 10) 2462MHz (Channel 11)

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

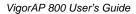
If you choose 11g Only, 11b Only or 11n Only, such feature will be available for you to set data transmission rate.

SSID4:	 the Wireless client will also change based on this MAC address. Reserved for Universal Repeater mode so it's not listed. 		
Channel :	2462MHz (Channel 11) 🔽		
Rate :	Auto 💌		
Packet-OVERDA	Auto 1 Mbps 2 Mbps 5.5 Mbps 11 Mbos		
Note :	1111000		

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 Auto launch when Windows start up Remember mini status position Auto hide mini status Set mini status always on top Enable IP Setting and Proxy Setting in Profile	Advence Setting Disable Radio Fragmentation Threshold : RTS Threshold : Frequency : Ad-hoc Channel:	234 234 802.11b/g/n - 2.4GH	7
Group Roaming Ad-hoc	Power Save Mode: Tx <u>B</u> urst :	Disable Disable	
WLAN type to connect Infrastructure and Ad-hoc network Infrastructure network only Ad-hoc network only Ad-hoc network only			
	OK	Cancel	oly





WMM Capable	To apply WMM parameters for wireless data transmission, please click the Enable radio button.		
Antenna	VigorAP 800 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% <mark>~</mark> 100% 80%		

3.8.2 Security

Wireless LAN >> Security Settings

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.

60% 30% 20% 10%

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

SSID 1	SSID 2	SSID 3	SSID 4		
Ν	1ode	Disabl	е	*	
_		16 000 Au in a			
WPA	et up <u>RADIUS Server</u>	IT 802.1X IS 6	enabled.		
v	VPA Algorithms	○ ткі	P O AES C	TKIP/AES	
P	ass Phrase				
к	ey Renewal Interval	3600	seconds		
P	MK Cache Period	10	minutes		
P	re-Authentication	🖲 Disa	able 🔾 Enable		
WEP					
	◉ Key 1 :				Hex 💙
	🔾 Key 2 :				Hex 💙
	🔾 Кеу 3 :				Hex 💌
) Key 4 :				Hex 💌
8	02.1× WEP	🔿 Disa	able 🔿 Enable	e	

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 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 800 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.
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 ','. Such feature is available for WEP mode.
	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	
Port	1812
Shared Secret	
Session Timeout	0

ОК

Use internal RADIUS Server There is a RADIUS server built in VigorAP 800 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, **3.10 RADIUS Server** to configure settings for internal server of VigorAP 800.

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.)

3.8.3 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).

less LAN >>	Access Control				
SSID 1	SSID 2	SSID 3	SSID 4		
	ţ	Policy: Disable		~	
		МАС	Address Filter		
	Inde;	<	MAC A	Address	
	Client's M	AC Address : Add Delet	: : : Edit	: : : Cancel	

Cancel

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 WLAN from LAN will separate all the WLAN stations from LAN based on the MAC Address list. 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 a new MAC address into the list. Add 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. OK Click it to save the access control list. Cancel Clean all entries in the MAC address list.

OK

3.8.4 WPS

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

Nireless LAN >> WPS (Wi-Fi Protected Setup)				
Enable WPS *				
Wi-Fi Protected Setup Informa	tion			
WPS Configured	Yes			
WPS SSID	DrayTek-LAN-A			
WPS Auth Mode	Open			
WPS Encryp Type	None			
AP PIN	22413482 Generate			
Device Configure				
Configure via Duch Button	Ctort BB C			

Configure via Push Button	Start PBC
Configure via Client PinCode	Start PIN
Status: The Authentication Mode is NOT	WPA/WPA2 PSK!!

Note: WPS can help your wireless client automatically connect to the $\ensuremath{\mathsf{Access}}$ point.

Q: WPS is Enabled. ♂: Waiting for WPS requests from wireless clients.

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 800 is properly configured, you can see 'Yes' message here.
WPS SSID	Display current selected SSID.
WPS Auth Mode	Display current authentication mode of VigorAP 800. Only WPA2/PSK and WPA/PSK support WPS.
WPS Encryp Type	Display encryption mode (None, WEP, TKIP, AES, etc.) of VigorAP 800.
AP PIN	The number displayed here is used for remote client entering the registrar's PIN code in remote station to make a network connection.
Configure via Push Button	Click Start PBC to invoke Push-Button style WPS setup procedure. VigorAP 800 will wait for WPS requests from wireless clients about two minutes. The WPS LED on t VigorAP 800 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 VigorAP 800 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).

