VigorAP 905

802.11ax Access Point

User's Guide

Version: 1.0

Firmware Version: V5.0.4

Date: June 11, 2025

Intellectual Property Rights (IPR) Information

• 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 device. The device is a complicated electronic unit that may be repaired only be authorized and qualified personnel. Do not try to open or repair the device yourself. Do not place the device in a damp or humid place, e.g. a bathroom. The device should be used in a sheltered area, within a temperature range of +0 to +40 Celsius. Do not expose the device 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. Do not power off the device when saving configurations or firmware upgrades. It may damage the data in a flash. Please disconnect the Internet connection on the device before powering it off when a TR-069/ ACS server manages the device. Keep the package out of reach of children. When you want to dispose of the device, please follow local regulations on conservation of the environment.
Warranty	We warrant to the original end user (purchaser) that the device will be free from any defects in workmanship or materials for a period of two (2) years 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 router via https://myvigor.draytek.com.
Firmware & Tools Updates	Due to the continuous evolution of DrayTek technology, all devices will be regularly upgraded. Please consult the DrayTek web site for more information on newest firmware, tools and documents. https://www.draytek.com

Table of Contents

Chapt	oter I Installation	V
	I-1 Introduction	1
	I-1-1 LED Indicators and Connectors	2
	I-2 Hardware Installation	4
	I-2-1 Wired Connection for PC in LAN	
	I-2-2 PoE Connection	
	I-2-3 Wall-mount Installation	
	I-3 Network IP Configuration	
	I-3-1 Windows 10 IP Address Setup	
	I-4 Accessing to Web User Interface	
	I-5 Dashboard	
	I-6 Two-factor Authentication	
Chapt	oter II Connectivity	
•	II-1 Configuration	
	II-1-1 Physical Interface	
	II-1-2 LAN	
	II-1-2-1 LAN Networks	
	II-1-2-2 Bind IP to MAC	
	II-1-2-3 DHCP Options	
	II-1-2-4 VLAN List	
	II-1-2-5 Interface VLAN	
	II-1-3 Wireless LAN	
	II-1-3-1 SSID	
	II-1-3-2 Radio Settings	
	II-1-3-3 Roaming	
	II-1-3-4 AP Discovery	
	II-1-3-5 WPS	
	II-1-3-6 Range Extender	
	II-1-3-7 WDS	
	II-1-4 Objects	
	II-1-4-1 MAC Object	
	II-1-4-2 MAC Group	
	II-1-4-3 Schedule	
	II-1-5 Notification Services	
	II-1-6 RADIUS	
	II-1-7 Certificates	
	II-1-7-1 Local Certificates	
	II-1-7-2 Trusted CA	
	II-1-7-3 Local Services	
	II-1-7-4 Backup & Restore	60
	II-2 Security	
	II-2-1 MAC Filtering Profile	
	II-2-1-1 MAC Filtering Profile	
	II-2-1-2 Backup & Restore	
	II-3 Virtual Controller - Wireless	
	II-3-1 Role Setup	
	II-3-2 Device	
	II-3-2-1 Device List	
	II-3-2-2 Mesh Status	
	II-3-2-3 AP Adoption	71

III-1 Device Settings 76 III-1-1 Device Settings 77 III-1-1-2 Device Name 78 III-1-1-2 System 78 III-1-1-2 Device Name 78 III-1-1-2 Device Name 79 III-1-1-2 System 79 III-1-2 System 81 III-2-2 System Information 84 III-1-2 System Report 88 III-1-3 Engle Permission 91 II-1-5 System Rebot 91 II-1-5 System Rebot 97 II-1-5 Wind DidCP Subnet 96 M-1-1/IPA DidCP Subnet 96 M-1-1/IPA DidCP Lass 97 W-1-12 ILVD Pheliphors Information 97 W-13 User Res Tool 97 W-13 User Res Tool 97 W-14 User Res 100	Chapter III Management	75
III-1-1 Time 77 III-1-1 Spring 78 III-1-1 Syring 78 III-1-2 TRofo 88 III-1-2 TRofo 88 III-1-2 TRofo 88 III-1-2 System Information 88 III-1-1 Backup and Pestore 88 III-1-1 Backup and Pestore 88 III-1-1 Backup and Pestore 89 III-1-1 System Rebot 96 III-1-1 DHCP Table 96 IV-1-1 DHCP Table 96 IV-1-1 DHCP Table 97 IV-1-2 LUP Rephors Information 97 IV-2 LUP Rephors Information 97 IV-2 LUP Rephors Information 97 IV-2 Consta Westreet Stats 100 IV-2 Consta New Network 101 IV-	III-1 System Maintenance	
III-1-1 Time 77 III-1-1 Spring 78 III-1-1 Syring 78 III-1-2 TRofo 88 III-1-2 TRofo 88 III-1-2 TRofo 88 III-1-2 System Information 88 III-1-1 Backup and Pestore 88 III-1-1 Backup and Pestore 88 III-1-1 Backup and Pestore 89 III-1-1 System Rebot 96 III-1-1 DHCP Table 96 IV-1-1 DHCP Table 96 IV-1-1 DHCP Table 97 IV-1-2 LUP Rephors Information 97 IV-2 LUP Rephors Information 97 IV-2 LUP Rephors Information 97 IV-2 Consta Westreet Stats 100 IV-2 Consta New Network 101 IV-	III-1-1 Device Settings	
III-1-13 Systeg 77 III-1-2 NMP 77 III-1-2 NAragement 81 III-1-2 Texted Control 81 III-1-2 Texted Control 81 III-1-2 Texted Control 83 III-1-2 System Information 84 III-1-3 Strike AMP 85 III-1-3 Externation 88 III-1-3 Externation 89 III-1-5 Externation 89 III-1-5 Externation 99 III-1-5 Externation 91 III-1-5 Externation 91 III-1-1 Externation 92 III-1-5 Externation 91 III-1-1 Externation 92 III-1-1 Externation 93 III-1-1 Externation 95 IV-1 Monitoring 95 IV-1 DHCP Table 96 IV-1-1 IVA DHCP Subnet 96 IV-1-1 IVA DHCP Subnet 97 IV-3 Systeg 98 IV-4 Utry DHCP Exase 97 IV-3 Systeg 98 IV-4 Utry DHCP Exase 97 <t< td=""><td></td><td></td></t<>		
III-1-12 Margement. 73 III-12 Margement. 81 III-12 Margement. 81 III-12 To Forso. 83 III-12 A Service Control. 83 III-12 A XMPP. 85 III-13 Firmware. 86 III-14 Backup and Restore. 86 III-15 Accounts & Permission. 89 III-15 Rocie Admin Account. 89 III-15 System Reboot 91 Chapter IV Others 95 IV-1 Monitoring 96 IV-1-1 IPACP Table 96 IV-1-1 IPACP Table 96 IV-1-1 IPACP Table 97 IV-1 IPACP Table 97 IV-1 UPP Righbors information. 97 IV-2 UDP Nighbors information.		
III-1-22 TR-059 81 III-1-22 TR-059 83 III-1-23 TR-059 83 III-1-24 XMPP 85 III-1-24 XMPP 85 III-1-24 XMPP 85 III-1-24 XMPP 85 III-1-34 Struware 86 III-1-15 Accounts & Permission 89 III-1-52 Role & Permission 91 III-1-11 PM4 DHCICP Submet 96 IV-1-1 IIP4 OHCICP Submet 96 IV-1-1 IIP4 OHCICP Submet 99 IV-1-2 IIP1 ROTO 100 IV-2 UDP Neighbors Information 97 IV-1-3 Web Syslog 100 <t< td=""><td></td><td></td></t<>		
III-1-2-1 Service Control. 81 III-1-2 System Information. 83 III-1-2 AXMPP 85 III-1-1 Firmware 86 III-1-1 Hackup and Restore 88 III-1-1 Hackup and Restore 88 III-1-1 Formware 86 III-1-1 Accurnts & Permission 89 III-1-5 Accurate Science 89 IIII-1-5 Accurate Science 89 III-1-5 Accurate Science 91 III-1-5 Accurate Science 91 III-1-5 Accurate Science 91 III-1-5 Accurate Science 91 III-1-5 Accurate Science 92 III-1-1 Protection 91 III-1-1 Protection 91 III-1-1 Protection 91 III-1-2 Protection 91 III-1-1 Protection 91 IIII-1-2 Protection 99 IIII-1-1 Protection 99 IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII		
III-12-3 System Information 44 III-13 Firmware 56 III-14 Backup and Restore. 56 III-14 Backup and Restore. 58 III-15 Accounts & Permission 59 III-15 Accounts & Permission 59 III-15 Accounts & Permission 59 III-15 Accounts & Permission 51 III-15 Accounts & Permission 51 III-15 Accounts & Permission 51 III-15 Accounts 55 IV-1 Monitoring 56 IV-1 Monitoring 56 IV-1 Monitoring 57 IV-1 Step 57 IV-1 Step 58		
III-12-4 XMPP 55 III-13-Erroware 56 III-14-Backup and Restore 58 III-15-Accounts & Permission 69 III-15-2 Kole & Permission 61 III-1-1 DHCP Table 66 III-1-2 LUP Neighbors Information 77 III-1-3 Clents List 100 IIII-1 Pud DHCP Lease 77 III-1 S Clents List 100 IIII-2 Clents List 100 IIIIIIIIII IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII		
III-1-3 Firmware 66 III-1-4 Backup and Restore 88 III-1-5-1 Local Admin Account 89 III-1-5-1 Local Admin Account 89 III-1-5-1 Local Admin Account 89 III-1-5-2 Role & Permission 91 III-1-5-2 Stole & Permission 91 III-1-5-System Reboot 94 Chapter IV Others 95 IV-1 Monitoring 96 IV-1-1 DHCP Table 96 IV-1-1 DHCP Table 96 IV-1-1 LIPA DHCP Subnet 96 IV-1-2 IVPA DHCP Lease 97 IV-1-2 LIVPA Neighbors Information 97 IV-1-3 LIVPA Neighbors Information 99 IV-1-4 Internet 199 IV-1-5 Clinits List 100 IV-2 Utility 101 IV-2 2 Trace Tool 102 IV-2 2 Trace Tool 102 IV-2 2 Trace Tool 103 IV-2 Create a New Network 107 V-3 Wizard 109 V-4 Login 112 V-4 Login 114 <		
III-14 Backup and Restore. 88 III-15 Accounts & Permission. 89 III-15-1 Local Admin Account. 89 III-15-2 Kole & Permission. 91 III-15-2 Kole & Permission. 91 III-15-2 Kole & Permission. 95 Chapter IV Others 95 IV-1 Monitoring. 96 IV-1 Monitoring. 96 IV-1-1 DPCP Table. 96 IV-1-1 IPv4 DHCP Subnet. 96 IV-1-1 IPv4 DHCP Subnet. 97 IV-1-2 LLPP Neighbors information. 97 IV-1-3 US System Restore. 99 IV-1-1 Fiv4 DHCP Lease 99 IV-1-1 Scilents List. 100 IV-2 Utility. 101 IV-2 Utility. 101 IV-2 Utility. 101 IV-2 Utility. 101 IV-2 Trace Tool 102 IV-2 Trace Tool 103 Chapter V Mobile APP, DrayTek Wireless 105 V-1 Introduction of DrayTek Wireless 106 V-2 Create a New Network 107 V-3 Wizard 109 V-4 Login 112		
III-1-5 Accounts & Permission 88 III-1-5-1 Local Admin Account 89 III-1-5-2 Role & Permission 91 III-1-5 System Reboot 94 Chapter IV Others 95 IV-1 Monitoring 96 IV-1-1 DHCP Table 96 IV-1-1 DHCP Table 96 IV-1-1-1 IP44 DHCP Subnet 96 IV-1-1-1 IP44 DHCP Lease 97 IV-1-2 IP44 DHCP Lease 97 IV-1-3 Web Syslog 98 IV-1-4 Internet 99 IV-1-5 Clients List 100 IV-2 Utility 101 IV-2 - 2 Uble Neighbors Information 102 IV-2 Utility 101 IV-2 - 2 Uble Neighbors 100 IV-2 - 2 Uble Neighbors 101 IV-2 - 2 Uble Neighbors 102 IV-2 - 2 Uble Solog 101 IV-2 - 2 Uble Neighbors 101 IV-2 - 2 Uble Neighbors 102 IV-2 - 2 Uble Solog 102 IV-2 - 2 Uble Solog 102 IV-2 - 2 New Ocl 102 IV-2 - 2 New Ocl 103 IV-2 - 2 Newo		
III-1-5-2 Role & Permission 91 III-1-6 System Reboot 94 Chapter IV Others 95 IV-1 Monitoring 96 IV-1-1 DHCP Table 96 IV-1-1 DHCP Table 96 IV-1-1 DHCP Table 96 IV-1-1 DHCP Subnet 96 IV-1-2 ILVP DHCP Lease 97 IV-1-3 LIDP Neighbors Information 97 IV-1-4 Internet 99 IV-2 Utility 100 IV-2 Utility 101 IV-2 Utility 101 IV-2 Trace Tool 102 IV-3 Web CLI 103 IV-2 Create a New Network 107 V-3 Wizard 109 V-4 Login 114 Chapter VI Troubleshooting 115 VI-1 Checking the Hardware Status	•	
III-1-6 System Reboot 94 Chapter IV Others 95 IV-1 Monitoring 96 IV-1-1 DHCP Table 96 IV-1-1 1P4 DHCP Subnet 96 IV-1-1 2P4 DHCP Lease 97 IV-1-2 LUD P NejRhbors Information 97 IV-1-3 Cilents List 100 IV-2 Utility 101 IV-2 Trace Tool 102 IV-2 Trace Tool 102 IV-2 Trace Tool 103 IV-2 Trace Tool 104 IV-2 Trace Tool 105 V-1 Introduction of DrayTek Wireless 106 V-2 Create a New Network 107 V-3 Wizard 109 V-4 Login 114 V-4 Login 115 VI-1 Checking the Hardware Status 116 VI-2 Checking the Network Connection Settings 117 VI-3 Pinging the Device 120 VI-3 Pinging the Device 120 VI-3 Pinging the Device 120 VI-4 Login 117 VI-3 Pinging the Device 120 VI-3 Pinging the Device 120 VI-3 Pinging the Dev		
Chapter IV Others 95 IV-1 Monitoring 96 IV-1-1 DHCP Table 96 IV-1-1 DHCP Table 96 IV-1-1 DHCP Table 97 IV-1-1 DP Neighbors Information 97 IV-1-2 IPVA DHCP Lease 97 IV-1-3 Web Systops 97 IV-1-3 Web Systops 98 IV-1-4 Internet 99 IV-2 Utility 101 IV-2 Utility 101 IV-2 Trace Tool 102 IV-2 Trace Tool 103 IV-2 Trace Tool 102 IV-2 Utility 101 IV-2 Trace Tool 102 IV-2 Trace Tool 102 IV-2 Trace Tool 102 IV-2 Trace Tool 102 IV-2 Trace Tool 103 IV-2 Trace Tool 104 IV-2 Trace Tool 105 V-1 Introduction of DrayTek Wireless 106 V-2 Create a New Network 107 V-3 Wizard 104 V-4 Login 114 Chapter VI Troubleshooting 115 VI-1 Checking the Hardware Status </td <td></td> <td></td>		
IV-1 Monitoring. 96 IV-1-1 DHCP Table 96 IV-1-1-1 IP4 DHCP Subnet 96 IV-1-2 ILDD Neighbors Information 97 IV-1-2 ILLDP Neighbors Information 97 IV-1-3 Web Sysiog 98 IV-1-4 Ilternet 99 IV-1-5 Clients List 100 IV-2 Utility. 101 IV-2-2 Trace Tool 101 IV-2-3 Web CLI 102 IV-2-3 Web CLI 103 Chapter V Mobile APP, DrayTek Wireless 106 V-2 Create a New Network 107 V-3 Wizard 109 V-4 Login 114 Chapter VI Troubleshooting 115 VI-1 Checking the Hardware Status 116 VI-2 Checking the Network Connection Settings 117 VI-3 For Windows 117 VI-3 For Windows 1120 VI-4 Betwice to Action Settings 1120 VI-3 For Windows 1120 VI-3 For Windows 1120 VI-3 For Windows 1120 VI-3 For Windows 1120 VI-4 Decking the Device 120		
IV-1-1 DHCP Table 96 IV-1-1-1 PV4 DHCP Subnet 95 IV-1-1-2 IPV4 DHCP Lease 97 IV-1-2 ILDP Neighbors Information 97 IV-1-3 Ubp Neighbors Information 97 IV-1-4 Internet 99 IV-2 Utility 100 IV-2 Utility 101 IV-2 Utility 101 IV-2 Trace Tool 102 IV-2 Trace Tool 103 Chapter V Mobile APP, DrayTek Wireless 106 V-2 Create a New Network 107 V-3 Wizard 109 V-4 Login 112 V-4 I Setup 114 Chapter VI Troubleshooting 115 VI-1 Checking the Hardware Status 116 VI-2 Checking the Network Connection Settings 117 VI-3 Progrig the Device 119 VI-3 Proc Mac OS 119 VI-3 Proc Mac OS 117 VI-3 Pror Windows 112 VI-4 Backing to Factory Default Setting 122 VI-4 Backing to Factory Default Setting 122 VI-4 Login Keeset 122	Chapter IV Others	
IV-1-1 IPV4 DHCP Subnet 96 IV-1-2 IPV4 DHCP Lease 97 IV-1-2 ILDP Neighbors Information 97 IV-1-3 Web Syslog 98 IV-1-4 Internet 99 IV-1-2 ILDP Neighbors Information 100 IV-2 Utility 101 IV-2-1 Ping Tool 101 IV-2-1 Ping Tool 101 IV-2-2 Trace Tool 102 IV-2-3 Web CLI 103 Chapter V Mobile APP, DrayTek Wireless 106 V-2 Create a New Network 107 V-3 Wizard 109 V-4 Login 112 V-4 I Setup 114 Chapter VI Troubleshooting 115 VI-1 Checking the Hardware Status 116 VI-2 Checking the Network Connection Settings 117 VI-3 Pior Windows 117 VI-3 Por Windows 117 VI-3 Pior Windows 112 VI-4 Der Mac OS 119 VI-3 Pior Windows 120 VI-4 Backing to Factory Default Setting 122 VI-4 Backing to Factory Default Setting 122 VI-4 Backing to Factory Default Setting <td>IV-1 Monitoring</td> <td></td>	IV-1 Monitoring	
IV-1-12 LDP Neighbors Information 97 IV-1-2 LLDP Neighbors Information 97 IV-1-2 Web Syslog 98 IV-1-4 Internet 99 IV-1-5 Clients List 100 IV-2 Utility 101 IV-2-1 Ping Tool 101 IV-2-2 Trace Tool 102 IV-2-3 Web CLI 103 Chapter V Mobile APP, DrayTek Wireless 106 V-2 Create a New Network 107 V-3 Wizard 109 V-4 Login 112 V-4 Login 114 Chapter VI Troubleshooting 112 V-4 Login 114 Chapter VI Troubleshooting 117 V-3 Checking the Hardware Status 116 VI-2 Checking the Network Connection Settings 117 VI-3 For Windows 117 VI-3 Program de Status 116 VI-3 Program de Status 117 VI-3 Program de Status 116 VI-3 Prof Windows 117 VI-3 Prof Windows 112 VI-3 Prof Windows 120 VI-3 Prof Windows 120 VI-3 Pr		
IV-1-2 LLDP Neighbors Information 97 IV-1-3 Web Syslog 98 IV-1-4 Internet 99 IV-1-5 Clients List 100 IV-2 Utility 101 IV-2 Utility 101 IV-2 Trace Tool 102 IV-2-3 Web CLI 103 Chapter V Mobile APP, DrayTek Wireless 106 V-2 Create a New Network 107 V-3 Wizard 109 V-4 Login 114 Chapter VI Troubleshooting 114 Chapter VI Troubleshooting 117 VI-3 Concetting the Hardware Status 116 VI-2 Checking the Hardware Status 117 VI-3 I For Windows 117 VI-3 I For Windows 117 VI-3 I For Windows 112 VI-3 Pinging the Device 120 VI-3 Pinging the Device 120 VI-3 I For Windows 120 VI-3 Pinging the Device 120		
IV-1-3 Web Syslog		
IV-1-4 Internet 99 IV-1-5 Clients List 100 IV-2 Utility 101 IV-2 Utility 101 IV-2.1 Ping Tool 101 IV-2.2 Trace Tool 102 IV-2.3 Web CLI 103 Chapter V Mobile APP, DrayTek Wireless 106 V-2 Create a New Network 107 V-3 Wizard 109 V-4 Login 112 V-4.1 Setup 114 Chapter VI Troubleshooting 115 VI-1 Checking the Hardware Status 116 VI-2 Checking the Network Connection Settings 117 VI-3 For Windows 117 VI-3 Pinging the Device 120 VI-4 Backing to Factory Default Setting 122 VI-4 Backing to Factory Default Setting 122 VI-4 Hardware Reset 122 VI-4-2 Hardware Reset 123	-	
IV-2 Utility. 101 IV-2-1 Ping Tool. 101 IV-2-2 Trace Tool. 102 IV-2-3 Web CLI. 103 Chapter V Mobile APP, DrayTek Wireless. 105 V-1 Introduction of DrayTek Wireless. 106 V-2 Create a New Network 107 V-3 Wizard 109 V-4 Login. 112 V-4 I Setup 114 Chapter VI Troubleshooting 115 VI-1 Checking the Hardware Status 116 VI-2 Checking the Network Connection Settings 117 VI-3 For Windows. 117 VI-3 Pinging the Device 120 VI-4 Backing to Factory Default Setting 122 VI-4 Backing to Factory Default Setting 122 VI-4 Lardware Reset 122 VI-4 Lardware Reset 123		
V-2-1 Ping Tool 101 IV-2-2 Trace Tool 102 IV-2-3 Web CLI 103 Chapter V Mobile APP, DrayTek Wireless 105 V-1 Introduction of DrayTek Wireless 106 V-2 Create a New Network 107 V-3 Wizard 109 V-4 Login 112 V-4.1 Setup 114 Chapter VI Troubleshooting 115 VI-1 Checking the Hardware Status 116 VI-2 Checking the Network Connection Settings 117 VI-3 Pinging the Device 119 VI-3 Pinging the Device 120 VI-3 Tor Windows 120 VI-3 Tor Windows 121 VI-3 Pinging the Device 120 VI-3 Tor Windows 120 VI-3 Tor Windows 120 VI-3 Tor Windows 120 VI-3 Tor Windows 120 VI-4 Backing to Factory Default Setting 122 VI-4 Backing to Factory Default Setting 122 VI-4 Hardware Reset 123	IV-1-5 Clients List	100
IV-2-2 Trace Tool 102 IV-2-3 Web CLI 103 Chapter V Mobile APP, DrayTek Wireless 106 V-1 Introduction of DrayTek Wireless 106 V-2 Create a New Network 107 V-3 Wizard 109 V-4 Login 112 V-4-1 Setup 114 Chapter VI Troubleshooting 115 VI-1 Checking the Hardware Status 116 VI-2 Checking the Network Connection Settings 117 VI-3-1 For Windows 117 VI-3-2 For Mac Os 119 VI-3 Pinging the Device 120 VI-3-1 For Windows 120 VI-3-2 For Mac Os (Terminal) 120 VI-4 Backing to Factory Default Setting 122 VI-4-1 Software Reset 122 VI-4-1 Software Reset 123	IV-2 Utility	
IV-2-3 Web CLI 103 Chapter V Mobile APP, DrayTek Wireless 105 V-1 Introduction of DrayTek Wireless 106 V-2 Create a New Network 107 V-3 Wizard 109 V-4 Login 112 V-4-1 Setup 114 Chapter VI Troubleshooting 115 VI-1 Checking the Hardware Status 116 VI-2 Checking the Network Connection Settings 117 VI-3 1 For Windows 119 VI-3 2 For Mac Os 119 VI-3 1 For Windows 120 VI-3 1 For Windows 120 VI-3 2 For Mac Os (Terminal) 120 VI-4 Backing to Factory Default Setting 122 VI-4 Software Reset 122 VI-4 Software Reset 122 VI-4 2 Hardware Reset 123	IV-2-1 Ping Tool	
Chapter V Mobile APP, DrayTek Wireless 105 V-1 Introduction of DrayTek Wireless 106 V-2 Create a New Network 107 V-3 Wizard 109 V-4 Login 112 V-4.1 Setup 114 Chapter VI Troubleshooting 115 VI-1 Checking the Hardware Status 116 VI-2 Checking the Network Connection Settings 117 VI-3 I For Windows 119 VI-3 Pinging the Device 120 VI-3 Pinging the Device 120 VI-3 Poinging the Device 120 VI-3 Poinging the Device 120 VI-3 L For Windows 120 VI-3 Pinging the Device 120 VI-3 Pinging the Device 120 VI-4 Backing to Factory Default Setting 122 VI-4 Backing to Factory Default Setting 122 VI-4-1 Software Reset 122 VI-4-2 Hardware Reset 123		
V-1 Introduction of DrayTek Wireless106V-2 Create a New Network107V-3 Wizard109V-4 Login.112V-4-1 Setup114Chapter VI TroubleshootingVI-1 Checking the Hardware StatusVI-1 Checking the Hardware Status116VI-2 Checking the Network Connection Settings117VI-3-1 For Windows117VI-3-2 For Mac Os119VI-3 Pinging the Device120VI-3-2 For Mac Os (Terminal)120VI-4 Backing to Factory Default Setting122VI-4-1 Software Reset122VI-4-2 Hardware Reset123	IV-2-3 Web CLI	
V-2 Create a New Network 107 V-3 Wizard 109 V-4 Login 112 V-4-1 Setup 114 Chapter VI Troubleshooting 115 VI-1 Checking the Hardware Status 116 VI-2 Checking the Network Connection Settings 117 VI-3 For Windows 117 VI-3 Pinging the Device 120 VI-3 Pinging the Reset 122 VI-4 Backing to Factory Default Setting 122 VI-4 Hardware Reset 122 VI-4 Lardware Reset 123	Chapter V Mobile APP, DrayTek Wireless	
V-3 Wizard 109 V-4 Login. 112 V-4-1 Setup 114 Chapter VI Troubleshooting 115 VI-1 Checking the Hardware Status 116 VI-2 Checking the Network Connection Settings. 117 VI-3-1 For Windows 117 VI-3-2 For Mac Os 119 VI-3 Pinging the Device 120 VI-3-1 For Windows 120 VI-3 Pinging the Device 120 VI-3-2 For Mac Os (Terminal) 120 VI-4 Backing to Factory Default Setting 122 VI-4 Backing to Factory Default Setting 122 VI-4-2 Hardware Reset 123	V-1 Introduction of DrayTek Wireless	
V-4 Login112V-4-1 Setup114Chapter VI Troubleshooting115VI-1 Checking the Hardware Status116VI-2 Checking the Network Connection Settings117VI-3-1 For Windows117VI-3-2 For Mac Os119VI-3 Pinging the Device120VI-3-1 For Windows120VI-3 Pinging the Device120VI-3 Pinging the Device120VI-3 For Mac Os (Terminal)120VI-4 Backing to Factory Default Setting122VI-4-1 Software Reset123VI-4-2 Hardware Reset123	V-2 Create a New Network	
V-4-1 Setup 114 Chapter VI Troubleshooting 115 VI-1 Checking the Hardware Status 116 VI-2 Checking the Network Connection Settings 117 VI-3-1 For Windows 117 VI-3-2 For Mac Os 119 VI-3 Pinging the Device 120 VI-3-1 For Windows 120 VI-3 Pinging the Device 120 VI-3-2 For Mac Os (Terminal) 120 VI-4 Backing to Factory Default Setting 122 VI-4-1 Software Reset 122 VI-4-2 Hardware Reset 123	V-3 Wizard	
Chapter VI Troubleshooting115VI-1 Checking the Hardware Status116VI-2 Checking the Network Connection Settings117VI-3-1 For Windows117VI-3-2 For Mac Os119VI-3 Pinging the Device120VI-3-1 For Windows120VI-3-2 For Mac Os (Terminal)120VI-4 Backing to Factory Default Setting122VI-4-1 Software Reset122VI-4-2 Hardware Reset123	V-4 Login	
VI-1 Checking the Hardware Status116VI-2 Checking the Network Connection Settings117VI-3-1 For Windows117VI-3-2 For Mac Os119VI-3 Pinging the Device120VI-3-1 For Windows120VI-3-2 For Mac Os (Terminal)120VI-3-2 For Mac Os (Terminal)120VI-4 Backing to Factory Default Setting122VI-4-1 Software Reset122VI-4-2 Hardware Reset123	V-4-1 Setup	
VI-1 Checking the Hardware Status116VI-2 Checking the Network Connection Settings117VI-3-1 For Windows117VI-3-2 For Mac Os119VI-3 Pinging the Device120VI-3-1 For Windows120VI-3-2 For Mac Os (Terminal)120VI-3-2 For Mac Os (Terminal)120VI-4 Backing to Factory Default Setting122VI-4-1 Software Reset122VI-4-2 Hardware Reset123	Chapter VI Troubleshooting	
VI-3-1 For Windows.117VI-3-2 For Mac Os.119VI-3 Pinging the Device .120VI-3 Pinging the Device .120VI-3-1 For Windows.120VI-3-2 For Mac Os (Terminal)120VI-4 Backing to Factory Default Setting.122VI-4-1 Software Reset .122VI-4-2 Hardware Reset.123		
VI-3-1 For Windows.117VI-3-2 For Mac Os.119VI-3 Pinging the Device .120VI-3 Pinging the Device .120VI-3-1 For Windows.120VI-3-2 For Mac Os (Terminal)120VI-4 Backing to Factory Default Setting.122VI-4-1 Software Reset .122VI-4-2 Hardware Reset.123	VI-2 Checking the Network Connection Settings	
VI-3-2 For Mac Os119VI-3 Pinging the Device120VI-3-1 For Windows120VI-3-2 For Mac Os (Terminal)120VI-4 Backing to Factory Default Setting122VI-4-1 Software Reset122VI-4-2 Hardware Reset123		
VI-3-1 For Windows		
VI-3-2 For Mac Os (Terminal)	VI-3 Pinging the Device	
VI-4 Backing to Factory Default Setting		
VI-4-1 Software Reset		
VI-4-2 Hardware Reset		

