TW-EAV510 AC-LTE CAT 6
ADSL2+/VDSL2 WLAN 802.11ac
Router

User Manual

V1.9
# Directory

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>5</td>
</tr>
<tr>
<td>- Introduction to your Router</td>
<td>5</td>
</tr>
<tr>
<td>Features</td>
<td>7</td>
</tr>
<tr>
<td>Physical Interface</td>
<td>8</td>
</tr>
<tr>
<td>Package Contents</td>
<td>9</td>
</tr>
<tr>
<td>Device Description</td>
<td>10</td>
</tr>
<tr>
<td>Network Configuration</td>
<td>14</td>
</tr>
<tr>
<td>Factory Default Settings</td>
<td>17</td>
</tr>
<tr>
<td>- Web Interface (Username and Password)</td>
<td>17</td>
</tr>
<tr>
<td>- Device LAN IPv4 settings</td>
<td>18</td>
</tr>
<tr>
<td>- DHCP server for IPv4</td>
<td>18</td>
</tr>
<tr>
<td>Configuration</td>
<td>18</td>
</tr>
<tr>
<td>- Configuration via Web Interface</td>
<td>18</td>
</tr>
<tr>
<td>Status</td>
<td>20</td>
</tr>
<tr>
<td>- Device</td>
<td>20</td>
</tr>
<tr>
<td>- 3G/4G/LTE Info</td>
<td>22</td>
</tr>
<tr>
<td>- LAN/WLAN Clients</td>
<td>22</td>
</tr>
<tr>
<td>- AP Neighbor</td>
<td>22</td>
</tr>
<tr>
<td>- IPv6</td>
<td>23</td>
</tr>
<tr>
<td>- Ethernet Port</td>
<td>23</td>
</tr>
<tr>
<td>- System Log</td>
<td>24</td>
</tr>
<tr>
<td>LAN</td>
<td>24</td>
</tr>
<tr>
<td>WLAN</td>
<td>26</td>
</tr>
<tr>
<td>- WLAN 2.4GHz / 5GHz</td>
<td>26</td>
</tr>
<tr>
<td></td>
<td>- Basic Settings</td>
</tr>
<tr>
<td></td>
<td>- Advanced Settings</td>
</tr>
<tr>
<td></td>
<td>- Security</td>
</tr>
<tr>
<td></td>
<td>- Access Control</td>
</tr>
<tr>
<td></td>
<td>- Site Survey</td>
</tr>
<tr>
<td></td>
<td>- WPS</td>
</tr>
<tr>
<td></td>
<td>- Status</td>
</tr>
<tr>
<td>WAN</td>
<td>31</td>
</tr>
<tr>
<td>- WAN Mode</td>
<td>31</td>
</tr>
<tr>
<td>- Default Routing</td>
<td>31</td>
</tr>
<tr>
<td>- Ethernet WAN</td>
<td>32</td>
</tr>
<tr>
<td>- PTM(VDSL) WAN</td>
<td>34</td>
</tr>
</tbody>
</table>
IPv6 Routing .......................................................... 78
IP/Port Filtering ...................................................... 79
Diagnostics .................................................................. 80
Ping ............................................................................. 80
Management .................................................................. 80
  Backup/Restore ......................................................... 80
  Password ...................................................................... 81
  Firmware Upgrade ..................................................... 81
ACL .............................................................................. 82
Time Zone ...................................................................... 83
Auto Reboot .................................................................. 83
Statistics ....................................................................... 84
  Interface ...................................................................... 84
  DSL .............................................................................. 84
Language ...................................................................... 85
Reboot ......................................................................... 86
Logout ......................................................................... 86
Introduction

Introduction to your Router

TW-EAV510 AC-LTE CAT 6 WLAN 802.11ac Router is a residential/small office gateway, especially designed for those who need to have the data, video and file sharing services beyond his home and office. It is an all-in-one advanced device integrating Wireless, Ethernet, 3G/4G/LTE, and NAS (Network Attached Storage) in one unit. As well as being IPv6-capable, the router supports super-fast fiber connections via dual-WAN connectivity through a Gigabit Ethernet WAN port. Also, it also has a USB port, allowing the device to act as a print server as well as a NAS (Network Attached Storage) device.

Maximum wireless performance
With an integrated 802.11ac Wireless Access Point, the device supports a data rate of up to 1200Mbps and is also compatible with 802.11b/g/n/ac equipment.

The Wireless Protected Access (WPA-PSK/WPA2-PSK) and Wireless Encryption Protocol (WEP) features enhance the level of transmission security and access control over wireless LAN. The router also supports the Wi-Fi Protected Setup (WPS) standard, allowing users to establish a secure wireless network by simply pushing a button. If your network requires wider coverage, the built-in Wireless Distribution System (WDS) repeater function allows you to expand your wireless network without the need for any external wires or cables.

3G/4G/LTE Mobility and Always-on Connectivity
With 3G/4G/LTE-based Internet connection, user can access Internet through 3G/4G/LTE, whether you are seated at your desk or taking a cross-country trip. The auto fail-over feature ensures optimum connectivity and minimum interruption by quickly and smoothly connecting to a 3G/4G/LTE network in the event that you ADSL/Fiber/Cable line fails. The device will then automatically reconnect to the ADSL/Fiber/Cable connection when it is
restored, reducing connection costs. These features are perfect for office situations when a constant and smooth WAN connection is critical.

IPv6 supported
Internet Protocol version 6 (IPv6) is a version of the Internet Protocol that is designed to succeed IPv4. IPv6 has a vastly larger address space than IPv4. This results from the use of a 128-bit address, whereas IPv4 uses only 32 bits. The new address space thus supports 2128 (about 3.4×10^38) addresses. This expansion provides flexibility in allocating addresses and routing traffic and eliminates the primary need for network address translation (NAT), which gained widespread deployment as an effort to alleviate IPv4 address exhaustion.

The device fully supports IPv6 (Internet Protocol Version 6), launched as the current IPv4 range is filling up, and IPv6 is gradually becoming the indispensable addressing system for savvy cloud computing users. Dual stack means the router is capable of running IPv4 and IPv6 in parallel during the transition period. With TeleWell IPv6 enabled devices.

Virtual AP
A “Virtual Access Point” is a logical entity that exists within a physical Access Point (AP). When a single physical AP supports multiple “Virtual APs”, each Virtual AP appears to stations (STAs) to be an independent physical AP, even though only a single physical AP is present. For example, multiple Virtual APs might exist within a single physical AP, each advertising a distinct SSID and capability set. Alternatively, multiple Virtual APs might advertise the same SSID but a different capability set – allowing access to be provided via WEB Portal, WEP, and WPA simultaneously. Where APs are shared by multiple providers, Virtual APs provide each provider with separate authentication and accounting data for their users, as well as diagnostic information, without sharing sensitive management traffic or data between providers. You can enable the virtual AP.

WEB Based GUI
It supports web-based GUI for configuration and management. It is user-friendly and comes with online help. It also supports remote management capability for remote users to configure and manage this product.

Firmware Upgradeable
Device can be upgraded to the latest firmware through the WEB based GUI.
Features

Network Protocols and Features
- IPv4 or IPv4 / IPv6 Dual Stack
- NAT, DMZ and ALG
- IPv6 Stateless / Stateful Address Auto-configuration
- IPv6 Router Advertisement
- DHCPv6
- Static Route
- Universal Plug and Play (UPnP) Compliant
- Dynamic Domain Name System (DDNS)
- Virtual Server, DMZ and one-to-one NAT
- SNTP, DNS relay, IGMP snooping and IGMP proxy for video service
- Management based-on IP protocol, port number and address

Firewall
- Built-in NAT Firewall
- Stateful Packet Inspection (SPI)
- DoS attack prevention
- Packet Filtering (v4/v6) - port, source IP address, destination IP address, MAC address
- URL Content Filtering (v4/v6) – string or domain name detection in URL string
- Wireless MAC Filtering

Virtual Private Network (VPN)
- PPTP Client / Server
- L2TP Client / Server
- OpenVPN Client / Server
- IPSec
- PPTP / L2TP / IPSec pass-through

Quality of Service Control
- Supports the DiffServ approach
- Traffic prioritization and bandwidth management based-on IPv4 protocol, port number and address
IPTV Applications
- IGMP Snooping and IGMP Proxy
- Quality of Service (QoS)

Wireless LAN
- Compliant with
  - IEEE 802.11 b/g/n/ac standards
  - 2.4 and 5G radio bands for wireless
  - Up to 300 Mbps (11n) and 900Mbps (11ac) wireless operation rate
- 64/128 bits WEP supported for encryption
- WPS (Wi-Fi Protected Setup) for easy setup
- Wireless Security with WEP / WPA-PSK / WPA2-PSK support

Management
- Web-based GUI for remote and local management (IPv4/IPv6)
- Firmware upgrades and configuration data upload and download via web-based GUI
- Embedded Telnet server for remote and local management
- Supports DHCP server / client

Physical Interface
- One RJ-11 port for VDSL / ADSL connection
- One WAN-Port 10/100/1000 Mbps auto-crossover (MDI / MDI-X) Switch
- Four LAN-ports 10/100/1000 Mbps auto-crossover (MDI / MDI-X) Switch
- One USB 3.0 for Printer / Storage
- One SIM card slot
- WLAN ON&OFF / WPS / Factory default reset button
- Power switch
- Power jack
- WLAN: 2 x 5 dBi external fixed antenna
- LTE: 2 x 3dBi detachable antenna with standard SMA socket
Package Contents

- TeleWell TW-EAV510 AC-LTE CAT 6 ADSL2+/VDSL2 WLAN 802.11ac Router
- User Manual
- RJ-45 Cat. 6 STP Ethernet cable
- Power adapter

Important note for using this router

Do not use the router in high humidity or high temperatures
Do not use the same power source for the router as other equipment.
Do not open or repair the case yourself. If the router is too hot, turn off the power immediately and have it repaired at a qualified service center.
Avoid using this product and all accessories outdoors.

