



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

User Manual

V1.9

Directory

Introduction.....	5
Introduction to your Router.....	5
Features.....	7
Physical Interface	8
Package Contents	9
Device Description	10
Network Configuration	14
Factory Default Settings	17
Web Interface (Username and Password).....	17
Device LAN IPv4 settings.....	18
DHCP server for IPv4.....	18
Configuration.....	18
Configuration via Web Interface.....	18
Status	20
Device.....	20
3G/4G/LTE Info	22
LAN/WLAN Clients.....	22
AP Neighbor	22
IPv6.....	23
Ethernet Port.....	23
System Log.....	24
LAN	24
WLAN	26
WLAN 2.4GHz / 5GHz	26
Basic Settings.....	26
Advanced Settings	27
Security.....	28
Access Control	29
Site Survey	30
WPS	30
Status.....	31
WAN	31
WAN Mode.....	31
Default Routing	31
Ethernet WAN	32
PTM(VDSL) WAN	34

ATM(ADSL) WAN	35
DSL Settings	36
3G/4G LTE Settings	37
VPN.....	39
PPTP.....	39
L2TP	48
IPSec	53
OpenVPN Server	59
OpenVPN Client.....	60
Services	62
DNS.....	62
Dynamic DNS.....	62
Firewall	63
ALG	63
IP/Port Filtering	64
MAC Filtering.....	65
Port Forwarding.....	65
URL Blocking.....	66
Domain Blocking.....	67
DMZ.....	68
DoS	68
UPnP.....	69
Samba.....	69
Printer Server	70
Advance.....	71
ARP Table.....	71
Routing	72
Multicast	72
Interface Grouping	73
IP QoS	74
QoS Policy.....	74
QoS Classification	75
IPv6.....	76
IPv6.....	76
RADVD	76
DHCPv6.....	77
MLD Proxy	77
MLD Snooping	78

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 2^{128} (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.

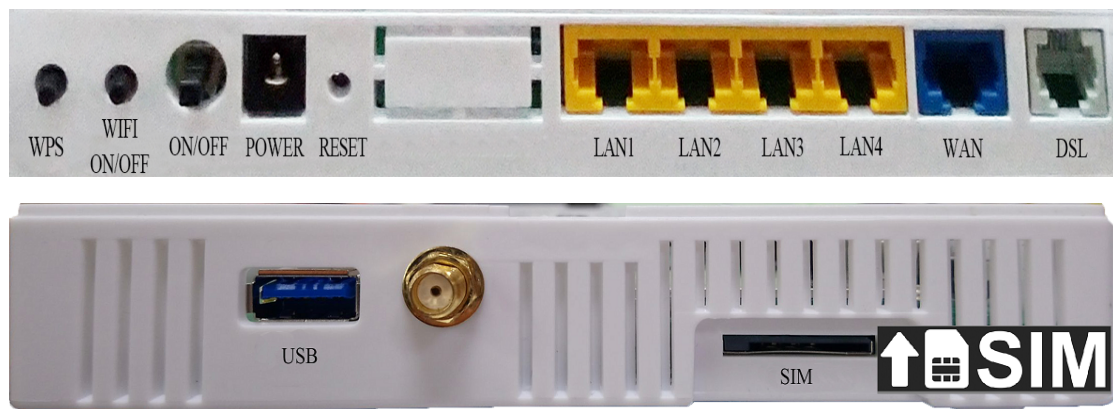
Device Description

The Front LEDs

</

	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



Port	Meaning
DSL	Connect the supplied Telephone cable to DSL port
WAN	Connect one end of Ethernet cable to the WAN port when connecting other fixed line modem
LAN1-4	Connect a Ethernet cable to one of the LAN ports when connecting to a PC or an office/home network
WiFi ON/OFF	Press and release quickly to enable or disable the 2.4G and 5G Wi-Fi function
RESET	Power on device and wait for 60 seconds, then press it 5 seconds or above to restore to factory default
WPS	Press and release quickly to enable the WPS function
Power	Connect the supplied power adapter to this jack
Switch or ON/OFF	Power ON / OFF switch
USB	Connect your storage or printer device

SIM	The slot to insert the Mini-SIM(2FF) card (Please power off and insert the SIM card, then power on)
Fixed Wi-Fi Antenna	The fixed antennas are for Wi-Fi 2.4G and 5G
Detachable LTE Antenna	Standard SMA socket and can change antenna by user self

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.