 $[\]mathbb{Q}$: WPS is Disabled.

3.8.5 AP Discovery

VigorAP 800 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 800 can be found. Please click **Scan** to discover all the connected APs.

Access Point Lis	st						
Select SSID	BSSID	RSSI	Channel	Encryption	Authentication		
			S	an			
See Channel S	Statistics						
Note: During th	ie scanning	process (a	bout 5 second:	s), no station is allo	wed to connect with the router		
AP's MAC Addr	ess]:[]:[]:[]:[: AP's	SSID		
Select as <u>Unive</u>	rsal Repeate	n – – – – – – – – – – – – – – – – – – –					
SSID		Displa	y the SSID o	of the AP scanned	l by VigorAP 800.		
BSSID		Displa	Display the MAC address of the AP scanned by VigorAP 800.				
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 800.				
Encryption		Displa	y the encryp	tion mode for the	e scanned AP.		
Authenticatio	n	Displa	y the authen	tication 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.					
Statistics		It disp	lays the stati	stics for the chan	nels used by APs.		
AP's MAC A	ddress	It disp	lays the MA	C address of the .	AP you selected.		
AP's SSID		It disp	lays the SSI	D of the AP you s	selected.		
Select as Univ Repeater	versal		-		N would work as station lected as a universal		

repeater. Choose one of the wireless APs from the Scan list.

3.8.6 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	R1
MAC Address (Optional)	
Channel	2417MHz (Channel 2) 💌
Security Mode	Open 💌
Encryption Type	None 💌
WEP Keys	
	ASCII 💌
🔘 Кеу 2 :	ASCII 💌
🔘 Кеу 3 :	ASCII 💌
🔘 Кеу 4 :	ASCII 💌

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

	OK Cancel			
SSID	Set the name of access point that VigorAP800 wants to connect to.			
MAC Address (Optional)	Type the MAC address of access point that VigorAP800 wants to connect to.			
Channel	Means the channel of 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.			
Security Mode	There are several modes provided for you to choose. Each mo will bring up different parameters (e.g., WEP keys, Pass Phra for you to configure.			
	Shared			

WPA/PSK WPA2/PSK

Open / Shared Mode

Wireless LAN >> Universal Repeater

Universal Repeater Parameters	
SSID	R1
MAC Address (Optional)	
Channel	2417MHz (Channel 2) 💌
Security Mode	Open 💌
Encryption Type	None 💌
WEP Keys	
⊙ Key 1 :	ASCII 💌
🔘 Кеу 2 :	ASCII 💌
🔘 Кеу 3 :	ASCII 🗸
🔘 Кеу 4 :	ASCII 💌

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

OK Cancel

Encryption Type	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 .
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

WPA/PSK Mode and WPA2/PSK Mode

Wireless LAN >> Universal Repeater

R1
2417MHz (Channel 2) 💌
WPA/PSK
ТКІР 💌
•••••

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

OK Cancel

Encryption Type	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").			



3.8.7 Station List

Wireless LAN >> Station List

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

AC Address	SSID	Auth	Encrypt
	Refresh]	
dd to Access Control :			

Add

ſ

MAC Address SSID	Display the MAC Address for the connecting client. 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.				
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.				

3.9 Wireless LAN (5G) Settings for AP Mode

When a 5G Dongle connects to VigorAP 800, only AP mode (the operation mode) is available for configuration. The AP mode allows wireless clients to connect to access point and exchange data with the devices connected to the wired network.



If no 5G dongle connected to VigorAP 800, an error message will be displayed and no function in this menu can be activated.

3.9.1 General Setup

By clicking the **General Setup**, a new web page will appear so that you could configure the general settings for wireless connection such as specifying SSID, selecting the wireless channel, isolate LAN connection and so on.

al Setting (IEEE 802.11)					
nable Wireless LAN					
Mode :	Mixe	d (11a+11	n) 🚩		
🗹 Enable 2 Subnet (Simula	te 2 APs)				
Hide SSID SSII	þ	Subnet	Isolate LAN	Isolate Member	VLAN ID (0:Untaqqed)
1 DrayTek-5G		LAN-A 💌			Ò
2		LAN-A 💌			0
3		LAN-A 💌			0
	SID from bein lients (statior		ne same SSID	cannot aci	cess for each
Channel :	5180	OMHz (Cha	nnel 36) 🛛 💌		
Extension Channel :	5200	OMHz (Cha	nnel 40) 🔽		

Enable Wireless LAN

Check the box to enable wireless function.