Warning

Do not use the router in high humidity or high temperatures.
Do not use the same power source for the router as other equipment.
Do not open or repair the case yourself. If the router is too hot, turn off the power immediately and have it repaired at a qualified service center.
Avoid using this product and all accessories outdoors.
Place the router on a stable surface.
Only use the power adapter that comes with the package. Using a different voltage rating power adapter may damage the router.
## Device Description

### The Front LEDs

<table>
<thead>
<tr>
<th>LED</th>
<th>Status</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>PWR</td>
<td>On</td>
<td>Steady green</td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td>Off</td>
</tr>
<tr>
<td></td>
<td>Steady Green</td>
<td>2.4G WiFi is ready for using</td>
</tr>
<tr>
<td></td>
<td>Flashing Green</td>
<td>There is no STAs association</td>
</tr>
<tr>
<td></td>
<td>Rapid Flashing Green</td>
<td>There is STAs association connection and traffic</td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td>2.4G WiFi is disabled</td>
</tr>
<tr>
<td>2.4G</td>
<td>Steady Green</td>
<td>5G WiFi is ready for using</td>
</tr>
<tr>
<td></td>
<td>Flashing Green</td>
<td>Data being transmitted/received</td>
</tr>
<tr>
<td></td>
<td>Rapid Flashing Green</td>
<td>There is STAs association connection and traffic</td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td>5G WiFi is disabled</td>
</tr>
<tr>
<td>5G</td>
<td>Flashing Green</td>
<td>Running WPS Configuration</td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td>WPS Stop</td>
</tr>
<tr>
<td>WPS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DSL</td>
<td>Steady Green</td>
<td>xDSL Showtime Phase</td>
</tr>
<tr>
<td></td>
<td>Quickly Flashing</td>
<td>xDSL Discovery/Training/Exchange Phase</td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td>No xDSL line connected</td>
</tr>
<tr>
<td>USB</td>
<td>On</td>
<td>USB device connected</td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td>USB device not connected</td>
</tr>
<tr>
<td>WAN</td>
<td>Steady Green</td>
<td>Ethernet Link Up</td>
</tr>
<tr>
<td></td>
<td>Flashing Green</td>
<td>Ethernet Link Up and traffic</td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td>Ethernet Link Down</td>
</tr>
<tr>
<td>LAN1~LAN4</td>
<td>Steady Green</td>
<td>Ethernet Link Up</td>
</tr>
<tr>
<td></td>
<td>Flashing Green</td>
<td>Ethernet Link Up and traffic</td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td>Ethernet Link Down</td>
</tr>
<tr>
<td>Internet</td>
<td>Steady Green</td>
<td>Device has a public IP via either static/DHCP/IPCP</td>
</tr>
</tbody>
</table>
Rapid Flashing Green | IP connected and traffic passing  
---|---  
Off | IP or PPPoE session is idle and dropped, or DSL not connected  

| 4G/LTE |  
|---|---  
On | LTE module initial successfully  
Off | LTE module initial failed  

The Rear Ports

<table>
<thead>
<tr>
<th>Port</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSL</td>
<td>Connect the supplied Telephone cable to DSL port</td>
</tr>
<tr>
<td>WAN</td>
<td>Connect one end of Ethernet cable to the WAN port when connecting other fixed line modem</td>
</tr>
<tr>
<td>LAN1-4</td>
<td>Connect a Ethernet cable to one of the LAN ports when connecting to a PC or an office/home network</td>
</tr>
<tr>
<td>WiFi ON/OFF</td>
<td>Press and release quickly to enable or disable the 2.4G and 5G Wi-Fi function</td>
</tr>
<tr>
<td>RESET</td>
<td>Power on device and wait for 60 seconds, then press it 5 seconds or above to restore to factory default</td>
</tr>
<tr>
<td>WPS</td>
<td>Press and release quickly to enable the WPS function</td>
</tr>
<tr>
<td>Power</td>
<td>Connect the supplied power adapter to this jack</td>
</tr>
<tr>
<td>Switch or ON/OFF</td>
<td>Power ON / OFF switch</td>
</tr>
<tr>
<td>USB</td>
<td>Connect your storage or printer device</td>
</tr>
<tr>
<td>SIM</td>
<td>The slot to insert the Mini-SIM(2FF) card (Please power off and insert the SIM card, then power on)</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Fixed Wi-Fi Antenna</td>
<td>The fixed antennas are for Wi-Fi 2.4G and 5G</td>
</tr>
<tr>
<td>Detachable LTE Antenna</td>
<td>Standard SMA socket and can change antenna by user self</td>
</tr>
</tbody>
</table>
Basic Installation

The router can be configured through your web browser. A web browser is included as a standard application in the following operating systems: Linux, Mac OS, Windows 8 / 7 / 98 / NT / 2000 / XP / Me / Vista, etc. The product provides an easy and user-friendly interface for configuration.

Please check your PC network components. The TCP/IP protocol stack and Ethernet network adapter must be installed. If not, please refer to your Windows-related or other operating system manuals.

There are ways to connect the router, either through an external repeater hub or connect directly to your PCs. However, make sure that your PCs have an Ethernet interface installed properly prior to connecting the router device. You ought to configure your PCs to obtain an IP address through a DHCP server or a fixed IP address that must be in the same subnet as the router. The default IP address of the router is 192.168.0.254 and the subnet mask is 255.255.255.0 (i.e. any attached PC must be in the same subnet and have an IP address in the range of 192.168.0.1 to 192.168.0.253).

The best and easiest way is to configure the PC to get an IP address automatically from the router using DHCP. If you encounter any problem accessing the router web interface it is advisable to uninstall your firewall program on your PCs, as they can cause problems accessing the IP address of the router. Users should make their own decisions on what is best to protect their network.

Please follow the following steps to configure your PC network environment.

Any TCP/IP capable workstation can be used to communicate with or through this router. To configure other types of workstations, please consult your manufacturer documentation.
Network Configuration

Configuring a PC in Windows 7

Go to Start. Click on Control Panel. Then click on Network and Internet.

When the Network and Sharing Center window pops up, select and click on Change adapter settings on the left window panel. Select the Local Area Connection, and right click the icon to select Properties.

IPv4:
Select Internet Protocol Version 4 (TCP/IPv4) then click Properties.

In the TCP/IPv4 properties window, select the Obtain an IP address automatically and Obtain DNS Server address automatically radio buttons. Then click OK to exit the setting. Click OK again in the Local Area Connection Properties window to apply the new configuration.
**IPv6:**
Select Internet Protocol Version 6 (TCP/IPv6) then click Properties
In the TCP/IPv6 properties window, select the Obtain an IPv6 address automatically and Obtain DNS Server address automatically radio buttons. Then click OK to exit the setting. Click OK again in the Local Area Connection Properties window to apply the new configuration.

Factory Default Settings

Before configuring your router, you need to settings.

Web Interface (Username and Password)

Administrator
Username: hallinta
Password: Please check the device label and it is random up to 16 characters.

Attention
If you have forgotten the username and/or password of the router, you can restore the device to its default setting by pressing the Reset Button more than 6 seconds.
Device LAN IPv4 settings

- IPv4 Address: 192.168.0.254
- Subnet Mask: 255.255.255.0

DHCP server for IPv4

- DHCP server is enabled
- Start IP Address: 192.168.0.100
- IP pool counts: 100

Configuration

Configuration via Web Interface

Open your web browser; enter the IP address of your router, which by default is 192.168.0.254, and click ok or press ‘Enter’ key on the keyboard, a login prompt window will appear.

Congratulations! You are now successfully logged in to the Firewall Router!
The TW-EAV510 AC-LTE CAT 6 also support the HTTPS connection, you can enter the URL: https://192.168.0.254 to establish the secure connection between your PC and Router.

With the HTTPS connection, you will get warning message as below (Google Chrome Browser).

![Warning Message]

Just click the link “ADVANCED”, and then click link “Proceed to 192.168.0.254 (unsafe)” to establish HTTPS connection with the router.
Once you have logged on to your TW-EAV510 AC-LTE CAT 6 WLAN 802.11ac Router via your web browser, you can begin to set it up according to your requirements. On the configuration homepage, the left navigation pane links you directly to the setup pages, which include:

## Status

## Device

The page below shows the basic system and WAN connection information.
# Device Status

This page shows the current status and basic settings of the device.

## Systems

<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model Name</td>
<td>TW-EAV310 AC-LTE CAT 6</td>
</tr>
<tr>
<td>Serial Number</td>
<td>RSRNBX1816000008387K</td>
</tr>
<tr>
<td>Uptime</td>
<td>2 min</td>
</tr>
<tr>
<td>Firmware Version</td>
<td>v138b720</td>
</tr>
<tr>
<td>CPU Usage</td>
<td>0.1%</td>
</tr>
<tr>
<td>Memory Usage</td>
<td>40%</td>
</tr>
<tr>
<td>Name Servers</td>
<td>61.31.1.1, 8.8.8.8</td>
</tr>
<tr>
<td>IPv4 Default Gateway</td>
<td>10.125.17.77</td>
</tr>
</tbody>
</table>

## DSL

<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operational Status</td>
<td>ACTIVATING</td>
</tr>
<tr>
<td>Upstream Speed</td>
<td>0 kbps</td>
</tr>
<tr>
<td>Downstream Speed</td>
<td>0 kbps</td>
</tr>
<tr>
<td>SNR (dB)</td>
<td>Down: 0.0 / Up: 0.0</td>
</tr>
<tr>
<td>Attenuation (dB)</td>
<td>Down: 0.0 / Up: 0.0</td>
</tr>
</tbody>
</table>

## LAN Configuration

<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>192.168.0.254</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>DHCP Server</td>
<td>Enabled</td>
</tr>
<tr>
<td>MAC Address</td>
<td>001EAB5651F</td>
</tr>
</tbody>
</table>

## WAN Configuration

<table>
<thead>
<tr>
<th>Interface</th>
<th>VPI/VCI</th>
<th>Encapsulation</th>
<th>Protocol</th>
<th>IP Address</th>
<th>Gateway</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADSL_0</td>
<td>0/33</td>
<td>LLC</td>
<td>mer1483</td>
<td></td>
<td></td>
<td>DOWN</td>
</tr>
<tr>
<td>ADSL_1</td>
<td>0/35</td>
<td>LLC</td>
<td>mer1483</td>
<td></td>
<td></td>
<td>DOWN</td>
</tr>
<tr>
<td>ADSL_2</td>
<td>0/100</td>
<td>LLC</td>
<td>mer1483</td>
<td></td>
<td></td>
<td>DOWN</td>
</tr>
<tr>
<td>VDSL_0</td>
<td>---</td>
<td>---</td>
<td>IPoE</td>
<td></td>
<td></td>
<td>DOWN</td>
</tr>
<tr>
<td>VDSL_1</td>
<td>---</td>
<td>---</td>
<td>IPoE</td>
<td></td>
<td></td>
<td>DOWN</td>
</tr>
<tr>
<td>EWAN_0</td>
<td>---</td>
<td>---</td>
<td>IPoE</td>
<td></td>
<td></td>
<td>DOWN</td>
</tr>
</tbody>
</table>

## 3G Configuration

<table>
<thead>
<tr>
<th>Interface</th>
<th>Protocol</th>
<th>IP Address</th>
<th>Gateway</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>3G/4G-LTE</td>
<td>DHCP</td>
<td>10.125.17.76</td>
<td>10.125.17.76</td>
<td>UP/ Disconnect</td>
</tr>
</tbody>
</table>

## PPTP Configuration

<table>
<thead>
<tr>
<th>Interface</th>
<th>Protocol</th>
<th>IP Address</th>
<th>Gateway</th>
<th>Status</th>
</tr>
</thead>
</table>

## L2TP/IPSec Configuration

<table>
<thead>
<tr>
<th>Interface</th>
<th>Protocol</th>
<th>Local IP Address</th>
<th>Remote IP Address</th>
<th>Status</th>
</tr>
</thead>
</table>

[Refresh]
3G/4G/LTE Info

This page shows 3G/4G/LTE network and dongle information.

<table>
<thead>
<tr>
<th>3G/4G/LTE Info</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>3G/4G/LTE Status</strong></td>
</tr>
<tr>
<td><strong>Operator Name</strong></td>
</tr>
<tr>
<td><strong>Frequency Band</strong></td>
</tr>
<tr>
<td><strong>Network Mode</strong></td>
</tr>
<tr>
<td><strong>Signal Strength</strong></td>
</tr>
<tr>
<td><strong>Card Name</strong></td>
</tr>
<tr>
<td><strong>Card Firmware</strong></td>
</tr>
</tbody>
</table>

LAN/WLAN Clients

This page shows all connected device’s information.

