

Tube-2HQP

PDF

2.4GHz 802.11b/g/n Outdoor AP/CPE User Guide

TABLE OF CONTENTS

| | 3 |
|------------------------------------|----|
| HARDWARE DESCRIPTION | 3 |
| HARDWARE INSTALLATION | 3 |
| INITIAL CONFIGURATION | 4 |
| CONNECTING TO THE LOGIN PAGE | 4 |
| STATUS PAGE | 5 |
| EASY SETUP | 5 |
| OPERATION MODE – AP ROUTER | 6 |
| SETTINGS – PPPoE(ADSL) | 6 |
| Settings – Static (Fixed IP) | 7 |
| SETTINGS – CABLE/DYNAMIC IP (DHCP) | 9 |
| Settings – PPTP | 10 |
| Settings – L2TP | 11 |
| OPERATION MODE – AP BRIDGE | 12 |
| OPERATION MODE – CLIENT ROUTER | 13 |
| OPERATION MODE – CLIENT BRIDGE | 15 |
| Advanced Setup | 16 |
| Management | 17 |
| Advanced Settings | 19 |
| OPERATION MODE | 21 |
| FIREWALL CONFIGURATION | 21 |
| MAC/IP/Port Filtering | 21 |
| VIRTUAL SERVER SETTINGS | 23 |
| DMZ | 24 |
| Firewall | 24 |

| CONTENT FILTERING | 25 |
|-------------------|----|
| NETWORK SETTINGS | 27 |
| WAN | 27 |
| LAN | |
| Advanced Routing | 31 |
| WIRELESS SETTINGS | 32 |
| BASIC | 32 |
| Security | 33 |

INTRODUCTION

The Tube-2HQP is a 1X1 MIMO IEEE 802.11b/g/n wireless outdoor AP/CPE which support data ratesup to 150Mbps. It is rain and splash proof when install in upright position. TUBE-2HQPalso supports N type connector and 802.3at/afStandard PoE for simplify installation.

HARDWARE INSTALLATION



◆□How to assembly the unit





INITIAL CONFIGURATION

The TUBE-2HQP, outdoor 2.4GHz AP/CPE offers a user-friendly web-basedmanagement interface for the configuration of all the unit's features. Any PC directly attached to the unit can access the management interface usinga web browser, such as Internet Explorer (version 6.0 or above).

CONNECTING TO THE LOGIN PAGE

It is recommended to make initial configuration changes by connecting aPC directly to the TUBE-2HQP's Ethernet port. The TUBE-2HQPhas a default IP address of 192.168.2.1 and a subnetmask of 255.255.255.0. You must set your PC IP address to be on thesame subnet as the TUBE-2HQP(that is, the PC and TUBE-2HQPaddresses must both start 192.168.2.x).To access the TUBE-2HQP's management GUI interface, followthese steps:

1. Use your web browser to connect to the management interface using the default IP address of 192.168.2.1.

2. Log into the interface by entering the default username "admin" and password "admin," then click OK.



STATUS PAGE

After logging in to the web interface, the Status page displays. The Homepage top-menu-bar shows the Status, Easy Setup, Advanced and Language.

| LAH Configuration | |
|---|--|
| LAN IP Address. 192,193,2,1 | 1 All Hermark: 355,365,365,9 |
| MAC Address: MODECASESTCAC | |
| Sextern Info | |
| Finanware Version V2.5 2012-06-27-13:35 | System Time Sun, 01 Jun 2012 12:04:39 |
| Operation Mode: AP Bindge mode | Whickess MAC Address - 00:000CAR000035 |
| | |

EASY SETUP

The Easy Setup is designed to help you to configure the basic settings required to get the TUBE-2HQPup and running. There are only a fewbasic steps you need to set up theTUBE-2HQPto get the connection.

Click on Easy Setup to bring up the wizard

| Operation Mode Setup | |
|---------------------------------|--|
| Please select on Operation Node | Please select an Operation Mode 💌 |
| Nex | Please select an Operation Mode AP Router |
| | AP Bidge Client Router |
| | Client Bridge |

If you want to configure a router connection, please select <u>AP Router</u> If you want to configure to an access point, please select <u>AP Bridge</u> If you want to configure to WISP, please select <u>Client Router</u> If you want to configure to WiFi client, please select <u>Client Bridge</u>

OPERATION MODE-AP ROUTER

Choose menu "Easy Setup" and select AP Router if you want to configure a router connection.

NOTE: The Ethernet port will convert into WAN port requiring you to configure your CPE via WLAN.

| Operation Node Setup | | | |
|----------------------|---------------------------------|-----------------------------------|--|
| | Please select an Operation Mode | Please select an Operation Mode 📼 | |
| | _ | Please select an Operation Mode | |
| | Nex | AP Router | |
| | | AP Undge | |
| | | Client Router | |
| | | Client Undge | |
| | | | |

SETTINGS – PPPoE(ADSL)

1) Select PPPoE to be assigned automatically from an Internet service provider (ISP) through a DSL modem using Point-to-Point Protocol over Ethernet (PPPoE).

| time incentions (mont) seconds | |
|--------------------------------|---|
| OHCP Mode | WWW Connections Cable/Dynamic IP (DHCP) - Static (Fixed IP) Cable/Dynamic IP (DHCP) |
| iset wc dna op | Hostname PPPPE (ADSL) PPTP L2TP |
| Primary DNUS Server | Secondary DNS Server |
| | Next Back |

2)

| Wilde Area Network (VIIAN) Settings | |
|---|---|
| | Connections PPPoE (ADSL) |
| PPPoE Mode | |
| User Name pppoe_user | |
| Password | Verify Password |
| Operation Mode Keep Alive | Keep Alive Mode: Redial Period 60 Second: |
| wan pppoe mta 1492 bytes (Default-1492) | |
| inst we das op | |
| Primary DHS Server | Secondary DNS Server |
| | Next Back |

- ◆□User Name Sets the PPPoE user name for the WAN port.
- ◆□**Password** Sets a PPPoE password for the WAN port.
- ◆□Verify Password Prompts you to re-enter your chosen password.
- ◆ **Operation Mode** Enables and configures the keep alive time and configures the on-demand idle time.

| 3) | |
|---------------------|----------------|
| secare ssid 1 title | 2 Help |
| Network Name (SSID) | SSID_NAME 1820 |
| secure wps choice | • |
| Security Node | Disable |
| Disable | |
| No Securi | |
| Done v | ireless back |

Security Setup

NetworkName (SSID)—SSID (Service Set Identification) must be assigned to all wireless devices in your network. Considering your wireless network security. Security Mode — Select the security method and then configure the required parameters. (Options: Disabled, WEP-AUTO, WPA-PSK, WPA2-PSK, WPA-Auto-PSK, WPA, WPA2, WPA-Auto, 802.1X; Default: Disabled)

SETTINGS – STATIC (FIXED IP)

 Select Static(Fixed IP), if your Internet service provider (ISP) to be permanent address on the Internet. A Static IP address is a number (in the form of a dotted quad)

| Wide Area Network (NUN) Settings | |
|----------------------------------|---|
| | WWW Connections Cable/Dynamic IP (DHCP) |
| DHCP Mode | State (Food P) Cable/Dynamic IP (DHCP) |
| | Hostname PPPrE (ADSL) |
| inst up day on | LZTP |
| Primary DNS Server | Secondare DNS Server |
| | |
| | Next Back |
| | Next Back |

2)

| Wide Area Network (WWN) Settings | |
|----------------------------------|----------------------|
| | Static (Fixed IP) |
| | |
| | 192.168.3.1 |
| | 255.255.255.0 |
| | |
| DNS Settings (Optional) | |
| Primary DNS Server | Secondary DNS Server |
| - Next - | Back |

◆□IP Address—Sets the static IP address.

◆□Subnet Mask—Sets the static IP subnet mask. (Default: 255.255.255.0)

◆ **Default Gateway**—The IP address of a router that is used when the requested destination IP address is not on the local subnet.