Mode

At present, VigorAP 800 can be connected by 11a only, 11n only (5G), Mixed (11a+11n) stations simultaneously. Simply choose Mixed (11a+11n) mode.

Mixed (11a+11n) 🎽
11a Only
11n Only (5G)
Mixed (11a+11n)

Enable 2 Subnet
(Simulate 2 APs)Check the box to enable the function for two independent subnets.
Once you enable this function, LAN-A and LAN-B would be
independent. Next, you can connect one router in LAN-A, and
another router in LAN-B. Such mechanism can make you feeling



	that you have two independent AP/subnet functions in one VigorAP 800.
	If you disable this function, LAN-A and LAN-B ports are in the same domain. You could only connect one router (no matter connecting to LAN-A or LAN-B) in this environment.
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 800 while site surveying. The system allows you to set three sets of SSID for different usage.
SSID	Set a name for VigorAP 800 to be identified. Default settings are DrayTek-LAN-A and DrayTek-LAN-B. When Enable 2 Subnet is enabled, you can specify subnet interface (LAN-A or LAN-B) for each SSID by using the drop down menu.
Isolate LAN	Check this box to make the wireless clients (stations) with the same SSID not accessing for wired PC in LAN.
	Note: If Isolate LAN is checked, do not type any value for VLAN ID.
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.
Channel	Means the channel of frequency of the wireless LAN. The default channel is 36 . 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	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.

3.9.2 Security

This page allows you to set security with different modes for SSID 1, 2, and 3 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 (5G) >> Security Settings

SSID 1	SSID 2	SSID 3		
Mode		Disable	~	
	RADIUS Server if 802	.1x is enabled.		
WPA				
WPA A	lgorithms	⊖ TKIP ○ AES ○) TKIP/AES	
Pass P	hrase			
Key Re	enewal Interval	3600 seconds		
РМК С	ache Period	10 minutes		
Pre-Au	uthentication	Oisable O Enable		
WEP				
🖲 Ke	y 1 :			Hex 💌
🔾 Ке	y 2 :			Hex 💌
🔾 Ке	уЗ:			Hex 💌
🔾 Ке	y 4 :			Hex 💌
802.1>	(WEP	O Disable O Enable	е	

Mode

There are several modes provided for you to choose.

Cancel

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	

ОК

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 800 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.
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 ','. Such feature is available for WEP mode.
	Hex ASCII Hex
902 1 ₂₂ W/FD	Disable Disable the WEP Energy price Data sent to the AP will

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 l	ink of RADI	J S Server to	o access into	o the follow	ving page fo	or more settings.

Radius Server			
✓Use internal RADIUS S	erver		
IP Address			
Port	1812		
Shared Secret			
Session Timeout	0		
	ОК		
Use internal RADIUS Server	There is a RADIUS server built in VigorAP 800 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, 3.10 RADIUS Server to configure settings for internal server of VigorAP 800.		
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.)		

3.9.3 Access Control

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

Wireless LAN (5G) >> Access Control

SSID 1	SSID 2	SSID 3		
	Policy: Di	sable	~	
		MAC Address Filter		
	Index	MAC A	ddress	
	Client's MAC Address	5: 🔜 : 🔜 : 🔜	: : :	
	Add	Delete Edit	Cancel	
		OK Cance		

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 WLAN from LAN will separate all the WLAN stations from LAN based on the MAC Address list.
	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.
ОК	Click it to save the access control list.
Cancel	Clean all entries in the MAC address list.

3.9.4 AP Discovery

VigorAP 800 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 800 can be found. Please click **Scan** to discover all the connected APs.

Wireless LAN (5G) >> Access Point Discovery

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

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

SSID	Display the SSID of the AP scanned by VigorAP 800.
BSSID	Display the MAC address of the AP scanned by VigorAP 800.
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 800.
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

3.9.5 Station List

Wireless LAN (5G) >> Station List

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

SSID	Auth	Encrypt
Pofroch)	
Keiresii]	
	Refresh	Refresh

Add

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.
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.

3.10 RADIUS Server

VigorAP 800 offers a built-in RADIUS server to authenticate the wireless client that tries to connect to VigorAP 800. The AP can accept the wireless connection authentication requested by wireless clients.