Chapter I Installation



I-1 Introduction

This is a generic International version of the user guide. Specification, compatibility and features vary by region. For specific user guides suitable for your region or product, please contact local distributor.

Thank you for purchasing this VigorAP 905, the concurrent dual-band wireless (2.4G/5G) access point offering high-speed data transmission.

Easy install procedures allow any computer users to set up a network environment in a 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!

VigorAP 905 also is a Power over Ethernet Powered Device which adopts the technology of PoE for offering power supply and transmitting data through the Ethernet cable.

I-1-1 LED Indicators and Connectors

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



LED	Status	Explanation
	On	A USB device is connected and active.
USB USB	Blinking	The data is transmitting (sending/receiving).
	On (Blue)	A normal connection (rate with 2500Mbps) is through its corresponding port.
LAN1	Blinking(Blu e)	The data is transmitting (sending/receiving).
LANT	On (White)	A normal connection (rate with 10/100/1000Mbps) is through its corresponding port.
	Blinking (White)	The data is transmitting (sending/receiving).
	On	The LAN port is connected.
LAN 2/3/4/5	Blinking	The data is transmitting.
	Off	The LAN port is disconnected.
() WPS	Blinking (quickly)	The WPS function is enabled and the system is waiting for a wireless station of connection.
VVI 5	Off	The WPS button is turned off.
24)	On	Wireless 5G/2.4G is ready.
53	Blinking	Ethernet packets are transmitting over wireless LAN.
WLAN	Off	Wireless 5G/2.4G is inactive.
22 ACT	On	The system is in boot-loader mode.
	Blinking (quickly)	The system is reset to the factory default setting.
	Blinking	The system is ready and can work normally. When the ACT LED blinks twice and then pauses for one second repeatedly, it indicates that the Internet connection is disconnected.

	On (WLAN LED blinking slowly)	The system is in TFTP mode.
	Off	The system is not ready or is failed.
$\langle \rangle$	On	The device is plugged in and the power switch is on.
PWR	Off	No power.

	Interface	Description
	PWR	PWR: Connecter for a power adapter.
WR		Power switch.
Pripeg P2	RST	Restore the default settings. Usage: Turn on the router. Press the button and keep for more than 10 seconds. Then the router will restart with the factory default configuration.
P3 P4 P5	WPS	 Wireless band will be switched /changed according to the button pressed and released. For example, 2.4G (On) and 5G (On) - in default. 2.4G (Off) and 5G (On) - pressed and released the button once. 2.4G (On) and 5G (Off) - pressed and released the button twice. 2.4G (Off) and 5G (Off) - pressed and released the button twice. 2.4G (Off) and 5G (Off) - pressed and released the button twice. 2.4G (Off) and 5G (Off) - pressed and released the button twice. 2.4G (Off) and 5G (Off) - pressed and released the button three times. WPS - When WPS function is enabled by web user interface, press this button for more than 2 seconds. The router will wait for any wireless client connecting to it through WPS.
	P2-P5	Connectors for local networked devices. In which the transmission rate for P1(only) can reach 2.5G. In addition, P1 can be supplied with PoE power.
	-	Connecter for a USB device (for temperature sensor).

I-2 Hardware Installation

This section will guide you through installing the VigorAP.

VigorAP can be installed under certain locations: wooden ceiling, plasterboard ceilings, light-weighted steel frame and wall.

(i) Note:

For the sake of personal safety, only trained and qualified personnel should install this access point.

I-2-1 Wired Connection for PC in LAN

 Connect VigorAP 905 to xDSL modem, router, or switch/hub in your network through the LAN 1 port of the access point by Ethernet cable.

You can also connect VigorAP 905 to a Vigor router via wireless connection. For detailed information, refer to VigorAP 905 User's Guide.

- 2. Connect a computer to other available LAN port. Make sure the subnet IP address of the PC is the same as VigorAP 905 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 905.
- 5. Check all LEDs on the front and back panel. The ACT LED on the front panel should blink; WAN/LAN LED on the back panel should be on if the access point is correctly connected to the xDSL modem, router or switch/hub.



I-2-2 PoE Connection

VigorAP 905 can gain power from the connected switch, e.g., VigorSwitch P2282x. PoE (Power over Ethernet) can break the install limitation caused by the fixed power supply.

- 1. Connect VigorAP 905 to a switch in your network through the LAN P1 (PoE) port of the access point by Ethernet cable.
- 2. Connect a computer to VigorSwitch P2282x. Make sure the subnet IP address of the PC is the same as VigorAP 905 management IP, e.g., **192.168.1.X**.
- 3. Power on VigorAP 905.

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.



I-2-3 Wall-mount Installation

For wall-mounting, refer to the following steps.

- 1. Drill two holes on the wall. The distance between the holes shall be 100mm. The recommended drill diameter shall be 6mm (15/64").
- 2. Fit screws into the wall using the appropriate type of screw plug.
- 3. Hang the VigorAP directly onto the screws.



I-3 Network IP Configuration

After the network connection is built, the next step you should do is setup VigorAP 905 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 in the same subnet as this AP. If it's not connected to the same DHCP Server with the AP or you're unsure, please follow the following instructions to configure your computer to use the static IP address in the same subnet as default IP address of this AP.

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 10 - please go to section I-3-1

I-3-1 Windows 10 IP Address Setup

Click the **Start** button (it should be located at lower-left corner of your computer), then click the **Settings** icon.



Double-click Network & Internet.

				W	/indows Settings				
				Find a settin	â.	8		•	
	System Depwy, journe normestions power		Devices Bilantovito, pormani, mouse		Phone (Ime your Android, Whone	۲	Network & Internet WF, flight mode, WH	₽ Ø	Personalisation Background, lock streen colours
	Apps Uninstall, defaults, optional features	8	Accounts Your accounts email, sync work, lamily.	(A)	Time & Language Speech region, date	8	Gaming Game bar, DVR, proadcasting, Game Mode	Ġ	Ease of Access Nerraton.megoiner.nigh- commut.
0	Cortana Cortana language, permesilone extinianteces	8	Privacy Location, camera	0	Update & Security Windows Update: resovery, backup				

Next, click Change adapter options.

Settings		
	Windows Settings	
	Final a setting .0	
← Settings		- 0
6 Home	Status	
Find a setting	Network status	Do you have a question?
Network & Internet		
🔿 Status		Make Windows better
in the second	Public network	voye on feedback
1 Ethernet	You're connected to the Internet	
🕾 Dial-up	If you have a limited data plan, you can make this network a metered connection or change other properties.	
ogo VPN	Obange connection properties	
🕑 Data usage	Strangen under regiments.	
Proxy	Change your network settings	
	Change adapter options View treweeks adapters and change, connection, suminge-	
	Shame options For the remember induction burlets the becaute what you want to uhare.	
	Network troubleshooter	

Click the local area connection.

	Windows Settings		
Settings A Home Find a setting Network & Internet Status	Status Network status		To you have a question? Get help Make Windows better Give no feedbacts
12 Ethernet ⇒ Dial-up ⇒ VPN ③ Data usage ⊕ Proxy	Metwork Connections Togarse - Cogarse	- D - M Second Her E - T	х ,> •

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

letworking S	haring			
Connect using	1:			
Realter	RTL8139/	810x Family Fast	Ethemet NIC	
This connection	on uses the t	following items:	Conf	igure
Cost Cost Cost Cost Cost Cost Cost Cost	net Protocol net Protocol Laver Topol	and the second second	1Pv6). <mark>1Pv4)</mark> kepper I/O Driv	er
Install		Uninstall	Prop	erties
Dentitien		-		
Description	Control Dr	10. 10.	Protocol The d	e 14

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

IP address: 192.168.1.9

Subnet Mask: 255.255.255.0

General	
You can get IP settings assigned aut this capability. Otherwise, you need for the appropriate IP settings.	
Obtain an IP address automatic	ally
• Use the following IP address:	
IP address:	192.168.1.9
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	192 . 168 . 1 . 1
💿 Obtain DNS server address aut	omatically
Use the following DNS server ad	ddresses:
Preferred DNS server:	168 . 95 1 . 1
Alternate DNS server:	
Validate settings upon exit	Ad <u>v</u> anced
	OK Cancel

I-4 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., Firefox).

- 1. Make sure your PC connects to the VigorAP 905 correctly.
- 2. Open a web browser on your PC and type http://192.168.1.2. A pop-up window will open to ask for username and password. Please type "admin/admin" on Username/Password and click OK.

	Username admin	
DrayTek VigorAP905	Password	0
VigorAP905		
	Lopin	

(i) Note:

You may either simply set up your computer to get IP dynamically from the router or set up the IP address of the computer to be in the same subnet as **the IP address of VigorAP 905.**

- If there is no DHCP server on the network, then VigorAP 905 will have an IP address of 192.168.1.2.
- If there is DHCP available on the network, then VigorAP 905 will receive it's IP address via the DHCP server.
- 3. Next, the page will appear to guide you change the login password.

You **MUST** change the login password before accessing the web user interface. Please set a new password for network security.

	admin / Set Password	
Change Password	Account	admin
	Current Password	
Your device is still using default password.	New Password	
	Confirm New Password	
For security reason please change password.		
		Uppercase characters
N		 Lowerstee characters
Change password	N	 Numbers or Special characters -1845%*6*0_H700-H

4. After clicking **Apply**, the Main Screen will pop up. When the homepage appears, view the configuration and modify the settings if you want.

DrayTek viso	rAP905				System Time (2025-04	VigorAP905 30 06:13:58	a admin
Searchi., Q.	Dashboard						Crehes
Device Menu 2 Intel Accent 5 Configuration C Security C Monitoring Manual V V	0 Clients 0 246 35		ight ch 3 ch 64	Light, 21% Light, 1%	SYSTEM Device Name LAN MAC Nystem Giptome Foreware ACS Server	VigorAP905 14:49:80:51:89:D0 1d 1h: 42m: 30s 5.0.4	
System Maintenance	PORT STATUS	SYSTEM	JSAGE		WIRELESS OVERVIE	See More +	
۶۰ Wireless ب	Pr(Mc) P2 P3 P4 P3 0 10/100M 0 1G 2.5G	CPU Usag		63%	2.4GHz Radio MAC SSID(1)	Enable 14:49:8C:51:89:D0 DrayTek-366100	
	LAN STATUS Name IP Address Subret M	ask DHCP	Primary DNS Second	lary DNS	5GHz Radio	Enable	
	[LAN] LAN1 192,168, [.87 255,255.	55.0 Off	8.8.8.8 8.8.4.4		MAC SSID(1)	16:49:8C:51:89:D0 DrayTek-366100	

5. The web page can be logged out by clicking **Log Out** on the top right of the web page. Or, logout the web user interface according to the chosen condition. The default setting is **Auto Logout**, which means the web configuration system will logout after 5 minutes without any operation. Change the setting of auto logout if you want.