<table>
<thead>
<tr>
<th>LAN/WLAN Clients</th>
</tr>
</thead>
<tbody>
<tr>
<td>This table shows more details of LAN and WLAN clients’ information in one page, so end user can know what client connects to device and how it connects.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Hostname</th>
<th>MAC Address</th>
<th>IP Address</th>
<th>IP Assignment</th>
<th>Expired Time (sec)</th>
<th>Interface</th>
<th>SSID</th>
<th>RSSI</th>
</tr>
</thead>
<tbody>
<tr>
<td>iPhone</td>
<td>70-79-6D-11-75-F1</td>
<td>192.168.0.101</td>
<td>Dynamic</td>
<td>8090</td>
<td>2.4G</td>
<td>TW-EAV510-2.4G-001</td>
<td>77</td>
</tr>
<tr>
<td></td>
<td></td>
<td>192.168.0.100</td>
<td>Static</td>
<td>---</td>
<td>Ethernet Port2</td>
<td>---</td>
<td>---</td>
</tr>
</tbody>
</table>

AP Neighbor

This page shows all WLAN AP’s information around your TW-EAV510 AC-LTE CAT 6.
IPv6

This page shows the current system status of IPv6.

IPv6 Status

This page shows the current system status of IPv6.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>IP Address</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>PPPoE</td>
<td>2001:b011:700d:1150:7619::fe0:18/64</td>
<td>up</td>
</tr>
<tr>
<td>IPv6 Link-Local Address</td>
<td>fe0::64</td>
<td></td>
</tr>
</tbody>
</table>

Ethernet Port

This page shows connection status and speed of each Ethernet port.
Ethernet Port Status

This page shows the current Ethernet Port status.

System Log

**System Log**: Enable or disable the system log function.

**Log Level**: Specify the log level to be logged.

**Display Level**: Specify the log level to be displayed.

**Save Log to File**: Click Save button to save all system log into a file and download it from WEB browser to your PC.

**Clear Log**: Click Reset button to clear all existing log.

LAN

This page allows user to set device LAN IP address and DHCP Server for your network.
## LAN Interface Settings

This page is used to configure the LAN interface of your Device. Here you may change the setting for IP addresses, subnet mask, etc.

<table>
<thead>
<tr>
<th>IP Address</th>
<th>192.168.0.254</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subnet Mask</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>

**IGMP Snooping:**  
- Default is enabled.

**Ethernet to Wireless Blocking:**  
- When it is enabled, all connected PC on Ethernet port cannot access to any WiFi Client.

## DHCP Settings

**DHCP Mode:**  
- NONE
- DHCP Server

Enable the DHCP Server if you are using this device as a DHCP server. This page lists the IP address pools available to hosts on your LAN. The device distributes numbers in the pool to hosts on your network as they request Internet access.

<table>
<thead>
<tr>
<th>IP Pool Range:</th>
<th>192.168.0.100 - 192.168.0.200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Lease Time:</td>
<td>86400 seconds (-1 indicates an infinite lease)</td>
</tr>
<tr>
<td>Domain Name:</td>
<td>telewell.oy</td>
</tr>
<tr>
<td>Gateway Address:</td>
<td>192.168.0.254</td>
</tr>
<tr>
<td>DNS option:</td>
<td>Use DNS Relay</td>
</tr>
</tbody>
</table>

**IP Address / Subnet Mask:** The local management IP address and mask of this device which is also the default gateway IP address for all PCs in local area network.

**IGMP Snooping:** IGMP snooping is designed to prevent hosts on a local network from receiving traffic for a multicast group they have not explicitly joined. Default is enabled.

**Ethernet to Wireless Blocking:** When it is enabled, all connected PC on Ethernet port cannot access to any WiFi Client.

**DHCP Mode:** Set to NONE to disable the DHCP Server function. DHCP Server is activated as default.
**IP Pool Range:** Setup IP pool range that will be used for DHCP Server. User can click “Show Client” button to show information for all DHCP Clients.

**Max Lease Time:** Setup lease time for clients, default is 86400s.

**Domain Name:** Enter the domain name for your local area network (optional).

**Gateway Address:** It is the IP that will be assigned and activated as DHCP client’s gateway IP.

**DNS option:** This allows you to assign a DNS Servers to the requesting PC.

**MAC-Based Assignment:** This page allows to make DHCP server to release the fixed IP address to specified MAC address always.

---

### WLAN

#### WLAN 2.4GHz / 5GHz

**Basic Settings**

This page is used to configure the parameters for WLAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

**WLAN Basic Settings**

- **Disable WLAN Interface**
- **Band:** 2.4 GHz (B+G+N)
- **Mode:** AP, Multiple AP
- **SSID:** TW-EAV510-2.4G-001
- **Channel Width:** 20MHz/40MHz
- **Control Sideband:** Lower
- **Channel Number:** 1
- **PWR:** H
- **Associated Clients:** Show Active WLAN Clients

[Apply Changes]
**Disable WLAN Interface:** The WLAN 2.4G/5G function will be disabled when it is checked.

**Band:** Specify the mode for Wireless standard support.

**Mode:** Default is Access Point mode.

**Multiple AP:** This device supports up to 3 external SSIDs which can be used for different service.

**SSID:** Network ID is used for identifying the Wireless LAN.

**Channel Width:** Select channel bandwidth for wireless, bigger bandwidth can get higher link rate. But it also depends on interference of your environment.

**Control Sideband:** This is available for 40MHz. Drop-down menu allows selecting upper sideband or lower sideband.

**Channel Number:** The radio channel number. The permissible channels depend on the Regulatory Domain. The factory default setting is auto channel selection.

**PWR:** Specify the transmitting power of your wireless signal.

- S: Small / M: Medium / H: High

**Associated Clients:** Here you can view information about the wireless clients.

### Advanced Settings

Here user can set some advanced parameters about wireless.

**WLAN Advanced Settings**

These settings are only for more technically advanced users who have a sufficient knowledge about WLAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fragment Threshold</td>
<td>2346 (236-2346)</td>
</tr>
<tr>
<td>RTS Threshold</td>
<td>2347 (0-2347)</td>
</tr>
<tr>
<td>Beacon Interval</td>
<td>100 (20-1024 ms)</td>
</tr>
<tr>
<td>Preamble Type</td>
<td>Long Preamble / Short Preamble</td>
</tr>
<tr>
<td>Broadcast SSID</td>
<td>Enabled / Disabled</td>
</tr>
<tr>
<td>Protection</td>
<td>Enabled / Disabled</td>
</tr>
<tr>
<td>Aggregation</td>
<td>Enabled / Disabled</td>
</tr>
<tr>
<td>Short GI</td>
<td>Enabled / Disabled</td>
</tr>
<tr>
<td>WMM Support</td>
<td>Enabled / Disabled</td>
</tr>
</tbody>
</table>

[Apply Changes]
**Fragment Threshold:** A threshold (in bytes) whether the packets will be fragmented and at what size. Packets succeeding the fragmentation threshold of 802.11n WLAN will be split into smaller units suitable for circuit size. While the packets smaller than fragmentation threshold will not be fragmented. Default is 2346, setting the fragmentation too low may result in poor performance.

**RTS Threshold:** Request to Send (RTS) threshold specifies the packet size, when exceeds the size, the RTS/CTS will be triggered. The default setting of 2347(max length) will disable the RTS.

**Beacon Interval:** The amount of time between beacon transmissions in is milliseconds. The default is 100ms and the acceptable is 20-1024. The beacon transmissions identify the presence of an access point.

**Preamble Type:** Set wireless LAN preamble type to long or short.

**Broadcast SSID:** user can only enter the SSID manually for connecting if Disabled box checked.

**Protection:** Turn off for maximized throughput. Turn on for greater security.

**Short GI:** This would provide an 11% increase in data rates once enabled. Using the Short Guard Interval will result in higher packet error rates when the delay spread of the RF channel exceeds the SGI, or if timing synchronization between the transmitter and receiver is not precise.

**WMM Support:** You can choose the enable or disable WMM which allows for priority of certain data over the wireless network

**Security**

Wireless security prevents unauthorized access or damage to computers using wireless network.

**WLAN Security Settings**

This page allows you to setup the WLAN security: Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

| SSID: Root AP - TW-EAV51D-2.4G-D68 |
| Encryption: WPA2 Mixed |
| WPA Cipher Suite: TKIP, AES |
| WPA2 Cipher Suite: TKIP, AES |
| Group Key Update Timer: 86400 |
| Pre-Shared Key: buvz863583234826 |
| Apply Changes |
SSID choice: Apply the security settings to selected SSID.

Encryption: User can select one of the following authentications to secure your wireless network: None, WPA, WPA2 or WPA2 Mixed.

WPA Cipher Suite: Specify what cipher suite can be used.

WPA2 Cipher Suite: Specify what cipher suite can be used.

Group Key Update: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). This is in seconds.

Pre-Shared Key: Enter the key for your wireless security setting. Maximum length is 16 characters.

Access Control

The page helps user to make better security for the wireless network.

**WLAN Access Control**

If you choose 'Allowed Listed', only those WLAN clients whose MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these WLAN clients on the list will not be able to connect the Access Point.

---

**Mode:** Disabled

Apply Changes

MAC Address: [ ] (ex. AABBCDDE011)

Add Reset

---

**Current Access Control List**

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>Select</th>
</tr>
</thead>
</table>

Add Selected Delete All

**Mode:** Select the mode for the action that will apply to the **Current Access Control List**.

**MAC Address:** Enter the WiFi client's MAC address. Enter the **Add** button to add MAC address to the list.

**Reset:** User can click this button to clear MAC address that just entered.
**Delete Selected:** Click the button to delete all selected MAC addresses in the field named Select.

**Delete All:** Delete all the MAC address on Current Access Control List table.

**Site Survey**

The page can help user to find what WiFi channel is used by other AP and find the best channel for you by yourself. Just click Refresh button to do WLAN side survey.

**WLAN Site Survey**

This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.

<table>
<thead>
<tr>
<th>SSID</th>
<th>BSSID</th>
<th>Channel Mode</th>
<th>Type</th>
<th>Encryption</th>
<th>RSSI</th>
<th>Channel Width</th>
</tr>
</thead>
<tbody>
<tr>
<td>Netcore</td>
<td>00:10:77:4e:08:2a</td>
<td>6-2 B-G-N</td>
<td>AP</td>
<td>WPA-PSK/WPA2-PSK</td>
<td>-68</td>
<td>20M/40M</td>
</tr>
</tbody>
</table>

**WPS**

WPS (Wi-Fi Protected Setup) feature is a standard protocol created by Wi-Fi Alliance. WPS is used to exchange the AP setting with Station and configure AP settings. This feature greatly simplifies the steps needed to create a Wi-Fi network for a residential or an office setting. The commonly known PIN method is supported to configure WPS.

**WiFi Protected Setup**

This page allows you to change the setting for WPS (WiFi Protected Setup). Using this feature allows your WLAN client to automatically synchronize its settings and easily connect to the Access Point within a minute.

- **Disable WPS**
- **Push Button Configuration:**
  - Start PBC
  - Apply Changes
Status

This page shows the current configuration of WiFi module.

**WLAN Status**

This page shows the current status of the WLAN.

<table>
<thead>
<tr>
<th>WLAN Configuration</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>AP</td>
</tr>
<tr>
<td>Band</td>
<td>5 GHz (A+N+AC)</td>
</tr>
<tr>
<td>SSID</td>
<td>TW-EAV510AC-LTE v2-5G-F1F</td>
</tr>
<tr>
<td>Channel Number</td>
<td>44</td>
</tr>
<tr>
<td>Encryption</td>
<td>WPA2</td>
</tr>
<tr>
<td>BSSID</td>
<td>00:1E:AB:56:5F:1F</td>
</tr>
<tr>
<td>Associated Clients</td>
<td>0</td>
</tr>
</tbody>
</table>

WAN

**WAN Mode**

The page is used to configure which WAN connection mode will be used or not.

**WAN Mode**

This page is used to configure which WAN to use of your Router.