RADIUS Server Configuration	I		
Enable RADIUS Server			
Users Profile (up to 96 use	rs)		
Username	Password	Confirm Password	Configure
			Add Cancel
NO.	Username		Select
Delete Selected	Delete All		
Authentication Client (up	to 16 clients)		
Client IP	Secret Key	Confirm Secret Key	Configure
			Add Cancel
NO.	Client IP		Select
Delete Selected	Delete All		

OK Cancel

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.
	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 800 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 800 as its external RADUIS server.
	Client IP – Type the IP address for the user to be authenticated by VigorAP 800 when the user tries to use VigorAP 800 as the external RADIUS server.
	Secret Key – Type the password for the user to be authenticated by VigorAP 800 while the user tries to use VigorAP 800 as the external RADIUS server.
	Confirm Secrete Key – Type the password again for confirmation.
	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.

3.11 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, Reboot System, Firmware Upgrade.

Below shows the menu items for System Maintenance.

System Maintenance
System Status
 TO 060

- TR-069
- Administration Password
- Configuration Backup
- Reboot System
- Firmware Upgrade.

3.11.1 System Status

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

System Status

Model Firmware Version Build Date/Time System Uptime Operation Mode

: VigorAP 800 : 1.0.2 : r1509 Fri Feb 25 10:26:12 CST 2011 : 0d 02:22:24 : Universal Repeater

	System		LAN-A
Memory total	: 30268 kB	MAC Address	: 00:50:7F:C9:1E:24
Memory left	: 10364 kB	IP Address	: 192.168.1.2
		IP Mask	: 255.255.255.0
	Wireless		LAN-B
MAC Address	: 00:50:7F:C9:1E:24	MAC Address	: 00:50:7F:C9:1E:24
SSID	: R1_AP800	IP Address	: 192.168.2.2
3310			

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.
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.

3.11.2 TR-069

System Maintenance >> TR-069 Settings

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.

URL	
Username	
Password	
CPE Settings	
Enable	
On	
URL	http://192.168.1.2:8069/cwm/CRN.html
Port	8069
Username	vigor
Password	
Note : Please set default g	ateway, no matter choose LAN-A or LAN-B.
Periodic Inform Settings	
Enable	
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)
	OK Cancel
CS Server	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.
PE 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 (LAN-A or LAN-B) for VigorAP 800 connecting to ACS server.
	Port – Sometimes, port conflict might be occurred. To solve such problem, you might change port number for CPE.
Periodic Inform Settings	The default setting is Enable . Please set interval time or schedule time for the AP to send notification to CPE. 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 maximum period is specified.

3.11.3 Administrator Password

This page allows you to set new password.

System Maintenance >> Administration Password

Adminstrator Settings	
Account	admin
Password	•••••
	OK Cancel

Account Type the name for accessing into Web User Interface.

Password

Type in new password in this filed.

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

3.11.4 Configuration Backup

Backup the Configuration

Follow the steps below to backup your configuration.

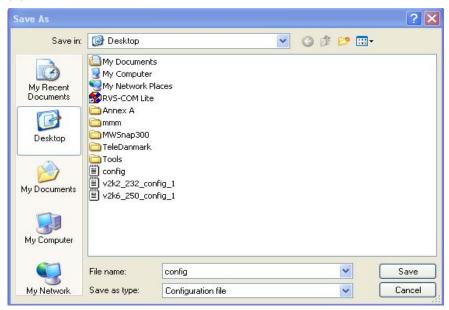
1. Go to **System Maintenance** >> **Configuration Backup**. The following windows will be popped-up, as shown below.

System Maintenance >> Configuration Backup			
Configuration	onfiguration 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 Image: 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.



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

System Maintenance >> Configuration Backup

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

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.

3.11.5 Reboot System

System Maintenance >> Reboot System

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

eboot System		
	Do You want to reboot your router ?	
	 Using current configuration 	
	O Using factory default configuration	

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

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



3.11.6 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.

irmware Update	
Select a firmware file.	
	Browse
Click Upgrade to upload the file. Upgrade	

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

3.12 Diagnostics

Diagnostic Tools provide a useful way to **view** or **diagnose** the status of your VigorAP 800. At present, only **System Log** is offered.