System Time : 2021-	01-01 01:05:51 a admin	VigorAP905 a admin System Time : 2021-01-01 01:02:49
	Auto Logout off 🗸	Auto Logout off 🗸
	 Get Password Two-factor Authentication Log Out 	off ☆ Set Passwc 1 min ☆ Two-factor ☆ Two-factor 10 min

(i) Note:

If you fail to access the web configuration, please go to the section "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.

I-5 Dashboard

Dashboard shows port status, LAN status, LAN usage, system status, and wireless overview information.

Click **Dashboard** from the main menu on the left side of the main page.

Dashboard									C Refresh
O Clients	© OVERVIEW © 2.4G © 5G	o o		Light d		Ught, 21% Light, 1%	SYSTEM Device Name LAN MAC System Uptime Firmware ACS Server	VigorAP905 14:49:BC:51:B9:D0 1d 1h: 42m: 30s 5.0.4	a
PORT STATUS			SYSTEN CPU US			63%	WIRELESS OVERVI	See More +	
	2 P3 P4	P5 2.5G	Memor	y Usage		41%	Radio MAC SSID(1)	Enable 14:49:BC:51:B9:D0 DrayTek-366100	
LAN STATUS							5GHz Badio	Enable	
Name	IP Address	Subnet Mask	DHCP	Primary DNS	Secondary DNS		MAC	16:49:BC:51:B9:D0	
[LAN] LAN1	192,168,1.87	255.255.255.0	Off	8.8.8.8	8.8.4.4		SSID(1)	DrayTek-366100	

I-6 Two-factor Authentication

If network security is highly concerned, two-factor authentication will be strongly recommended. For using two-factor authentication for accessing VigorAP;

- 1. Get and install Google Authenticator (iOS/Android) first.
- 2. Login VigorAP by using the user account and password.

	Username admin	
Dray Tek VigorAP905	Password	ø
	Logen	

3. Select **Two-factor Authentication.**

System Time : 2021-01-	VigorAP905 01 01:14:47 admin
	Auto Logout off 🗸
SYSTEM	🔒 Set Password
Device Name	v 📀 Two-factor Authentication
LAN MAC	1 🕒 Log Out
System (Intime	0d 1h: 16m: 38s

4. On the following page, switch the toggle of **Enable** to enable the function.

		_ multi-
Two Factor Authentic	ation	
Assaurt	admin	
Emable		
Samet	GNJUMSJYIS3XEUCOGVJUIM2ZOU2WGTKEIE3DOSRZPJDE232JPAZXGODMGNDHK3SW	
20.000		
QR Code		
Validation Code		
Apply		
- The second sec		

5. Use your cell phone to scan the QR-Code shown on the page. A key will be created randomly on the cell phone. Enter that key on the box of Verification Code and click the **Apply** button.

		L1 Harrow
Two Factor Authentica	tion	
Account	ádmin	
Enable		
Sixcivit	GNJUM5JYIS3XEUCOGVJÚIM2ZOU2WGTKEIE3DOSRZPJDE232JPAZXGODMGNBHK3SW	
Ige Code		
Visidation Loda	typinal	
- And where		

- 6. Logout VigorAP.
- 7. Re-login VigorAP. The first login web page requires you to enter the original user account and password. After clicking the Login button, the *second* login web page appears. Please enter the authentication code (created randomly) obtained from the APP (Google Authenticator) on your cell phone and click the Verify button.



This page is left blank.

Chapter II Connectivity

II-1 Configuration

II-1-1 Physical Interface

Configure the general settings for LAN interface. Open **Configuration >> Physical Interface**.

SearchQ	Configuration	/ Physical Interface		CRefresh
	Setup the inte	erface		
evice Menu				
Dashboard				
			2.56	
LAN			P1(PoE) P2 P3 P4 P5	
Wireless LAN				
Objects			10/100M 1G 2.5G	
Notification Services				
RADIUS				
Certificates	Ethernet			
Security				
a Monitoring	Name	Function	Status	
	P1	LAN		
g Utility	P2	LAN		
System Maintenance	> F2	DAN		
	P3	LAN		
irtual Controller	P4	LAN		
		Dan		
- Wireless				

Available settings are explained as follows:

ltem	Description				
Ethernet					
Name	Displays the name of the Ethernet port (P1 to P5).				
Function	Displays current function of the Ethernet port.				
Status	Switch the toggle to enable or disable the Ethernet port.				
USB					
Interface	Displays the name of the USB.				
Enabled	In default, the USB interface is enabled.				
	LED				
Interface	Displays the name of the LED.				
Enabled	In default, the LED on the device will be always on.				
	However, the LED can be turned on or off after a specified number of minutes has elapsed to meet certain requirements.				
	For this, switch the toggle to enable this setting.				
LED Sleep Schedule	The LED can be turned on or off based on the settings configured in the selected schedule (defined under Configuration>>Objects) profile to fulfill specific requirements.				

	When LED is slept, it can be woken up by pressing one of the following buttons:
	 Factory Reset on the front panel
	• Wake up LED on this configuration page
	Note that if the schedule is set with repeat type and applied here, the LED on the device will be turned on and turned off at specified time periodically and automatically.
	Button
Configuration Reset	Switch the toggle to enable/disable the function.
Button	If disabled, the function of the Reset button will be invalid.
Cancel	Click to discard the modification.
Apply	Click to save the settings.

(i) Note:

Switch these two icons by click the mouse cursor on them.

🔵 - means "Enable".

- means "Disable".

II-1-2 LAN

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

II-1-2-1 LAN Networks

Open **Configuration>>LAN** and select the **LAN Networks** tab to open the following page.

Search, Q		③Reset CRefresh
Device Menu (?) Dashboard	LAN Networks Bind IP to MAC DHCP Options VLAN List Interface VLAN LAN Networks	
3 Configuration	Name [LAN] LAN1	
Physical Interface ILAN Wireless LAN	LAN Network Configuration	
Objects Notification Services	LAN Network Configuration DHCP Some IP	
RADIUS Certificates	Subnet Mask 255.255.0/24 ~	
Security	5 Default Gateway () 192.168.1.1	
🔂 Monitoring	> Primary DNS Server () 8.8.8	
BS Utility	Secondary DNS Server () 8.8.4.4	
🍕 System Maintenance	2 Management VLAN 1 (Default VLAN) ~	
Virtual Controller ≻ Wireless	DHCP Server Configuration	
	DHCP Server On De Resy	
	Cancel Apply	

Available settings are explained as follows:

ltem	Description		
LAN Network Configurati	on		
LAN Network Configuration	 Select the connection type for the LAN network. DHCP - DHCP stands for Dynamic Host Configuration Protocol. DHCP server can automatically dispatch related IP settings to any local user configured as a DHCP client. Static IP 		
	When DHCP is selected		
Primary DNS Server	You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server. If your ISP does not provide it, the device will automatically apply default DNS Server IP address: 194.109.6.66 to this field.		
Secondary DNS Server	You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server. If your ISP does no provide it, the device will automatically apply default secondary DNS Server IP address: 194.98.0.1 to this field.		
Management VLAN	VigorAP 905 supports tag-based VLAN for wireless clients accessing Vigor device. Only the clients with the specified VLAN ID can access into VigorAP 905.		
	Select a number as VLAN ID tagged on the transmitted packet. "None" means no VALN tag.		
	When Static IP is selected		
IP Address	Enter a private IP address for connecting to a local private network		

	(Default: 192.168.1.2).
Subnet Mask	Enter 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.
Primary DNS Server	You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server. If your ISF does not provide it, the device will automatically apply default DNS Server IP address: 194.109.6.66 to this field.
Secondary DNS Server	You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server. If your ISP does not provide it, the device will automatically apply default secondary DNS Server IP address: 194.98.0.1 to this field.
Management VLAN	VigorAP 905 supports tag-based VLAN for wireless clients accessing Vigor device. Only the clients with the specified VLAN ID can access into VigorAP 905.
	Select a number as VLAN ID tagged on the transmitted packet. "None" means no VALN tag.

DHCP Server	 On - Lets the device assign IP address to every host in the LAN. Off - Lets you manually or use other DHCP server to assign IP address to every host in the LAN. Relay - Specify which subnet that DHCP server is located the relay agent should redirect the DHCP request to.
Start IP Address	It is available when On is selected as the DHCP Server. 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 device is 192.168.1.2, the starting IP address must be 192.168.1.3 or greater, but smaller than 192.168.1.254.
IP Pool Counts	It is available when On is selected as the DHCP Server. Enter a value of the IP address pool for the DHCP server to end with when issuing IP addresses.
Gateway IP Address	It is available when On is selected as the DHCP Server. Enter a value of the gateway IP address for the DHCP server.
Lease Time	It is available when On is selected as the DHCP Server. It allows you to set the leased time for the specified PC.
Primary DNS	It is available when On is selected as the DHCP Server. You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server. If your ISP does not provide it, the device will automatically apply default DNS Server IP address: 194.109.6.66 to this field.
Secondary DNS	It is available when On is selected as the DHCP Server. You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server. If your ISP does not provide it, the device will automatically apply default DNS Server IP address: 194.109.6.66 to this field.
DHCP Server IP Address	It is available when Relay is selected as the DHCP Server.

DHCP Server Configuration - Available when Static IP is selected

	Enter a value of the IP address for the DHCP server.
Cancel	Click to discard the modification and return to the previous page.
Apply	Click to save the settings.

II-1-2-2 Bind IP to MAC

This function is used to bind the IP and MAC address in LAN to have a strengthening control in network. With the Bind IP to MAC feature you can reserve LAN IP addresses for LAN clients. Each reserved IP address is associated with a Media Access Control (MAC) address.

	Q	Configuration / LAN					() Result
		LAN Networks Bind IP to M	IAC DHCP Options VLAN List Interface VL	AN			
evice Menu	_	Bind IP to MAC					
Dashboard							
		+ Add				Search	Max: 30
Physical Interface		Comment	MAC Address		IP Address		Option
Wireless LAN							
Objects							
Notification Services							
RADIUS							
Certificates							
> Security	2						
Monitoring	ż						
3 Utility							
System Maintenance							
rtual Controller	-						
Wireless),						

Available settings are explained as follows:

ltem	Description
+Add	Click to create a new profile.
Comment	Displays a brief description for the entry.
MAC Address	Displays the MAC address used by the entry.
IP Address	Displays the IP address used by the entry.
Option	Edit - Click to modify the selected profile. Delete - Click to delete the selected entry.

To modify an existing profile, select a file and click **Edit.**

To add a new profile, click the **+Add** link to get the following page.



Available settings are explained as follows:

ltem	Description
Comment	This is an optional field to identify this IP Address – MAC Address pair.
MAC Address	Use the drop-down menu to select a MAC address
IP Address	Use the drop-down menu to select an IP address.
Cancel	Discard the settings and return to the previous page.
Apply	Click it to save the settings and return to the previous page.

II-1-2-3 DHCP Options

DHCP packets can be processed by adding option number and data information when such function is enabled and configured.

This page allows you to configure additional DHCP client options.

	Configuration / LAN			③ Reset
evice Manu	LAN Networks Bind IP to MAC DHCP Option	s VLAN List Interface VLAN		
	DHCP Options			
ອັ Dashboard				
	+ Add		Search.	Mapp 50
Physical Interface	Option Number	Data Type	Data	Option
Wireless LAN				
Objects				
Notification Services				
RADIUS				
Certificates				
Security >				
Monitoring				
utility >				
System Maintenance				
tual Controller				
Wireless >				

Available settings are explained as follows:

ltem	Description
+Add	Click to create a new profile.
Option Number	Displays the number used by this profile.
Data Type	Displays the data type.
Option	Edit - Click to modify the selected profile. Delete - Click to delete the selected entry.

To modify an existing profile, select a file and click Edit.

To add a new profile, click the **+Add** link to get the following page.



Available settings are explained as follows:

ltem	Description
Option Number	Enter a number (0 to 255) for this function.
Data Type	Choose the type (ASCII or Hex or Address List) for the data to be stored. Type of data in the Data field:
	• ASCII Character - A text string. Example: /path.
	 Hexadecimal Digit - A hexadecimal string. Valid characters are from 0 to 9 and from a to f. Example: 2f70617468.
	• Address List - One or more IPv4 addresses, delimited by commas.
Data	Enter the content of the data to be processed by the function of DHCP option.
Cancel	Discard the settings and return to the previous page.
Apply	Click it to save the settings and return to the previous page

II-1-2-4 VLAN List

Virtual Local Area Networks (VLANs) allow you to subdivide your LAN to facilitate management or to improve network security.

	Configuration / LAN			TReset C Refresh
	LAN Networks Bind IP	to MAC DHCP Options VLAN List Interface	/LAN	
evice Menu	VLAN List			
ት Dashboard				
	+ Add			Max
Physical Interface	VLAN ID	Name	LAN Network	Option
	1	Default VLAN	[LAN] LAN1	@ Edit
Wireless LAN				
Objects				
Notification Services				
RADIUS				
Certificates				
Security	>			
Monitoring	2 C			
Utility	5			
System Maintenance	>			
tual Controller				
Wireless	¥.			

Available settings are explained as follows:

ltem	Description
+Add	Click to create a new profile.
VLAN ID	Displays the number used by this profile.
Name	Displays the name of the VLAN profile.
LAN Network	Displays the LAN network used by the VLAN profile.
Option	Edit - Click to modify the selected profile. Delete - Click to delete the selected entry.

To modify an existing profile, select a file and click **Edit.**

To add a new profile, click the **+Add** link to get the following page.

ks Bind IP to MAC D	HCP Options VLAN List Interface VLAN		×
		VLAN ID ①	100
	Name	Name	100_VLAN
	Default VLAN	LAN Network	Please select 🤛
			[LAN] LAN1

Available settings are explained as follows:

ltem	Description
VLAN ID	Enter the value as the VLAN ID number.
Name	Enter a name to represent the VLAN profile.
LAN Network	Select the LAN network used by the VLAN profile.
Cancel	Discard the settings and return to the previous page.
Apply	Click it to save and apply the settings.

II-1-2-5 Interface VLAN

This page allows you to configure the LAN port settings to assure the VLAN profile can work normally.

Dervice Manul Implementation Implem		Configuration / LAN				3
Possbaard Interface VLAN Settings Physical Interface Ethernet Physical Interface Ethernet VA/ Ethernet VA/ Pol1 Colpects Pol1 Colpects Pol2 Pol2 Truek v I Default VLAN Secondry I Default VLAN Montering I Default VLAN System Maintenance I Default VLAN Vitual Controller I Default VLAN		LAN Networks Bind IP	to MAC DHCP Options	VLAN List Interfac	e yLAN	
Cardifordiance Ethernet Physical Interface Physical Interface Variess LAN Ethernet Objects Pod 1 Nutrikoon Services Pod 1 RADIUS Pod 1 Certificates Pod 1 Objects Pod 1 Trunk v 1 (Default VLAN) v Ad VLAN Servict VLAN Socurity 1 (Default VLAN) v Montoring 1 (Default VLAN) v System Maintenance 1 Virtual Controller 1		Interface VLAN Settings				
Physical Interface Ethernet Wireless LAN Ethernet Objects Point Objects Point Nuclification Services Point RADRUS Point Certification Services Point RADRUS Point Trunk 1 [Default VLAN] AVVANti Seed VLANti Security 1 [Default VLAN] Windtorling 1 [Default VLAN] Suttimity 1 [Default VLAN] VIRING 1 [Default VLAN]						
Wireless LAN Ethemet Indeface Pent Type Undagged VLAN Tagged VLAN Objects Pent 1 Trunk V 1 (Default VLAN) V AV VLAN: Send VLAN: Notification Services Pent 2 Trunk V 1 (Default VLAN) V AV VLAN: Send VLAN: RADIOS Pent 2 Trunk V 1 (Default VLAN) V AV VLAN: Send VLAN: Certification Services Pent 3 Trunk V 1 (Default VLAN) V AV VLAN: Send VLAN: Security Security 1 (Default VLAN) V AV VLAN: Send VLAN: Wondowring Pent 4 Trunk V 1 (Default VLAN) V AV VLAN: System Maintenance Pent 5 Trunk V 1 (Default VLAN) V AV VLAN:	Physical Interface	Ethernet				
Objects Peri 1 Truesk 1 1 Default VLANjo Al VLANs Selicit VLANjo Notification Services Peri 2 Truesk 1 1 Default VLANjo Al VLANs Selicit VLANjo RADUS Peri 3 Truesk 1 1 Default VLANjo Al VLANs Selicit VLANjo Security Peri 3 Truesk 1 Default VLANjo Al VLANs Selicit VLANjo Security Peri 4 Truesk 1 Default VLANjo Al VLANs Selicit VLANjo Wonitoring Peri 5 Truesk 1 Default VLANjo Al VLANs Selicit VLANjo System Maintenance 1 Truesk 1 Default VLANjo Al VLANs Selicit VLANjo		Ethernet	Interface Port Type	Untagged VLAN	Tagged VLAN	
RORUS PPI 2 Turk 1(Default VLAN) AVXAN Swedt VLANS Centificates Poil 3 Truek ~ 3 (Default VLAN) AVXAN Swedt VLANS Security 3 Poil 4 Truek ~ 1(Default VLAN) AVXAN Swedt VLANS 3M Anitoring 3 Poil 5 Truek ~ 1(Default VLAN) AVXAN Swedt VLANS Winterfaces 3 Poil 5 Truek ~ 1(Default VLAN) AVXAN Swedt VLANS			Port 1 Trunk ~	1 (Default VLAN) ~	All VLANs Select VLANs	
Security Part 4 Trunk 1 [Default VLAN] AVVLAN Select VLANS 30 Monitoring 5 Part 5 Trunk 1 [Default VLAN] AVVLANS Select VLANS 32 Monitoring 5 Part 5 Trunk 1 [Default VLAN] AVVLANS Select VLANS 32 Monitoring 5 System Maintenance 1 1 (Default VLANS) AVVLANS Select VLANS			Port 2 Trunk ~	1 (Default VLAN) ~	All VLANS Select VLANS	
Bit Monitoring 3 Port 5 Truck 1 (Default VLAN) All VLANs Select VLANs Bit Unitity 3 System Maintenance 1	Certificates		Port 3 Trunk ~	1 (Default VLAN) ~	All VLANS Splect VLANS	
PortS Trunk V 1 (Default VLAN) V VLAN Select VLAN System Maintenance ; Virtual Controller	Security :		Port.4 Trunk ~	1 (Default VLAN) ~	All VILANS Select VLADIS	
ی System Maintenance ه ، الا الا المالية المالية المالية المالية المالية المالية المالية المالية المالية المالي	Monitoring		Port 5 Trunk ~	1 (Default VLAN)->	All VLANS Select VLANS	
Virtual Controller	BS Utility					
	🖏 System Maintenance					
Se Winders 3						
	≻ Wireless					

Available settings are explained as follows:

ltem	Description			
Interface	Displays the Ethernet port number.			
Port Type	 Trunk - A trunk port can transmit data from multiple VLANs. Access - Transmits the data to and from a specific VLAN. An access port is only assigned to a single VLAN, it sends and receives frames that aren't tagged and only have the access VLAN value. 			
Untagged VLAN	Use the drop-down list to select a VLAN ID as the untagged VLAN. The connected host sends its traffic without any VLAN tag on the frames. However, when the frame reaches this interface (LAN port), It will be added with the VLAN tag.			
Tagged VLAN	 Select to enable 802.1Q tagging on this VLAN. The device will add specific VLAN number to all packets on the LAN while sending them out. All VLANs - All VLAN will be tagged. Select VLANs - Only the selected VLAN will be tagged. 			
	Tagged VLAN			
	,			
	Tagged VLAN			
Cancel	Tagged VLAN All VLANs Select VLANs			

II-1-3 Wireless LAN

VigorAP 905 is a highly integrated wireless local area network (WLAN) for 2.4/5 GHz 802.11b/g/n/ax WLAN applications. It supports channel operations of 20/40 MHz at 2.4 GHz and 20/40/80/160 MHz at 5 GHz. VigorAP 905 can support data rates up to 2.4 Gbps/4.8Gbps in 802.11ax 80/160 MHz bandwidth.