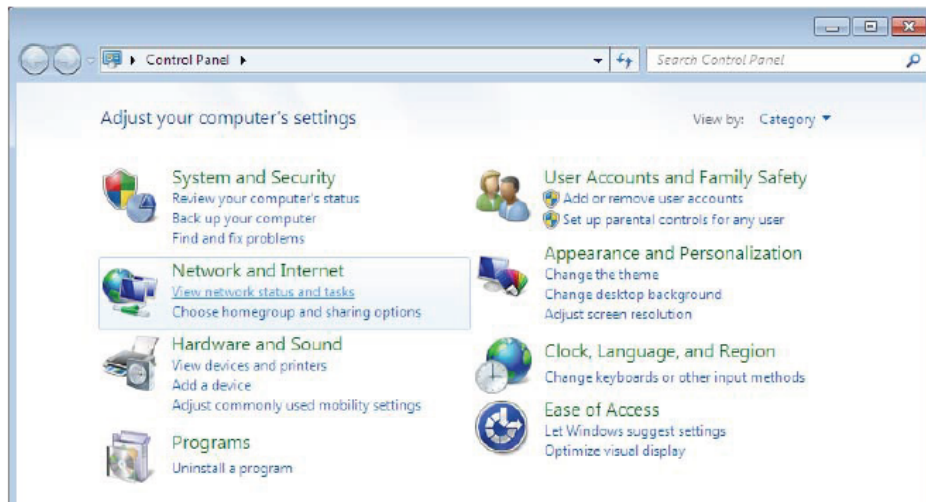
Please follow the following steps to configure your PC network environment.

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

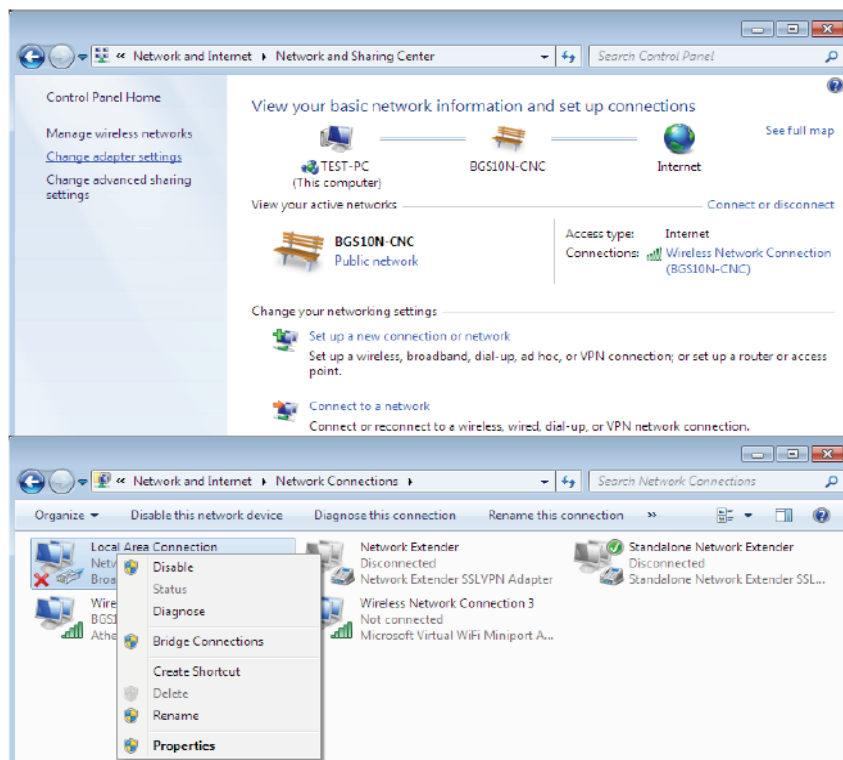
Go to Start. Click on Control Panel. Then click on Network and Internet.