WAN Mode:  ✔ ATM  ✔ Ethernet  ✔ PTM  [Submit]

Default Routing

This page is used to configure the priority of each WAN connection. Top one has
higher priority than lower one. If you have multi-WAN connection available, it will do auto failover and auto fallback according to the priority setting here.

**Default Routing Gateway Priority**

Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority of the WAN interface is connected. Priority order can be changed by up and down them back in again.

**Ethernet WAN**

The page is used to configure the parameters and protocol for the Ethernet WAN port.

**Ethernet WAN Configuration**

The page is used to configure the parameters for Ethernet WAN.

- **Enable VLAN:**
- **VLAN ID:**
- **Channel Mode:**
- **Enable Bridge:**
- **Bridge Mode:**
- **Enable NAPT:**
- **Channel:**
- **Enable IGMP Proxy:**
- **WAN IP Settings:**
  - **Type:**
  - **Local IP Address:**
  - **Subnet Mask:**
  - **Request DNS:**
  - **Primary DNS Server:**
  - **Secondary DNS Server:**

**Profile:** Select the profile for configuration or new link to create a new profile.

**Enable VLAN:** User can check this box to enable the VLAN on specify profile.

**VLAN ID:** Assign a VLAN ID tag between 0 and 4094
**802.1p Mark**: Select an 802.1p priority level between 0 and 7.

**Channel Mode**: Select the channel mode for WAN connection.

**Bridge Mode**: Set bridge mode to make all transparent between Ethernet and WAN or PPPoE packet only.

**Enable NAPT**: Enable/Disable the NAT function for WAN connection.

**Channel**: Enable/Disable the channel.

**Default Route**: Specify the profile will be activated as default gateway for Internet connection or not.

**Enable QoS**: Enable/Disable the QoS for WAN connection.

**MTU**: Most ISP offers MTU value to users.

**Enable IGMP-Proxy**: Enable/Disable the IGMP Proxy. If disabled, the IPTV will not work with NAT enabled mode.

**IP Protocol**: Setup profile’s IP protocol to be IPv4 only, IPv6 only or IPv4/IPv6 dual stack.

When **Channel Mode** is set to **IPoE**, you will have the options below.

**Type**: Setup the WAN interface is use static IP or activate as DHCP client and get WAN IP from ISP.

**Local IP Address/Remote IP Address/Subnet Mask**: Enter the IP address, subnet mask and gateway address that provided by your ISP.

**Request DNS**: If this option is enabled, the device will use the DNS Server IP that assigned from ISP. It is only work when **Type** is set to **DHCP**.

**Primary DNS Server/Secondary DNS Server**: Input the primary and secondary DNS server if necessary.

When **Channel Mode** is set to **PPPoE**, you will have the options below.

**Username/Password**: Enter the PPPoE username/password that provided by your ISP.

**Type**: Specify the PPP connection should be always on (**Continuous**) or only make connection when necessary (**Connect on Demand**) or manually to make Connect/Disconnect.

**Idle Time (sec)**: Specify the idle time for disconnecting the PPPoE connection.

**Authentication Method**: Specify the authentication method for PPPoE connection.

When **IP Protocol** is set to **IPv6** or **IPv4/IPv6**, you will have the options below.

**Address Mode**: Specify the mode for getting or setting IPv6 address.

**Enable DHCPv6 Client**: Pass the IPv6 address to LAN network when box checked.
The page is used to configure the parameters and protocol for the VDSL2 WAN port.

**Profile**: Select the profile for configuration or new link to create a new profile.

**Enable VLAN**: User can check this box to enable the VLAN on specify profile.

**VLAN ID**: Assign a VLAN ID tag between 0 and 4094

**802.1p_Mark**: Select an 802.1p priority level between 0 and 7.

**Channel Mode**: Select the channel mode for WAN connection.

**Bridge Mode**: Set bridge mode to make all transparent between Ethernet and WAN or PPPoE packet only.

**Enable NAPT**: Enable/Disable the NAT function for WAN connection.

**Channel**: Enable/Disable the channel.

**Enable QoS**: Enable/Disable the QoS for WAN connection.

**MTU**: Most ISP offers MTU value to users.

**Default Route**: Specify the profile will be activated as default gateway for Internet connection or not.

**Enable IGMP-Proxy**: Enable/Disable the IGMP Proxy. If disabled, the IPTV will not work with NAT enabled mode.

**IP Protocol**: Setup profile’s IP protocol to be IPv4 only, IPv6 only or IPv4/IPv6 dual
When **Channel Mode** is set to **IPoE**, you will have the options below.

**Type**: Setup the WAN interface is use static IP or activate as DHCP client and get WAN IP from ISP.

**Local IP Address/Remote IP Address/Subnet Mask**: Enter the IP address, subnet mask and gateway address that provided by your ISP.

**Request DNS**: If this option is enabled, the device will use the DNS Server IP that assigned from ISP. It is only work when **Type** is set to **DHCP**.

**Primary DNS Server/Secondary DNS Server**: Input the primary and secondary DNS server if necessary.

When **Channel Mode** is set to **PPPoE**, you will have the options below.

**Username/Password**: Enter the PPPoE username/password that provided by your ISP.

**Type**: Specify the PPP connection should be always on (**Continuous**) or only make connection when necessary (**Connect on Demand**) or manually to make Connect/Disconnect.

**Idle Time (sec)**: Specify the idle time for disconnecting the PPPoE connection.

**Authentication Method**: Specify the authentication method for PPPoE connection.

When IP Protocol is set to **IPv6** or **IPv4/IPv6**, you will have the options below.

**Address Mode**: Specify the mode for getting or setting IPv6 address.

**Enable DHCPv6 Client**: Pass the IPv6 address to LAN network when box checked.

### ATM(ADSL) WAN

**ATM(ADSL) WAN Configuration**

This page is used to configure the parameters for ATM(ADSL) WAN.

<table>
<thead>
<tr>
<th>Select</th>
<th>Interface</th>
<th>Mode</th>
<th>VPI</th>
<th>VC1</th>
<th>Encapsulation</th>
<th>NAPT</th>
<th>ICMP</th>
<th>Remote IP</th>
<th>UseName</th>
<th>Default Route</th>
<th>Status</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ADSL_0</td>
<td></td>
<td>0</td>
<td>35</td>
<td>LLC</td>
<td>on</td>
<td>on</td>
<td></td>
<td></td>
<td>on</td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ADSL_1</td>
<td></td>
<td>0</td>
<td>35</td>
<td>LLC</td>
<td>on</td>
<td>on</td>
<td></td>
<td></td>
<td>on</td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ADSL_2</td>
<td></td>
<td>0</td>
<td>35</td>
<td>LLC</td>
<td>on</td>
<td>on</td>
<td></td>
<td></td>
<td>on</td>
<td>Enabled</td>
<td></td>
</tr>
</tbody>
</table>

**Delete Selected**
**VPI/VCI/Encapsulation/Channel Mode**: Enter the information from your ISP.

**Enable NAPT**: Enable/Disable the NAT function for WAN connection.

**Channel**: Enable/Disable the channel.

**Enable QoS**: Enable/Disable the QoS for WAN connection.

**Default Route**: Specify the profile will be activated as default gateway for Internet connection or not.

**Enable IGMP-Proxy**: Enable/Disable the IGMP Proxy. If disabled, the IPTV will not work with NAT enabled mode.

**IP Protocol**: Setup profile’s IP protocol to be IPv4 only, IPv6 only or IPv4/IPv6 dual stack.

When **Channel Mode** is set to **1483 MER**, you will have the options below.

**Type**: Setup the WAN interface is use static IP or activate as DHCP client and get WAN IP from ISP.

**Local IP Address/Remote IP Address/Subnet Mask**: Enter the IP address, subnet mask and gateway address that provided by your ISP.

**Request DNS**: If this option is enabled, the device will use the DNS Server IP that assigned from ISP. It is only work when **Type** is set to **DHCP**.

**Primary DNS Server/Secondary DNS Server**: Input the primary and secondary DNS server if necessary.

When **Channel Mode** is set to **PPPoE/PPPoA**, you will have the options below.

**Username/Password**: Enter the PPPoE username/password that provided by your ISP.

**Type**: Specify the PPP connection should be always on (**Continuous**) or only make connection when necessary (**Connect on Demand**) or manually to make Connect/Disconnect.

**Idle Time (sec)**: Specify the idle time for disconnecting the PPPoE connection.

When **Channel Mode** is set to **PPPoE/PPPoA**, you will have the options below.

**Address Mode**: Specify the mode for getting or setting IPv6 address.

**Enable DHCPv6 Client**: Pass the IPv6 address to LAN network when box checked.

**DSL Settings**

This screen allows you to set DSL parameters. DSL knowledge is required to configure these settings. Contact your ISP to make sure that these parameters are correct.
**DSL Settings**

This page is used to configure the parameters for the bands of your Device.

**DSL Modulation:**
- G.Lite
- G.Dmt
- T1.413
- ADSL2
- ADSL2+
- VDSL2

**AnnexL Option:** (Note: Only ADSL 2 supports AnnexL)
- Enabled

**AnnexM Option:** (Note: Only ADSL 2/2+ support AnnexM)
- Enabled

**VDSL2 Profile:**
- 8a
- 8b
- 8c
- 8d
- 12a
- 12b
- 17a
- 30a

**ADSL Capability:**
- Enabled Bitswap
- Enabled SRA

[Apply Changes]

Please keep these settings as default from ISP, it may make DSL connection broken if set to wrong parameters.

**3G/4G LTE Settings**

3G/4G LTE dongle related settings can be found in this page.
3G/4G LTE Settings

This page is used to configure the parameters for your 3G network access.

3G/4G LTE WAN: Enable/Disable the 3G/4G LTE module detection function.
Network Preference: Specify the network preference you preferred.
PIN Code: Enter the PIN code for your SIM card (optional).
APN: Enter the APN name if required by your ISP. The default value should work with most ISPs.
Dial Number: Enter the dialed number that is provided by your ISP, the default value should work with most ISPs.
Authentication: Select the authentication type that is provided by your ISP.
Username: Enter the username that is provided by your ISP (optional).
Password: Enter the password that is provided by your ISP (optional).
**Time:** The period value for sending keep alive packet, default is 30 seconds.

**IP Address:** Enter the IP address that keep alive packet should send to. Empty means use the primary DNS server IP address which assigned from Service Provider.

**NAPT:** Enable/Disable the NAT.

**Default Route:** Setup the 3G/4G LTE connection will be used as default gateway or not.

**MTU:** Most ISP offers MTU value to users.

**Extra AT Command:** User can issue specify the AT command after 3G/LTE modem initialized.

---

**VPN**

**PPTP**

This page is for setting PPTP Server, Client and account.

### PPTP VPN Configuration

This page is used to configure the parameters for PPTP mode VPN.

**PPTP VPN:** 
- Disable
- Enable

**PPTP Server**
- **Authentication Type:** CHAP
- **Encryption Mode:** NONE
- **Local IP Address:** 992.168.0.254

**Server Account**
- **Name:**
- **Username:**
- **Password:**
- **Peer IP:** optional, e.g. 10.0.0.1
- **Peer Subnet Mask:** optional, e.g. 255.255.255.255

**PPTP Server Table**

<table>
<thead>
<tr>
<th>Select</th>
<th>Name</th>
<th>Enable</th>
<th>Username</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete Selected</td>
<td>Save</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**PPTP Client**
- **Name:**
- **Username:**
- **Authentication Type:** CHAP
- **Default Gateway:**
- **Peer IP:** optional, e.g. 10.0.0.1
- **Peer Subnet Mask:** optional, e.g. 255.255.255.255

**PPTP Client Table**

<table>
<thead>
<tr>
<th>Select</th>
<th>Name</th>
<th>Interface</th>
<th>Server</th>
<th>Default Gateway</th>
<th>Peer Network</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete Selected</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**PPTP VPN:** Enable/Disable PPTP function.