Diagonostics >> System Log

System Maintenance >> Firmware Upgrade

System Log Information <u>Clear</u> <u>Refresh</u> 🗌 Line	wrap
Od 02:11:12 syslogd started: BusyBox v1.12.1	~
0d 02:11:12 kernel: klogd started: BusyBox vl.12.1 (2011-02-25 10:27:36 CST)	
Od 02:11:12 kernel: flag: 0x0	
0d 02:11:12 kernel: ravid 0: 0x0	
0d 02:11:12 kernel: ravid 1: 0x0	
0d 02:11:12 kernel: ravid 2: 0x0	
0d 02:11:12 kernel: ravid 3: 0x0	
0d 02:11:12 kernel: ravid 4: 0x0	
0d 02:11:12 kernel: ravid 5: 0x0	
0d 02:11:12 kernel: ravid 6: 0x0	
0d 02:24:19 kernel: LOG#1 40:d3:2d:a0:f7:d3 successfully associated	
0d 02:24:25 kernel: LOG#2 40:d3:2d:a0:f7:d3 has disassociated	
0d 02:25:25 kernel: RT305x_ESW: Link Status Changed	
0d 02:28:24 kernel: LOG#3 00:1d:4f:d5:c1:39 successfully associated	
0d 02:30:08 kernel: LOG#4 78:1d:ba:15:2b:13 successfully associated	
0d 02:30:09 kernel: Rcv Wcid(2) AddBAReq	\sim
<u><</u>	>

3.13 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.



Click **Support Area>>Application Note**, the following web page will be displayed.

Dray Tek		繁體中文	English	Login	Search Go
About	DrayTek Produ	cts Support	Education	Partners	Contact Us
ome > Support > Application Notes					
Application Notes - Latest Application				Applica	tion Notes
01. How to use Windows Disk Management to format the	USB Disk ?	2	009/09/09	Latest A	pplication
02. How to make a call between ATA24 without IP PBX or	SIP server	2	009/08/25	General	
03. Vigor Router to NETGEAR with IPSec tunnel		2	009/07/20	Dual WA	N
04. SSL VPN Tunnel		2	009/07/16	VolP	
05. How to Access the Computers and Shared Files via Sa	amba Protocol?	2	009/06/18	Bandwid	th Management
06. SSL Web Proxy		2	009/06/18	IP Filter/	Firewall
07. How to use VNC and RDP via SSL VPN?		2	009/06/18	USB	
08. Vigor2950 Host-to-LAN VPN with LDAP Authentication	1	2	009/06/01	VPN	
09. How to build LAN to LAN IPSec VPN by using X.509 C			009/03/31		st to LAN VPN orker to Vigor)

Click **Support Area>>FAQ**, the following web page will be displayed.

Dray Tek		繁體中文	English	Login	Search Go
About DrayTek Pi	roducts	Support	Education	Partners	Contact Us
lome > Support > FAQ					
FAQ - Latest FAQ				FAQ	
01. What types of 3G modem / cellphone are compatible with Vigor router	?	2	009/10/01	Latest F	AQ
02. How to use PRTG monitors network traffic Vigor Router		2	009/09/22	Basic	
03. What is Powerline Networking?		2	009/09/15	Advance	d
04. What are the benefits of networking devices found at home?		2	009/09/15	NAT	
05. What is the maximum wire length that powerline technology can comm	nunicate ove	r? 2	009/09/15	VPN	
06. Is VigorPlug's powerline technology compatible with other home netwo	orking techno	logies 2	009/09/15	DHCP	
(including phone line, powerline, and RF)?	-			Wireless	3
07. Will Powerline technology interfere with ADSL services?		2	009/09/15	VolP	
08. How does Powerline networking handle co-interference between two ac	djacent hom	es 2	009/09/15	QoS	
using powerline technology? How is eavesdropping prevented?				ISDN	
				-	

Click **Support Area>>Product Registration**, the following web page will be displayed.

Dray Tek				English	Login	Search Go
	About DrayTek	Products	Support	Education	Partners	Contact Us
Home > DrayTek Member						
DrayTek Member						
Dear DrayTek new & existing users,					Sign up	
For enhancing the users' satisfaction level while ut	ilizing our site and rec	ceiving even bet	ter service fro	om DrayTek,	Forgot Pa	assword
we have designed this membership page. Please product(s).	complete the membe	rship registrati	on and then r	egister your		
Already a DrayTek Member – Just sign-in b						
Want to become a DrayTek Member – Click Forgot username or password – Click "Forg			he membersh	ip form.		
Benefits for DrayTek Members						
Receiving e-news letters about latest firmwa		rchased produc	ts.			
Software and firmware available online for do Chances to win prizes.	wnload.					
Many more benefits only for DrayTek members are	coming soon.					

This page is left blank.

VigorAP 800 User's Guide



4.1 Upgrade Firmware for Your Modem

Before upgrading your device firmware, you need to install the Router Tools. The file **RTSxxx.exe** will be asked to copy onto your computer. Remember the place of storing the execution file.