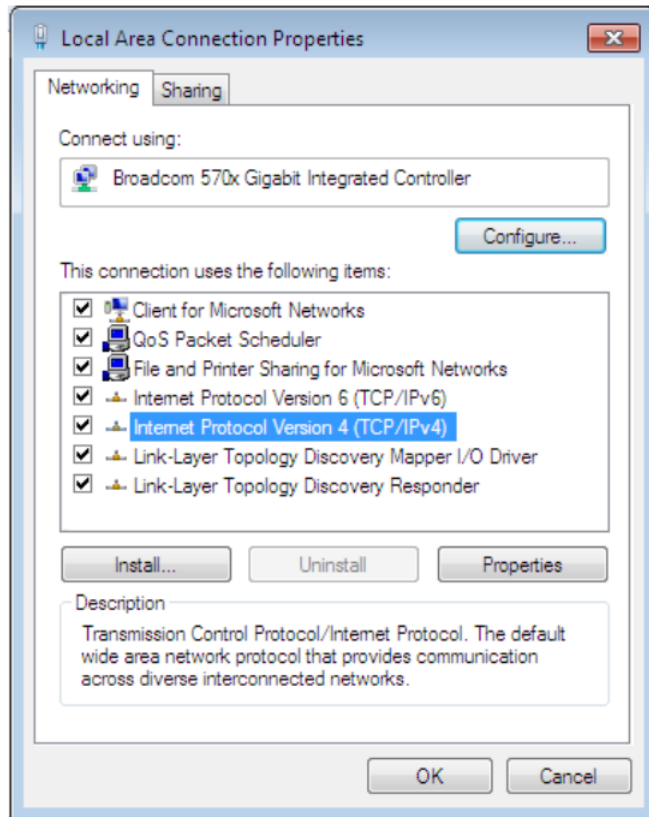
When the Network and Sharing Center window pops up, select and click on Change adapter settings on the left window panel.

Select the Local Area Connection, and right click the icon to select Properties.

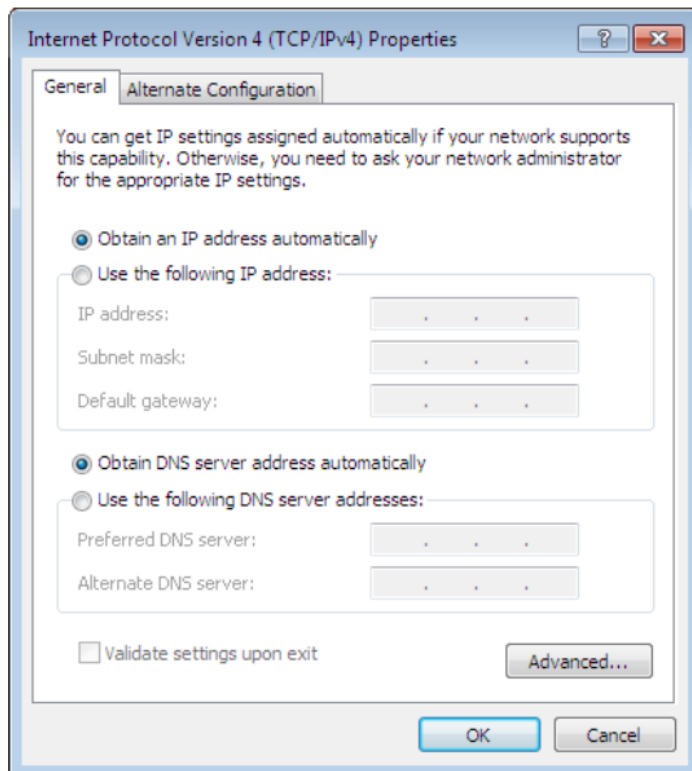
IPv4:



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

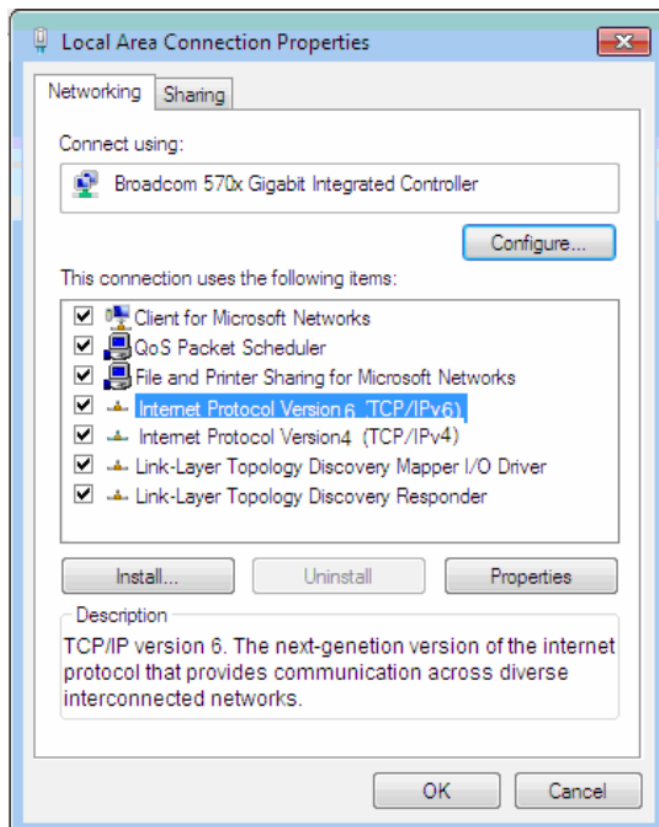


In the TCP/IPv4 properties window, select the Obtain an IP address automatically and Obtain DNS Server address automatically radio buttons. Then click OK to exit the setting. Click OK again in the Local Area Connection Properties window to apply the new configuration.

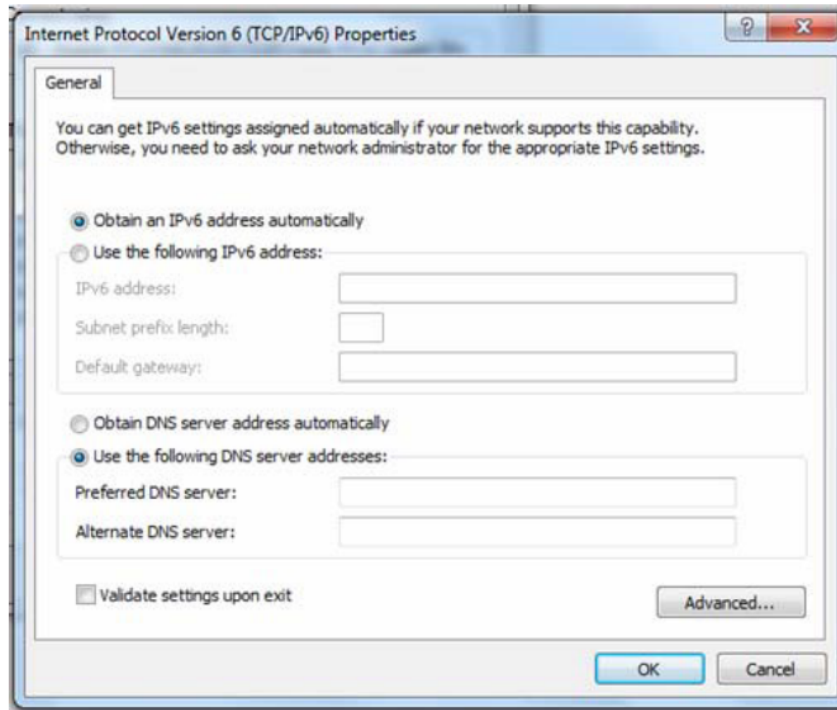


IPv6:

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

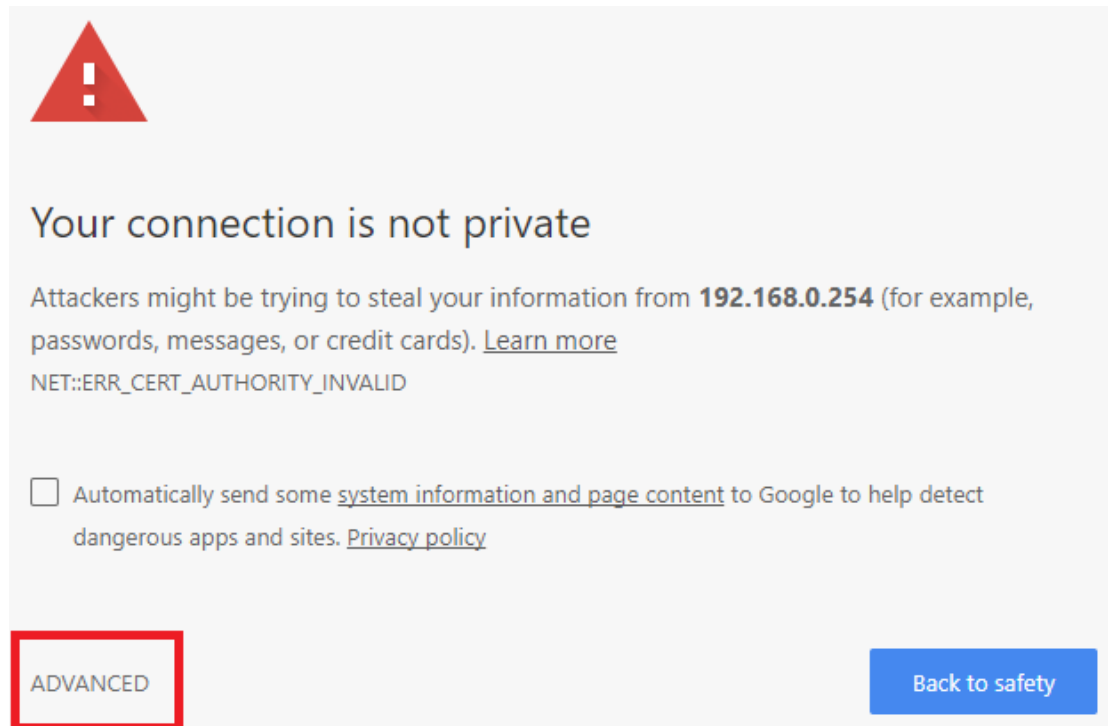
Open your web browser; enter the IP address of your router, which by default is 192.168.0.254, and click ok or press 'Enter' key on the keyboard, a login prompt window will appear.



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).



Just click the link “ADVANCED”, and then click link “Proceed to 192.168.0.254 (unsafe)” to establish HTTPS connection with the router.



Your connection is not private

Attackers might be trying to steal your information from **192.168.0.254** (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR_CERT_AUTHORITY_INVALID

☐ Automatically send some [system information and page content](#) to Google to help detect dangerous apps and sites. [Privacy policy](#)

HIDE ADVANCED

[Back to safety](#)

This server could not prove that it is **192.168.0.254**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

[Proceed to 192.168.0.254 \(unsafe\)](#)

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.