**PPTP Server**
**Authentication Type:** Setup the authentication type for client.

**Encryption Mode:** Setup MPPE encryption for PPTP tunnel, MPPE can only be enabled when Auth. Type set to MS-CHAPV2.

**Assigned to Peer IP Address start from:** Enter the IP address that will be assigned to remote PPTP client. The IP address cannot in DHCP IP Pool range.

**Local IP Address:** Enter the IP address for PPTP tunnel interface. Default is set to device LAN IP address. Example: 192.168.0.254.

**Server Account**
- **Name:** Enter the name for this account profile.
- **Account:** Enable/Disable this account.
- **Username:** Enter the username for login authentication.
- **Password:** Enter the password for login authentication.
- **Peer IP:** Enter the peer side LAN IP address for LAN to LAN type.
- **Peer Subnet Mask:** Enter the peer side LAN subnet mask for LAN to LAN type.

**PPTP Client**
- **Name:** Enter the name for this client rule.
- **Server IP Address:** Specify the remote PPTP server IP address or domain name.
- **Username:** Enter the username for PPTP login authentication.
- **Password:** Enter the password for PPTP login authentication.
- **Authentication Type:** Setup the authentication type for connecting to PPTP server. This setting must follow server side.
- **Encryption Mode:** Setup MPPE encryption for PPTP tunnel, MPPE can only be enabled when Auth. Type set to MS-CHAPV2. This setting must follow server side.
- **Default Gateway:** Make this PPTP tunnel as default gateway for all local traffic when it is checked.
- **Peer IP:** Enter the peer side LAN IP address for LAN to LAN type.
- **Peer Subnet Mask:** Enter the peer side LAN subnet mask for LAN to LAN type.

**How to for PPTP Server/Client**

**Example 1**

TW-EAV510 AC in below pic left side is activated as PPTP Server and TW-EAV510 AC in below right side is activated as PPTP Client.
Remote Access

**TW-EAV510 (PPTP Server)**
1. Go to **WAN -> VPN -> PPTP**, enable the PPTP VPN
2. Setup PPTP Server and press *Apply* button
3. Add new user account, don’t need input Peer IP/ Peer Subnet Mask.

<table>
<thead>
<tr>
<th>PPTP Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Type: CHAP</td>
</tr>
<tr>
<td>Assigned to Peer IP Address start from: 192.168.100.200</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Server Account</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name: admin</td>
</tr>
<tr>
<td>Password: admin</td>
</tr>
<tr>
<td>Peer Subnet Mask: optional, e.g. 255.255.255.0</td>
</tr>
</tbody>
</table>

**TW-EAV510 AC (PPTP Client)**
1. Go to **WAN -> VPN -> PPTP**, enable the PPTP VPN, Setting PPTP Client as below.

<table>
<thead>
<tr>
<th>PPTP Server Table</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select</td>
</tr>
<tr>
<td>-------</td>
</tr>
<tr>
<td>admin</td>
</tr>
</tbody>
</table>
Click **Add** button to save account settings.

2. After click **Add** button, **PPTP Client Table** would add one connection, if setup all correctly VPN connection should be connected. You can also click **Disconnect** button to disconnect the PPTP connection.

3. Go to **Status -> Device**, you can check **PPTP Configuration** on page below, When **Status** shows **up**, you can access to remote network now. Below is Device Info for reference.

**LAN to LAN**

**TW-EAV510 (PPTP Server)**
1. Go to **WAN -> VPN -> PPTP**, enable the PPTP VPN
2. Setup PPTP Server and press **Apply** button
3. Add new user account, enter remote network’s IP address for Peer IP/ Peer Subnet Mask.
4. After pressing the **Add** button, the **PPTP Server Table** would add the account as shown below.

**TW-EAV510 AC (PPTP Client)**

1. Go to **WAN -> VPN -> PPTP**, enable the PPTP VPN, setting PPTP Client as shown below. For LAN to LAN, you need to enter peer network information.

2. After clicking the **Add** button, the **PPTP Client Table** would add one connection. If the setup is correct, the VPN connection should be connected. You can also click the **Disconnect** button to disconnect the PPTP connection.

3. Go to **Status -> Device**, you can check the **PPTP Configuration**. When **Status** shows **up**, both local and remote networks can access each other. Below is Server Info for reference.
Example 2

TW-EAV510 is activated as PPTP Server and Windows 10 is activated as PPTP Client for Remote Access.

TW-EAV510 (PPTP Server)
1. Same setting with Remote Access.
2. Don’t need input Peer IP/ Peer Subnet Mask.

<table>
<thead>
<tr>
<th>PPTP Server</th>
<th>Authentication Type</th>
<th>Assigned to Peer IP Address</th>
<th>Encryption Mode</th>
<th>Local IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>CHAP</td>
<td>192.168.100.254</td>
<td>NONE</td>
<td>192.168.0.254</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Server Account</th>
<th>Name</th>
<th>Username</th>
<th>Peer IP</th>
<th>Account</th>
<th>Password</th>
<th>Peer Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>admin</td>
<td>admin</td>
<td>optional_e.g. 10.0.0.1</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PPTP Server Table</th>
<th>Name</th>
<th>Enable</th>
<th>Username</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>✔</td>
<td>admin</td>
<td>admin</td>
<td>admin</td>
</tr>
</tbody>
</table>

Windows 10 (PPTP Client)
1. Make sure PC can access internet.
2. Go to Control Panel -> Network and Internet -> Network and Sharing Center -> click Setup a new connection or network to add a new PPTP connection.
3. Select **Connect to a workplace**.

4. Select **No, create a new connection** and click **Next** button for next step.
5. Select **Use my Internet connection (VPN)**.

6. Enter the PPTP Server address/domain to field named **Internet address**. Please make sure your domain name address is work correctly if you are use domain name instead of IP address. Click **Create** button finish the PPTP client settings on Windows.

7. Enter the **username** and **password** that set on TW-EAV510/510AC’s PPTP Server and click **OK** button to connect to PPTP Server.
8. After connected, you can access remote network now.

9. If you have problem connect with PPTP VPN via PC, please check Control Panel -> Network and Internet -> Network and Sharing Center, click Change adapter settings on left side, would show VPN Connection then right click to select Properties -> Security. Choose Type of VPN to Point to Point Tunneling Protocol(PPTP), and choose Allow these protocols also according to VPN server Authentication Type to enable authentication. Please check as below.
L2TP

This page is for setting L2TP Server, Client and Account.
**L2TP VPN Configuration**

This page is used to configure the parameters for L2TP mode VPN.

**L2TP Server**

- **Authentication Type**: Setup the authentication type for client.
- **Encryption Mode**: Setup MPPE encryption for L2TP tunnel, MPPE can only be enabled when Auth. Type set to MS-CHAPV2.
- **Tunnel Authentication**: Enable/Disable the tunnel authentication.
- **Secret Key**: Enter the secret key for tunnel authentication.
- **Assigned to Peer IP Address start from**: Enter the IP address that will be assigned to remote L2TP client. The IP address cannot in DHCP IP Pool range.
- **Local IP Address**: Enter the IP address for L2TP tunnel interface. Default is set to device LAN IP address. Example: 192.168.0.254.

**Server Account**

- **Name**: Enter the name for this account profile.
- **Account**: Enable/Disable this account.
- **Username**: Enter the username for login authentication.
- **Password**: Enter the password for login authentication.
Peer IP: Enter the peer side LAN IP address for LAN to LAN type.
Peer Subnet Mask: Enter the peer side LAN subnet mask for LAN to LAN type.

L2TP Client
Name: Enter the name for this client rule.
Server IP Address: Specify the remote L2TP server IP address or domain name.
Username: Enter the username for L2TP login authentication.
Password: Enter the password for L2TP login authentication.
Tunnel Authentication: Enable/Disable the tunnel authentication.
Secret Key: Enter the secret key for tunnel authentication.
Authentication Type: Setup the authentication type for connecting to L2TP server. This setting must follow server side.
Encryption Mode: Setup MPPE encryption for L2TP tunnel, MPPE can only be enabled when Auth. Type set to MS-CHAPV2. This setting must follow server side.
Default Gateway: Make this PPTP tunnel as default gateway for all local traffic when it is checked.
Peer IP: Enter the peer side LAN IP address for LAN to LAN type.
Peer Subnet Mask: Enter the peer side LAN subnet mask for LAN to LAN type.

How to for L2TP Server/Client

Example 1

TW-EAV510 AC in below pic left side is activated as L2TP Server and TW-EAV510 AC in below pic right side is activated as L2TP Client.
Remote Access

**TW-EAV510 (L2TP Server)**
4. Go to **WAN -> VPN -> L2TP**, enable the L2TP VPN
5. Setup L2TP Server and press **Apply** button
6. Add new user account, don’t need input Peer IP/ Peer Subnet Mask.

![L2TP Server Configuration](image)

Click **Add** button to save changes.

**TW-EAV510 AC (L2TP Client)**
1. Go to **WAN -> VPN -> L2TP**, enable the L2TP VPN, Setting L2TP Client as below.

![L2TP Client Configuration](image)

Click **Add** button to save account settings.
2. After click **Add** button, **L2TP Client Table** would add one connection, if setup all correctly VPN connection should be connected. You can also click **Disconnect** button to disconnect the L2TP connection.
3. Go to Status -> Device, you can check **L2TP Configuration** on page below, When Status shows up, you can access to remote network now. Below is Device Info for reference.

<table>
<thead>
<tr>
<th>Interface</th>
<th>Protocol</th>
<th>Local IP Address</th>
<th>Remote IP Address</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp11</td>
<td>PPP</td>
<td>172.160.0.201</td>
<td>192.168.0.254</td>
<td>up</td>
</tr>
</tbody>
</table>

**LAN to LAN**

**TW-EAV510 (L2TP Server)**

1. Go to **WAN -> VPN -> L2TP**, enable the L2TP VPN.
2. Setup L2TP Server and press **Apply** button.
3. Add new user account, enter remote network’s IP address for Peer IP/ Peer Subnet Mask.

**L2TP Server**

- **Authentication Type**: CHAP
- **Assigned to Peer IP Address start from**: 172.160.0.200
- **Local IP Address**: 192.168.0.254
- **Secret Key**: 12345678

**Server Account**

- **Name**: user
- **Username**: user
- **Peer IP**: 192.168.10.254
- **Peer Subnet Mask**: 255.255.255.0

4. After press **Add** button, **L2TP Server Table** would add account as below.

<table>
<thead>
<tr>
<th>Select</th>
<th>Name</th>
<th>Enable</th>
<th>Username</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>user</td>
<td></td>
<td>user</td>
<td>user</td>
</tr>
</tbody>
</table>

**TW-EAV510 AC (L2TP Client)**

4. Go to **WAN -> VPN -> L2TP**, enable the L2TP VPN, Setting L2TP Client as below. For LAN to LAN, you need to enter peer network information.
Click **Add** button to save account settings.

5. After click **Add** button, **L2TP Client Table** would add one connection, if setup all correctly VPN connection should be connected. You can also click **Disconnect** button to disconnect the L2TP connection.

6. Go to **Status -> Device**, you can check **L2TP Configuration** on page below, When **Status** shows **up**, you can access to remote network now. Below is Device Info for reference.