(i) 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.

VigorAP 905 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 905.

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 905 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 905) with the encryption of WPA and WPA2.



It is the simplest way to build connection between wireless network clients and VigorAP 905. 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 905 automatically.

(i) Note:

This function is available for the wireless station with WPS supported.

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

On the side of VigorAP 905 series which served as an AP, 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 905.



Band Steering
Band Steering detects if the wireless clients are capable of 5GHz operation, and steers them to that frequency. It helps to leave 2.4GHz band available for legacy clients and improves users' experience by reducing channel utilization.



If dual-band is detected, the AP will let the wireless client connect to less congested wireless LAN, such as 5GHz to prevent network congestion.



(i) Note:

To make Band Steering work successfully, SSID and security on 2.4GHz also MUST be broadcasted on 5GHz.

II-1-3-1 SSID

By clicking the SSID tab, a web page will appear so that you could set the SSID, the security mode, and the password.

Search Q					DReset
Device Menu (?) Dashboard	SSID Radio Settings Roaming	AP Discovery WIPS Range Extender	WDS		
Energy continer Physical Interface	+Add SSID @-	Enabled Security	Password	VLAN Scheduled O	Max 10 n 2.40Hz 50Hz Option
LAN Winters LAN Objects Natification Services RADIUS Certificates Security Security Monitoring Monitoring Littley System Maintenance Virtual Controller	DrayTek-365100	WPAJAWPA2 Personal	•	Plase select~	V D Zist
≻ Wireless					

ltem	Description
+Add	Click to set a new SSID.
SSID Name	Displays the name of the SSID.
Enabled	Switch the toggle to enable or disable this entry.
Security	Displays the security mode used by this entry. If required, use the drop-down list to select another mode.
Password	Displays the password used by this entry.
VLAN	Displays the VLAN to which this SSID belongs.
Scheduled On	 Select Always or any other schedule profile. Always - This WLAN profile will be active all the time. Or, use the drop-down list to select a preset schedule profile. Before choosing, please go to Configuration>>Object to create schedule profiles (at least one).
2.4GHz	Switch the toggle to enable or disable this entry. If enabled, this entry will be applied to 2.4GHz wireless network.
5GHz	Switch the toggle to enable or disable this entry. If enabled, this entry will be applied to 5GHz wireless network.
Option	Edit - Click to modify the selected profile. Delete - Click the selected entry. The default SSID can not be deleted.
Cancel	Discard the settings and return to the previous page.
Apply	Save and apply the settings.

To add a new SSID profile, click **+Add** to create new entry boxes.

D Radio Settings Roaming	AP Discovery	WPS Range Extender	WDS							
ID										
Add										Mas
sin	Enabled	Security	Password ()		VLAN	Scheduled On	2.4GHz	5GHz	Option	
DrayTek-366.00		WPA3/WPA2 Personal ~		۵	Please select \sim	Always On $\!$			@ Edit	
SSID		WPA3/WPA2 Personal V		•	Please select	Always On V			0 Edit	1 Delete

To edit an existing SSID, click the **Edit** link to get to the following page.

RD ()	DrayTek 5189D0		
bled			
ecurity	WPA3/WPA2 Personal	w.	
assword @		@	
AN (D)	None 🗢		
meduled On	Always On 🗠		
SID Band			
IGHZ			
He	•		
D Settings			
C Filtening List	Dicultion 😪		
alate Client from Wireless	C20		
	C08		

ed. e the function.
when to the app from
r you to choose from. <u>security:</u> ersonal, WPA2 Personal, only WPA clients and the red in PSK. The WPA encrypts he radio using the key, which cered manually in this field below 802.1x authentication. transmitted from the radio using Shared Key) entered manually in y negotiated via 802.1x PA2, or Auto as WPA mode. rise, WPA2/WPA Enterprise - The smitted from the radio using the ed Key) entered manually in this

	authentication.					
	 OWE - WPA3 also introduces a new open and secure connection mode; "Opportunistic Wireless Encryption" (OWE). It allows the clients to connect without a password, ideal for hotspot networks, but the connection between each individual client is uniquely encrypted behind the scenes. 					
	Below shows the modes with basic security;					
	 WPA Personal - 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. 					
	 WPA Enterprise - 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 Personal - Accepts only WEP clients and the encryption key should be entered in WEP Key. 					
	• None - The encryption mechanism is turned off.					
Password	Enter 8~63 ASCII characters, such as "012345678". This feature is available for WPA Personal or WPA2 Personal or WPA2 / WPA Personal mode, WPA3 Personal or WPA3/WPA2 Personal .					
RADIUS Server	This feature is available for WPA3 Enterprise, WPA2 Enterprise, WPA2/WPA Enterprise, and WPA Enterprise mode.					
	Use the drop-down list to select a RADIUS server setting.					
	Note : Before configuring the RADIUS server, go to Configuration>>RADIUS to create external RADIUS profiles (at least one) first.					
VLAN	Select VLAN ID # for this SSID. Packets transferred from this 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 None by default, it means disabling the VLAN function for the SSID.					
Scheduled On	Select Always or any other schedule profile.					
	Always - This WLAN profile will be active all the time.					
	Or, use the drop-down list to select a preset schedule profile.					
	Before choosing, please go to Configuration>>Object to create schedule profiles (at least one).					
	SSID Band					
2.4GHz/5GHz	Select 2.4GHz and/or 5GHz for applying to this wireless LAN setting.					
	SSID Settings					
MAC Filtering List	Disabled - Disable the function of using MAC Filtering List.					
	Or, use the drop-down list to select a preset profile.					
	Before choosing, please go to Security>>MAC Filtering to create MAC filtering profiles (at least one).					

Wireless	Makes the wireless clients (stations) with the same SSID not access fo each other.			
Hide SSID	Switch the toggle to enable or disable the function.			
	Prevents 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 905 while site surveying. The system allows you to set four sets of SSID for different usage.			
	WPA Settings			
WPA Algorithm	This feature is available for WPA2 Personal, WPA2/WPA Personal, WPA2 Enterprise, WPA2/WPA Enterprise, WPA Personal, or WPA Enterprise mode.			
	Select TKIP, AES, or TKIP/AES as the algorithm for WPA.			
Key Renewal Interval	 WPA uses a shared key for authentication to the network. However, normal network operations use a different encryption key that is randomly generated. This randomly generated key 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. This feature is available for WPA3 Personal, WPA3/WPA2 Personal, WPA2/WPA Personal, WPA3 Enterprise, WPA2 Enterprise, WPA2/WPA Enterprise, WPA Personal, WPA Enterprise mode. 			
	WEP Settings			
Default Key	This feature is available for WEP Personal mode.			
	Four keys can be entered here, but only one key can be selected at a time. The format of WEP Key is restricted to 5 ASCII characters or 10 hexadecimal values in 64-bit encryption level, or restricted to 13 ASCII characters or 26 hexadecimal values in 128-bit encryption level. The allowed content is the ASCII characters from 33(!) to 126(~) except '#' and ','.			
Кеу # Туре	Hex/ASCII - 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(~) excep '#' and ','. This feature is available for WEP Personal mode.			
Key #	Enter 5 ASCII characters or 10 hexadecimal values in 64-bit encryption level, or 13 ASCII characters or 26 hexadecimal values in 128-bit encryption level. This feature is available for WEP Personal mode.			
Cancel	Discard the settings and return to the previous page.			

Click **Apply** to save the settings and return to the previous page.

II-1-3-2 Radio Settings

This page is to determine the wireless radio setting, like channel, physical mode, channel bandwidth, transmit power and etc.

Search	٩	Configuration / Wireless LAN		() Revel
and and an owned		SSID Radio Settings Ro	aming AP Discovery WPS Range Extender WDS	
Device Menu	-	Radio Settings		
 Dashboard 				
a configuration				Advanced Mode: OFF
Physical Interface		2.4GHz Radio		
LAN		Enabled		
Wireless LAN		Mode	Mixed (11b+11g+11n+11ax)	
Objects		Transmit Power	100%	
Notification Services				
RADIUS		Channel	Auto Select 🗸 🗸	
Certificates		Channel Bandwidth	Auto 20/40 MHz \sim	
Security	÷	Current Channel	Channel 4	
	2	Current Extension Channel	Channel 8	
88 Utility	5	Update Channel	Scan and Update	
🖏 System Maintenance	>		Note: Execute a one-time channel optimization for this AP. This would result in wireless downtime for few minutes	
Virtual Controller		Updated Channel Result		
and the second se				
>+ Wireless	2	5GHz Radio		
and the second second		finabled		
		Moda	Allend It suffault suffant	

Item	Description			
Advanced Mode	ON/OFF - Click the button to show or hide more settings.			
	2.4GHz Radio			
Enabled	Switch the toggle to enable or disable the function.			
Scheduled On	Select Always or any other schedule profile.			
	Always - This WLAN profile will be active all the time.			
	Or, use the drop-down list to select a preset schedule profile.			
	Before choosing, please go to Configuration>>Object to create schedule profiles (at least one).			
Mode	At present, VigorAP can connect to 11b only, 11g only, 11n only, Mixed (11b+11g), Mixed (11g+11n), Mixed (11b+11g+11n) and Mixed (11b+11g+11n+11ax) stations simultaneously. Simply choose Mixed (11b+11g+11n+11ax) mode.			
Transmit Power	The default setting is the maximum (100%). Lowering down the value may degrade the range and throughput of wireless.			
Channel	Means the channel of frequency of the wireless LAN. You may switch the channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select Auto Select to let the system determine for you.			
Channel Bandwidth	Auto 20/40 MHz– The AP will scan for nearby wireless AP, and then use 20MHz if the number of AP is more than 10, or use 40MHz if it's not.			
	20 MHz- The device will use 20MHz for data transmission and receiving between the AP and the stations.			
	40 MHz- The device will use 40MHz for data transmission and receiving between the AP and the stations.			
Current Channel	Displays current channel number.			

Current ExtensionDisplays current extension channel.Channel				
Update Channel	Scan and Update - Click to select the best channel again when Auto Select i s selected as the Channel setting.			
Updated Channel Result	Displays the bes	t channel after pressing the Scan and Update button		
	Update Channel	Scan and Update		

Note: Execute a one-time channel optimization for this AP.

	Updated Channel Result New Channel: 9
	5GHz Radio
Enabled	Switch the toggle to enable or disable the function.
Scheduled On	Select Always or any other schedule profile.
	Always - This WLAN profile will be active all the time.
	Or, use the drop-down list to select a preset schedule profile.
	Before choosing, please go to Configuration>>Object to create schedule profiles (at least one).
Mode	At present, VigorAP can connect to 11a only, 11n only (5G), Mixed (11a+11n), Mixed (11a+11n+11ac), and Mixed (11a+11n+11ac+11ax) stations simultaneously. Simply choose Mixed (11b+11g+11n+11ax) mode.
Transmit Power	The default setting is the maximum (100%). Lowering down the value may degrade the range and throughput of wireless.
Channel	Means the channel of frequency of the wireless LAN. You may switch the channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select Auto Select to let the system determine for you.
Channel Bandwidth	20 MHz- The device will use 20MHz for data transmission and receiving between the AP and the stations.
	40 MHz- The device will use 40MHz for data transmission and receiving between the AP and the stations. It is for wireless LAN 2.4GHz only.
	80 MHz- The device will use 80MHz for data transmission and receiving between the AP and the stations.
	160 MHz- The device will use 160MHz for data transmission and receiving between the AP and the stations.
Current Channel	Displays current channel number.
Update Channel	Scan and Update - Click to scan current channel used.
Updated Channel Result	Displays current channel used.
	Update Channel Scan and Update Note: Execute a one-time channel optimization for this AP.
	Updated Channel Result New Channel: 9

Band Steering Settings

5Ghz Client Minimum	If it is enabled, VigorAP will detect if the wireless client is capable of
RSSI	dual-band or not within the time limit.

	The wireless station has the capability of a 5GHz network connection, yet the signal performance might not be satisfied. Therefore, when the signal strength is below the value set here while the wireless station connecting to VigorAP, VigorAP will allow the client to connect to the 2.4GHz network.
Bel	ow shows more settings if the Advance Mode is ON
Antenna	Configure the number of antenna for transmission and reception.
Fragment LengthSets the Fragment threshold of wireless radio. Do not modif default value if you don't know what it is. The default value i	
RTS Threshold	Minimize the collision (unit is bytes) between hidden stations to improve wireless performance.
	Set the RTS threshold of wireless radio. Do not modify the default value if you don't know what it is. The default value is 2347.
Country Code	VigorAP broadcasts country codes by following the 802.11d standard. However, some wireless stations will detect/scan the country code to prevent conflict occurred. If conflict is detected, the wireless station will be warned and is unable to make a network connection. Therefore, changing the country code to ensure a successful network connection will be necessary for some clients.
WMM Capable	To apply WMM parameters for wireless data transmission, switch the toggle to enable the function.
APSD Capable	APSD (Automatic Power-Save Delivery) is an enhancement over the power-saving mechanisms supported by Wi-Fi networks. It allows access points to buffer traffic before transmitting it to wireless devices, thus allowing wireless devices to enter into power saving mode which reduces power consumption. Not all wireless clients support APSD properly, and the only way to find out if APSD is appropriate for your network is to experiment.
Airtime Fairness	Try to assign similar airtime to each wireless station by controlling TX traffic. Switch the toggle to enable the function.
Cancel	Discard the settings and return to the previous page.
Apply	Click it to save and apply the settings.

II-1-3-3 Roaming

The network signal for a single wireless access point might be limited by its coverage range. Therefore, if you want to expand the wireless network in a large exhibition with a quick method, you can install multiple access points with enabling the Roaming feature for each AP to reach the purpose of expanding wireless signals seamlessly.

These access points connecting for each other shall be verified by pre-authentication. This page allows you to enable the roaming feature and the pre-authentication.

Search Q	Configuration / Wireless LAN	(1) Reset
Device Manu (?) Dashboard Configuration Physical Interface LNN White LAN Objects Notification Services RADIUS	SSID Radio Settings Roaming AP Discovery WPS Range Extender WDS Fast Roaming Enabled 802.11r B02.11r B	*
Certificates Security Security Security Security System Maintenance Virtual Controller	Assisted Roaming by Signal Strength (RSSI) Enabled Assisted Roaming Signal Strength Threshold - @saming Signal ranges isodiam -starking SS dBm.(Default: -85) Assist roaming when adjacent AP Signal is better than parpeare angles isodiam -starking SS dB.(Default: 5)	

Item	Description			
Fast Roaming				
Enable 802.11r	Enable 802.11r - Switch the toggle to enable the 802.11r protocol (also known as Fast Basic Service Set (BSS) Transition. If enabled, the acces point will improve the roaming experience for the wireless clients.			
802.11r Mode	Over the DS - Transmit the handshake messages between the client and the new AP using the distribution system. In response to signal strength change, the client can communicate with the other AP through the original AP with Action Frames (FT Request and FT Response).			
	 Over the Air - Transmits the messages directly over the wireless network. In response to the needs of signal strength change, the clier can communicate directly with the other AP using a fast roaming authentication algorithm (without requiring reauthentication at every AP). Note that both APs must ping each other via DS (Distribution System) 			
	WDS.			
Enabled 802.11k	Switch the toggle to enable the 802.11k protocol (also know as Radio Resource Management (RRM)). If enabled, the access point will optimize the performance of wireless networks.			
Pre-Authentication for 802.1x	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 handof delay perceivable by a mobile node. It makes roaming faster and mor secure. (Only valid in WPA2)			
	Switch the toggle to enable/disable 802.11x Pre-Authentication.			
	Enable - Enable IEEE 802.1X Pre-Authentication.			
	Disable - Disable IEEE 802.1X Pre-Authentication.			
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 Enterprise mode.			
	Assisted Client Roaming			

Assisted Roaming by Signal Strength	When the link rate of wireless station is too low or the signal received by the wireless station is too worse, VigorAP 905 will automatically detect (based on the link rate and RSSI requirement) and cut off the network connection for that wireless station to assist it to connect another Wireless AP to get better signal. Enabled – Enable the function.
	Assisted Roaming Signal Strength Threshold – When the signal strength of the wireless station is below the value (dBm) set here and adjacent AP (must be DrayTek AP and support such feature too) with higher signal strength value (defined in the field of Assist roaming when adjacent AP signal is better than) is detected by VigorAP 905, VigorAP 905 will terminate the network connection for that wireless station. Later, the wireless station can connect to the adjacent AP (with better RSSI).
	Assist roaming when adjacent AP signal is better than - Specify a value as a threshold.
Cancel	Discard the settings and return to the previous page.
Apply	Click it to save and apply the settings.

II-1-3-4 AP Discovery

VigorAP 905 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.

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

Search_	۹	Configuration / Wireless LAN SSD Radio Settings Roaming AP Discovery WPS Range Extender WDS						C Refrech	
Device Menu (?) Dashboard	8	AP Discovery							
 Configuration Physical Interface LAN Windess LAN 	ľ	Start AP Discovery Radio Information	Scen Note: Scanning process	s would result in wireless downtime	e for few minutes				
Objects Notification Services			2.4GHz	5GHz					
RADIUS Certificates		Mode	Mixed(11b+11g+11n+11ax)	Mixed(11a+11n+11ac+11ax)					
Security	×	Current Channel	4	128					
	à.	Channel Utilization	9%	1%					
設 Utility	ă.	Channel Width	20/40 MHz	160 MHz					
🖏 System Maintenance	\$	Neighbor AP List							
Virtual Controller									
\$→ Wireless	5	SSID	BSSID	Signal Strength (RSSI)	Band	Channel :	Mode	Security	Encryption
		DrayTek-3D1250	14:49 bc 7a c0 58	1095	2.4GHz	4	11b/g/n/ax	WPA2/WPA Personal	AES
			16 49 hr 1a c0 58	15%	2 AGH>	.4	11h/n/n/ax	WP3/WPA2 Personal	AFS

Each item is explained as follows:

ltem	Description			
Start AP DiscoveryScan - Discover all the connected AP. The results will be shown on the box above this button				
Radio Information				

Mode, Current Channel, Channel Utilization, Channel Width	A table lists the radio information for this VigorAP 905.				
	Neighbor AP List				
SSID	Displays the SSID of the AP scanned by VigorAP 905.				
BSSID	Displays the MAC address of the AP scanned by VigorAP 905.				
Signal Strength (RSSI)	Displays the signal strength of the access point. RSSI is the abbreviation of Received Signal Strength Indication.				
Band	Displays the wireless band(2.4GHz/5GHz) used by the AP.				
Channel	Displays the wireless channel used for the AP that is scanned by VigorAP 905.				
Mode	Displays the physical mode used by the scanned AP.				
Security	Displays the security mode used by the scanned AP.				
Encryption	Displays encryption mode (None, WEP, TKIP, AES, etc.) of AP.				

II-1-3-5 WPS

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

Search	Q	Configuration / Wireless LAN		1 Reset C Refresh
Device Menu	2	SSID Radio Settings Ro WPS	arming AP Discovery WPS Range Extender WDS	
Configuration Physical Interface	R	Enabled	Note: only WPA2/WPA Personal security mode support WPs.	
LAN Wireless LM/ Objects		Band 2.4GHz SSID	2.4GHz SGHz DrayTek-S189D0	
Notification Services RADIUS Certificates	I	Method 1 : WPS Button	Sam PBC	
Security	3	Method 2 : Using PIN Code		
函 Monitoring 器 Utility	3 0	Generate PIN code from	Client 73156788	
🔦 System Maintenance	2		Connect	
Virtual Controller	ġ.	Connection Status	luire	
		Cancel Apply		

Available settings are explained as follows:

ltem	Description		
Enabled	Switch the toggle to enable/disable the WPS setting.		
Band	Specify which wireless band (2.4G/5G) will be used for this connection mode.		
	• 2.4GHz		
	• 5GHz		
2.4GHz/5GHz SSID	Displays the SSID setting for 2.4GHz/5GHz.		
	Method 1: WPS Button		
Enable WPS	Click Start PBC to invoke Push-Button style WPS setup procedure. VigorAP 905 will wait for WPS requests from wireless clients about two minutes.		
	Method 2: Using PIN Code		
Generate PIN code from	Client - Use wireless client's PIN code to securely connect it to the Wi-Fi network.		
Client PIN Code	Enter a number as the PIN code from the wireless client.		
Connect	Click to build WPS connection between this AP and another station.		
Apply	Click it to save and apply the settings.		
Cancel	Discard the settings.		