- 1. Go to www.draytek.com.
- 2. Access into **Support** >> **Downloads**. Please find out **Firmware** menu and click it. Search the model you have and click on it to download the newly update firmware for your router.

	About DrayTek	Products	Support	Education	Partners	Contact U
ome > Support > Download	s					
Downloads - Firmware					Downlo	ads
Model Name	Firmware Version	Re	lease Date		Firmware	
Vigor120 series	3.2.2.1	2	6/06/2009		Driver	
Vigor2100 series	2.6.2	2	6/02/2008		Utility	
Vigor2104 series	2.5.7.3	1:	3/02/2008		Utility In	troduction
Vigor2110 series	3.3.0	2	5/06/2009		Datashee	
Vigor2200/X/W/E	2.3.11	22	2/09/2004			• ertification
Vigor2200Eplus	2.5.7	18	8/02/2009			entineation
Vigor2200USB	2.3.10	1	6/03/2005			

3. Access into **Support >> Downloads**. Please find out **Utility** menu and click it.

		About I	DrayTek I	Products	Support	Education	Partners	Contact U	
ome > Support > Ut	ility								
Utility							Downlo	ads	
Tools Name	Release Date	Version	OS		Support	Model	Firmware		
Router Tools	2009/06/18	4.2.0	MS-Win	dows	All Mod	ules			
Syslog Tools	2009/06/18	4.2.0	MS-Winde	AS-Windows XP		ules	Driver		
-,,			MS-Vi	sta			Utility		
VigorPro Alert Notice	2009/06/03	1.1.0	MS-Winde	ows XP	VigorPro 10	0 series	Utility In	troduction	
Tools		(Multi- language)	MS-Vi	sta	VigorPro 55 VigorPro 55		Datashee	t	
					VigorPro 53	00 series	R&TTE C	ertification	
Smart VPN Client	2009/05/25	3.6.3	MS-Winde	ows XP	All Mod	ules			
		(Multi-	MS-Vi	sta					
		language)							
Smart Monitor	2009/03/25	2.0	MS-Wind	ows XP	Vigor2950	series			
					MaarDro 55	10 cories			

4. Click on the link of **Router Tools** to download the file. After downloading the files, please decompressed the file onto your host.



5. Double click on the icon of modem tool. The setup wizard will appear.



- 6. Follow the onscreen instructions to install the tool. Finally, click **Finish** to end the installation.
- 7. From the **Start** menu, open **Programs** and choose **Modem Tools XXX** >> **Firmware Upgrade Utility**.

៉ Firmware Upgrade	Utility 3.5.1	
Time Out(Sec.) 5	Router IP:	
Port 69	Firmware file:	
Password:	Abort	Send

- 8. Type in your modem IP, usually 192.168.1.2.
- 9. Click the button to the right side of Firmware file typing box. Locate the files that you download from the company web sites. You will find out two files with different extension names, **xxxx.all** (keep the old custom settings) and **xxxx.rst** (reset all the custom settings to default settings). Choose any one of them that you need.

🎒 Firmware Upgrade	Utility 3.5.1
Time Out(Sec.) 5	Router IP:
Port	Firmware file:
69 Password:	C:\Documents and Settings\Carrie
	Abort Send

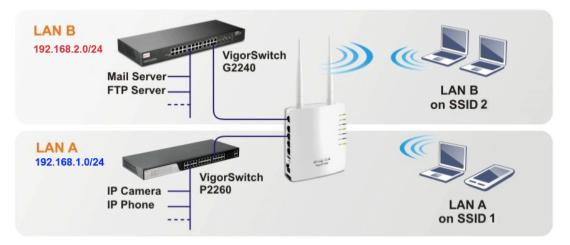
10. Click Send.

៉ Firmware Upgrade	Utility 3.5.1
Time Out(Sec.) 5	Router IP:
Port	Firmware file:
69 Password:	C:\Documents and Settings\Carrie
	Abort Send
Sending)

11. Now the firmware update is finished.

4.2 How to set different segments for different SSIDs in VigorAP 800

VigorAP 800 supports two network segments, LAN-A and LAN-B for different SSIDs. With such feature, the user can dispatch SSIDs with different network segments for reaching the target of managing wireless network. See the following figure.