◆ Primary DNS Server—The IP address of the Primary Domain Name Server. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses. To specify a DNS server, type the IP addresses in the text field provided. Otherwise, leave the text field blank.

◆□Secondary DNS Server — The IP address of the Secondary DomainName Server.

| 3) | |
|---------------------|--------------------|
| secure said 1 title | 😡 Help |
| Network Name (SSID) | SSID_NAME III 103a |
| secure wps choice | • |
| Security Mode | Disable • |
| Disable | |
| No Securi | |
| Done | ireless back |

Security Setup

Network Name (SSID) —SSID (Service Set Identification) must be assigned to all wireless devices in your network. Considering your wireless network security. Security Mode — Select the security method and then configure the required

parameters. (Options: Disabled, WEP-AUTO, WPA-PSK, WPA2-PSK, WPA-Auto-PSK, WPA, WPA2, WPA-Auto, 802.1X; Default: Disabled)

SETTINGS – CABLE/DYNAMIC IP (DHCP)

 Select Cable/Dynamic IP (DHCP), if your Internet service provider (ISP) use a DHCP service to assign your Router an IP address when connecting to the Internet.

| Wide Area Network (MIAN) Settings | |
|-----------------------------------|--|
| WAN Como | Cable Dynamic IP (DHCP) . |
| DHCP Mode | Static (Fixed IP) Cable Denamic IP (DHCP) |
| Hos | Insme PPPeE (ADSL) pptp 1700 |
| inet we das op | LEIP |
| Primary DNS Server | Secondary DHS Server |
| - No. | at Back |

2)

| =) | |
|----------------------------------|--------------------------|
| Wide Area Retwork (WAN) Selfunga | |
| WAN Connections | Cable/Dynamic IP (DTICP) |
| DBDP Mode | |
| Hostname | DHOP |
| | |
| mel wit das up | |
| Primary DNS Server | Secondary DNS Server |
| Next | Eack |

The host name that you selected from the DHCP service provider.

3)

| secure sold 1 title | telp |
|------------------------------------|------|
| Network Name (SSID) SSID_NAME Hide | |
| secure wps choice 📃 | |
| Security Mode Disable | |
| | |
| | |
| Done wireless back | |

Security Setup

Network Name (SSID) —SSID (Service Set Identification) must be assigned to all wireless devices in your network. Considering your wireless network security. Security Mode — Select the security method and then configure the required parameters. (Options: Disabled, WEP-AUTO, WPA-PSK, WPA2-PSK, WPA-Auto-PSK, WPA, WPA2, WPA-Auto, 802.1X; Default: Disabled)

SETTINGS - PPTP

1) Select PPTP, if you are using PPTP service to gain connection to the Internet.

| Wide Area Network (NIAN) Settings | |
|-----------------------------------|---|
| | WWW Connections Cable Dynamic IP (DHCP) . |
| | Static (Fixed IP) |
| DHCP Mode | Cable/Dynamic IP (DHCP) |
| | Hostsame popp |
| | LZTP |
| inet we das op | |
| Primary DNS Server | Secondary DHS Server |
| | |
| | Next Back |
| | |

2)

| Wide Area Hetwork (WAN) Settings | | | | _ |
|----------------------------------|------|------|--|---|
| | | PPTP | | |
| PPTP lilode | | | | |
| Server IP pptp_server | | | | |
| User Name pptp_user | | | Password | |
| Address Illode Dynamic 💌 | | | | |
| Operation Bode Keep Alive 💌 | | | Keep Alive Mode: Redial Period 60 Seco | |
| inet wc das op | | | | |
| Primary DNS Server | | | Secondary DNS Server | |
| | Next | Back | | |

- Server IP Sets the PPTP server IP Address. (Default: pptp_server)
- ◆□User Name Sets the PPTP user name for the WAN port.
- ◆ **Password** Sets a PPTP password for the WAN port.
- ◆ Address Mode Sets a PPTP network mode. (Default: Dynamic IP)
- ◆ **Operation Mode** Enables and configures the keep alive time.

◆ Primary DNS Server — The IP address of the Primary Domain Name Server. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses. To specify a DNS server, type the IP addresses in the text field provided. Otherwise, leave the text field blank.

◆ Secondary DNS Server — The IP address of the Secondary Domain Name Server.

3)

| secure ssid 1 little | Melp |
|----------------------|----------------|
| | SSID_NAME Hide |
| | • |
| | Disable |
| | |
| | |
| | |
| Done | ireless back |

Network Name (SSID) —SSID (Service Set Identification) must be assigned to all wireless devices in your network. Considering your wireless network security. Security Mode — Select the security method and then configure the required parameters. (Options: Disabled, WEP-AUTO, WPA-PSK, WPA2-PSK, WPA-Auto-PSK, WPA, WPA2, WPA-Auto, 802.1X; Default: Disabled)

SETTINGS – L2TP

Wilde Area Network (WIAN) Settings

WAN Connections

Cable Oynamic IP (DHCP)

Static (Fixed IP)
Cable Oynamic IP (DHCP)

Hostname
Primary DNS Server

Next
Back

1) Select L2TP, if you are using PPTP service to gain connection to the Internet.

2)

| Wilde Area Network (WWN) Settings | | |
|-----------------------------------|----------------------|---|
| | WAN Connections L2TP | • |
| L2TP Mode | | |
| Server IP 12tp_server | | |
| User Name 12tp_user | | Password |
| Address Illode Static 💌 | | |
| IP Address | | |
| Subnet Illank | | |
| Operation Hode Keep Alive 💌 | | Keep Alive Bode: Redial Period 60 Seconds |
| inst we dos op | | |
| Primary DNS Server | | Secondary DHS Server |
| | Next Back | |

- Server IP Sets the L2TP server IP Address. (Default: I2tp_server)
- ◆□User Name Sets the L2TP user name for the WAN port.
- ◆ Password Sets a L2TP password for the WAN port.
- ◆□Address Mode Sets a L2TP network mode. (Default: Dynamic IP)

• Operation Mode — Enables and configures the keep alive time.

◆ Primary DNS Server — The IP address of the Primary Domain Name Server. A DNS maps numerical IP addresses to domain names and canbe used to identify network hosts by familiar names instead of the IP addresses. To specify a DNS server, type the IP addresses in the text field provided. Otherwise, leave the text field blank.

◆□Secondary DNS Server — The IP address of the Secondary DomainName Server.

| 3) | | |
|---------------------|------------------------------------|--------|
| secure sold 1 title | | 设 Help |
| | Network Name (SSID) SSID_NAME Hide | |
| | secure wps choice 📃 | |
| | Security Mode Disable . | |
| Disable | | |
| | | |
| | Done wireless back | |

Network Name (SSID)—SSID (Service Set Identification) must be assigned to all wireless devices in your network. Considering your wireless network security. Security Mode — Select the security method and then configure the required parameters. (Options: Disabled, WEP-AUTO, WPA-PSK, WPA2-PSK, WPA-Auto-PSK, WPA, WPA2, WPA-Auto, 802.1X; Default: Disabled)

OPERATION MODE-AP BRIDGE

Choose menu "Easy Setup" and select AP Bridge if you want to configure to an access point.