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

II-1-3-6 Range Extender

VigorAP can act as a wireless repeater which will help you to extend the networking wirelessly. The access point can act as Station and AP at the same time. It can use the Station function to connect to a Root AP and use the AP function to service all wireless clients within its coverage.

search	Configuration / Wireless LAN	38	leset C Refresh
Device Menu (2) Dashboard Triffgiralion Physical Interface LAN Witteney (A) Objects Notification Services	SSID Radio Settings Roa Range Extender Enabled Band Peer SSID	aming AP Discovery WPS Range Extender WDS	sawntime for few
RADIUS Certificates	Updated Status Peer MAC Address (Optimise)		
Security	Channel	Auto 🗸	
Monitoring	Security Mode	WPA2 Personal	
88 Utility	WPA Algorithms	AES	
🖏 System Maintenance	Password	۵	
Virtual Controller) Wireless	Connection Status	Disconnect	
	Cancel Apply		

ltem	Description		
Enabled	Switch the toggle to enable/disable the Range Extender setting.		
Band	Specify which wireless band (2.4G/5G) will be used for this connection mode.		
	• 2.4GHz		
	• 5GHz		
Peer SSID	Enter the SSID of the access point that VigorAP 905 wants to connect to.		
	Scan and Update - Scan the peer SSID and connect to it again.		
	Update Status		
Peer MAC Address (Optional)	Enter the MAC address of the access point that VigorAP 905 wants to connect to.		
Channel	Means the channel of frequency of the wireless LAN. You may switch the channel if the selected channel is under serious interference.		
	At present, only Auto is available for selection which lets the system determine for you.		
Security Mode	There are several modes provided for you to choose from. Each mode will bring up different parameters for you to configure.		
	WPA3 Personal		
	WPA2 Personal		
	OPEN		
WPA Algorithm	This option is available when WPA3 Personal or WPA2 Personal is selected as Security Mode .		
	At present, only AES is available for selection.		
Password	This option is available when WPA3 Personal or WPA2 Personal is selected as Security Mode .		
	Enter 8~63 ASCII characters, such as "012345678".		
Connection Status	Displays current connection status.		
Cancel	Discard the settings.		
Apply	Click it to save and apply the settings.		

II-1-3-7 WDS

Wireless Distribution System (WDS) is a protocol for linking access points (AP) wirelessly.

Search Q	Configuration / Wireless LAN SSID Radio Settings Roaming AP Discovery WPS	Range Extender WDS			③Reset C Refresh
Device Menu (?) Dashboard	WDS	Kunge Extendes			
Contiguration Physical Interface LAN	Enabled Mode HE (11ax) 2.4GHz WDS List	~			ý.
Wireless LAN Objects Notification Services RADIUS	+ Add Peer MAC Address ()	Enabled	Security	Password ①	Mas: 4
Certificates	SGHz WDS List				~
Monitoring Monitoring Set Utility System Maintenance	+Add Peer MAC Address @	Enabled	Security	Password ①	Max: 4
Virtual Controller)+ Wireless y					
	Cancel Apply				

ltem	Description					
Enabled	Switch the toggle to enable/disable the WDS setting.					
Mode	Select the physical mode for this WDS setting.					
	• HE(11ax)					
	• VHT(11ac)					
	 HTMIX(11n) 					
	2.4GHz WDS List					
+Add	Creates a new WDS entry for wireless band 2.4GHz.					
Peer MAC Address	Displays the peer MAC addresses					
	Enter the peer MAC addresses in these fields. Up to four peer MAC					
	addresses may be entered in this page. Select the checkbox in front of a MAC address to enable it.					
Enabled	Switch the toggle to enable/disable this setting.					
Security	Displays the security type.					
Password	Displays the password for TKIP/AES mode.					
	5GHz WDS List					
+Add	Creates a new WDS entry for wireless band 5GHz.					
Peer MAC Address	Displays the peer MAC addresses					
	Enter the peer MAC addresses in these fields. Up to four peer MAC addresses may be entered in this page.					
Enabled	Switch the toggle to enable/disable this setting.					
Security	Displays the security type.					
Password	Displays the password for TKIP/AES mode.					

Cancel	Discard the settings.
Apply	Click it to save and apply the settings.

II-1-4 Objects

II-1-4-1 MAC Object

The MAC address of local or remote clients can be specified in the MAC Object page.

SearchQ.	Configuration / Objects			③Reset C Refresh
evice Menu	MAC Object MAC Group Schedule			
b Dashboard	MAC Object			
	+ Add			Saurert. Maie 192
Physical Interface	Object Name	MAC Address	Used in	Option
LAN				
Wireless LAN				
Notification Services				
RADIUS Certificates				
) Security				
Monitoring				
utility >				
System Maintenance				
tual Controller				
Wireless				

To add a new MAC object profile, click the **+Add** link to get the following page.

	Object Name 🕕	MKT_1000
	MAC Address ①	
MAC Address		
	11000	
		Cancel App

ltem	Description
------	-------------

Object Name	Enter a name that identifies this object.			
MAC Address	Enter the MAC address of the client.			
Cancel	Discard current settings and return to the previous page.			
Apply	Save the current settings and exit the page.			

II-1-4-2 MAC Group

Multiple **MAC Objects** can be placed into a **MAC Group**.

Configuration / Objects				() Reset C Refresh
	chedule			
MAC Group				
+ Add				hamin Mair S
Group Name	Objects Included	Used in	Selected Objects	Option
	MAC Object MAC Group S MAC Group + Add	MAC Object MAC Group Schedule MAC Group + Add	MAC Object MAC Group Schedule + Add Group Name Objects Included Used in	MAC Object MAC Group Schedule MAC Group + Add Group Name Objects included Used in Selected Objects

To add a new MAC group profile, click the **+Add** link to get the following page.

		Available MAC Object	
Froup Name 🕢	MKT_D	Select MAC Objects	Search
elected Objects	+ Add Max: 12	Object Name	MAC Address
	Object Name MAC Address Option MKT_1000 14:49:8C(36:61100 🖗 DeMa	MKT_1000.	1449/BCI26/61700
Cancel Apply			Clos

Available settings are explained as follows:

ltem	Description
Group Name	Enter a name that identifies this profile.
Selected Objects	+Add - Click to open the page with available objects.

Available MAC Object						
Select MAC Objects Search - Enter the MAC object name to display existed MAC objects.						
Object Name	Select the object(s) to be grouped under the current MAC group. The selected one will be shown under the Selected Objects on the left side.					
Cancel	Discard current settings and return to the previous page.					
Apply	Save the current settings and exit the page.					

II-1-4-3 Schedule

This page allows you to set schedule profiles that can be used for the VigorAP to dial up to the Internet at a specified time. It is especially useful for each WLAN SSID to access the Internet network at different time periods by assigning different schedule profiles.

The schedule is also applicable to other functions.

SearchQ	Configurat	ion / Objects						() Reset
	MAC Object	t MAC Group	chedule					
Device Menu	Schedule							
(?) Dashboard								
	+ Add						Search	Max: 20
Physical Interface	Name	Enabled	Start Date	Start Time (Hr: Min.)	End Time (Hr. Min.)	Repeat	In Use	Option
LAN								
Wireless LAN								
Notification Services								
RADIUS Certificates								
Security								
Monitoring	3							
8 Utility	5							
System Maintenance	5							
/irtual Controller								
}⊷ Wireless	2							

To add a new schedule profile, click the **+Add** link to get the following page.

Simetuli			×
		Name ()	Test_AP
Start Date Start Time (Hr. Min.)	End Time (Hr: Min.)	Enabled	
State Date State (m. mar.)		Start Date	2025-05-05
		Start Time (Hr: Min.)	11 🗸 : 53 🗸
		End Time (Hr: Min.) 🛈	00 ~ : 00 ~
		Repeat	Once 🗸
			Cancel Apply

ltem	Description				
Name	Enter the name of the schedule profile.				
Enabled	Switch the toggle to enable/disable the schedule profile.				
Start Date	Specify the starting date of the schedule.				
Start Time (Hr:Min.)	Specify the starting time of the schedule.				
End Time (Hr:Min.)	Specify the ending time of the schedule.				
Repeat	Specify how often the schedule will be applied.				
	Once - The schedule will be applied just once.				
	Daily - The schedule will be applied every day based on the above settings.				
	• End Repeat - Switch the toggle to enable/disable the daily function				
	• End Repeat Date - The schedule is valid until that day.				
	Weekly - Specify which days in one week should perform the schedul				
	• Every - Select the days in one week.				
	• End Repeat - Switch the toggle to enable/disable the daily function				
	• End Repeat Date - The schedule is valid until that day.				
	Monthly - The schedule will be applied every month .				
	• End Repeat - Switch the toggle to enable/disable the daily function				
	• End Repeat Date - The schedule is valid until that day.				
	Cycle - Enter a number as cycle duration. Then, any action applied this schedule will be executed per several days. For example, "3" is selected as cycle duration. That means, the action applied such schedule will be executed every three days since the date defined on the Start Date.				
	• Every (days)- Enter a number.				
	• End Repeat - Switch the toggle to enable/disable the daily function				

• End Repeat Date - The schedule is valid until that day.		
Cancel	Discard the settings.	
Apply	Click it to save the settings and exit the page.	

II-1-5 Notification Services

VigorAP can send messages related to the system and the wireless LAN to DrayTek Wireless APP.

	q	Configuration / Notification	Services			@ Reset C Refres
		App Notifications				
Device Menu	-					
(P) Dashboard		Enabled				
		Connected Devices				
Physical Interface						
LAN		Devices				
Wireless LAN						
Objects						
		Test Notifications	Send Test Notification			
RADIUS		Send Status				
Certificates						
Security	2	Notification Message				
🔂 Monitoring		Category		Enable	Content	
88 Utility	5	System		00	WUVSSH/Telnet Login	
🖏 System Maintenance	•	Wireless LAN		1.20	Mesh Node online/offline	
Virtual Controller						
}→ Wireless	5					
		Cancel Apply				

Available settings are explained as follows:

ltem	Description
	App Notifications
Enabled	Switch the toggle to enable/disable the function of sending notification to the DrayTek Wireless APP.
	Connected Devices
Devices	Display the name (device ID) of the mobile phone(s) connected and submitted to DrayTek Wireless APP. Note that the little bell on the top-right corner of the APP must be turned on to receive the message from VigorAP 905.
Test Notifications	Send Test Notification – Press to send a message to DrayTek Wireless APP.
Send Status	Display the test result after pressing the Send Test Notification button
	Notification Message
Category	At present, only two categories are available.
Enable	Switch the toggle to enable/disable the category.
Content	Display the detailed information for the selected category.

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

II-1-6 RADIUS

Remote Authentication Dial-In User Service (RADIUS) is a security authentication client/server protocol that supports authentication, authorization and accounting, which is widely used by Internet service providers. It is the most common method of authenticating and authorizing dial-up and tunneled network users.

This web page is used to configure settings for external RADIUS server. Then WLAN users of VigorAP will be authenticated and accounted by such server for network application.

	Q. Configura	ition / RADIUS		
	External	RADIUS		
Device Menu	+ Add			Mas: 4
 Dashboard 	+ Add Name	Primary Authentication Server	Secondary Authentication Server	Option
	, and			opanin
Physical Interface				
LAN				
Wireless LAN				
Objects				
Notification Services				
Certificates				
Security	- 5			
🖽 Monitoring	×			
88 Utility				
🌯 System Maintenance	÷			
Virtual Controller				
3- Wireless	5			

To edit an existing profile, click the **Edit** link of the selected profile to make modifications.

lame ()					
uthentication					
ADIUS Authentication					
uthentication Server	+Add			Materia 2	
	Priority Server IP	Secret	Authentication Port	Option	
	0 172.16.3.62		© 1812	@ Delete	

To add a new profile, click the **+Add** link to get the following page.

ltem	Description
Name	Enter the name of the server profile.
	Authentication

RADIUS Authentication	Switch the toggle to enable/disable the function.			
Authentication Server	+Add - Click to create a new server profile.			
	• Priority - Only two external server can be used.			
	• Server IP - Enter the IP address of the external RADIUS server.			
	 Secret - Enter the password for the user to be authenticated by VigorAP 905 while the user tries to use VigorAP 905 as the RADIUS server. 			
	• Authentication Port - Enter a port number for the RADIUS server.			
	• Option - Click Delete to remove the selected entry.			
Cancel	Discards the settings and exits the page.			
Apply	Click it to save the settings and exit the page.			

II-1-7 Certificates

A digital certificate is an electronic document issued by a certification authority (CA) to an entity to prove ownership of a public key. It contains identifying information including the issued-to party's name, a serial number, expiration dates etc., and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. Vigor AP supports digital certificates that conform to the X.509 standard.

In this section, you can generate and manage local digital certificates, and import trusted CA certificates. Be sure that the system time is correct on the access point so that certificates will not be erroneously considered to be invalid because of an incorrect system time falling outside of the certificate's valid time period. The easiest way to accomplish this is by periodically synchronizing the system time to a Network Time Protocol (NTP) server.

II-1-7-1 Local Certificates

You can generate, import or view local certificates on this page.

	Local Certificates						
Dashboard	Local Certificates						
	+ Add					Search.	Maxer 20
Physical Interface	Certificate Name	Status	Source	CA Imported	Valid From	Valid Until	Option
LAN	Default_Certificate	Valid	Internal	Ur.	2021/01/01 01:00:03	2022/01/31 01:00:03	C Regimerate
Wireless LAN							
Objects							
Notification Services							
RADIUS							
Monitoring							
8 Utility :							
R opiny :							
System Maintenance							

ltem	Description
+Add	Creates a new certificate.
View	Displays the content of the certificate.

	20 3000	Backup & R	estole			×
					Certificate Name ①	Default_Certificate
					Version	V3
	100.0	Source	CA imported	Valid Fe	Status	Valie
	-	insernal		2021/01	Source	Internal
					CA Imported	~
					Subject_Name	ν.
	_				Country (L)	TW
					State (1)	Hsinchu
	_				Location ()	Hsinchu
	_				Organization(O)	DrayTek
	_				Organization Unit (UO)	DrayTek
	_				Common Name (CIV)	www.draytek.com
	_				Email(1)	
					Issuer	~
	_				Contimos Name//11	www.drautek.com
generate	Rege	nerate t	he certifica	te.		

To add a new local certificate profile, click the **+Add** link to get the following page.

Certificate Name 🕡		
Method	Generate CSR Import Certificate & Keys	
Кеу Туре	RSA-2048 Bit	
Algorithm	SHA-256	
Subject Alternative Nan	ne	
Туре	IP Address Domain Name Email	
IP Address 🕕		
Subject Name		
Country(C) 🙆		
state (s // 🕖.		
Location (L 0		
Organization(()) ()		
Organization Unit(OU) ()		
Organization Unitrool ()		

Item	Description			
Certificate Name	Enter the name that identifies the certificate.			
Method	Generate CSR - Generate a new local certificate. Import Certificate & Keys - Vigor access point allows you to generate a certificate request and submit it the CA server, then import it as "Local Certificate". If you have already gotten a certificate from a third party, you may import it directly. The supported types are PKCS12 Certificate and Certificate with a private key.			
	Method - Generate CSR			
Кеу Туре	Displays the key type used by the certificate.			
Algorithm	Displays the algorithm for generating the certificate.			
Туре	Select the type of Subject Alternative Name and enter its value.			

	 IP Address Domain Name Email 			
Country (C)	Enter the country name (code) in which your organization is located.			
State (ST)	Enter the state or province where your organization is located.			
Location (L)	Enter the city where you're your organization is located.			
Organization (O)	Enter the legal name of your organization.			
Organization Unit (OU)	Enter the department within your organization that you wish to be associated with this certificate.			
Common Name (CN)	Enter the fully-qualified domain name / WAN IP that will be used to reach your server.			
Email (E)	Enter the email address of the entry.			
Cancel	Discard current settings and return to the previous page.			
Apply	Save the current settings and exit the page.			

Method - Import Certificate & Keys

File Type	Vigor AP allows you to generate a certificate request and submit it the CA server, then import it as "Local Certificate". If you have already gotten a certificate from a third party, you may import it directly. The supported types are PKCS12 Certificate and Certificate with a private key.
	Certificate Only - Local certificate.
	• Upload Certificate - Click Choose a file to select a local certificate file.
	PKCS12 - Users can import the certificate whose extensions are usually .pfx or .p12. And these certificates usually need passwords. PKCS12 is a standard for storing private keys and certificates securely. It is used in (among other things) Netscape and Microsoft Internet Explorer with their import and export options.
	• Upload PKCS12 File - Click Choose a file to select a PKCS12 certificate file.
	• Password - Enter the password associated with the certificate and key files.
	Certificate & Keys - It is useful when users have separated certificates and private keys. And the password is needed if the private key is encrypted.
	• Upload Certificate - Click Choose a file to select a local certificate file.
	• Upload Key - Click Choose a file to select a key file.
	• Password - Enter the password associated with the certificate and key files.
Cancel	Discards current settings and return to the previous page.
Apply	Save the current settings and exit the page.

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

II-1-7-2 Trusted CA

The user can build RootCA certificates (up to three) if required.

When the local client and remote server are required to make certificate authentication (e.g., Radius EAP-TLS authentication) for wireless connection and avoid the attack of MITM, a trusted root certificate authority (Root CA) will be used to authenticate the digital certificates offered by both ends.

However, the procedure of applying for digital certificates from a trusted root certificate authority is complicated and time-consuming. Therefore, Vigor AP offers a mechanism that allows you to generate root CA to save time and provide convenience for general users. Later, such root CA generated by the DrayTek server can perform the issuing of the local certificate.

Root CA can be deleted but not edited. If you want to modify the settings for a Root CA, please delete the one and create another one by clicking Create Root CA.

search	٩	Configuration / Certi	Local Services	Backup & Res	itore						
Device Menu (?) Dashboard	8	Trusted Certificate									
🚊 Contiguration		+ Add							Search_		Max: 20
Physical Interface		Certificate Name	Status		Common Name	Valid From	Va	ilid Until		Option	é i
LAN Wireless LAN Objects Notification Services RADIUS Security Security Monitoring Security System Maintenance Virtual Controller + Wireless	• • • •	Root CA	Empty							2 Crei	ate

Available settings are explained as follows:

ltem	Description		
+Add	Creates a new trusted certificate.		
Option	Create - Click to open the configuration page.		

To create a new RootCA, click **Create** to get the following page.

Local Services Backup	& Restore		×
		Key Type Algorithm	RSA-2048 Bit SHA-256
Status Empty	Common Name	Subject Alternative Name	
		IP Address ① Subject Name	IP Address Domain Name Email
		Country(C) ① Common Name(CN) ①	TW
		State (ST) ① Location(L) ① Organization(O) ①	
		Organization Unit(OU) 🕐 Email(E)	

Available settings are explained as follows:

Item	Description
Кеу Туре	Displays the key type (set to RSA).
Algorithm	Displays the algorithm.
	Subject Alternative Name
Туре	Select the type of Subject Alternative Name and enter its value.
	Subject Name
Country (C)	Enter the country name (code) in which your organization is located.
Common Name (CN)	Enter the fully-qualified domain name / WAN IP that will be used to reach your server.
State (ST)	Enter the state or province where your organization is located.
Location (L)	Enter the city where you're your organization is located.
Organization (O)	Enter the legal name of your organization.
Organization Unit (OU)	Enter the department within your organization that you wish to be associated with this certificate.
Email (E)	Enter the email address of the entry.
Cancel	Discard current settings and return to the previous page.
Apply	Click to submit generate request to the CA server.

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

To upload a certificate, click the **+Add** link to get the following page.

		x
Upipad Cermicata	🗀 choose a file	

Available settings are explained as follows:

ltem	Description	
Upload Certificate	hoose a file - Select an existing certificate.	
Cancel	Discards the settings and exits the page.	
Apply	Click it to save the settings and exit the page.	

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

II-1-7-3 Local Services

This page allows you to set different categories and services for the local certificate(s) to prevent security warning messages popped up due to using different browsers.