System	
Model Name	TW-EAV510 AC-LTE CAT 6
Serial Number	RRNHBX1816000008387K
Uptime	2 min
Firmware Version	1.1.00-45
DSP Version	v136h720
CPU Usage	0.1%
Memory Usage	40%
Name Servers	61.31.1.1, 8.8.8.8
IPv4 Default Gateway	10.125.17.77
DSL	
Operational Status	ACTIVATING.
Upstream Speed	0 kbps
Downstream Speed	0 kbps
SNR (dB)	Down: 0.0 / Up: 0.0
Attenuation (dB)	Down: 0.0 / Up: 0.0
LAN Configuration	
IP Address	192.168.0.254
Subnet Mask	255.255.255.0
DHCP Server	Enabled
MAC Address	001EAB565F1F

WAN Configuration						
Interface	VPI/VCI	Encapsulation	Protocol	IP Address	Gateway	Status
ADSL_0	0/33	LLC	mer1483			DOWN
ADSL_1	0/35	LLC	mer1483			DOWN
ADSL_2	0/100	LLC	mer1483			DOWN
VDSL_0	---	---	IPoE			DOWN
VDSL_1	---	---	IPoE			DOWN
EWAN_0	---	---	IPoE			DOWN

3G Configuration				
Interface	Protocol	IP Address	Gateway	Status
3G/4G/LTE	DHCP	10.125.17.76	10.125.17.76	UP / <div>Disconnect</div>

PPTP Configuration				
Interface	Protocol	IP Address	Gateway	Status

L2TP/IPSec Configuration				
Interface	Protocol	Local IP Address	Remote IP Address	Status

Refresh

3G/4G/LTE Info

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

3G/4G/LTE Info

3G/4G/LTE Info

3G/4G/LTE Info	
3G/4G/LTE Status	UP
Operator Name	46697
Frequency Band	3 Band & Frequency
Network Mode	LTE
Signal Strength	<div><div></div><div></div><div></div><div></div></div> -69dbm
Card Name	LTE WIRELESS MODEM
Card Firmware	M1.0.7_E1.0.0_A1.1.4

LAN/WLAN Clients

This page shows all connected device's information.

LAN/WLAN Clients

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.

Hostname	MAC Address	IP Address	IP Assignment	Expired Time (sec)	Interface	SSID	RSSI
iPhone	70-70-0D-11-75-F1	192.168.0.101	Dynamic	86396	2.4G	TW-EAV510-2.4G-001	-77
---	50-E5-49-5F-7F-D5	192.168.0.100	Static	---	Ethernet Port2	---	---

[Refresh](#)

AP Neighbor

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

AP Neighbor

This table shows Neighbor AP to know channel usage around end user's house.

WLAN 2.4GHz

SSID	BSSID	Channel Mode	Type	Encryption	RSSI	Channel Width
Netcore	08:10:77:e4:d8:2a	6+2 B+G+N	AP	WPA-PSK/WPA2-PSK	-68	20M/40M
Office-2.4G	74:19:f8:e0:2d:09	9 B+G+N	AP	WPA2-PSK	-85	20M

WLAN 5GHz

SSID	BSSID	Channel Mode	Type	Encryption	RSSI	Channel Width
Office-5G	74:19:f8:e0:2d:0a	64 5320MHz (5310~5330MHz) A+N+AC	AP	WPA2-PSK	-85	58 5290MHz (5250~5330MHz) 20M/40M/80M

Refresh

IPv6

This page shows the current system status of IPv6.

IPv6 Status

This page shows the current system status of IPv6.

LANConfiguration

IPv6 Address	2001:b011:700d:1150:7619:f8ff:fee0:18/64
IPv6 Link-Local Address	fe80::/64

Prefix Delegation

Prefix	2001:b011:700d:1150::/64
--------	--------------------------

Interface	VPI/VCI	Encapsulation	Protocol	IP Address	Status
ppp0_ptm0_1	---	---	PPPoE	2001:b011:700d:5b0:7619:f8ff:fee0:1f/64	up
ptm0_0	---	---	IPoE		up

Refresh

Ethernet Port

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

Ethernet Port Status

This page shows the current Ethernet Port status.