**IPSec**

This page is for setting IPSec connection.
**Remote**

**IPSec Gateway Address:** Enter the remote IPSec gateway address.

**LAN IP address:** Enter the remote local IP address that will access to this IPSec tunnel.

**Subnet Mask:** Enter the remote local subnet mask that will access to this IPSec tunnel.

**Local**

**WAN IP address:** Enter local WAN IP address which will be used for connecting to remote IPSec gateway address.

**LAN IP address:** Enter the local LAN IP address that will access to this IPSec tunnel.

**Subnet Mask:** Enter the local subnet mask that will access to this IPSec tunnel.

**Security Option**

**Encapsulation Type:** Select the encapsulation type for tunnel using.

**Pre-shared key:** Enter the pre-shared key for IPSec tunnel.
**Advanced Options:** Make it checked to modify the advanced setting for IKE phase 1 and 2.

**IKE Phase 1**
**Mode:** Default is Main mode.

**IKE Algorithm**
**Encryption Algorithm:** Select the algorithm that will be used for tunnel connection.
**Integrity Algorithm:** Select the algorithm that will be used for tunnel connection.
**Select Diffie-Hellman Group:** Select the group that will be used for tunnel connection.

**IKE Phase 2**
**Security Algorithm**
**Encryption Algorithm:** Select the algorithm that will be used for tunnel connection.
**Integrity Algorithm:** Select the algorithm that will be used for tunnel connection.
**Select Diffie-Hellman Group:** Select the group that will be used for tunnel connection.

**Note:** Both sides must use the same IKE phase 1 and 2 settings for creating IPSec tunnel.

**How to for IPsec**

**Example**

Both TW-EAV510 AC are enable IPsec function. IPSec is point-to-point, no server and client distinguish.
Remote Side

TW-EAV510 AC

1. Go to **WAN -> VPN -> IPSec**, in **Remote** part fill in other side WAN IP or domain, router LAN IP, for **Local** part, isn’t necessary fill in, because system will automatically enter, input Pre-Shared Key for authenticate, like as below picture.

   Click **Add/Save** button to save changes.

2. After Add the new config, **Key Life Time** would add one connection, user can disable/enable or delete selected.
Local Side

1. Go to **WAN -> VPN -> IPSec**, input other side router WAN IP like as below picture.

   This page is used to configure the parameters for IPsec mode VPN.

<table>
<thead>
<tr>
<th>Remote:</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPSec gateway address</td>
</tr>
<tr>
<td>LAN IP address</td>
</tr>
<tr>
<td>Subnet Mask</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Local:</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAN IP address</td>
</tr>
<tr>
<td>LAN IP address</td>
</tr>
<tr>
<td>Subnet Mask</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security Option:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encapsulation Type</td>
</tr>
<tr>
<td>Pre-Shared Key</td>
</tr>
<tr>
<td>Advanced Options</td>
</tr>
</tbody>
</table>

   Click **Add/Save** button to save changes.

2. After Add the new config, **Key Life Time** would add one connection, user can disable/enable or delete selected.

3. After both side setup ready, use PC launch CMD, try to ping other side PC, first time should be time out then would ping successfully. Now you can access to remote network.
Microsoft Windows (Version 10.0.14393)
(c) 2016 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>
C:\WINDOWS\system32>
C:\WINDOWS\system32>
C:\WINDOWS\system32> ping 192.168.10.100

Ping 192.168.10.100 with 32 bytes of data:
Request timed out.
Reply from 192.168.10.100: bytes=32 time=1ms TTL=126
Reply from 192.168.10.100: bytes=32 time=1ms TTL=126
Reply from 192.168.10.100: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.10.100:
   Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
   Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\WINDOWS\system32> ipconfig

Windows IP Configuration

Wireless LAN adapter Wi-Fi:
   Media State : Media disconnected
   Connection-specific DNS Suffix : .

Ethernet adapter 乙太網路:
   Connection-specific DNS Suffix : telewell.com
   Link-local IPv6 Address . . . . . . . . : fe80::f100:45a5:c12f:8ef6%20
   IPv4 Address . . . . . . . . . . . . . : 192.168.0.100
   Subnet Mask . . . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . . . : 192.168.0.254
OpenVPN Server

OpenVPN Server Configuration

OpenVPN Server & Client:  □ Disable  ■ Enable

Apply

OpenVPN Server

Protocol:  TCP  ▼
Port Number:  443
Tunnel Subnet:  10.8.1.0
Tunnel Mask:  255.255.255.0
Cipher Encryption:  BF-CBC  ▼
HMAC Authentication:  SHA1  ▼
Enable LZO:  □

Apply

Certificate Authority (CA): [Generate CA]

-----BEGIN CERTIFICATE-----
HTIKc5Ca0Cojk4vCA/gT/A6K16:gw/cf2F18h4G0G4xO1G89AgJyA4HPkU7egH2h
BA4K81E9U0d0v8/4sp974T4h19TX7h10XTT3Y1T80&W97cF3X7tF781c84313Yy9KXG13W9111F
vH8%18+tGy63W81Pc2sU1xh710Xj2+sMzO82Xg8gE1%9G35B91s30R39UA/tD7E9mzgG9U028
AqC0FyCr3p93m9H4S81E3C1k4y97V1c84313Yy9KXG13W9111F
vH8%18+tGy63W81Pc2sU1xh710Xj2+sMzO82Xg8gE1%9G35B91s30R39UA/tD7E9mzgG9U028
AqC0FyCr3p93m9H4S81E3C1k4y97V1c84313Yy9KXG13W9111F
vH8%18+tGy63W81Pc2sU1xh710Xj2+sMzO82Xg8gE1%9G35B91s30R39UA/tD7E9mzgG9U028
AqC0FyCr3p93m9H4S81E3C1k4y97V1c84313Yy9KXG13W9111F
vH8%18+tGy63W81Pc2sU1xh710Xj2+sMzO82Xg8gE1%9G35B91s30R39UA/tD7E9mzgG9U028
AqC0FyCr3p93m9H4S81E3C1k4y97V1c84313Yy9KXG13W9111F
vH8%18+tGy63W81Pc2sU1xh710Xj2+sMzO82Xg8gE1%9G35B91s30R39UA/tD7E9mzgG9U028
AqC0FyCr3p93m9H4S81E3C1k4y97V1c84313Yy9KXG13W9111F
vH8%18+tGy63W81Pc2sU1xh710Xj2+sMzO82Xg8gE1%9G35B91s30R39UA/tD7E9mzgG9U028
AqC0FyCr3p93m9H4S81E3C1k4y97V1c84313Yy9KXG13W9111F
vH8%18+tGy63W81Pc2sU1xh710Xj2+sMzO82Xg8gE1%9G35B91s30R39UA/tD7E9mzgG9U028
AqC0FyCr3p93m9H4S81E3C1k4y97V1c84313Yy9KXG13W9111F
vH8%18+tGy63W81Pc2sU1xh710Xj2+sMzO82Xg8gE1%9G35B91s30R39UA/tD7E9mzgG9U028
AqC0FyCr3p93m9H4S81E3C1k4y97V1c84313Yy9KXG13W9111F
vH8%18+tGy63W81Pc2sU1xh710Xj2+sMzO82Xg8gE1%9G35B91s30R39UA/tD7E9mzgG9U028
AqC0FyCr3p93m9H4S81E3C1k4y97V1c84313Yy9KXG13W9111F
vH8%18+tGy63W81Pc2sU1xh710Xj2+sMzO82Xg8gE1%9G35B91s30R39UA/tD7E9mzgG9U028
AqC0FyCr3p93m9H4S81E3C1k4y97V1c84313Yy9KXG13W9111F

-----END CERTIFICATE-----

OpenVPN Account

Name:  
Username:  
Password:  

Add

OpenVPN Account Table

<table>
<thead>
<tr>
<th>Select</th>
<th>Name</th>
<th>Username</th>
<th>Password</th>
</tr>
</thead>
</table>

Delete

OpenVPN Server & Client: This option is to Enable/Disable OpenVPN Server and Client function.

Protocol: Select the protocol for OpenVPN. It can be TCP or UDP.
Port Number: Enter the port number for OpenVPN, default is 443.
**Tunnel Subnet:** The IP subnet for tunnel interface, the system will generate the subnet for clients automatically.

**Tunnel Mask:** The subnet mask for tunnel interface.

**Cipher Encryption:** Select the encryption method.

**HMAC Authentication:** Select the authentication way.

**Enable LZO:** Make it checked to enable data compression.

**Certificate Authority (CA):** You can click “Generate CA” button to generate the CA, all clients must use this CA for OpenVPN connection.

---

**OpenVPN Account**

This is for creating the user account for remote OpenVPN client to login TW-EAV510 OpenVPN Server.

**Name:** The alias name for this account.

**Username:** The name will be used for authentication.

**Password:** The password will be used for authentication.

---

**OpenVPN Client**
**OpenVPN Client Configuration**

**OpenVPN Server & Client:** This option is to Enable/Disable OpenVPN Server and Client function.

- **Name:** The alias name for this OpenVPN client profile.
- **Server IP:** Enter the remote OpenVPN Server IP address.
- **Protocol:** Select the protocol for OpenVPN. It can be TCP or UDP.
- **Port Number:** Enter the port number for OpenVPN, default is 443.

**OpenVPN Client**

- Name:
- Server IP:
- Protocol: TCP
- Port Number: 443
- Username:
- Password:
- Cipher Encryption: BF-CBC
- HMAC Authentication: SHA1
- LZO:
- Default Gateway:
- Server CA:

**OpenVPN Trusted CA**

- Name:

```
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
```

- CA:

**OpenVPN Server & Client:** This option is to Enable/Disable OpenVPN Server and Client function.

- **Name:** The alias name for this OpenVPN client profile.
- **Server IP:** Enter the remote OpenVPN Server IP address.
- **Protocol:** Select the protocol for OpenVPN. It can be TCP or UDP.
- **Port Number:** Enter the port number for OpenVPN, default is 443.
**Username:** The name will be used for authentication.

**Password:** The password will be used for authentication.

**Cipher Encryption:** Select the encryption method.

**HMAC Authentication:** Select the authentication way.

**Enable LZO:** Make it checked to enable data compression.

**Default Gateway:** When box checked, all traffic will through this OpenVPN tunnel to remote site first.

**Server CA:** Select the CA file that will be certificated by remote OpenVPN Server.

### OpenVPN Trusted CA

**Name:** The alias name for trusted CA.

**CA:** Copy and paste the content of trusted CA.

---

**Services**

**DNS**

**Dynamic DNS**

The Dynamic DNS function allows you to alias a dynamic IP address to a static hostname, allowing users whose ISP does not assign them a static IP address to use a domain name. This is especially useful for hosting servers via your ADSL/VDSL connection, so that anyone wishing to connect to you may use your domain name, rather than having to use your dynamic IP address, which changes from time to time. This dynamic IP address is the WAN IP address of the router, which is assigned to you by your ISP.

Each DDNS Provide has different settings. You will first need to register and establish an account with the Dynamic DNS / No-IP/dy.fi provider using their website, for
example https://dyn.com/dns/.

Dynamic DNS Configuration

This page is used to configure the Dynamic DNS address from DynDNS.com or No-IP. Here you can Add/Remove to configure Dynamic DNS.

Enable:  
DDNS Provider: DynDNS.com  
Hostname:    
Interface: Any  

DDNS Settings:

User Name:    
Password:    
Interval: 8 Hour  

Add  Modify  Remove

Dynamic DNS Table

Select  State  Hostname  User Name  Service  Interval(sec.)  Status  Interface

Firewall

ALG

The ALG Controls enable or disable protocols over application layer.

ALG On-Off Configuration

This page is used to enable/disable ALG services.