	Configuration / Certificates			3 Res
evice Menu		Services Backup & Restore		
ት Dashboard	Local Services			
	Categories	Services.	Local Certificate	
Physical Interface	Web Server	HTTPS	Onfaur, Certificate 😔	
Wireless LAN	Web Server	TR069	Default_Certificate	
Objects Notification Services RADIUS	Note:			
	Certificate only and CSR cannot be applied to	lócal services.		
Security				
Monitoring				
; Utility 3				
System Maintenance				
rtual Controller				
• Wireless)				

Available settings are explained as follows:

ltem	Description	
Local Certificate	Select a local certificate (has been imported to Vigor device) with full key and authentication information.	
	Certificate without key phrase or CSR (certificate signing request) file cannot be selected as local certificate.	
Cancel	Discards the settings and exits the page.	
Apply	Click it to save the settings and exit the page.	

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

II-1-7-4 Backup & Restore

You can back up or restore the Local and Trusted CA certificates on the access point to a file.

Device Menu	1.2.2.2.2.2	
Dashboard	Backup & Restore	
	Backup	
Physical Interface	Баскар	
LAN	Selected item	Select All
Wireless LAN		Local Certificates
Objects		Trusted Certificate Authorities
Notification Services	Password Protection	
RADIUS	Password	0
	Confirm Password	
Security	Contirm Rassword	•
		Backup
	and the second se	
88 Utility	Restore	
System Maintenarice	Restore from Backup File	C Remove
	file has Password Protection	
Virtual Controller	Password	•
→ Wireless	Passion	

Item	Description		
	Backup		
Selected Item	 Select All Local Certificates Trusted Certificate Authorities 		
Password Protection	 Enabled - Switch the toggle to enable or disable the function. Password - Enter the password with which you wish to encrypt the certificate. Confirm Password - Enter the password again. Backup - Click to download the certificate. 		
	Restore		
Restore from Backup File	rom BackupClick to select the backup file you wish to restore.Restore - Click to retrieve the certificate.		
File has Password Protection	Enabled - Switch the toggle to enable or disable the function. Password - Enter the password that was used to encrypt the certificates.		

II-2 Security

II-2-1 MAC Filtering Profile

VigorAP may restrict wireless access to specified wireless clients only by referencing a MAC address black/white list.

The administrator may block wireless clients by inserting their MAC addresses into a black list, or only allow some wireless clients to connect by inserting their MAC addresses into a white list.

II-2-1-1 MAC Filtering Profile

This page allows to set the MAC Filtering Profiles (up to 10) that will be applied to SSID (configured on Configuration>>Wireless LAN>>SSID) to meet different needs.

	Q. Security / MAC Filter			③Reset C Refresh
Device Menu (?) Dashboard	MAC Filtering Profile MAC Filtering Profi			
🛱 Configuration	+ Add Name	Policy	Included Devices	Max: 10 Option
Security MAC FUNCTION (PMpMile MAC FUNCTION Monitoring Unity System Maintenance Virtual Controller Wireless	*			

Available settings are explained as follows:

ltem	Description
+Add	Click to create a new entry.
Edit	Click to modify the selected entry.
Delete	Click to remove the selected entry.

			×
Name	100		
Policy	Groubled Allow List Block List]	
Туре	Manual MAC Ditjets MAC Grou	up	
Device List	+Add	Sparch	Mass ITE
	Name N	IAC Address ())	
_			
Cancel Apply			

To add a new MAC filtering profile, click the **+Add** link to get the following page.

ltem	Description			
Name	Enter the name of the profile.			
Policy	If enabled, set Allow Li Allow List - Specify onl list can access this Vig Block List - Specify onl	 Disabled - Disable this profile. If enabled, set Allow List or Block List. Allow List - Specify only the name with the MAC address defined in the list can access this VigorAP. Block List - Specify only the name with the MAC address defined in the list will be blocked to access this VigorAP. 		
Туре	Manual – Enter the MA MAC Object – Select th MAC object will be allo MAC Group – Select th	 Determine which wireless clients can be applied to SSID. Manual – Enter the MAC address of certain device one by one. MAC Object – Select the MAC object(s). All the MAC address under the MAC object will be allowed or blocked. MAC Group – Select the MAC group(s). All the MAC objects under the MAC group will be allowed or blocked. 		
Device List	It is available when All +Add - Create a new e 100 Disabled Allow List Block Li +Add	ntry of a device with		5
	Name	MAC Address ①	<u></u>	Option
	TE_ST	14:49:BC:36:61:00		🕅 Delete
Cancel	Discard the settings.			
	Click it to save the settings and exit the page.			

II-2-1-2 Backup & Restore

This page allows you to save the access control policies and black & white lists as a profile, which can be used for restoration purposes.

Search	q	Security / MAC Filtering Profile			
a constant		MAC Filtering Profile Backu	p & Restore		
Device Menu		Backup & Restore			
(?) Dashboard		backup & Restore			
n Configuration	5-	Download Backup File	Download		
Securry	-	Restore from Backup Pile		Restore	
MAC filtering Profile					
🔂 Monitoring	s.				
88 Utility	*				
🖏 System Maintenance	÷				
Virtual Controller					
}→ Wireless	x.				

ltem	Description
Download Backup File	Download - Click to save the MAC filtering profile.
Restore from Backup File	Click to select the backup file (MAC filtering profile) you wish to restore. Restore - Click to retrieve the MAC filtering profile.

II-3 Virtual Controller - Wireless

This feature allows users to establish and manage a network of DrayTek devices connected by Wireless or Wired links.

The network consists of one Root and multiple Nodes. Root controls this network and syncs configurations to Nodes. Normally Root and Nodes use the same Wireless SSID/security, and Wireless clients can connect to any of them.

For Mesh networks, Root is also the outlet to the Internet. All devices of a network are in the same Group. The root can add a new Node to its Group or delete members from its Group. Users can choose VigorMesh or EasyMesh to establish the Mesh network. If Mesh is disabled, a network with wired links alone could still be established as long as AP Management is enabled.

Mesh Root and Mesh Node

Mesh Root indicates that this device would be another device's uplink connection.

As a Mesh Root, the device must connect to a gateway with an Ethernet cable first to have an Internet connection.

As a Mesh Node, the device can connect to the Mesh Root or Mesh Node within the same Mesh Group via Wireless or Wired links.

VigorMesh

VigorMesh is a DrayTek proprietary Mesh function. Pleae note that, within VigorMesh network,

- The total number allowed for Group members is 8 (including the Mesh Root).
- The maximum number of hop is 3.

Refer to the following figure:



EasyMesh

EasyMesh is a standard Mesh protocol of Wi-Fi Alliance.

II-3-1 Role Setup

This page can determine the role of the VigorAP connecting to the computer physically. And set up its Mesh function and AP Management function.

Search_	a	Wireless / Role Setup		③Reset C Refresh
Device Menu		Role Setup		
(?) Dashboard	-			Advanced Mode: OFF
		Device Role	Auto	
Configuration	2	Current Device Role	Node	
Security	>	Group Admin Account 💮	admin	
	>	Group Admin Password		
88 Utility		Password Status	Use random password	
🖏 System Maintenance	3	Mesh Setup		
Virtual Controller		Mesh Version	Vigor Mesh (R2) / EasyMesh (R3)	
3- Weekes		Enable Mesh		
Role Setup Device		Mesh Protocol	Vigor Mech EasyMesh	
Device		Current Uplink	Wired	
		Group Name	DrayTekMesh	
		AP Management Setup		
		Enable AP Management		
Jacobie State				

Item	Description		
	Role Setup		
Device Role	Auto - The device can switch between a Root and a Node based on the actual situation.		
	Root – The device is a Root. It controls the network and syncs configurations to the Nodes of its Group.		
	If Mesh is enabled, the device must connect to a gateway with an Ethernet cable to have an Internet connection.		
	Node – The device is a Node. It is managed by a Root if it has joined a Group.		
	If Mesh is enabled, the device can connect to the network through wireless.		
	Auto Root Node		
Current Device Role	Displays the current role of the device.		
Group Admin Account	Set an account for the system administrator to manage the mesh nodes. The account configured here will replace the account name defined for each node to ensure the mesh node's account security.		
Group Admin Password	Set a password for the system administrator to manage the mesh nodes.		
	The password configured here will replace the password defined for		

	each node to ensure the mesh node's account security.
	Mesh Setup
Enable Mesh	Switch the toggle to enable/disable the mesh function.
Mesh Protocol	Select the mesh protocol to manage the mesh network.
	 Vigor Mesh - A protocol developed by DrayTek.
	• EasyMesh - A protocol defined by WiFi alliance.
Uplink	It is available only when Node / VigorMesh is selected as Device Role <i>A</i> Mesh Protocol.
	Set the uplink of the device.
	 Auto - If the Ethernet port is connected and the device can access its gateway, use Wired uplink. Otherwise, use the Wireless uplink.
	• Wired - Fixed on the Wired uplink.
	• Wireless - Fixed on the Wireless uplink.
Current Uplink	It is available only when Auto or Node / VigorMesh is selected as Device Role / Mesh Protocol.
	Displays the current uplink.
Group Name	Displays the name of the current Mesh Group. It is available only when Auto or Root / VigorMesh is selected as Device Role / Mesh Protocol.
	If required, change the name.
Mesh Onboarding Mode	It is available only when EasyMesh is selected as Mesh Protocol.
	• PBC - Means the push-button configuration.
Start PBC Onboarding	It is available only when EasyMesh is selected as Mesh Protocol and PBC is selected as Mesh Onboarding Mode.
	 Start PBC - Triggers the WPS connection to build network between node backhaul and the root fronthaul.
	AP Management Setup
Enable AP Management	Switch the toggle to enable/disable the AP Management.
Default AP Profile	Follow Root - Click to synchronize the same configuration to the node managed by root AP.
	Advanced Mode: On
Wireless Uplink Band	It is available only when Auto or Node / VigorMesh is selected as Device Role / Mesh Protocol.
	Select available Wireless bands for connecting with uplink
Wireless Downlink Band	It is available only when VigorMesh is selected as Mesh Protocol.
	Select available Wireless bands for connecting with downlink.
Preferred Wireless Uplink Device	It is available only when Auto or Node / VigorMesh is selected as Device Role / Mesh Protocol.
	Select a Mesh member as the first priority when choosing Wireless uplink.
Preferred Wireless Uplink Timeout(min)	It is available only when Auto or Node / VigorMesh is selected as Device Role / Mesh Protocol.
	Set the time period (1 to 10 minutes) to wait for the Preferred Wireles Uplink Device.
Auto Wireless Uplinks Optimization	It is available only when Auto or Root / VigorMesh is selected as Device Role / Mesh Protocol.
---------------------------------------	--
	It is selected in default.
	If enabled, after changing the environment of the Mesh network, Root will perform reselect to reconstruct the Mesh network.
Log Level	It is available only when VigorMesh is selected as Mesh Protocol. Select Basic or Detailed. Related information will be shown on Syslog.
Cancel	Discard the settings.
Apply	Click it to save the settings.

II-3-2 Device

II-3-2-1 Device List

This page displays general information about the belonging group.

	Q. Wireless / Device	sh Status AP Ado							31	Reset CRefresh
Device Menu Deshboard Configuration	Device List	ST30003 87 A00	pour						Search_	Max: 20
 Security 	Name	MAC	IP Address	SSID	Status	Role	WLAN Clients (2.4G/5G)	Firmware Version	System Uptime	Option
전 Monitoring	VigorAP905	14498C5189D0	192.168.1.10		Online	Node	0/0	5.0.1	0d 5h 30m 36s	/ Edit
38 Utility										
System Maintenance	*									
Virtual Controller										
Role Setup										

ltem	Description
Edit	Click to modify the settings of the selected device. The settings for the APs are slightly different based on the role of the Root and Node. Settings for the AP (as the Node):

Online VigorAP905 Node	×	
s 192.168.1.10 Online VigorAP905 Node	VigorAP905	Name
Online VigorAP905 Node	1449BC51B9D0	MAC
VigorAP905 Node	192.168.1.10	IP Address
VigorAP905 Node		55ID
VigorAP905 Node ents (2,46/56) 0/0	Online	Status
	VigorAP905	Model
ents (2,4G/5G) 0/0	Node	Role
	0/0	WLAN Clients (2,4G/5G)
Version 5.0.1	5.0.1	Firmware Version
ptime 0d 5h 30m 36s	0d 5h 30m 36s	System Uptime

II-3-2-2 Mesh Status

Displays general information of the Mesh network.

This page is available only when **Mesh** is enabled (**Virtual Controller>>Role Setup**).

Search	Q. Wi	reless /	Device								C Refresh
		vice Lis	t Mesh Status	AP Adop	tion						
evice Menu	M	esh Sta	atus								
Dashboard											
Configuration	2									Search	Mass 253
) Security	> N	ame	MAC Address	Role	Hop	Uplink Device	Uplink Interface	Signal Strength	Uplink Rate (TX/RX)	Uplink Uptime	Option
3 Monitoring											
8 Utility											
System Maintenance											
rtual Controller											
Role Setup											

Available settings are explained as follows:

ltem	Description
Name	Displays the name of the device (for identification).
MAC Address	Displays the MAC address of the device.
Role	Displays the role of the device.
Нор	Displays the number of Wireless links from the device to Root. "0" means the device is using a Wired uplink.
Uplink Device	Displays the MAC address of the device that this device connects to.
Uplink Interface	Displays the interface which the device is using to connect to uplink.
Signal Strength	Displays the signal strength of the device to its uplink.
Uplink Rate(Tx/RX)	It is available only when VigorMesh is selected as Mesh Protocol. Displays the link rate of the device to its uplink.
Uplink Uptime	It is available only when VigorMesh is selected as Mesh Protocol. Displays how long the device is online.
Option	Click View to modify the selected mesh device.

Device List	Mesh Status AF	Adopt	ion			C Refresh
Mesh Status						>
					нор.	
					Uplink Device	00:1D:AA:10:27:22
Name	MAC Address	Role	Нор	Uplink Device	Uplink interface	Wireless 5GHz (Ch36)
VigorAP1062C	00:1D:AA:10:27:22	Root	0	N/A	Uplink Quality	
N1	00:1D:AA:64:10:15	Node	1	00:1D:AA:10:27:22	Signal Strength	-56dBm/86%
					Uplink Rate (TX/RX)	1755M/1755M
					Uplink Uptime	0d 02:11:22
					Mesh Action	
					Optimize Uplink	Optimize
					Preferred Wireless Uplink Device	N/A
					Set Preferred Wireless Uplink Device	
						Set

Optimize All Mesh Links - It is available only when **VigorMesh** is selected as Mesh Protocol and the device is a Root.

Press the **Optimize** button to perform reselect to reconstruct the Mesh network.

Optimize Uplink - It is available only when **VigorMesh** is selected as Mesh Protocol and the device is a Wireless Node.

Press the **Optimize** button to disconnect the device from Mesh network. The device might connect to a better uplink later.

Preferred Wireless Uplink Device - It is available only when **VigorMesh** is selected as Mesh Protocol and the device is a Node.

Displays the Preferred Wireless Uplink of the device.

Set Preferred Wireless Uplink Device - It is available only when **VigorMesh** is selected as Mesh Protocol and the device is a Node. Select a Mesh member and press the **Set** button to set the Preferred Wireless Uplink Device of the device.

II-3-2-3 AP Adoption

Search and add new Nodes to the device's Group.

This page is available when Current Device Role is Root.

It is also available when Device Role is Auto and Device List contains only the device itself.



Available settings are explained as follows:

ltem	Description
Status	Displays whether the Scan button is available now.
Start AP Discovery	Press the Scan button to search new Nodes.
AP Discovery Result	Displays the scanned result.
	Adopt AP - Select the checkbox if you want to add the device into a Group.
	MAC - Displays the MAC address of the device.
	Model - Displays the model of the device.
	Signal Strength - Displays the signal strength of the device if it was found through the Wireless.
	Device Name - Insert the name of the device for identification.
Cancel	Discard current settings.
Apply	Click to add the selected device(s) into the Group.

Tips for VigorMesh Network Setup

• VigorMesh supports auto uplink. If a device could not access its gateway, it becomes a Wireless Node automatically.

A Mesh Root or a Wired Mesh Node should be able to ping its gateway through Ethernet.

• VigorMesh can add new Mesh Nodes into Mesh Group through both Wireless and Wired. However, we recommend to connect new Nodes to the Root by Ethernet cables and add them into Mesh Group first.

Wait until the configuration sync finishes. And then move the Nodes to their destinations.

- VigorMesh supports up to 3 hops. However, it is suggested to connect the Mesh network with less than or equal to 2 hops.
- It is suggested to make the Uplink Signal Strengths of all Wireless Mesh Nodes be larger than -65 dBm.
- A Wireless Mesh Node with an Ethernet cable should not loop to another Node.
- If the Mesh Root disappears and there are online Wired Mesh Nodes with Device Role Auto, one of the Wired Mesh Nodes will become a Mesh Root automatically.
- A VigorMesh Group can be reset by the "Reset" button on Virtual Controller >> Wireless >> Device >> Device List.
 - If resetting a Mesh Root,
 - All online Mesh Nodes will be informed to reset.
 - For those Mesh Nodes unable to reset, reset them manually.
 - If resetting a Mesh Node,
 - The device will become a New Node again.
 - The Wireless SSID settings of the device will be reset, too.

Troubleshooting:

- Check the country code and Wireless channels.
- Check the firmware version. Please make sure all Mesh members are in the newest firmware version.
- Check the Current Device Role and Current Uplink of the device.
- Please make sure that the device is not in DFS CAC detection.
- Check the channel load. Make sure it is not over 70%.

Tips for EasyMesh Network Setup

- Set up multiple mesh devices with uplink RSSI larger than -65dBm.
- Setup is recommended to use wired connection and device list to add devices.
- EasyMesh network supports up to 3 hops of devices. However, it is suggested to connect with less than or equal to 2 hops.
- EasyMesh is not suggested to join existing VigorMesh Environment.
- The maximum of devices number is (ssid_num * device_num <= 56) -> device_num is the max device number

How to set up a VigorMesh group?

The following steps will guide you how to setup a VigorMesh Group.

Please access the web of the device which you want to use it as the Root.

1. (Optional) Open Virtual Controller>>Wireless>>Role Setup.

Set **Group Admin Password**. This value will be the Administrator Password of the Nodes after they join the Mesh Group and complete configuration sync.

Wireless / Role Setup		🕲 Reset 📿 Refrest
Role Setup		
Device Role	Auto 🗸	Advanced Mode: OFF
Current Device Role	Node	
Group Admin Account 🕕	admin	
Group Admin Password 🕧	······ ©	
Password Status	Use random password	
Mesh Setup		
Enable Mesh		
Mesh Protocol	Vigor Mesh EasyMesh	
Current Uplink	Wireless	
Group Name	DrayTekMesh	
AP Management Setup		
Enable AP Management		
Cancel Apply		

2. Open Virtual Controller>>Wireless>>Device>>AP Adoption. Click the Scan button.

evice List Mesh Status	AP Adoption					
AP Adoption						
itatus	Scan butte	on is n	ot availa	ble! (Current De	evice Role is No	de.)
itart AP Discovery	Scan					
AP Discovery Result	Adopt AP	MAC	Model	Signal Strength	Device Name	
			NO REC	ords Found		

3. Wait until the searching result appears.

Choose the device(s) you want to add to the Group and set the names for identification.

Click the **Apply** button and wait for it to finish the procedure.

	AP Discovery Result Adopt AP MAC Model Signal Strength Device Name
14:49:BC:51:B7:9F VigorAP1062C -92dBm(weak) 00:1D:AA:66:44:66 VigorAP1062C -94dBm(weak)	
00:1D:AA:66:44:66 VigorAP1062C -94dBm(weak)	
	14:49:BC:51:B7:9F VigorAP1062C -92dBm(weak)
00:1D:AA:64:10:15 VigorAP1062C -61dBm(good) N1	00:1D:AA:66:44:66 VigorAP1062C -94dBm(weak)
	00:1D:AA:64:10:15 VigorAP1062C -61dBm(good) N1

4. Refer to Virtual Controller>>Wireless>>Device>>Device List and Virtual Controller>> Wireless >> Device >>Mesh Status for viewing the result.