2)

| secure ssid 1 title | Help |
|---------------------|----------------|
| | SSID_NAME HISH |
| | • |
| | Disable |
| | |
| | |
| Done | reless back |

Network Name (SSID) —SSID (Service Set Identification) must be assigned to all wireless devices in your network. Considering your wireless network security. Security Mode — Select the security method and then configure the required parameters. (Options: Disabled, Open, Shared, WEP-AUTO, WPA-PSK, WPA2-PSK, WPA2-PSK, WPA2, WPA1_WPA2, 802.1X;

OPERATION MODE-CLIENT ROUTER

In the Client Router mode is also known as WISP. The TUBE-2HQPwireless side is connected to the remote AP (Base-Station) as in Client Infrastructure mode. Between the wireless and LAN is the IP sharing router function. This is used to share Client Router connection. The WAN is on the wireless side.

| Operation Node Setup | | | |
|----------------------|---------------------------------|---------------------------------|--|
| | Please select an Operation Mode | Client Rooter | |
| | _ | Please select an Operation Mode | |
| | Nex | AP Router | |
| | | AP Undge | |
| | | Client Router | |
| | | Client Undge | |
| | | | |
| | | | |

2) Press Site Survey button and look for available wireless networkthen click on the SSID that you attempt to connect to it; Alfa_B is the SSID that we are going to connect in this example. PressNextbutton when finished.

| la List | | | | | | | | |
|------------------|--|--|---------------------------------------|---|-------------------|---|---|--|
| ict I | Profile S.S. | D BSSID | | Authentication | | Encryption | _ | Network Type |
| | | | | | | | No Wirele | ss Profile Rulest |
| costile cotor | | | | | | | | |
| prome setup | fia Name | | | | | urk Tune Jeferstre | | Cite Curvey |
| | | | | | | manada manada | | ane adivey |
| | SSID | | | | | optional) | | |
| | rity Hode Disa | bled 💌 | | | | | | |
| | rt settings | | _ | _ | | | | |
| | distance | | 0.7 | basic miles (1.1 | basic km | • | | |
| | ktimeout 35 | | | | | | | |
| | X Power | This field is require | ed. dBm | | | | | |
| | | | | minders be | ele. | | | |
| | | | | WE GIGSS DO | | | | |
| Teol Carried | De . | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | - 10 | | | and the second |
| Polite List | the second s | | | | | Encryption | | Network Type |
| Select | Profile | SSID BSSID | _ | Authenticatio | 4 | - care Jpoon | COLUMN DATE: NO. | |
| Select | Profile . | SSID BSSID | | Authenticatio | 0 | Constituted in | COLUMN TRANS | × |
| Select | Profile ss site survey | SSID BSSID | Rate | Authenbcatto | Changel | Authentication | Encryption | X |
| Select Select | Profile : ss site survey SSID Alfa II | BSSID BSSID D0:C0:CASE240cm | Rate | Authenbcatio | Channel | Authentication | Encryption TKIP/CCMP | X Network Type |
| Select | Profile ss site survey SSID Alfa_B AP121 | 55ID B55ID B55ID 00:C0:CA:5F:40:C2 00:C0:CA:60:48:E2 | Rate 11 Mb/s 54 Mb/s | Authenbcabo Signal Strength 8/94(-89.dBm) 50/94(-76.dBm) | Channel 6 | Authentication WPA1-Personal WPA2-Personal | Encryption TKIP/CCMP CCMP | Network Type Infrastructure Infrastructure |
| Select | Profile ss site survey SSID Alfa_8 AP121 Laser | 550 B550 B5510 00:C0:C4:5F:40:C2 00:C0:C4:50:48:E2 B0:48:74:85:01:C4 | Rate 11 Mb/s 54 Mb/s 54 Mb/s | Authenticatio Signal Strength 8/94(-89 dilm) 50/94(-76 dilm) 0/94(-95 dilm) | Channel 6 6 | Authentication WPA1-Personal WPA2-Personal WPA2-Personal | Encryption TKIP/CCMP CCMP CCMP | X Network Type Infrastructure Infrastructure Infrastructure |

it shows the Profile Name, SSID, BSSID, and encryption type received from your target network and press **Next** button to continue.

| prof curren | 1\$\$y | | | | | | |
|--------------|------------------|---------|------------------------|---------------------|-----------------|-----------------|----------------------|
| | | | | | | | |
| | | | | | | | |
| Pofile List | ļ. | | | | | | |
| Select | Profile | SSID | B S SID | Authentication | Encr | yption | Network Type |
| | | | | | | No Wi | reless Profile Rules |
| prof profile | setup | | | | | | |
| | Profile Name | Alfa_B | | | Network Type | Infarstrature 💌 | Site Survey |
| | SSID | Alfa_B | | | BSSID(optional) | 00.C0.CA.5F:40 | C2 |
| | Security Mode | WPA-PSK | | | Encryption | Auto(TKIP/CCM | P) 💌 |
| | Pass Phrase | | | | | | |
| basic ack t | limeout setting: | | | | | | |
| | asic distance | | 0.7 | basic miles (1.1 ba | ssic km) | | |
| basi | ic acktimeout | 35 | | | | | |
| | TX Power | The | Tield in required. dBm | | | | |
| | | | Next | wireless bad | sk 🔄 | | |
| | | | | | | | |

3) Finally, you need to tell the system about IP address received from WAN, DHCP

| Hostname, and DNS Server then press Next bu | utton to finish the wizard. |
|---|-----------------------------|
|---|-----------------------------|

| Wide Area Network (WAN) Settings | WAN Connections Calde/Dynamic IP (DHCP) |
|----------------------------------|---|
| DHCP Mode | Destaura 10.055 |
| Inct we day op | |
| Pomory DBS Server | Secondary DHS Server |
| | Next Hark |

OPERATION MODE-CLIENT BRIDGE

In the Client Bridgemode yourTUBE-2HQPwill behave just the same as Wireless adapter. With Client Bridges, the WLAN and the LAN are on the same subnet. Consequently, NAT is no longer used and services that are running on the original network.



2) Press Site Survey button and look for available wireless networkthen click on the SSID that you attempt to connect to it; Alfa_B is the SSID that we are going to connect in this example. PressNextbutton when finished.

| prof currently | y . | | | | | | |
|----------------|---------------|-------------------|-------------|------------------|-----------------|----------------|--------------|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| Select | Profile | 5510 05510 | | Authentication | Encry | plion | Network Type |
| | | | | | | | |
| prof profile s | | | | | | | |
| | Profile Name | | | | Network Type | nfarstrature 💌 | Site Survey |
| | S SID | | | | BSSID(optional) | | |
| | ecarity Mode | Disabled • | | | | | |
| | | | | | | | |
| | isic distance | | 0.7 | basic miles (1.1 | basic km) | | |
| | c acktimeout | 35 | | | | | |
| | TX Power | This field is req | uired dilim | | | | |
| | | | Next | wireless bac | ck | | |

| Polile List | 1 | | | | | | | | |
|------------------|---|--------------------------|-----------------------------|----------------------------|--|-------------------|--|---------------------------------|--------------------------------|
| Enlarge Colorest | Profile | SSID | BSSID | | Authenticatio | 0 | Encryption | | Network Type |
| prof wireles | ss site survey | | | _ | | _ | | | |
| prof wireles | ss site survey | | BSSID | Rate | Signal Strength | Channel | Autbentication | Encryption | Network Type |
| prof wireles | ss site survey SSID Alfa_ii | 00:C0:CA:5 | ESSID F:40:02 | Rate 11Mb/s | Signal Strength 8/94(-89 dBm) | Channel 6 | Authentication | Encryption TKIP/CCMP | Network Type |
| select | ss site survey SSID Alfa_B AP121 | 00:C0:C4:5 00:C0:C4:6 | ESS1D F:40:C2 0:48:E2 | Rate 11 Mb/s 54 Mb/s | Signal Strength B/94(-89 dBm) 50/94(-76 dBm) | Channel 6 6 | Authentication WPA1-Personal WPA2-Personal | Encryption TKIP/CCMP CCMP | Network Type Infrastructure |

3) Now, it shows the Profile Name, SSID, BSSID, and encryption type received from your target network and press **Next** button to finish the wizard.