ALG Type:

FTP  Enable  Disable  
H.323  Enable  Disable  
RTSP  Enable  Disable  
L2TP  Enable  Disable  
SIP  Enable  Disable  
PPTP  Enable  Disable  

Apply Changes
IP/Port Filtering

Entries in this table are used to restrict certain types of data packets through the Gateway. The use of such filters can be helpful in securing or restricting your local network.

<table>
<thead>
<tr>
<th>Outgoing Default Action</th>
<th>Transmitting Traffic</th>
<th>Deny</th>
<th>Allow</th>
<th>Apply Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incoming Default Action</td>
<td>Receiving Traffic</td>
<td>Deny</td>
<td>Allow</td>
<td>Apply Changes</td>
</tr>
</tbody>
</table>

Direction: Specify the direction of traffic.
Protocol: Specify the protocol of traffic.
Rule Action: Specify what action will be applied to this rule.
Source IP Address/Subnet Mask/Port: Enter the information of traffic that will be hooked by filter.
Destination IP Address/Subnet Mask/Port: Enter the information of traffic that will be hooked by filter.

Outgoing Default/Incoming Default Action: Specify the default action for the unmatched traffic in Current Filter Table.

Direction: Specify the direction of traffic.
Protocol: Specify the protocol of traffic.
Rule Action: Specify what action will be applied to this rule.
Source IP Address/Subnet Mask/Port: Enter the information of traffic that will be hooked by filter.
Destination IP Address/Subnet Mask/Port: Enter the information of traffic that will be hooked by filter.
MAC Filtering

MAC Filtering

Entries in this table are used to restrict certain types of data packets from your local network to the Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

**Default Action**: Specify the default action for the unmatched traffic in **Current Filter Table**.

**Source MAC Address**: Enter the information of traffic that will be hooked by filter.

Port Forwarding

In TCP/IP and UDP networks a port is a 16-bit number used to identify which application program (usually a server) incoming connections should be delivered to. Some ports have numbers that are pre-assigned to them by the IANA (the Internet Assigned Numbers Authority), and these are referred to as “well-known ports”. Servers follow the well-known port assignments so clients can locate them. If you wish to run a server on your network that can be accessed from the WAN (i.e. from other machines on the Internet that are outside your local network), or any application that can accept incoming connections (e.g. Peer-to-peer/P2P software such as instant messaging applications and P2P file-sharing applications) and are using NAT (Network Address Translation), then you will usually need to configure your router to forward these incoming connection attempts using specific ports to the PC on your network running the application. You will also need to use port forwarding if you want to host an online game server. The reason for this is that
when using NAT, your publicly accessible IP address will be used by and point to your router, which then needs to deliver all traffic to the private IP addresses used by your PCs. Please see the WAN configuration section of this manual for more information on NAT.

The device can be configured as a virtual server so that remote users accessing services such as Web or FTP services via the public (WAN) IP address can be automatically redirected to local servers in the LAN network. Depending on the requested service (TCP/UDP port number), the device redirects the external service request to the appropriate server within the LAN network. This part is only available when NAPT is enabled.

**Port Forwarding**

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

**URL Blocking**

If website’s URL or keyword matches the pre-defined URL/keyword here, the connection to this URL/keyword will be blocked.
Domain Blocking

If any domain matches the pre-defined domain here, the connection to this domain will be blocked.

Domain Blocking Configuration

This page is used to configure the blocked domain. Here you can add/delete the blocked domain.

Domain Blocking:

<table>
<thead>
<tr>
<th>Disable</th>
<th>Enable</th>
<th>Apply Changes</th>
</tr>
</thead>
</table>

Domain:

Add

Domain Blocking Configuration:

<table>
<thead>
<tr>
<th>Select</th>
<th>Domain</th>
</tr>
</thead>
</table>

Delete Selected | Delete All
DMZ

The DMZ Host is a local computer exposed to the Internet. When setting a particular internal IP address as the DMZ Host, all incoming packets will be checked by Firewall and NAT algorithms before being passed to the DMZ host, when a packet received does not use a port number used by any other Virtual Server entries.

DMZ Configuration

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

DoS

This page helps user to setup protection for DOS attack.

DoS Configuration

DoS (Denial-of-Service) attack which is launched by a hacker aims to prevent legal users from taking normal services. On this page you can take precautions to prevent some kinds of DOS attack.

- Enable DoS Block
- Whole System Flood: SYN
- Whole System Flood: FIN
- Whole System Flood: UDP
- Whole System Flood: ICMP
- Pre-Source IP Flood: SYN
- Pre-Source IP Flood: FIN
- Pre-Source IP Flood: UDP
- Pre-Source IP Flood: ICMP
- TCP/UDP PortScan
- ICMP Smurf
- IP Land
- IP TearDrop
- PingOfDeath
- TCP Scan
- TCP synWithData
- UDP Bomb
- UDP EchoChargen

- Enable Source IP Blocking

Apply Changes
UPnP

This page allows user to enable/disable the UPnP function.

**UPnP Configuration**

This page is used to configure UPnP. The system acts as a daemon when you enable it and select WAN interface (upstream) that will use UPnP.

UPnP:  
- [ ] Disable  
- [ ] Enable  

Apply Changes

Samba

This page allows user to enable/disable the Samba server when USB storage is connected.

**Samba Configuration**

This page allows users to configure Samba.

Samba:  
- [ ] Disable  
- [ ] Enable  

Server String:  

Apply Changes

**Samba:** Enable/Disable the Samba server.  
**Server String:** Descriptive string for the Samba server  
User ID: hallinta  
Password: Same as WEB GUI login password.  

**How to access Samba:**  
On a connected PC, go directly to Start -> Run, enter \192.168.0.254.
Printer Server

The page shows the printer URL when printer is connected to device via USB.

**Printer URL(s)**

This page is used to show printer URL(s).

http://192.168.0.254:631/printers/lp0

Refresh

Printer installation on Windows 10

Go to Settings -> Add printer & scanners, then click *Add a printer or scanner*.

Select “Select a shared printer by name”, copy the printer URL that shows on device WEB GUI (Advanced -> Printer) and past it here.
Click Next button and follow the instruction by Windows 10.

**Advance**

**ARP Table**

Details of ARP information can be found here.

**User List**

This table shows a list of learned MAC addresses.

<table>
<thead>
<tr>
<th>IP Address</th>
<th>MAC Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.2</td>
<td>50-e5-49-5f-7e-d5</td>
</tr>
</tbody>
</table>

[Refresh]
Routing

Enter the static routing information for an entry to the routing table. Click Add button when you are finished.

Routing Configuration

Enable: Checked to enable static route function.
Destination/Subnet Mask: Enter the destination IP address and the subnet mask.
Next Hop: Specify the gateway IP address for routing to next network.
Metric: Metric is a policy for router to commit router, to determine the optimal route. Enter one number greater than or equal to 0.
Interface: Select an interface this route associated.

Multicast

Multicast is one of the three network transmission modes, Unicast, Multicast, and Broadcast. It is a transmission mode that supports point-to-multipoint connections between the sender and the recipient. IGMP protocol is used to establish and maintain the relationship between IP host and the host directly connected multicast router. IGMP stands for Internet Group Management Protocol, it is a communications protocols used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and the adjacent multicast routers to establish multicast group members.
IGMP Proxy Configuration

**IGMP Version:** Enter the supported IGMP version v2 and v3, default is IGMP v2.

**Query Interval:** Enter the periodic query interval time (sec) the multicast router sending the query message to hosts to understand the group membership information.

**Query Response Interval:** Enter the response interval time (sec).

**Last Member Query Interval:** Enter the last member response interval time (sec).

**Robustness Value:** Enter the router robustness parameter, the greater the robustness value, the more robust the querier is.

---

**Interface Grouping**

Interface grouping is a function to group interfaces, known as VLAN. A Virtual LAN, is a group of hosts with the common set of requirements that communicate as if they were attached to the same broadcast domain, regardless of the physical location. Each group will perform as an independent network.
**IP QoS**

**QoS Policy**

**IP QoS Configuration**

**QoS Policy**

This page is used to configure the QoS policy and queue. If select PRIO of policy, the lower numbers imply a greater precedence. If select WRR of policy, please input the weight of this queue. Default is 40:30:20:10. After configuration, please click 'Apply Changes'.

<table>
<thead>
<tr>
<th>Policy</th>
<th>PRIO</th>
<th>WRR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Q2</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Q3</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Q4</td>
<td>4</td>
<td></td>
</tr>
</tbody>
</table>

**QoS Bandwidth Config**

This part is used to configure the bandwidth of different types of WAN. If select Disable, CPE will select the appropriate bandwidth based on WAN. If select Enable, User is allowed to configure specific bandwidth of WAN.

**User Defined Bandwidth:**

| Total Bandwidth Limit: 5024 Kb |

Apply Changes

**IP QoS:** Enable/Disable the IP QoS function.

**Policy:** Specify the policy for queue.

**Total Bandwidth Limit:** Specify the bandwidth of your WAN connection.
QoS Classification

This page is used to add or delete classification rule. *(After add a new rule, please click 'Apply Changes' to take effect.)*

<table>
<thead>
<tr>
<th>Mark</th>
<th>Classification Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDName</td>
<td>VLAN ID</td>
</tr>
</tbody>
</table>

Click the **Add** button to add QoS rule.

**Add QoS Classification Rules**

This page is used to add a IP QoS classification rule.

**Rule Name:**

**Assign IP Precedence/DSCP/802.1p**

- **VLAN ID (1-4095):**
- **Precedence:**
- **DSCP:**
- **802.1p:**

**Specify Traffic Classification Rules**

**IP QoS Rule by type:**

- **WAN:**

**Rule Name:** Enter the rule name.

**VLAN ID:** Enter the VLAN ID that will be assigned to the matched traffic.

**Precedence:** Specify which queue will be used.

**DSCP:** Select the DSCP mark.

**802.1p:** Specify the 802.1p value.

**IP QoS Rule by type:** Select the type which will be used to hook the traffic for applying the QoS rule.

**WAN:** Specify which WAN interface will be applied.
IPv6

IPv6 Configuration

This page is used to configure IPv6 enable/disable.

IPv6:  
- Disable
- Enable

Apply Changes

IPv6: Enable or Disable the IPv6 function.

RADVD

RADVD Configuration

This page is used to setup the RADVDs configuration of your device.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MaxRtrAdvInterval</td>
<td>600 seconds</td>
</tr>
<tr>
<td>MinRtrAdvInterval</td>
<td>198 seconds</td>
</tr>
<tr>
<td>AdvManagedFlag</td>
<td>off</td>
</tr>
<tr>
<td>AdvOtherConfigFlag</td>
<td>off</td>
</tr>
</tbody>
</table>

Apply Changes

MaxRtrAdvInterval: The maximum time allowed between sending unsolicited multicast router advertisements from the interface, in seconds. Must be no less than 4 seconds and no greater than 1800 seconds.

MinRtrAdvInterval: The minimum time allowed between sending unsolicited multicast router advertisements from the interface, in seconds. Must be no less than 3 seconds and no greater than 0.75 * MaxRtrAdvInterval.
AdvManagedFlag: When set, hosts use the administered (stateful) protocol for address autoconfiguration in addition to any addresses autoconfigured using stateless address autoconfiguration.

AdvOtherConfigFlag: When set, hosts use the administered (stateful) protocol for autoconfiguration of other (non-address) information.

**DHCPv6**

**DHCPv6 Settings**

This page is used to configure DHCPv6 Server.