Wireless / Devic	ce									
Device List	Mesh Status	AP Adoption						ť	🛈 Reset 🕐	Refresh
Device List										
										Max: 50
Name	MAC	IP Address	SSID	Status	Role	WLAN Clients (2.4G/5G)	Firmware Version	System Uptime	Option	
VigorAP1062C	001DAA102722	192.168.1.10	DrayTek- 102722	Online	Root	0/0	1.5.1_RC8	0d 4h 58n	n 24s 🧷 Edit	
VigorAP1062C	001DAA641015	192.168.1.11	DrayTek- 102722	Online	Node	0/0	1147.8df8de432f_B6	eta Od 1h OOn	n 45s 🧷 Edit	🕆 Delete
Wireless / Devi	ce									
Device List	Mesh Status	AP Adoption							C	Refresh
Mesh Status										
Name	MAC Address	Role Ho	p Uplink D	levice	Uplin	nk Interface	Signal Strength	Uplink Rate (TX/RX)	Uplink Uptime	Option
VigorAP1062C	00:1D:AA:10:27:2	22 Root 0	N/A					·;	0d 02:15:33	View
N1	00:1D:AA:64:10:	15 Node 1	00:1D:A	A:10:27:22	2 Wire	eless 5GHz (C	h36) -56dBm/86%	1755M/1755N	/ 0d 02:11:22	© View

Chapter III Management



III-1 System Maintenance

For the system setup, there are several items that you have to know the way of configuration: Device Settings, Management, Firmware, Backup & Restore, Accounts & Permission, System Reboot, and Registration & Services.

III-1-1 Device Settings

The user can modify the time, device name, and Syslog for the device.

III-1-1-1 Time

Open System Maintenance>>Device Settings and click the Time tab.

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

Search Q,	System Maintenance / Device Set	tings	3 Reset	CRefresh
	Time Device Name Syslog	SNMP		
Device Menu	Time and Date			
 Dashboard 	Time and Date			
🛱 Configuration >	System Time	2021-01-01 05:51:52		
⊘ Security >	Time Setting			
🔂 Monitoring	Set Time	Automotically with Time Server Manually		
28 utility ;	Time Server	time.google.com		
K System Maintenance	Time Zone	(UTC) Greenwich Mean Time : Dublin 🔍		
Device Setting Management	Interface	Auto v		
Firmware	Daylight Saving	00		
Backup & Restore		Test Time Server Connection		
Account & Permission	Server Status			
System Reboot Registration & Services	More settings 😒			
Virtual Controller				
> Wireless ;				
	Cancel Apply			

Available parameters are explained as follows:

Item	Description
	Time and Date
System Time	Display current time.
	Time Setting
Set Time	 Determine the method (automatically or manually) to set the time. Automatically with Time Server - Set the system time by retrieving time information from the specified network time server using the Network Time Protocol (NTP). Manually - Set the system time using the time reported by the web browser.
When Automatically with Time Server is selected as Set Time	 Time Server - Enter the web site of the primary time server. Time Zone - Select the time zone where the access point is located. Interface - Renew the time through the interface selected by VigorAP automatically.

	Daylig	kt Sa	ving -	Enab	le Dav	/light	Savin	g Time	(DST) if it is applicabl
	your l		-	-	,	0			
	Updat	te Tim	1e - Fo	rce to	o rene	w cur	rent t	time se	tting.
	Conne	ection	Statu	s - Di	splays	s last	updat	te time	status.
	More	Settir	1 gs - C	lick to	o oper	n adv	anced	setting	gs for the time server
			•						terval (30min or 60m e periodically.
			-				-		time server, please Secondary Server.
			n dary natica		ace -	Backı	ip inte	erface f	for renewing the time
		enabl	-	nter a	custo				hen Daylight Saving is able the DST - Defaul
When Manually is	Time	Zone	- Seleo	t the	time	zone	where	e the A	P is located.
selected as Set Time	Date -	Use	the dr	op-do	own ca	alend	ar to s	specify	correct date.
	12	2021-0	4-26				1		
	F						1	1	L.
	-	202	1 APR				<	>	
		S	- tid	ų,	ð.	1÷	E.	¢0	
		ÁPI	2			1	2	3	
		4	5	6	7	8	9	10	
		11	12	13	14	15	16	17	
		18	19	20	21	22	23	24	
	-	25	26	27	28	29	30		
		c	L			c ·	L .		
		roniz	e with	-					tes, and seconds. Sync the time setting v
Apply	Save t	he cu	irrent	settin	igs an	d ren	ew th	e syste	m time.
Cancel									vious page.

After finishing this web page configuration, please click **Apply** to renew the system time.

III-1-1-2 Device Name

Display the device name. Change the name if you want.

Open System Maintenance>>Device Settings and click the Device Name tab.

SearchQ	System Maintenance / Device Settings	DResol
Locacia del	Time Device Name Syslog SNMP	
Device Menu	Device Name	
(?) Dashboard	Device Name	
😴 Configuration >	Device Name () VigorAP905	
Security 5		
🔂 Monitoring		
😫 Utility 💡		
4, Syttem Mandersmot		
Device Sellinge		
Management		
Firmware		
Backup & Restore		
Account & Permission		
System Reboot		
Registration & Services		
Virtual Controller		
}- Wireless ;		

III-1-1-3 Syslog

SysLog function is provided for users to monitor the device.

Open System Maintenance>>Device Settings and click the Syslog tab.

	q	System Maintenance / Devi	ce Settings		
		Time Device Name	Syslog SNMP		
evice Menu		Syslog Settings			
Dashboard		-)			
🖆 Configuration		Logging Destinations	External Server		
Security	×	Log Message	User Access Log		
죠 Monitoring			Z LAN Log		
BS Utility			System Log		
	*		WIFI Basic Log		
			Mesh Log		
			APM Log		
Management		Syslog Servers			
Firmware Backup & Restore					
Account & Permission		+Add		Mao: 3	
System Reboot		Server IP ()	Port 🕥	Option	
Registration & Services		192.168.1.10	514	1 Delete	
Virtual Controller					

Available parameters are explained as follows:

ltem	Description
	Syslog Settings
Logging Destinations	Select External Server to display Log Message and Syslog Servers for detailed configuration.
Log Message	Select to send the corresponding message of user access, interface, and system information to Syslog.
	Syslog Servers

+Add	Click to display new entry boxes for creating a new Syslog server profile. The maximum number of Syslog servers to be added is "3".
Server IP	Enter the IP address of the Syslog Server.
Port	Enter the port number of the Syslog Server.
Option	Delete - Click it to remove the selected server profile.
Apply	Save the current settings and exit the page.

III-1-1-4 SNMP

This section allows you to configure settings for SNMP services.

The SNMPv3 is more secure than SNMP through the use of encryption (supports AES and DES) and authentication (supports MD5 and SHA) for the management needs.

Search	٩	System Maintenance / Device	Settings	(3) Reset
		Time Device Name Sy	slog SNMP	
Device Menu		SNMP		
Dashboard		2000		
Seconfiguration	5	Enabled		
Security	>	SNMP service also sh	all be enabled for internet access in System Maintenance >> Management	
🗃 Monitoring	2			
28 Utility	>	Manager		
🗞 System Maintoninios		Manager Host	Any Specific Heat	
Device Settings				
Management		Query		
Firmware		Get Community 🕕	public	
Backup & Restore Account & Permission		Set Community 🕡	private	
System Reboot		Query Port	161	
Registration & Service	s.	Agent		
Virtual Controller		SNMPv3 Agent Enabled	0	
⊶ Wireless	ć	SNMPy2c Agent Enabled		
		Cancel Apply		

Available parameters are explained as follows:

ltem	Description
	SNMP
Enabled	Switch the toggle to enable/disable the SNMP function. If enabled, Manager, Query, Agent and Trap settings will be valid for you to configure.
	Manager
Manager Host	Any - Any IP can be set as the manager host.
	Specific Host - Specify a host (IPv4 or IPv6) or hosts (both IPv4 and IPv6).
	Enter the IPv4 address with subnet mask / IPv6 address with specified prefix length of hosts that are allowed to issue SNMP commands. If these field are left blank, any IPv4/IPv6 LAN host is allowed to issue SNMP commands.
	Query
Get Community	Enter the Get Community string. The default setting is public . Devices

	that send requests to retrieve information using get commands must
	pass the correct Get Community string. The maximum allowed length is 23 characters.
Set Community	Enter the Set Community string. The default setting is private . Devices that send requests to change settings using set commands must pass the correct Set Community string. The maximum length of the text is 23 characters.
Query Port	Displays the port number used by the query server.
	Agent
SNMPv3 Agent Enabled	Switch the toggle to enable/disable the SNMPv3 function. If enabled, specify corresponding settings. Agent SIMPV2 Agent Enabled Username (USM) O Authentication Password O Privacy Privacy Password O Disabled Disabled SIMPV2 Agent Enabled Trap SIMPV2 Agent Enabled Disabled Disabled Disabled Disabled Disabled Trap SIMPV2 Agent Enabled Disabled Disabled Disabled Disabled Disabled SIMPV2 Agent Enabled Dis
SNMPv2c Agent Enabled	Switch the toggle to enable/disable the SNMPv2 function.
SNMPv1 Agent Enabled	Switch the toggle to enable/disable the SNMPv1 function.
	Тгар
Enabled	Switch the toggle to enable/disable the Trap function.
Trap Version	 Select the trap version. V1 V2c V3
Trap Community	Enter the Trap Community string. The default setting is public. Device that send unsolicited messages to the SNMP console must pass the correct Trap Community string. The maximum length of the text is 23 characters.
Trap Port	Enter the port number used for the Trap server.
Notification Host IP	Select the type of the notification host.

	IPv6
Notification Host(IPv4)	+Add - Enter the IPv4 address of hosts that are allowed to be sent SNMP traps.
Notification Host(IPv6)	+Add - Enter the IPv6 address of hosts that are allowed to be sent SNMP traps.
Trap Events	Select the event(s) to apply the settings configured in this page.
Apply	Save the current settings and exit the page.

III-1-2 Management

III-1-2-1 Service Control

This page allows you to manage the general settings, management services, and TLS/SSL Encryption setup.

SearchQ	System N	laintenarice / Ma	nagement	
	Service C	ontrol TR-065	Syster	m Information
Device Menu	General			
(?) Dashboard				
Seconfiguration	Auto Logo	put	l.	off
Security >				
🖽 Monitoring)	Manage	ment Services		
BS Utility	Enforce H	TTPS Access		29
A Appenditementer	Allow PIN	G from LAN		D
Device Settings	LLDP		- 6	D
Manageraga				-
Firmware		Port ()	(default	LAN Access
Backup & Restore Account & Permission	HTTP	80	(80)	
System Reboot	HTTPS	-443	(443)	
Registration & Services	SSH	22	(22)	
Virtual Controller				
S+ Wireless	Teinet	23	(23)	
	SNMP	161	(161)	•
	TLS/SSL	Encryption		

ltem	Description		
	General		
Auto Logout	If "off" is selected, the function of auto-logout for the web user interface will be disabled. The web user interface will be open until you click the Logout icon manually.		



Management Services					
Enable the checkbox to allow system administrators to login Vigor device via HTTPS.					
Allow all PING packets from LAN.					
LLDP Switch the toggle to enable/disable the LLDP service.					
Specify user-defined port numbers for the HTTP, HTTPS, SSH, Telnet and SNMP servers.					
Select the checkbox to allow system administrators to login from LAN interface.					
TLS/SSL Encryption					
Switch the toggle to enable the function of TLS 1.3/1.2 if required.					
Discard current settings and return to the previous page.					
Save the current settings and exit the page.					

(i) Note:

Switch these two icons by click the mouse cursor on them.



🤇 - means "Disable".

III-1-2-2 TR-069

Vigor device supports the TR-069 standard for remote management of customer-premises equipment (CPE) through an Auto Configuration Server, such as VigorACS.

SearchQ	System Maintenance / M	fanagement	③Reset CRefnesh
	Service Control TR.0	69 System information XMPP	
Device Menu	ACS and CPE Settings		
 Dashboard 	ACS and CPE Settings		
후 Configuration >	TR-069		
Security >			
🔂 Monitoring 5	ACS Server		
88 utility 5		https://	
	URL ①	Witzerd	
Device Settings	Username 💿		
		Note: Usemame support characters: a-z.A-Z.0-9, @%	
Firmware			
Backup & Restore	Password ()	•	
Account & Permission		Note: Password support characters: a-zA-Z/0-9,%i\$/()=7*@#.	
System Reboot			
Registration & Services	Test Connection		
Virtual Controller			
≻ Wireless >	① Make sure to ap	pply and save settings first before running the test.	
		Test Conversion Result (2025-05-05-05:52:33) Test With Inform Error	
	Cancel Apply		

ltem	Description				
TR-069	Switch the toggle to enable or disable the function.				
	If enabled, settings available for TR-069 will be shown below.				
	ACS Server				
URL	Enter the URL for connecting to the ACS.				
	Wizard - Click it to enter the IP address of VigorACS server, port number and the handler.				
Username/Password	Enter the credentials required to connect to the ACS server.				
Event Code	Use the drop down menu to specify an event to perform the test.				
	Test Connection - Click it to send a message based on the event code selection to test if such CPE is able to communicate with VigorACS server.				
	More settings				
CPE Client	This section specifies the settings of the CPE Client.				
	Protocol - Select Https if the connection is encrypted; otherwise select Http.				
	Port - In the event of port conflicts, change the port number of the CPE.				
	Username / Password - Enter the username and password that the VigorACS will use to connect to the CPE.				
Periodic Inform Settings	Enable / Disable - Switch the toggle to enable or disable the function. The default setting is Enable, which means the CPE Client will periodically connect to the ACS Server to update its connection parameters at intervals specified in the Interval Time field.				
	Time Interval - Set interval time or schedule time for the device to send notification to CPE.				

STUN Settings	Auto – Select to set the STUN port of the server.				
	Enabled / Disabled - Select to enable or disable the function.				
	If select Enabled , please enter the relational settings listed below:				
	• Server Address - Enter the IP address of the STUN server.				
	• Server STUN Port - Enter 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. 				
Apply	Save the current settings and exit the page.				
Cancel	Discard current settings and return to the previous page.				

III-1-2-3 System Information

The System Information displays basic information (e.g., device name, LAN MAC, firmware version, build date/time, ACS server and etc.) of Vigor device.

	System Maintenance / Mar	agement	CRefresh
	Service Control TR-069	System information XMPP	
Device Menu	System Information		
(?) Dashboard	System		
Configuration >	Device Name	VigorAP905	
Security >	LAN MAC	14:49:8C:51:89:D0	
G Monitoring	System Uptime	4d 23h: 32m: 31s	
BS Utility >	Firmware	5.0.4	
Device Settings	ACS Server		
		See More +	
Firmware			
Backup & Restore			
Account & Permission System Reboot			
Registration & Services			
Neground a services			
Virtual Controller			
}+ Windess ,			

III-1-2-4 XMPP

XMPP is an abbreviation of Extensible Messaging and Presence Protocol. If your access point is registered with the XMPP server, it can help VigorACS manage the access point under NAT at any time without obstruction.



Switch the toggle of Enable/Disable to enable or disable the XMPP feature.

III-1-3 Firmware

Before firmware upgrade, please **download** the newest firmware from the DrayTeks website or FTP site **first**. The DrayTek website is www.draytek.com (or local DrayTeks website) and the FTP site is ftp.draytek.com.

Open **System Maintenance>>Firmware**. 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).

Search	a.	System Maintenance / Firmwar	e		
Device Menu		Firmware			
State of the local division of the local div	-				
 Dashboard 		Current Firmware Version	5.0.4		
	3.	Firmware for upload		Lupioad	
⊘ Security	5				
🖽 Monitoring	5.				
88 Utility	*				
🖉 Symmetrikansen					
Device Settings					
Management					
Throward					
Backup & Restore					
Account & Permission					
System Reboot					
Registration & Services					
Virtual Controller					
}→ Wireless	8				

Then click **Upload** and wait for a few seconds.



When the upload is finished, please click the **Restart** button.



Wait for a while until the system finishes the rebooting.

	×
Rebooting	
Web UI will be redirected in few seconds.	
65 4 SECONDS	
Or Access Now ->	

III-1-4 Backup and Restore

This function can be used to backup/restore the **VigorAP** settings.

Search_ Q	System Maintenance / Backup & Restore	
Device Menu	Download Configuration Backup	
Device Settings	Download Configuration Backup Password Protection Password Protection Password O Download Download Download Restore from 8 Configuration Backup Restore from 8 Configuration Backup Restore from 8 Configuration Backup	
Management Firmware Raj King & Heatow Account & Permission System Reboot Registration & Services Virtual Controller)+ Wireless	Heitore except the login password C	

ltem	Description					
Download Configuration Backup						
Password Protection	For the sake of security, the configuration file for the access point can be encrypted. Switch the toggle to enable or disable the function.					
Password	Enter several characters as the password for encrypting the configuration file.					
Download	Click it to backup the configuration file.					
	Restore from a Configuration Backup					
Restore from Backup File	Click to locate the file for restoring. Restore - Click to execute the restoration.					
Restore except the login password	Switch the toggle to enable or disable the function.					
File has Password Protection	Switch the toggle to enable or disable the function. If enabled, a password will be required for restoring the configuration.					
Restore Password	Enter a password for configuration restoration.					

III-1-5 Accounts & Permission

This page allows you to modify current administration account and password.

III-1-5-1 Local Admin Account

	System Maint	tenance / Account & Permi	ssion				() Reset	C Refrest
	Local Admin	Account Role & Permiss	sion					
Device Menu	Local Admin	Account						
Dashboard								
Configuration 5	+ Add							Marc
Security >	Account	Role	Status	Last Login at	Last Login IP	Created Time	Option	
Monitoring 5	admin	Administrator	Active	2021-01-01 04:13:03	192.168.1.1	2021-01-01 00:01:39	2 Edit	IT Delete
; Utility ,								
Device Settings								
Management								
Firmware								
Backup & Restore								
System Reboot								
Registration & Services								
• Wireless 5								

Available settings are explained as follows:

ltem	Description			
+Add	Create a new account profile.			
Edit	Modify the selected account profile.			
Delete	Remove the selected account profile.			

To modify an existing profile, select the one and click the **+Edit** link to open the setting page.

To add a new profile, Click **+Add**.

		×
Account 🕕	admin	
New Password 🕕	······ @	
Confirm New Password 🛈	······ •	
	At least 8 characters	
	 Uppercase characters 	
	✓ Lowercase characters	
	✓ Numbers or Special characters -t@#\$%^&*()_=/?[]{<>\	
Role	None 🗸	
Status	Active 🗸	
Account Info		
Created Time	e.	
_		
Cancel Apply		

Available settings are explained as follows:

ltem	Description			
	Local Admin Account			
Account	Display the name of the account.			
New Password	Enter a new password in this field. The length of the password is limited to 83 characters.			
Confirm New Password	Enter the new password again.			
Role	 Specify the role of the account. Administrator Guest User-defined role (created on the Role & Permission page) 			
Status	Active - Enable the selected account profile. Inactive - Disable the selected account profile.			
Cancel	Discard current settings and return to the previous page.			
Apply	Save the current settings and exit the page.			

Click **Apply** to save the settings.

III-1-5-2 Role & Permission

This page allows to create new roles which can be applied to local admin account.

The default roles are Administrator and Guest.

SearchQ	System Maintenance / Account &	Permission		3 Ret
	Local Admin Account Role & F	ermission		
Device Menu	Role & Permission			
Dashboard	and the second se			
Configuration	+Add		Max: 64	
∂ Security >	100			
Monitoring	Role	Administrator	Guest	
🖞 Utility ,	Left Menu Path			
System Mautonance	▶ Device Menu	Read-write	Read-only	
Device Settings	 Dashboard 	Read-write	Read-only	
Management	 Configuration 	Read-write	Read-only	
Firmware	Security	Read-write	Read-only	
Backup & Restore	Monitoring	Read-write	Read-only	
	Utility	Read-write	Read-only	
System Reboot				
Registration & Services	 System Maintenance 	Read-write	Read-only	
/irtual Controller	 Virtual Controller 	Read-write	Read-only	
- Wireless	 Wireless 	Read-write	Read-only	

ltem	Description
+Add	Create a new role profile.
Role	Lists all of the features that a role can have.

To create a new role profile, click **+Add**. A new role will be added on to the page.