| prof curren | thy in class | | | | | | |
|--------------|-----------------|---------|------------------------|----------------------|--------------------|---------------|---------------------|
| | | | | | | | |
| Pofile List | | | | | | | |
| Select | Profile | SSID | BSSID | Authentication | Елстурі | ion | Network Type |
| | | | | | | No Wir | eless Profile Rules |
| prof profile | setup | | | | | | |
| | Profile Name | Alfa_B | | | Network Type | arstrature 💌 | Site Survey |
| | SSID | Alfa_B | | | BSSID(optional) 00 | C0 CA 5F 40 | 2 |
| | ecurity Mode | WPA-PSK | | | Encryption A | uto(TKIP/CCMP | 0 🖃 |
| | Pass Phrase | | | | | | |
| basic ack 0 | ineout settings | | | | | | |
| br | ssic distance | | 0.7 | basic miles (1.1 bas | iic km) | | |
| basi | c acktimeout | 35 | | | | | |
| | TX Power | 7/10 | field is required. dBm | | | | |
| | | | Next | wireless back | | | |

ADVANCED SETUP

In the Advanced Manual Bar, it includes all the settings such as firmware upgrade, LAN, WAN and wireless settings that change the RF behaviors. It is important to read through this section before attempting to make changes.

| Advanced |
|-----------------------|
| Management |
| Advanced Settings |
| Operation Mode |
| System Log |
| Tools |
| Firewall Settings |
| MAC/IP/Port Filtering |
| Virtual Server |
| DMZ |
| Firewall |
| QoS |
| Content Filtering |
| Network Settings |
| WAN |
| LAN |
| VLAN |
| DHCP Static Leases |
| Advanced Routing |
| Wireless Settings |
| Basic |
| Advanced |

MANAGEMENT

The Management section is provided for configuration of administrative needs such as language type, user name / Password, firmware upgrade, export and import settings, load factory defaults and reboots system.

| System Herugerssell | | | | | | | | |
|------------------------|------------------|-----------------|-----------------------|----------------|-------------------|--|--|--|
| Wab Interface Settings | Freemark Upprade | Configuration . | Load Factory Defailts | Autoost System | Schululing Nation | | | |
| | | | admin | | | | | |
| | | | | | | | | |
| | | | ADDY | | | | | |
| | | | | | | | | |

◆□**Password** — The new password must not exceed 32 characters in length and must not include any spaces. Enter the new password a second time to confirm it.

| Nah Interface Saltings | ermane läpyrade | Configuration | Load Pactory Delpatts | Robert Sector |
|------------------------|-----------------|----------------------------|----------------------------|---------------|
| | | a version V2.5 1 Second | 912-66-27-1305 Bitterre | |
| | | 001030 | | |

Software Version - This displays the current firmware version.

To upgrade the Router's firmware, follow these instructions below:

- 1. Download a more recent firmware upgrade file from our website.
- 2. Type the path and file name of the update file into the **File** field. Or click the **Browse** button to locate the update file.
- 3. Click the Upgrade button.

Note:

- New firmware versions are posted at our website and can be downloaded for free. There is no need to upgrade the firmware unless the new firmware has a new feature you want to use. However, when experiencing problems caused by the Router rather than the configuration, you can try to upgrade the firmware.
- 2. When you upgrade the Router's firmware, you may lose its current configurations, so before upgrading the firmware please write down some of your customized settings to avoid losing important settings.
- 3. Do not turn off the Router or press the Reset button while the firmware is being upgraded, otherwise, the Router may be damaged.
- 4. The Router will reboot after the upgrading has been finished.

| liek Interface Settings | Faceware Opprada | Configuration | Load Factory Defaults | Robust Epitano | Schubulog Auburt |
|-------------------------|------------------|---------------|-----------------------|----------------|------------------|
| | Kepert | | Report. | | |
| | | | Import. | Browse | |
| | | | Digost. | | |

• Export Settings — Click the Export Button to download current router configuration to your PC.

◆□Import Settings — Click the Import Button to browse for the configuration file that is currently saved on your PC. Click Import to overwrite all current configurations with the one in the configuration file.

| | ay a real of the managements | | | | |
|---|------------------------------|-----------------------------------|-----------------------|---------------|--------------------|
| l | Web Interface Settings | Ferriware Oppsale - Configuration | total Entury Defaults | Reland System | Scholulury Related |
| | | | Load Default | | |

◆□Load Factory Defaults — If you have problems with TUBE-2HQP, which might be a result from changing some settings, but you are unsure what settings exactly, you can restore the factory defaults by click the Load Default Button.

| System Management | | | | | |
|------------------------|------------------|---------------|-----------------------|---------------|-------------------|
| Web Interface Settings | Firmware Upgrade | Configuration | Load Factory Defaults | Reboot System | Scheduling Reboot |
| | | Reboot System | Refront Now1 | | |

◆□**Reboot System** — If you want to reboot the TUBE-2HQP, click the Reboot Now Button.

ADVANCED SETTINGS

The Advanced Settings section is provided for configuration of Time Zone, DDNS, UPnP, SNMP, and SSH.



◆□**Time Zone Settings**— The Time Zone Settings allows you to configure, update and maintain the correct time on the TUBE-2HQP's internal system clock.

◆□SNTP Server — Enter the address of an SNTP server to receive time updates.

◆□SNTP synchronization (minutes) — Specify the interval between SNTP server updates.

| Baie Zone Bellings Triffel Berlings UPAR Said | dags Ann fallings. And fallings. | |
|---|---|--|
| | North any Section of Contract | |

DDNS Settings — DDNS lets you assign a fixed host and domain name to dynamic Internet IP address. It is useful when you are hosting your own website, FTP server, or other server behind the TUBE-2HQP. Before using this feature, you need to sign up for DDNS service at <u>www.dyndns.org</u>, a DDNS service provider.

- ◆□User Name Sets the DDNS user name for the connection.
- ◆□**Password** Sets a DDNS password for the connection.
- ◆□HostName The host name that you selected from the DDNS service provider.

| Annual Indiana | | | | | |
|--------------------|---------------|-----------------|----------------|---------------|--|
| Nam. Your Settings | DONI Settings | Linker Saltings | Salat Settings | - HAR BARDoop | |
| | | | . 14894 | | |

UPNP Settings- UPnP permits network devices to discover other network device(s) preference and establish functional network services for data sharing, communication, and entrainment. Default setting is Disabled.



SNMP Settings-Managing devices on IP networks. Default setting is Disabled.



SSH Settings-Secure Shell. Enable your TUBE-2HQPunit to access secure shell (SSH) based network device. Default setting is Disabled.

OPERATION MODE

The Operation Mode content four modes: AP Bridge, AP Router, Client Router and Client Bridge.

| aliana . | | Advanced | Eight + |
|-----------------------------|----------|---|---------|
| Deverties Multi-Containment | | | |
| | -Apple - | AP Roder AP Bridge Clerit Riadar Clerit Riadar Clerit Ridge | |

◆ AP Bridge— The wired Ethernet and wireless are bridged together. Once the mode is selected, all WAN related functions will be disabled.

◆ **AP Router**—The Ethernet port will convert into WAN port requiring you to configure your CPE via WLAN.

◆ Client Router—TheTUBE-2HQPwill behave just the same as the client mode for wireless function. However, router functions are added between the wireless WAN side and the Ethernet LAN side. Therefore, the WSIP subscriber can share the WISP connection without the extra router.

Client Bridge—TheTUBE-2HQPwill behave just the sameas Wireless adapter.With Client Bridges, the WLAN and the LAN are on the same subnet. Consequently, NAT is no longer used and services that are running on the original network.