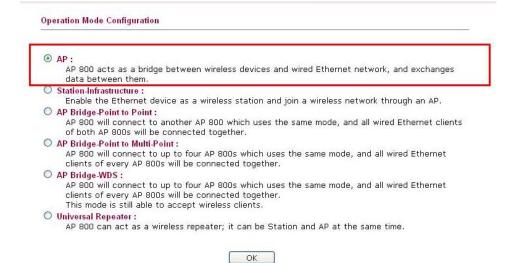
In the above figure, VigorAP 800 is used to control the wireless network connection. It can separate the wireless traffic between accessing internal server and the usage of video. Wireless station connecting to VigorAP 800 with SSID 1 can get the IP address with the network segment of 192.168.1.0/24 (LAN-A); wireless station connecting to VigorAP800 with SSID 2 can get the IP address with the same network segment of 192.168.2.0/24 (LAN-B).

LAN-B : 192.168.2.0/24 \rightarrow for internal server

LAN-A : 192.168.1.0/24 \rightarrow for video traffic

Below shows you how to configure the web page for VigorAP 800:

1. In the page of **Operation Mode**, click **AP** mode.



2. Open **Wireless LAN** >> **General Setup**. Choose the subnet **LAN-A** for SSID 1 and choose **LAN-B** for SSID 2. Specify the wireless channel. Then, click **OK** to save the configuration.

able W	ireless LAN							
Mode :		M	lixed(11	b+11g+:	11n) 💌			
					and the second sec			
Ena Hide	able 2 Subnet (Sim		I solate :	Isolate	VLAN I	D		
SSIL	SSID	Subnet			0:Untage		Mac Clor	пe
1	SSID 1	LAN-A 🚩			0			
2	SSID 2	LAN-B 🚩			0]		
з 🔲		LAN-A 💌			0]		
4		LAN-A 💌			0	1		
Hide SS Isolate MAC CI	Member: Wireles other one: Set the the Wir	e MAC addres: reless client w	tions) w s of SSI vill also (vith the D 1. Thi change	e MAC ao based or	ldresse this M	s of other S: AC address.	SIDs an Please
Isolate MAC CI	Member: Wireles other one: Set the the Wir notice	s clients (sta e MAC addres reless client w that the last	tions) w s of SSI vill also o byte of	vith the D 1. The change I this MA	e MAC ao based or C addres	ldresse this M	s of other S: AC address.	SIDs an Please
Isolate	Member: Wireles other one: Set the the Wir notice	s clients (sta e MAC addres reless client w that the last	tions) w s of SSI vill also o byte of	vith the D 1. The change I this MA	e MAC ao based or	ldresse this M	s of other S: AC address.	SIDs Plea:
Isolate MAC CI Extens Packet I T x E Note : 1.T x Bu	Member: Wireles other one: Set the the win notice el : iion Channel : -OVERDRIVE Burst urst only supports	ss clients (sta e MAC address reless client w that the last 2 11g mode.	tions) w s of SSI vill also o byte of 462MHz 442MHz	vith the (D 1. Thi change I this MA (Channi (Channi	e MAC ac based or C addres el 11) ¥ el 7) ¥	ldresse this M s must	s of other S: AC address, be a multipl	SIDs a Please e of 8.
Isolate MAC CI Extens Packet I T x E Note : 1.T x Bu	Member: Wireles other., one: Set the the win notice el : ion Channel : -OVERDRIVE Burst	ss clients (sta e MAC address reless client w that the last 2 11g mode.	tions) w s of SSI vill also o byte of 462MHz 442MHz	vith the (D 1. Thi change I this MA (Channi (Channi	e MAC ac based or C addres el 11) ¥ el 7) ¥	ldresse this M s must	s of other S: AC address, be a multipl	SIDs ar Please e of 8.

3. Open **Wireless LAN** >> **Security Settings**. Set the encryption method and set the password for SSID 1 and SSID 2 respectively.

SSID 1	SSID 2	SSID 3	SSID 4			
M	ode	Mixe	d(WPA+WPA2))/PSK 🛛 📉		
Se WPA	et up <u>RADIUS Serve</u>	<u>r</u> if 802.1x is	s enabled.			
0.000.000	PA Algorithms	() T	KIP OAES	O TKIP/	AES	
Pa	ass Phrase		•••••			
Ke	ey Renewal Interva	3600) seconds			
PN	/K Cache Period	10	minutes			
Pr	e-Authentication) D	isable OEnab	ile		
WEP						
) Key 1 :					Hex 💌
() Key 2 :					Hex 👻
	Кеу 3:					Hex 👻
) Key 4 :					Hex 👻
80	2.1× WEP	OD	isable O Ena	able		

4. Open LAN>General Setup to configure the settings for enabling DHCP server on LAN-A/LAN-B. If there is a DHCP server configured in the same network segment, skip this step.