Local Admin Account	Role & Permission		
Role & Permission			
+Add			Max: 64
Role	Administrator	Guest	Role_1
Left Menu Path			🛍 Delete
Device Menu	Read-write	Read-only	Read-only 🗸

ltem	Description						
+Add	Create a new role profile.						
Role_1	The field of profile name. New added profile will be named as Role_#. To modify the name, simply click the name and enter a new string (e.g., Role_MKT).						
	Local Admin Account Role & Permission						
	Role & Permission						
	+Add Max: 64						
	Role Administrator Guest Role_MKT ×						
	Left Menu Path						
	► Device Menu Read-write Read-only Read-only ✓						
Left Menu Path	Lists all of the features that a role can have.						
	The role of Administrator have the highest authority for accessing VigorAP.						
	The role of Guest have the lowest authority for accessing VigorAP.						
	The authority of the user-defined roles must be based on the conditions selected respectively.						
Delete	Remove the selected user-defined role profile.						
	Specify the permission for each menu item for the user-defined role.						
Read-only 🗸	Deny - The permission for the menu item on the left side is not allowed for the user-defined role profile.						
	Read-only - The permission for the menu item on the left side allowed						
Deny	for the user-defined role profile to be read-only. Read-write - The permission for the menu item on the left side						
Read-only	allowed for the user-defined role profile to be both read-only and						
Read-write	written.						

Apply

Save the current settings and exit the page.

After finished the settings, click **Apply.** The new role can be seen and selected on **System Maintenance>>Account & Permission>>Local Admin Account**.

		×
Account ()	admin	
New Password 🕥	•	
Confirm New Password 🛈	\$	
	At least 8 characters	
	 Uppercase characters 	
	Lowercase characters	
	Numbers or Special characters -!@#\$%^&*()_=/?[]{<>\	
Role	None 🗸	
Status	None	
Account Info	Administrator	
Created Time	Guest	
	Role_MKT	
	New role	
Cancel Apply		

III-1-6 System Reboot

The Web user interface may be used to restart your VigorAP. Open **System Maintenance >> System Reboot** to get the following page.

search	a	System Maintenance / System Re	boot
Device Menu		System Reboot	
(?) Dashboard		Reboot With	Current Configuration Factory Default
🚔 Configuration	>		Reboor
Security	5		
	5	Auto Reboot Time Schedule	
28 Utility	5	Enable Auto Reboot Schedule	
Image: System Mainlenance Device Settings Management Firmware Backup & Restore Account & Permission System Retoot Registration & Services Virtual Controller		Schedule Profile	source your detilent. Note: 1. End Time in the schedule reboot will be ignored. 2. Time setting recommend to use Automatically with Time Server.
> wireless	3	Cancel Apply	

ltem	Description
Reboot With	Select one of the following options, and press the Reboot button to reboot the VigorAP.
	Current Configuration – Select this option to reboot the VigorAP. using the current configuration.
	Factory Default – Select this option to reset the VigorAP's configuration to the factory defaults before rebooting.
Reboot	Reboot the device immediately.
Enable Auto Reboot Schedule	Switch the toggle to enable/disable the auto reboot schedule function. If it is enabled, select the schedule profile as the basis to reboot the router.
Schedule Profile	Select up to 4 user-configured schedules.

Chapter IV Others



IV-1 Monitoring

IV-1-1 DHCP Table

This page provides information on IP address assignments. This information is helpful in diagnosing network problems, such as IP address conflicts, etc.

Click **Refresh** to reload this page with the most up-to-date information.

IV-1-1-1 IPv4 DHCP Subnet

This page shows the DHCP server status, IP range, IP pool, Used IP, and percentage of utilization for each LAN interface.

SearchQ	Monitoring / DHCP	Table						C Refresh
	IPv4 DHCP Subret	IPv4 DHCP Lease						
Device Menu	IPv4 DHCP Subne	t						
 Dashboard 								
	5						Search	Man: 255
⊘ security	5 Name	DHCP Server Status	IP Range	IP Pool	Used IP	Utilization		
Anonomy	[LAN] LAN1	Disabled						0%
DHCB Table								
LLDP Neighbors information								
Web Syslog								
Internet								
Clients List								
🔛 Utility	>							
🔧 System Maintenance	s							
Virtual Controller								
}- Wineless								

IV-1-1-2 IPv4 DHCP Lease

This page shows the remaining time of the IPv4 DHCP lease of the device.

	Q	Monitoring / DHCP	Table					C Refresh
		IPv4 DHCP Subnet	IPv4 DHCP Lease					
Device Menu		IPv4 DHCP Lease						
 Dashboard 								
Configuration	÷						Search	Max: 255
Security	÷.	Subnet	IP Address	MAC Address	Host Name	Туре	Leased Time	
		[LAN] LAN1	192.168.1.1	14:49:8C:36:61:00		Static	Fixed IP	
		[LAN] LAN1	192.168.1.100	08:8F:88:D5:DD:A9		Static	Fixed IP	
LLDP Neighbors information								
Web Syslog								
Internet								
Clients List								
Utility								
System Maintenance	*							
irtual Controller								
Wireless								

IV-1-2 LLDP Neighbors Information

This page allows the system administrator to understand the topology of network devices and the relationships between devices. Usually, information includes:

- System name
- System Description
- IPv4/IPv6 address (optional)
- Port ID
- Port Description
- Time
- Time to Live

Search_	Q	Monitoring / LLDP Neighbors information								CRefresh		
Device Menu	8	LLDP Ne	ighbors info	mation								
(?) Dashboard											Search	
	÷	Local Port	Chassis ID	System Name	System Description	Management Address(IPv4)	Management Address(IPv6)	System Capabilities	Port ID	Port Description	Time	Time to Live(sec)
Security	÷.											
Monitoring	1											
DHCP Table												
Web Syslog												
Internet												
Clients List												
88 Utility	× .											
System Maintenance	*											
Virtual Controller												
}- Wireless	>											

IV-1-3 Web Syslog

Log related to setting configuration and/or actions performed by this device can be stored on web Syslog.

Search_	a	Monitoring / Web Syslog					C Refresh
Device Menu		Web Syslog					
 Dashboard 	-	Enabled Web Syslog					
😄 Configuration	2	Loop Logging Option	Override Oldest Logs Stop When Full				
Security							
A Monitonne:		Export as TXT Expo	Type	Content	Filter: All Type	✓ Search	Max: 1000
DHCP Table		1000	- the	Contain			
LLDP Neighbors Information							
Web Sysing							
Internet Clients List							
88 Utility	>						
🖏 System Maintenance							
Virtual Controller	-						
>+ Wireless	5						
		Cancel Apply					

Available settings are explained as follows:

Item	Description						
Enabled Web Syslog	Switch the toggle to enable or disable the function.						
	If enabled, Loop Logging Option will be shown as follows.						
Loop Logging Option	Override Oldest Logs - Vigor router system will backup all existed information on the flash onto the host and clean up the information from the flash. Later, it will start a new record.						
	Stop when Full - Vigor router system will stop to record the user information onto the flash.						
Export	Click it to export the log records as a file (.TXT or .json).						
Clear All	Click it to clear all log records on this page.						
Filter	Select the type of log to display on this page.						
Cancel	Discard current settings and return to the previous page.						
Apply	Save the current settings and exit the page.						

Click Apply to save the settings.

IV-1-4 Internet

	Monitoring / Internet	⊖ Refresh
Device Menu	Internet	
Dashboard	Enabled Internet Detection	
Seconfiguration	Internet Status N/A	
Security		
DHCP Table	Detection Interval 1 min ~	
LLDP Neighbors information	Necord Syslog	
Web Syslog	When Internet is disconnected	
Clients List	Blink LED	
😵 Utility		
🖇 System Maintenance		
Virtual Controller		
+ Wireless		
	Cancel Apply	

This feature can help users realize whether the internet is disconnected.

ltem	Description
Enabled Internet Detection	Switch the toggle to enable or disable the feature of Internet detection.
Internet Status	Display current Internet status (e.g., N/A, Connected, Connected [WAN IP=xxx.xxx.xxx] and Disconnected).
Detection Method	Vigor system provides three types of detection method.
	Check DNS
	Check Gateway
	Ping Host
	If Ping Host is selected, enter the Vigor system's Host IP address to perform the detection work.
Detection Interval	VigorAP device will detect the Internet connection with the interval (1) sec, 1 min, 10 min and 30 min) selected here.
Record Syslog	Switch the toggle to enable or disable the feature.
	If this feature is enabled, information about Internet disconnections will be recorded in the SysLog.
Blink LED	Switch the toggle to enable or disable the feature.
	When the ACT LED blinks twice and then pauses for one second repeatedly, it indicates that the Internet connection is disconnected.
Cancel	Discard current settings.
Apply	Save the current settings.

IV-1-5 Clients List

	a	Monitoring	g / Clients	List												CR	etresh
Device Menu		Clients Lis	st														
 Dashboard 	-	S Add M	AC Filterin	ng from Clie	ents Max 51	2.									Searth		± 4
	>	Name	MAC	Up Time	Link Speed	RSSI	SSID	Usage Up	Usage Down	СН	Band	IP B	V PSM	Physical Mode	Auth Mode	Encrypt Type	
Security	3							4									
DHCP Table																	
LLDP Neighbors information																	
Web Syslog																	
Internet																	
器 Utility	>																
🖏 System Maintenance	>																
Virtual Controller	-																
>- Wireless	2																

It provides the information related to the wireless clients connecting to the VigorAP 905.

IV-2 Utility

IV-2-1 Ping Tool

The user can perform the ping job for specified IP (host) to diagnose if the data transmission via the Vigor system is well or not.

Device Menu Image: Device Menu Image: Device Menu Image: Device Menu Image: Configuration Image: Device Menu Image: Devi	Search	q	Utility / Ping Tool				
Configuration Ping from: Auto Configuration Ping to Host/IP Address () Security Parket Size (byte) Security Ping Count Monitoring Ping Count Minitoring Ping interval (sec) Minitoring Ping interval (sec) Monitoring Ping interval (sec) Virtual Controller Virtual Controller	Davica Manu		Ping Tool				
Configuration Ping to Host/IP Address () Image: Security Parkiet Size (byte) Image: Security Ping Count Image: Tool Ping interval (sec) Image: Tool Image: Tool Ima	and the second s		Ping from	Auto	~		
Security Packet Size (byte) 64 Monitoring Ping Count 4 Ming Tool Image Tool 1 Trace Tool Clear Non Virtual Controller Image Tool Image Tool			Ping to Host/IP Address ()				
Monitoring Ping Count 4 Withity: Ping Interval (sec.) 1 Range Tool Clear Kun Trace Tool Virtual Controller Virtual Controller			Packet Size (byte)	64	~		
Willily Ping interval (sec.) Ning Tool Trace Tool Web CLI System Maintenance Virtual Controller			Ping Count	4	14 ²		
Birrig Tabl Clear Nun Trace Tool Web CLI Virtual controller			Ping interval (sec.)	4	~		
Web CLI System Maintenance , Virtual Controller				Clear N.	un l		
System Maintenance							
Virtual Controller							
	🖏 System Maintenance	•					
j→ Wireless s	Virtual Controller	=					
	>+ Wireless	5					

Item	Description
Ping from	Choose Auto for the router to select the WAN interface.
Ping to Host/IP Address	Enter the host / IP address that you want to ping.
Packet Size (byte)	Select the packet size for the ping job.
Ping Count	Select the quantity of the packet being pinged.
Ping Interval (sec.)	Select a time interval (unit:second) for the system to ping the IP address specified above.
Clear	Remove the settings and return to the factory settings.
Run	Perform the ping job.

IV-2-2 Trace Tool

The user can perform the traceroute job for specified IP (host) to diagnose if the data transmission via the Vigor system is well or not.

	à	Utility / Trace Tool		
Device Menu		Trace Tool		
(?) Dashboard		IP Version	(Dod	
	,	Trace Through	Auto 🗸	
Security	,	Protocol	ICMP UBP	
Honitoring	,	Host / IP Address		
		Trace Count	3 🗸	
Ping Tool		Мах Нор	30 ~	
			Clear Run	
Web CLI				
No. System Maintenance	e ş			
Virtual Controller				
>- Wireless	\$			

ltem	Description
IP Version	Select the IP version. At present, only IPv4 is available for selection.
Trace Through	Trace through specific interface. Only Auto is available for selection.
Protocol	Select ICMP or UDP protocol.
Host/IP Address	Enter the host / IP address that you want to traceroute.
Trace Count	Select the max hops for traceroute, select none for unlimited.
Мах Нор	Set the maximum number of hops to search for the target.
Clear	Remove the settings and return to the factory settings.
Run	Perform the ping job.
IV-2-3 Web CLI

It is not necessary to use the telnet command via DOS prompt. The changes made by using web console have the same effects as modified through web user interface. The functions/settings modified under Web Console also can be reviewed on the web user interface.

Click the **Web Console** icon on the top of the main screen to open the following screen.

Open the page of **Utility>>Web CLI**.

Search Q	Utility / Web CLI
	WebCl Username: admin Password: Vigor> help Show available commands
Vinity Ping Tool Trace Tool with Ca System Maintenance	quit Disconnect history Show a list of previously run commands enable Turn on privileged commands exit Exit from current mode config Configure exec execute
Virtual Cantroller > Wirdess	vigor>

This page is left blank.

Chapter V Mobile APP, DrayTek Wireless



V-1 Introduction of DrayTek Wireless

VigorAP 905 supports Android/iOS APP : DrayTek Wireless. The mobile user can find the APP through Apple App Store / Google Play Store.

After downloading the APP, a mobile user is able to access and login the configuration page of VigorAP.

(i) Note:

Before using the DrayTek Wireless APP, please **ENABLE** your Wi-Fi feature first. Then, select the Wi-Fi network with Vigor access point(s) connected physically.

It is not necessary to connect to VigorAP physically. The mobile user must connect to one network with the same subnet as the VigorAP.

V-2 Create a New Network

1. Run DrayTek Wireless APP.



- 2. The system will open the NETWORK page to ask you create a new network first.
- 3. There are two methods for creating a new network. Click "+" or press the search button

A: Click "+" to enter the next page. Enter the required information for the device that you want to create a network.



B: Press the search button. Later, the system will show the device searched. Select the one you want and click the name to get the detailed information.



4. After clicking **Create Network**, a new network will be shown on the screen.





The wizard can assist to configure mesh root and mesh node(s).

1. Click and hold the network item till available actions (**Wizard, Edit** and **Delete**) shown on the screen. Select and click **Wizard**.



2. On the next page, enter the SSID and the password for VigorAP and click **Connect.** When a summary page appears, click the **Next** button.



3. Enter the username and the password of VigorAP, click **OK**. On the WiFi Name & Password page, define the WiFi Name and the Password. Then click the **Next** button.

9:25	*	9:36	~
Establi	sh connection	K Back Quick S	tart Wizard Cancel
SSID	Dray920		
Device MAC	00:10:AA:99:04:20	0 0	
Assigned IP	172,173405	Operation Wili Mode Setup	Admin Finish Password Finish
Enter User	name and Password	Wifi Name	& Password
		1111	3/32
Cancel	ОК	1111111	7/64
	Next		
Germi	an to another	1	lext

4. On the **Password Setting** page, enter the admin password and confirm the password. Then click **Next** for the APP to verify the password. If successful, the **Finish** button will appear.





Run DrayTek Wireless APP.



Available settings are explained as follows:

ltem	Description
Network	Create a new network.
Connect	Connect to a device (AP/CPE).
Diagnostic	Analyze the current Wi-Fi network to check the network quality.

Support	Display a list of models supported by this APP.
About	Display the version information of this APP.

V-4-1 Setup

For checking the general information of certain device, click the existing item under the Network list to open the **Dashboard** of the selected device.



Click **Setup** to access into the web user interface of VigorAP 905. On the following page, enter the username and the password. Click **Login** to get the dashboard of the access point.

9:19	*	9:20	* =
s	etup	K Se	tup
		Dra Vigor	yTek AP1062C
		Dashboard	CRefresh
D	English C	SYSTEM	
Dra	y Tek	Device Name	
Vigor	AP1062C	Root	
Username		LAN MAC	
		14:49:BC:51:B7:9E	
Password		System Uptime	
	- 000	16d 16h 51m 7s	
		Firmware	
12		1332.091d83af78_Beta	
	agin	Build Date/Time	
		Fri Jun 9 08:34:45 UTC :	0000
		mjun 9 08.34.45 01C.	2023
		Web Version	
		issue_1257_2-r3132.127	/bd96
		Core Version	
		r526.41d5e26	
Cas	0	(a)	0
Carol Summer V	Serie:	Conditioned	Dimiting .

Chapter VI Troubleshooting



VI-1 Checking the Hardware Status

Follow the steps below to verify the hardware status.

- 1. Check the power line and cable connections. Refer to "I-2 Hardware Installation" for details.
- 2. Power on the device. 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 **"I-2 Hardware Installation"** to execute the hardware installation again. And then, try again.

VI-2 Checking the Network Connection Settings

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.

VI-3-1 For Windows

(i) Note:

The example is based on Windows 7 (Professional Edition). As to the examples for other operation systems, please refer to the similar steps or find support notes in **www.draytek.com**.

1. Open All Programs>>Getting Started>>Control Panel. Click Network and Sharing Center.



2. In the following window, click **Change adapter settings**.



3. Icons of network connection will be shown on the window. Right-click on **Local Area Connection** and click on **Properties**.



4. Select Internet Protocol Version 4 (TCP/IP) and then click Properties.

Connect using:	000 MT Network Conn	ection
This connection uses	the following items:	Configure
Client for Mic	Filter Driver	da ka
E Internet Prot	ter Sharing for Microsoft cool Version S (TCP/IP cool Version 4 (TCP/IP	

5. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**. Finally, click **OK**.

neral Alternate Configuration		- II : e			
u can get IP settings assigned (is capability, Otherwise, you ne r the appropriate IP settings,					
Obtain an IP address autom					
IP address:	É		101	1	-
Subnet mask:	Ē	<i>.</i>	- 00	4	-
Default gateway	Г	ų.	X	1	
Obtain DNS server address	automatio	ally	٦		
C Use the following DNC corre			J	_	_
Preferred DNS server:	E		- ii	4	
Akernaté DNS serveri	[ę.	<u>i</u>	Ŧ	
✓ Validate settingsupon wit.				Adv	anced

VI-3-2 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.

000	Network	0
Show All Displays Sou	Network Startup Disk	
Lo	ocation: Automatic 🛟	
TCP/		
Configure IPv4:	Using DHCP	
IP Address:	192.168.1.10 Renew DHCP	Lease
	255.255.255.0 DHCP Client ID: (If required) 192.168.1.2	
DNS Servers:		(Optional)
Search Domains:		(Optional)
IPv6 Address:	fe80:0000:0000:0000:020a:95ff:fe8d:72e4	(?)
Click the lock to p	revent further changes. Assist me)	oply Now

VI-3 Pinging the Device

The default gateway IP address of the device is 192.168.1.2. For some reason, you might need to use "ping" command to check the link status of the device. **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 V-2)

Please follow the steps below to ping the device correctly.

VI-3-1 For Windows

- 1. Open the **Command** Prompt window (from **Start menu> Run**).
- 2. Type **cmd**. 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.

VI-3-2 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.

000	Terminal — bash — 80x24	
Welcome to Darwin! Vigor10:~ draytek\$	n 3 02:24:18 on ttyp1 ping 192.168.1.1 (92.168.1.1): 56 data bytes	2
64 bytes from 192.1 64 bytes from 192.1 64 bytes from 192.1	168.1.1: icmp_seq=0 tt1=255 time=0.755 ms 168.1.1: icmp_seq=1 tt1=255 time=0.697 ms 168.1.1: icmp_seq=2 tt1=255 time=0.716 ms 168.1.1: icmp_seq=3 tt1=255 time=0.731 ms 168.1.1: icmp_seq=4 tt1=255 time=0.72 ms	
192.168.1.1 pir 5 packets transmith	ed, 5 packets received, 0% packet loss /max = 0.697/0.723/0.755 ms	

VI-4 Backing to Factory Default Setting

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

(i) 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.

VI-4-1 Software Reset

You can reset the device 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 device will return all the settings to the factory settings.

System Maintenance / System Reboot		
System Reboot		
Reboot With	Current Centiguration Factory Default Reboot	
Auto Reboot Time Schedule		
Enable Auto Reboot Schedule		
Schedule Profile	Sector Your Options Note: 1. End Time in the schedule reboot will be ignored. 2. Time setting recommend to use Automatically with Time Server.	

VI-4-2 Hardware Reset

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



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

VI-5 Contacting DrayTek

If the AP 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.