FIREWALL CONFIGURATION

MAC/IP/PORT FILTERING

MAC/IP/Port filtering restricts connection parameters to limit the risk of intrusion

and defends against a wide array of common hacker attacks. MAC/IP/Port filtering allows the unit to permit, deny or proxy traffic through its MAC addresses, IP addresses and ports. The TUBE-2HQPallows you define a sequential list of permit or deny filtering rules. This device tests ingress packets against the filter rules one by one. A packet will be accepted as soon as it matches a permit rule, or dropped as soon as it matches a deny rule. If no rules match, the packet is either accepted or dropped depending on the default policy setting.

| Adama (| - | Tana Se | 2000 | Advant | ced i | Lange of the | Fish (+) |
|--------------------------|-------------------|-------------|--------------------|-------------------|-----------|--------------|----------|
| Dist Settion | | | | | | | |
| 10 | HICE THE FREE | Disable (*) | Distant Distant | Name: Dept. (Dev | Accepted | | |
| | | | | | | | |
| | | | A2019 | 1001.1 | | | |
| · Correlati Desical | Print Marry rates | | | | | | |
| RACES INTO | WCat | Araba IBP | 3.07 Protec | 10 109 | 579 Au/20 | Cienters | 10 |
| Others would be accepted | | | | | | | |

◆□MAC/IP/Port Filtering— Enables or disables MAC/IP/Port Filtering.

(Default: Disable)

◆ Default Policy — When MAC/IP/Port Filtering is enabled, the default policy will be enabled. If you set the default policy to "Dropped", all incoming packets that don't match the rules will be dropped. If the policy is set to "Accepted," all incoming packets that don't match the rules are accepted. (Default: Dropped)

- ◆ MAC Address Specifies the MAC address to block or allow traffic from.
- ◆□DIP—Specifies the destination IP address to block or allow traffic from.
- ◆□SIP—Specifies the source IP address to block or allow traffic from.

◆□Protocol — Specifies the destination port type, TCP, UDP or ICMP.

◆ **Destination Port Range** — Specifies the range of destination port to block traffic from the specified LAN IP address from reaching.

◆ Source Port Range — Specifies the range of source port to block traffic from the specified LAN IP address from reaching.

- ◆□Action Specifies if traffic should be accepted or dropped. (Default: Accept)
- **Comment** Enter a useful comment to help identify the filtering rules.

◆ **Current Filtering rules**— The Current Filter Table displays the configured IP addresses and ports that are permitted or denied access to and from.

- > No. The table entry number.
- > MAC Address Displays a MAC address to filter.
- > Destination IP Address (DIP)— Displays the destination IP address.
- Source IP Address (SIP)— Displays the source IP address.
- > **Protocol** Displays the protocol type.
- > **Destination Port Range (DPR)** Displays the destination port range.
- Source Port Range (SPR) Displays the source port range.

- > Action Displays if the specified traffic is accepted or dropped.
- **Comment** Displays a useful comment to identify the filter rules.

VIRTUAL SERVER SETTINGS

Virtual Server (sometimes referred to as Port Forwarding) is the act of forwarding traffic from one network node to another based on received protocol port number. This technique can allow an external user to reach a port on a private IP address (inside a LAN) from the outside through a NATenabled router.

| Virtual Server | | | | |
|------------------------|--------------|-------------------------|----------|--------|
| | | Virtual Server Enable - | | |
| Apply | | | | |
| Virtual Server Setting | te | | | |
| | | IP Address | | |
| | | Private Port | | |
| | | Public Port | | |
| | | Protocol TCP&UDP | | |
| | | Comment | | |
| | | | | |
| | | Apply Reset | | |
| Current Virtual Serve | rs in system | | | |
| No. | IP Address | Port Mapping | Protocol | Commen |
| | | Delete Selected Reset | | |

◆ Virtual Server — Selects between enabling or disabling port forwarding the virtual server. (Default: Disable)

◆ **IP Address** — Specifies the IP address of a server on the local network to allow external access.

- ◆□Private Port The protocol port number on the local server.
- ◆□Public Port The protocol port number on the router's WAN interface.
- ◆ Protocol Specifies the protocol to forward, either TCP, UDP, or TCP&UDP.

◆ **Comment** — Enter a useful comment to help identify the port forwarding service on the network.

◆ **Current Virtual Servers in System**— The Current Port Forwarding Table displays the entries that are allowed to forward packets through the TUBE-2HQP's firewall.

- > No. The table entry number.
- IP Address The IP address of a server on the local network to allow external access.

- > **Port Mapping** displays the port mapping for the server.
- > **Protocol** Displays the protocol used for forwarding this port.
- Comment Displays a useful comment to identify the nature of the port to be forwarded.

DMZ

DMZ is to specified host PC on the local network to access the Internet without any firewall protection. Some Internet applications, such as interactive games or video conferencing, may not function properly behind the firewall. By specifying a Demilitarized Zone(DMZ) host, the PC's TCP ports are completely exposed to the Internet, allowing open two-way communication. The host PC should be assigned astatic IP address (which is mapped to its MAC address) and this must beconfigured as the DMZ IP address.

| DNZ Settings | |
|----------------|----------|
| DNZ Settings | Fraile x |
| DMZ IP Address | |
| | |
| Apply | Reset |
| | |
| | |

• DMZ Settings — Sets the DMZ status. (Default: Disable)

◆ **DMZ IP Address** — Specifies an IP address on the local network allowed unblocked access to the WAN.

FIREWALL

Firewall functions which will help to protect your network and computer. You can utilized firmware functions to protect your network from hackers and malicious intruders.

| Remote Management Access | |
|--------------------------------------|--------------|
| Remote Management (via WAN) | Deny 💌 |
| Remote Management Port | 2020 |
| Pies from WAN Filter | |
| Ping from WAN Filter | Allow . |
| | |
| Stateful Packet Inspection (SPI) | |
| SPI Firewall | Disable • |
| | |
| Network Address Translation Settings | |
| Network Address Translation | Enable 💌 [7] |
| | |
| PPPoE Passthrough Settings | |
| PPPoE Passthrough Setup | Disable - |
| | |
| Apply | Reset |

◆ **Remote Management (via WAN)**— allow or deny to manage the router from anywhere on the Internet.

◆□Remote Management Port— The port that you will use to address the management from the Internet. For example, if you specify port 2020, then to access the TUBE-2HQPfrom Internet, you would use a URL of the form: http://xxx.xxx.xxx.xxx.2020/

◆ Ping from WAN Filter — When Allow, the TUBE-2HQPdoes not respond to ping packets received on the WAN port.

◆□SPI Firewall — SIP firewall help to keep track of the state of network connections (such as TCP streams, UDP communication) traveling across it. It is programmed to distinguish legitimate packets for different types of connections. Only packets matching a known active connection will be allowed by the firewall; others will be rejected.

◆□Network Address Translation — NAT is the process of modifying IP address information in IP packet headers while in transit across a traffic routing device.

CONTENT FILTERING

The TUBE-2HQPprovides a variety of options for blocking Internet access based on content, URL and host name.

| CONTRACT PART, BARDINGS. | | |
|--------------------------|------------------------------|--|
| Webs URL Filter Settlegs | Wids Buit Filter Settings | |
| Lineast Web URL Ellins | | |
| 1.000 | 181. | |
| | Delirte Beent | |
| | Add a till filles supp(s):// | |
| | Add Reset | |
| | | |
| | | |

◆ Web URL Filter Settings — By filtering inbound Uniform Resource Locators (URLs) the risk of compromising the network can be reduced. URLs are commonly used to point to websites. By specifying a URL or a keyword contained in a URL traffic from that site may be blocked.

- ◆□Current URL Filters Displays current URL filter.
- \square Add a URL Filter Adds a URL filter to the settings.
- ◆ Delete a URL Filter Deletes a URL filter entry from the list.

◆ Web Host Filter Settings — AllowsInternet content access to be restricted based on web address keywords and web domains. A domain name is the name of a particular web site. For example, for the address www.HOST.com, the domain name is HOST.com. Enter the Keyword then click "Add."