**DHCPv6 Mode:**  
- **NONE**  
- **DHCPServer(Auto)**

Auto Config by Prefix Delegation for DHCPv6 Server

**DHCPv6 Mode:** Set to **DHCPServer(Auto)** to assign the IPv6 address to all LAN clients or set to **NONE** to disable it.

**MLD Proxy**

The MLD Proxy feature provides a mechanism for a device to generate MLD membership reports for all entries or a user-defined subset of these entries on the device’s upstream interface. The MLD proxy feature enables a device to learn proxy group membership information, and forward multicast packets based upon that information.

**MLD ProxyConfiguration**

This page be used to configure MLD Proxy.
MLD Proxy: Enable or disable the MLD Proxy function.

WAN Interface: Set the upstream interface for MLD Proxy. The WAN interface must have IPv6 enabled for showing here.

MLD Snooping

Similar to IGMP snooping, listens in on the MLD conversation between hosts and routers by processing MLD packets sent in a multicast network, and it analyzes all MLD packets between hosts and the connected multicast routers in the network. Without MLD snooping, multicast traffic is treated in the same manner as broadcast traffic - that is, it is forwarded to all ports. With MLD snooping, multicast traffic of a group is only forwarded to ports that have members of that group.

MLD Snooping Configuration

This page is used to configure MLD Snooping.

MLD Snooping:  

Enable or disable the MLD Snooping function.

IPv6 Routing

IPv6 Static Routing Configuration

This page is used to configure the IPv6 static routing information. Here you can add/delete static IP routes.

Enable:  
Destination:  
Next Hop:  
Metric:  
Interface:  

Add Route  Update  Delete Selected  Delete All  Show Routes

Static IPv6 Route Table:

Select  State  Destination  Next Hop  Metric  Interface
Enable: Checked to enable static route function.
Destination: Enter the destination IPv6 address.
Next Hop: Specify the gateway IPv6 address for routing to next network.
Metric: Metric is a policy for router to commit router, to determine the optimal route. Enter one number greater than or equal to 0.
Interface: Select an interface this route associated.

IP/Port Filtering

IPv6 IP/Port Filtering

Entries in this table are used to restrict certain types of data packets through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

<table>
<thead>
<tr>
<th>Outgoing Default Action</th>
<th>Deny</th>
<th>Allow</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incoming Default Action</td>
<td>Deny</td>
<td>Allow</td>
</tr>
</tbody>
</table>

Direction: **Outgoing**  Protocol: **TCP**  Rule Action: **Deny**  **Allow**

Source Interface ID:  Destination Interface ID:  Source Port:  Destination Port:  Add

Current Filter Table:

<table>
<thead>
<tr>
<th>Select</th>
<th>Direction</th>
<th>Protocol</th>
<th>Source Interface ID</th>
<th>Source Port</th>
<th>Destination Interface ID</th>
<th>Destination Port</th>
<th>Rule Action</th>
</tr>
</thead>
</table>

Outgoing Default/Incoming Default Action: Specify the default action for the unmatched traffic in Current Filter Table.
Direction: Specify the direction of traffic.
Protocol: Specify the protocol of traffic.
Rule Action: Specify what action will be applied to this rule.
Source Interface ID/Destination Interface ID: Enter the information of traffic that will be hooked by filter.
Source/Destination Port: Enter the port information of traffic that will be hooked by filter.
Diagnostics

Ping

This page will help you to diagnostic the status of your Network. You can use “Ping” methods in this page. After you input the IP address, click Go button.

**Ping Diagnostics**

This page is used to send ICMP ECHO_REQUEST packets to network host. The diagnostic result will then be displayed.

**Host Address:**

Go

Management

This page allows user to reboot your device. All services will be terminated during rebooting.

Backup/Restore

This page allows user to backup or restore the router settings to/from file.

**Backup and Restore Settings**

This page allows you to backup current settings to a file or restore the settings from the file which was saved previously. Besides, you could reset the current settings to factory default.

**Backup Settings to File:** [Backup...]

**Restore Settings from File:** [Browse...] [Restore]

**Reset Settings to Default:** [Reset]
Password

The administrator password can be changed by this page. Suggest to change default password for better security protection.

**Password Configuration**

This page is used to set the account to access the web server of your device. Emptying the username and password field will disable the protection.

**User Name:**

[Username]

**Old Password:**


**New Password:**


**Confirmed Password:**


[Apply Changes]

Firmware Upgrade

The firmware keeps enhancement and improvement. This page allows user to upgrade to a new firmware once it is available.

Click “Upgrade(auto)” button will upgrade the up to date firmware from remote server, please make sure the Internet connection is work before clicking.
Firmware Upgrade

This page allows you to upgrade the firmware to the latest version. Do NOT switch the power of the device off during the upload, as this will make the system unbootable.

- **Upload firmware with default configuration**
  - **Browse…** No file selected.
  - **Upgrade**  **Upgrade(auto)**

**Important:** Please don’t power off the router during upgrade, otherwise it may damage your router.

ACL

This page allows user to allow/block to access the router’s service with specify IP address or network on both LAN and WAN direction.

**ACL Configuration**

This page is used to configure the IP Address for the Access Control List. If ACL is enabled, only the IP address in the ACL Table can access the CPE. Here you can add/delete the IP Address.

**Note:** Once ACL is enabled, the device’s HTTP service are not reachable from the WAN interface if the default login password is not changed!

<table>
<thead>
<tr>
<th>ACL Capability:</th>
<th>Disable</th>
<th>Enable</th>
<th><strong>Apply Changes</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable:</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interface:</td>
<td>LAN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP Address:</td>
<td></td>
<td></td>
<td>0.0.0.0 -&gt; Allows connections from anywhere.</td>
</tr>
<tr>
<td>Subnet Mask:</td>
<td></td>
<td></td>
<td>0.0.0.0 -&gt; Allows connections from anywhere.</td>
</tr>
</tbody>
</table>

**Service Name**

<table>
<thead>
<tr>
<th>LAN</th>
<th>Any</th>
<th>TELNET</th>
<th>HTTP</th>
<th>HTTPS</th>
<th>PING</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**ACL Table**

<table>
<thead>
<tr>
<th>Select</th>
<th>State</th>
<th>Interface</th>
<th>IP Address</th>
<th>Services</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Enable</td>
<td>LAN</td>
<td>0.0.0.0</td>
<td>web, https, ping</td>
<td>80,443</td>
</tr>
<tr>
<td></td>
<td>Enable</td>
<td>WAN</td>
<td>0.0.0.0</td>
<td>ping</td>
<td></td>
</tr>
</tbody>
</table>
**ACL Capability:** The router’s all service will be opened and can be accessed by any direction if set to disable. Default is enable.

**Time Zone**

Setup the Time Zone and NTP server here to correct and sync the time on the router.

**Time Zone Configuration**

You can maintain the system time by synchronizing with a public time server over the Internet.

<table>
<thead>
<tr>
<th>Current Time:</th>
<th>Year: 1970</th>
<th>Mon: 1</th>
<th>Day: 1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Hour: 8</td>
<td>Min: 57</td>
<td>Sec: 59</td>
</tr>
</tbody>
</table>

**Time Zone Select:** Europe/Helsinki (UTC+02:00)

- **Enable Daylight Saving Time**
- **Enable SNTP Client Update**

**WAN Interface:** Any

**SNTP Server:**
- time.stdtime.gov.tw
- clock.stdtime.gov.tw

[Apply Changes] [Refresh]

**Auto Reboot**

User can specify two time schedules to force device to reboot automatically.

**Auto Reboot**

This page is used to configure time schedule and reboot your system.

<table>
<thead>
<tr>
<th>Configure Schedule</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Schedule</td>
</tr>
<tr>
<td>1. Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat ☑ 00:00 : 00</td>
</tr>
<tr>
<td>2. Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat ☑ 00:00 : 00</td>
</tr>
</tbody>
</table>

[Apply]
Statistics

Interface

This page shows the statistics of each interface. Click *Reset Statistics* button to reset counter.

**Interface Statistics**

This page shows the packet statistics for transmission and reception regarding to network interface.

<table>
<thead>
<tr>
<th>Interface</th>
<th>Rx pkt</th>
<th>Rx err</th>
<th>Rx drop</th>
<th>Tx pkt</th>
<th>Tx err</th>
<th>Tx drop</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAN PORT1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>LAN PORT2</td>
<td>741</td>
<td>0</td>
<td>0</td>
<td>1040</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>LAN PORT3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>LAN PORT4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>WLAN 2.4G</td>
<td>520</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>WLAN 5G</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ADSL_0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ADSL_1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ADSL_2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>VDSL_0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>VDSL_1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>EWAN_0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>6</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>USB 3G/4G</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

[Refresh]  [Reset Statistics]

DSL

This page shows more details of your xDSL line.
DSL Statistics

<table>
<thead>
<tr>
<th>Mode</th>
<th>VDSL2-30A Annex A</th>
</tr>
</thead>
<tbody>
<tr>
<td>TFS-TC</td>
<td>PTM</td>
</tr>
<tr>
<td>Latency</td>
<td>Fast</td>
</tr>
<tr>
<td>Status</td>
<td>SHOWTIME.</td>
</tr>
<tr>
<td>Power Level</td>
<td>L0</td>
</tr>
<tr>
<td>Uptime</td>
<td>00:15:49</td>
</tr>
<tr>
<td>G.Vector</td>
<td>Off</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Downstream</th>
<th>Upstream</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trellis</td>
<td>On</td>
<td>On</td>
</tr>
<tr>
<td>SNR Margin (dB)</td>
<td>27.0</td>
<td>10.8</td>
</tr>
<tr>
<td>Attenuation (dB)</td>
<td>32765.0</td>
<td>3.0</td>
</tr>
<tr>
<td>Output Power (dBm)</td>
<td>12.0</td>
<td>14.0</td>
</tr>
<tr>
<td>Attainable Rate (Kbps)</td>
<td>230792</td>
<td>116224</td>
</tr>
<tr>
<td>G.INP</td>
<td>Off</td>
<td>Off</td>
</tr>
<tr>
<td>Rate (Kbps)</td>
<td>101063</td>
<td>101033</td>
</tr>
<tr>
<td>R (number of check bytes in RS code word)</td>
<td>16</td>
<td>16</td>
</tr>
<tr>
<td>N (RS codeword size)</td>
<td>255</td>
<td>255</td>
</tr>
<tr>
<td>L (number of bits in DMT frame)</td>
<td>13549</td>
<td>13537</td>
</tr>
<tr>
<td>S (RS code word size in DMT frame)</td>
<td>0.15</td>
<td>0.15</td>
</tr>
<tr>
<td>D (interleaver depth)</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Delay (mscc)</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>INP (DMT frame)</td>
<td>0.004</td>
<td>0.004</td>
</tr>
<tr>
<td>FEC errors</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>OH Frame</td>
<td>1123080</td>
<td>788004</td>
</tr>
<tr>
<td>OH Frame errors</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total ES</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total SES</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total US</td>
<td>313</td>
<td>0</td>
</tr>
<tr>
<td>Total LOSS</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>Last Link Rate</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Full Init</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Failed Full Init</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Synchronized time(Second)</td>
<td>941</td>
<td></td>
</tr>
<tr>
<td>Synchronized number</td>
<td>3</td>
<td></td>
</tr>
</tbody>
</table>

Language

This page allows user to configure the WEB GUI display language.
Multi-Lingual Setting

This page is used to set multi-lingual.
Language Select:  

Update selected language

Reboot

Click the Reboot button to reboot the device immediately.

Reboot

This page is used to reboot your system.

Logout

This page will force the user logout immediately by clicking Logout button.

Logout

This page is used to logout from the Device.