Ethernet TCP / IP and D			
LAN-A IP Network Configuration		DHCP Server Configuration	
IP Address	192.168.1.2	● Enable Server ○ Disa	ble Server
Subnet Mask	255.255.255.0	Start IP Address	192.168.1.10
Default Gateway	· · · · · · · · · · · · · · · · · · ·	End IP Address	192.168.1.100
		Subnet Mask	255.255.255.0
		Default Gateway	192.168.1.2
		Lease Time	86400
		Primary DNS Server	168.95.1.1
		Secondary DNS Server	168.95.192.1
LAN-B IP Network Cont	figuration	DHCP Server Configuration	n
IP Address	192.168.2.2	Inable Server ○ Disa	ble Server
Subnet Mask	255.255.255.0	Start IP Address	192.168.2.10
		End IP Address	192.168.2.100
		Subnet Mask	255.255.255.0
		Default Gateway	192.168.2.2
		Lease Time	86400
		Primary DNS Server	168.95.1.1
		Secondary DNS Server	168.95.192.1

5. After finishing the above settings, the wireless equipment connecting to VigorAP 800 with SSID 1 can get the IP address assigned by LAN-A 192.168.1.0/24 for accessing the internal server. The wireless equipment connecting to VigorAP 800 with SSID 2 can get the IP address assigned by LAN-B 192.168.2.0/24 for using the video/audio uploading and downloading services.



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.

5.1 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 **LAN** 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.

5.2 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

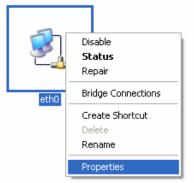


The example is based on Windows XP. As to the examples for other operation systems, please refer to the similar steps or find support notes in **www.draytek.com**.

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:					
 Client for Microsoft Networks File and Printer Sharing for Microsoft Networks 					
🗹 📮 QoS Packet Scheduler					
Internet Protocol (TCP/IP)					
Install					
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 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.				
Use the following IP address: -				
IP address:				
S <u>u</u> bnet mask:				
Default gateway:	and the second second			
Obtain DNS server address au	tomatically			
O Use the following DNS server addresses:				
Preferred DNS server:				
Alternate 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.

	Network	
ow All Displays So	Sund Network Startup Disk	
ow All : Displays Sc	Sund Network Startup Disk	
	Location: Automatic	
	Show: Built-in Ethernet	
ТСІ	P/IP PPPoE AppleTalk Proxies Ethernet	
Configure IPv4	: Using DHCP	
Configure inve		
IP Address	: 192.168.1.10 Renew DH0	CP Lease
Subnet Mask	: 255.255.255.0 DHCP Client ID:	
Router	: 192.168.1.1 (If required))
		,
DNS Servers	:	(Optional)
Garanta Damaina		
Search Domains	:	(Optional)
IPv6 Address	: fe80:0000:0000:0000:020a:95ff:fe8d:72e4	
		0
	Configure IPv6	(?)



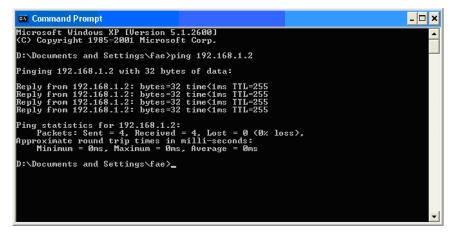
5.3 Pinging the Modem from Your Computer

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.

\varTheta 🖯 🕘 Ter	minal — bash — 80x24
Last login: Sat Jan 3 02:24:18 Welcome to Darwin! Vigor10:~ draytek\$ ping 192.168 PING 192.168.1.1 (192.168.1.1) 64 bytes from 192.168.1.1: icmp 64 bytes from 192.168.1.1: icmp	3.1.1 : 56 data bytes p_seq=0 ttl=255 time=0.755 ms
64 bytes from 192.168.1.1: icm; 64 bytes from 192.168.1.1: icm; 64 bytes from 192.168.1.1: icm; ^C	o_seq=3 ttl=255 time=0.731 ms
 192.168.1.1 ping statistics 5 packets transmitted, 5 packet round-trip min/avg/max = 0.697, Vigor10:~ draytek\$ 	cs received, 0% packet loss

5.4 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

Reboot System

Do You want to reboot your router ?

O Using 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.

5.5 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.