- ◆□Current Host Filters Displays current Host filter.
- ◆ Add a Host Filter Enters the keyword for a host filtering.
- ◆ **Delete a Host Filter** Deletes a Host filter entry from the list.

| Wides URL Filter Settings | Webs Hust Filter Settings | |
|-----------------------------|---------------------------|---|
| Correct Malanta intel Ellip | | |
| 80 | | Host (Keyword) |
| | Defets | Reset |
| | And a limit Descented T | |
| | CONTRACTOR OF THE | and the second se |
| | Add. | Revel |
| | | |

NETWORK SETTINGS

WAN

In this section, there are several connection types to choose from; Static IP, DHCP, PPPoE, PPTP and L2TP. If you are unsure of your connection method, please contact your Internet Service Provider.

CABLE/DYNAMIC IP (DHCP)

| ()) | Weit & the Barborn (1998) Linkson |
|--|--|
| | Gita Type in P (D40*) + |
| | Service Se |
| | our our |
| The second se | Contraction of the second s |
| SAS In the Life Avenue, and a second s | |
| Contraction of the local division of the loc | Senter(3) See |
| | |
| | and the second se |

◆□Hostname — Specifies the host name of the DHCP client.

◆ Primary DNS Server — The IP address of the Primary Domain Name Server. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses. To specify a DNS server, type the IP addresses in the text field provided. Otherwise, leave the text field blank.

◆ Secondary DNS Server — The IP address of the Secondary Domain Name Server.

PPPoE (ADSL)

| | | ctores PPPuE (ADSL) | |
|---------------------|-----------------------------|---------------------|-----------------------|
| | | | |
| | User Same popoe_user | | |
| | Passavel | Tertly Password | |
| | Operation Hode Keep Aline • | | tar Period 60 Seconds |
| | 1432 tyles (Default-1482) | | |
| | | | |
| Primary 2015 Server | Secondary 2013 Serve | | |
| | Acci | y Cancel | |

◆□User Name — Sets the PPPoE user name for the WAN port.

◆ Password — Sets a PPPoE password for the WAN port.

◆□Verify Password — Prompts you to re-enter your chosen password.

◆ **Operation Mode** — Enables and configures the keep alive time and configures the on-demand idle time.

STATIC IP (FIXED IP)

| | Wikit Connections Static (Fixed IP) |
|--------------------|-------------------------------------|
| | |
| | IP AADINGS 192,168.3.1 |
| | Subout Marak 255 255 0 |
| | default Gateway |
| | |
| Primary DRS Server | Secondary DRS Server |
| | |
| | Apply Cancel |
| | |

◆□IP Address—Sets the static IP address.

◆□Subnet Mask—Sets the static IP subnet mask. (Default: 255.255.255.0)

• Default Gateway—The IP address of a router that is used when the requested destination IP address is not on the local subnet.

◆□Primary DNS Server—The IP address of the Primary Domain Name Server. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses. To specify a DNS server, type the IP addresses in the text field provided. Otherwise, leave the text field blank.

◆□Secondary DNS Server — The IP address of the Secondary DomainName Server.

PPTP

| PPTP Mode | |
|---------------------------|---|
| Server IP pptp_server | |
| User Name pptp_user | Password |
| Address IIode Static IP 📼 | |
| IP Address | |
| Subnet Illask | |
| Operation Bode Keep Alve | Keep Alive Mode: Redial Period 60 Seconds |
| DHS Settings (Optional) | |
| Primary DNS Server | Secondary DHS Server |
| | Apply Cancel |

Server IP — Sets the PPTP server IP Address. (Default: pptp_server)

User Name — Sets the PPTP user name for the WAN port.

Password — Sets a PPTP password for the WAN port.

Address Mode — Sets a PPTP network mode. (Default: Dynamic IP)

◆□Operation Mode — Enables and configures the keep alive time.

◆ Primary DNS Server — The IP address of the Primary Domain Name Server. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses. To specify a DNS server, type the IP addresses in the text field provided. Otherwise, leave the text field blank.

Secondary DNS Server — The IP address of the Secondary Domain Name Server.

IPSec

| Wide Area Network (Wikit) Settings | |
|--|----------------------------|
| WHIT CO | mections (PSSC . |
| was ipoe: mode | |
| Connection addresss family Pod • | IP fact Operation Hode add |
| Plac Connection Type Road Warriar Tunnel . | PES(DH Group madp1024 - |
| Plac Authentication 2014-1 # | #SecEnception AES |
| SA connection Life Time Nours | NE Kep Tota 3 Times |
| Local IP Address | Peer IP Address |
| Local Subset | Poer Subset |
| Local Gateway | Pour Gateway |
| 895ec Tutmel Name accCCNN | Plac Secret Ray |
| 1P Sec Key Life Sine 12h hours | |
| NAT Transversal | Perfect Forward Secrets |
| 19 Sec Compression 📃 | Páec Com. Reep Alve |
| Plac 1 | hanned UP |
| DHS Settings (Optional) | |
| Primary DRS Server Secondary DRS Se | ner |
| | pply Cancel |

Verify the desire settings and use scroll down for more options.

- IPSec Connection Type –Use drop down menu to select from Road Warrior Tunnel, Host to Host Tunnel, Subnet to Subnet Tunnel, Host to Host Transport, Pass trough, Drop, or Reject. Default setting is Road Warrior Tunnel
- ◆□IPSec Authentication- Use drop down menu to select from SHA-1, or MD5. Default setting is SHA1.
- SA Connection Life Time –Specify how often each SA should be rekeyed, measured in hour.
- Local IP address / Subnet / Gateway–Local end point IP address, Subnet, and Gateway IP address.
- ◆□IPSec Operation Mode Use drop down menu to select from Add, Route Start, Manual, or Ignore. Default setting is Add.
- IKE Key Retry–Specify maximum retry limits for negotiate key to Internet Key Exchange.

◆□Peer IP address / Subnet / Gateway –Remote end point IP address, Subnet, and Gateway IP address.

L2TP

| L2TP Node | |
|-----------------------------|---|
| Server IP 12tp_server | |
| User Name 12tp_user | Password |
| Address Mode Static IP • | |
| IP Address | |
| Subnot Mask | |
| Operation Mode Keep Alive • | Keep Alive Mode: Redial Period 60 Seconds |
| DNS Settings (Optional) | |
| Primary DNS Server | Secondary DNS Server |
| | Apply Cancel |

- Server IP Sets the L2TP server IP Address. (Default: I2tp_server)
- ◆□User Name Sets the L2TP user name for the WAN port.
- ◆□Password Sets a L2TP password for the WAN port.
- ◆ Address Mode Sets a L2TP network mode. (Default: Dynamic IP)
- ◆□Operation Mode Enables and configures the keep alive time.

◆□Primary DNS Server — The IP address of the Primary Domain Name Server. A DNS maps numerical IP addresses to domain names and canbe used to identify network hosts by familiar names instead of the IP addresses. To specify a DNS server, type the IP addresses in the text field provided. Otherwise, leave the text field blank.

Secondary DNS Server — The IP address of the Secondary DomainName Server.

LAN

In this section, the LAN settings are configured based on the IP Address and Subnet Mask. The IP address is also used to access this Web-based management interface. It is recommended to use the default settings if you do not have an existing network.

| LAN Setup | |
|------------------------------|-------------------|
| IIAC Address | 00-C0-CA-S0-BB-AC |
| IP Address | 152.168.2.1 |
| Subnot Mask | 255.255.255.0 |
| DHCP Selup | |
| DHCP Server | DHCP Server . |
| Local Domain Name (Optional) | |
| Start IP Address | 192.168.2.100 |
| End IP Address | 192.168.2.199 |
| Lease Time | One day • |
| Apply | Cancel |

 \square IP Address — The IP address of TUBE-2HQPon the local area network.

(Default: 192.168.2.1)

Subnet Mask— The subnet mask of TUBE-2HQPon the local area network

◆ **DHCP Server**— The DHCP Server is to assign private IP address to the

TUBE-2HQPin your local area network(LAN). The default LAN IP address is

192.168.2.1, changing IP address will also change the DHCP server's IP subnet.

ADVANCED ROUTING

In this section, allow to configure routing feature in the TUBE-2HQP.

| Millia mell | na ren | Der | distantia | | | | | | |
|-----------------------------|---|---|----------------------------------|-----------------------------|--------------|---------------|------------------|--------------------------------|--------|
| | | | We Ho | et et | | | | | |
| | | | and the second second | | | | | | |
| | | | and LA | N 💌 | | | | | |
| | | | and the second second | | | | | | |
| | | | | - | | | | | |
| | | A | ppiy. | THEFT | | | | | |
| | | | | | | | | | |
| Contract on the | | | | | | | | | |
| No. | ding labir in the options Destination | Autoank | Gateway | -Raga | Matric | Ref | Use | Interface | Commun |
| arient fil NO. 1 | Uniq table in the option 1 Desteamon 1965/15205.255 | Averaitik 205.255.255.255 | Galeway 0000 | Rapp S | Montic D | | U140 0 | LAN(brit) | Commo |
| No. Contraction | Desidentian Desidentian 265/255/255/255 192/168/2/0 | Annualità 205 255 255 255 2 255 255 255 2 | Gateway 00000 100000 | torp 5 | Matric 0 | 0 0 | Use 0 0 | LINGTONO LAN(MO) LAN(MO) | Commun |
| NU | Dentitution Dentitution 265255265255 182108.2.0 | Normana 205 255 265 265 215 255 255 0 | Galeway 0000 0000 | Rep 5 | Shattic D | 9 0 | 0100 01 01 | LAN(bro) | Commun |
| NA. NA. NI. | Destination Destination 2052/05/205/205 192/108/2/0 | Normana 205 255 255 255 255 255 255 2 255 255 255 | Gateway 0000 0000 siste | Report | Mettic D | Rut Q 0 | 0 0 0 | LAN(DIO) | Commu |
| | Destination Destination 205295205255 1921082.0 | 1000000 205 255 255 255 255 255 255 2 255 255 255 | Galeway 0000 0000 sista | Filippi S T Resolt | Metric C | 0 0 | 0 | LAN(DO) | Commen |
| | Denteuton Denteuton 265 255 255 255 192 108 2 0 | Normana 255 255 255 255 255 255 255 2 255 255 2 | Gateway 0000 0000 sista | Report | Matric D | Rut Q Q | 0 | LAN(br0) | Commu |
| Terrent To NO. 1 2 | Ching bable in the operation Desidentical 255 255 255 255 192 108 2 0 192 108 2 0 | Normalia 205 255 255 255 255 215 255 255 255 0 215 255 255 2 | Gateway 0000 0000 sista | Resol | Namic O | 9 9 0 | Utw O | LAN(br0) | Commu |

◆ **Destination** — The IP addressof packets that can be routed.

◆□**Type**— Defines the type of destination. (Host: Signal IP address / Net: Portion of Network)

- ◆ **Netmask** Displays the subnetwork associated with the destination.
- ◆□Gateway— Defines the packets destination next hop

◆□Interface— Select interface to which a static routing subnet is to be applied

◆□Comment— Help identify the routing

◆□**RIP**—Enable or disable the RIP(Routing Information Protocol) for the WAN or LAN interface.

WIRELESS SETTINGS

BASIC

| Basic Wireless Settings | |
|--------------------------|--------------------------|
| | Access Point |
| | • |
| | Germany Set Country Code |
| | 2437 MHz (Channel 6) |
| | Scan |
| | WiFi 11gn HT20 • |
| | Upper Channel - |
| | 0.8 miles (km) |
| ACK Timeout | 36 |
| SSID Security Settings | |
| | SSID NAME Hide |
| | • |
| | Disable |
| Apply | Cancel |

◆ Wireless On/Off — Enables or Disable the radio. (Default: Turn On)

♦□Wireless Mode — There are 4 wireless mode, those are Access Point, WDS Access Point, WDS Repeater and WDS Client

Note.

If WEP authentication is selected for WDS communication, you will then only have one set of encryption for the entire channel.

◆□Network Name (SSID) — The name of the wireless network service provided by the TUBE-2HQP. Clients that want to connectto the network must set their SSID to the same as that of TUBE-2HQP.

◆ Multiple SSID — One additional VAP interface supported on the device.

• Frequency (Channel) — The radio channel that the TUBE-2HQPuses to communicate with wireless clients.

◆□Network Mode — Defines the radio operating mode.

SECURITY

| SSID I Security Settings | |
|--------------------------|--|
| Network Name (SSID) | SSID NAME 105 |
| WPS Chaice | • |
| Encryption Settings | Disable |
| Apply | Disable WEPA-AUTO WPA-PSK WPA2 WPA2PSK WPA-AUTO WPA-AUTO-PSK 802.1x |

WIRED EQUIVALENTPRIVACY (WEP)

WEP provides a basic level of security, preventing unauthorized access to the network, and encrypting data transmitted between wireless clients and an access point. WEP uses static shared keys (fixed-length hexadecimal or alphanumeric strings) that are manually distributed to all clients that want to use the network. When you select to use WEP, be sure to define at least one static WEP key for user authentication or data encryption. Also, be sure that the WEP shared keys are the same for each client in the wireless network.



◆ WEP-AUTO — Allows wireless clients to connect to the network using Open-WEP (uses WEP for encryption only) or Shared-WEP (uses WEP for authentication and encryption).

◆□Encrypt Type — Selects WEP for data encryption (OPEN mode only).

◆ Security Key Index — Selects the WEP key number to use for authentication or data encryption. If wireless clients have all four WEP keys configured to the same values, you can change the encryption key to any of the settings without having to update the client keys.

◆ WEP Keys — Sets WEP key values. The user must first select ASCII or hexadecimal keys. Each WEP key has an index number. Enter key values that match the key type and length settings. Enter 5 alphanumeric characters or 10 hexadecimal digits for 64-bit keys, or enter 13 alphanumeric characters or 26 hexadecimal digits for 128-bit keys. (Default: Hex, no preset value)

Note.

If WEP authentication is selected for WDS communication, you will then only have one set of encryption for the entire channel.

WPA & WPA2

Wi-Fi Protected Access (WPA) was introduced as an interim solution for the vulnerability of WEP pending the adoption of a more robust wireless security standard. WPA2 includes the complete wireless security standard, but also offers backward compatibility with WPA.

| SID I Security Settings |
|--|
| Network Name (SSID) SSID NAME 10de |
| WPS Choice |
| Encryption Settings WPA |
| WPA Algorithms 🕒 TKIP 🔯 O CCMP(AES) 🔍 Auto |
| Key Renewal Interval(Secconds) 60 |
| IP Address |
| Port |
| Shared Secret |
| Apply Cancel |

◆□WPA — Clients using WPA for authentication.

◆□WPA2 — Clients using WPA2 for authentication.

◆□WPA-Auto— Clients using WPA or WPA2 for authentication.

◆ **WPA Algorithms** — Selects the data encryption type to use. (Default is determined by the Security Mode selected.)

TKIP — Uses Temporal Key Integrity Protocol (TKIP) keys for encryption. WPA specifies TKIP as the data encryption method to replace WEP. TKIP avoids the problems of WEP static keys by dynamically changing data encryption keys.

■ AES — Uses Advanced Encryption Standard (AES) keys for encryption. WPA2 uses AES Counter-Mode encryption with Cipher Block Chaining Message Authentication Code (CBC-MAC) for message integrity. The AES Counter-Mode/CBCMAC Protocol (AESCCMP) provides extremely robust data confidentiality using a 128- bit key. Use of AES-CCMP encryption is specified as a standard requirement for WPA2. Before implementing WPA2 in the network, be sure client devices are upgraded to WPA2-compliant hardware.

■ Auto Uses either TKIP or AES keys for encryption. WPA and WPA2 mixed modes allow both WPA and WPA2 clients to associate to a common SSID. In mixed mode, the unicast encryption type (TKIP or AES) is negotiated for each client.

• Key Renewal Interval — Sets the time period for automatically changing data encryption keys and redistributing them to all connected clients.

RADIUS Server — Configures RADIUS server settings.

◆□IP Address — Specifies the IP address of the RADIUS server.

◆□Port — The User Datagram Protocol (UDP) port number used by the

RADIUS server for authentication messages. (Range: 1024-65535; Default: 1812) **Shared Secret** — A shared text string used to encrypt messages between the access point and the RADIUS server. Be sure that the same text string is specified on the RADIUS server. Do not use blank spaces in the string. (Maximum length: 20 characters)

WPA-PSK & WPA2-PSK

Wi-Fi Protected Access (WPA) was introduced as an interim solution for the vulnerability of WEP pending the adoption of a more robust wireless security standard. WPA2 includes the complete wireless security standard, but also offers backward compatibility with WPA. For small home or office networks, WPA and WPA2 provide a simple "personal" operating mode that uses just a pre-shared key for network access. The **WPA Pre-Shared Key (WPA-PSK)** mode uses a common password phrase for user authentication that is manually entered on the access point and all wireless clients. Data encryption keys are automatically generated by the access point and distributed to all clients connected to the network.

| SSID1 Security Settings | |
|-------------------------|---------------------------|
| | SSID NAME |
| | • |
| | WPA2-PSK |
| | THEP [7] O COMPLAES) Auto |
| | 60 |
| | Generator |
| Apply | Cancel |
| | |

◆□WPA-PSK — Clients using WPA with a Pre-shared Key are accepted for authentication.

◆□WPA2-PSK — Clients using WPA2 with a Pre-shared Key are accepted for authentication.

◆□WPA- Auto-PSK — Clients using WPA or WPA2 with a Preshared

Key are accepted for authentication. The default data encryption type is TKIP/AES.

◆ **WPA Algorithms** — Selects the data encryption type to use. (Default is determined by the Security Mode selected.)

TKIP — Uses Temporal Key Integrity Protocol (TKIP) keys for encryption. WPA specifies TKIP as the data encryption method to replace WEP. TKIP avoids the problems of WEP static keys by dynamically changing data encryption keys.

■ AES — Uses Advanced Encryption Standard (AES) keys for encryption. WPA2 uses AES Counter-Mode encryption with Cipher Block Chaining Message Authentication Code (CBC-MAC) for message integrity. The AES Counter-Mode/CBCMAC Protocol (AESCCMP) provides extremely robust data confidentiality using a 128- bit key. Use of AES-CCMP encryption is specified as a standard requirement for WPA2. Before implementing WPA2 in the network, be sure client devices are upgraded to WPA2-compliant hardware.

■ Auto Uses either TKIP or AES keys for encryption. WPA and WPA2 mixed modes allow both WPA and WPA2 clients to associate to a common SSID. In mixed mode, the unicast encryption type (TKIP or AES) is negotiated for each client.

◆□Pass Phrase — The WPA Preshared Key can be input as an ASCII string (an easy-to-remember form of letters and numbers that can include spaces) or Hexadecimal format. (Range: 8~63 ASCII characters, or exactly 64 Hexadecimal digits)

• Key Renewal Interval — Sets the time period for automatically changing data encryption keys and redistributing them to all connected clients.

IEEE 802.1X ANDRADIUS

IEEE 802.1X is a standard framework for network access control that uses a central RADIUS server for user authentication. This control feature prevents unauthorized access to the network by requiring an 802.1X client application to submit user credentials for authentication. The 802.1X standard uses the Extensible Authentication Protocol (EAP) to pass user credentials (either digital certificates, user names and passwords, or other) from the client to the RADIUS server. Client authentication is then verified on the RADIUS server before the client can access the network. Remote Authentication Dial-in User Service (RADIUS) is an authentication protocol that uses software running on a central server to control access to RADIUS-aware devices on the network. An authentication server contains a database of user credentials for each user that requires network access. The WPA and WPA2 enterprise security modes use 802.1X as the method of user authentication. IEEE 802.1X can also be enabled on its own as a security mode for

user authentication. When 802.1X is used, a RADIUS server must be configured and be available on the connected wired network.

| SSID I Security Settings | |
|--------------------------|----------------|
| Network Name (SSID) | SSID NAME Hide |
| | • |
| | 802.1× |
| | |
| | |
| | |
| Apply - | Cancel |

RADIUS Server — Configures RADIUS server settings.

◆□IP Address — Specifies the IP address of the RADIUS server.

◆□Port — The User Datagram Protocol (UDP) port number used by the

RADIUS server for authentication messages. (Range: 1024-65535; Default: 1812) Shared Secret — A shared text string used to encrypt messages between the access point and the RADIUS server. Be sure that the same text string is specified on the RADIUS server. Do not use blank spaces in the string. (Maximum length: 20 characters)

WI-FI PROTECTED SETUP(WPS)

Wi-Fi Protected Setup (WPS) is designed to ease installation and activation of security features in wireless networks. WPS has two basic modes of operation, Push-button Configuration (PBC) and Personal Identification Number (PIN). The WPS PIN setup is optional to the PBC setup and provides more security. The WPS button on the Wireless Router can be pressed at any time to allow a single device to easily join the network. The WPS Settings page includes configuration options for setting WPS device PIN codes and activating the virtual WPS button.

| SSD1 Security Settings | |
|------------------------|-----------------------------------|
| Network Name (55ID) | SSID NAME Hide |
| WPS Choice | 8 |
| WPS Summary | |
| | SSID NAME |
| | |
| | |
| | WPA-PSK . |
| WPA Algorithms | TRIP [7] CCMP(AES) Auto |
| | 60 |
| | Generator |
| Apply | Cancel |

- \square WPS SSID The service set identifier for the unit.
- ◆□AP PIN Displays the PIN Code for the Wireless Router.
- ◆□Device Name— WPS name for connecting to the device.

• Encryption Settings — Selects between methods of broadcasting the WPS beacon to network clients wanting to join the network:

WPA Algorithms — Select the data encryption type to use. (Default is determined by the Security Mode selected.)

◆□**TKIP** — Uses Temporal Key Integrity Protocol (TKIP) keys for encryption. WPA specifies TKIP as the data encryption method to replace WEP. TKIP avoids the problems of WEP static keys by dynamically changing data encryption keys.

◆□AES — Uses Advanced Encryption Standard (AES) keys for encryption. WPA2 uses AES Counter-Mode encryption with Cipher Block Chaining Message Authentication Code (CBC-MAC) formessage integrity. The AES

Counter-Mode/CBCMAC Protocol (AESCCMP) provides extremely robust data confidentiality using a 128- bit key. Use of AES-CCMP encryption is specified as a standard requirement for WPA2. Before implementing WPA2 in the network, be sure client devices are upgraded to WPA2-compliant hardware.

◆ ▲ Auto — Uses either TKIP or AES keys for encryption. WPA and WPA2 mixed modes allow both WPA and WPA2 clients to associate to a common SSID. In mixed mode, the unicast encryption type (TKIP or AES) is negotiated for each client.

◆□Key Renewal Interval — Sets the time period for automatically changing data encryption keys and redistributing them to all connected clients.

◆□Pass Phrase — The WPA Preshared Key can be input as an ASCII string (an easy-to-remember form of letters and numbers that can include spaces) or Hexadecimal format. (Range: 8~63 ASCII characters, or exactly 64 Hexadecimal digits)

Federal Communications Commission (FCC) Statement

You are cautioned that changes or modifications not expressly approved by the part responsible for compliance could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1) this device may not cause harmful interference, and

2) this device must accept any interference received, including interference that may cause undesired operation of the device.

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

-Reorient or relocate the receiving antenna.

-Increase the separation between the equipment and receiver.

-Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

-Consult the dealer or an experienced radio/TV technician for help.

FCC RF Radiation Exposure Statement:

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