Ethernet Port Status	
LAN Port1	not-connected
LAN Port2	Up, 1000Mb, Full
LAN Port3	not-connected
LAN Port4	not-connected
EWAN Port	not-connected

Refresh

System Log

System Log

System Log :	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Log Level :	Infomational ▼
Display Level :	Infomational ▼
<p>Apply Changes</p>	
Save Log to File:	Save...
Clear Log:	Reset

System Log

Refresh

Date/Time	Facility	Level	Message
-----------	----------	-------	---------

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..

IP Address:	<input type="text" value="192.168.0.254"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>
IGMP Snooping:	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled
Ethernet to Wireless Blocking:	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled

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.

IP Pool Range:	<input type="text" value="192.168.0.100"/> - <input type="text" value="192.168.0.200"/>
	<input type="button" value="Show Client"/>
Max Lease Time:	<input type="text" value="86400"/> seconds (-1 indicates an infinite lease)
DomainName:	<input type="text" value="telewell.oy"/>
Gateway Address:	<input type="text" value="192.168.0.254"/>
DNS option:	<input checked="" type="radio"/> Use DNS Relay <input type="radio"/> Set Manually
<input type="button" value="Apply Changes"/> <input type="button" value="MAC-Based Assignment"/>	

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

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.

☐ **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.

Fragment Threshold:	<input type="text" value="2346"/>	(256-2346)
RTS Threshold:	<input type="text" value="2347"/>	(0-2347)
Beacon Interval:	<input type="text" value="100"/>	(20-1024 ms)
Preamble Type:	<input checked="" type="radio"/> Long Preamble <input type="radio"/> Short Preamble	
Broadcast SSID:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	
Protection:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	
Aggregation:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	
Short GI:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	
WMM Support:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	

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

SSID:

Encryption:

WPA Cipher Suite: ☒ TKIP ☒ AES

WPA2 Cipher Suite: ☒ TKIP ☒ AES

Group Key Update Timer:

Pre-Shared Key:

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 Suit: 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. AABBCDD0011)

Add

Reset

Current Access Control List

MAC Address	Select
-------------	--------

Delete 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.

SSID	BSSID	Channel Mode	Type	Encryption	RSSI	Channel Width
Netcore	08:10:77:e4:d8:2a	6+2 B+G+N	AP	WPA-PSK/WPA2-PSK	-68	20M/40M
Office-2.4G	74:19:f8:e0:2d:09	9 B+G+N	AP	WPA2-PSK	-85	20M

Refresh

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.

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

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

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 if the WAN interface is connected. Priority order can be changed by up and down them back in again.

USB 3G/4G
VDSL_1
VDSL_0
ADSL_2
ADSL_1
ADSL_0
EWAN_0

↑

↓

Apply Changes

Ethernet WAN

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

Ethernet WAN Configuration

This page is used to configure the parameters for Ethernet WAN

EWAN_0 ▼

Enable VLAN: ☐

VLAN ID:

802.1p_Mark

Channel Mode:

Enable Bridge: ☐

Bridge Mode:

Enable NAPT: ☒

Enable QoS: ☐

Channel: ☒ Enable ☐ Disable

MTU:

Enable IGMP-Proxy: ☒

WAN IP Settings: Type: ☐ Fixed IP ☒ DHCP

Local IP Address:

Remote IP Address:

Subnet Mask:

IP Unnumbered ☐

Request DNS: ☒ Enable ☐ Disable

Primary DNS Server:

Secondary DNS Server:

Apply Changes

Delete

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.

PTM(VDSL) WAN

The page is used to configure the parameters and protocol for the VDSL2 WAN port.

PTM(VDSL) WAN Configuration

This page is used to configure the parameters for PTM(VDSL) WAN

VDSL_0 ▾

Enable VLAN: ☐

VLAN ID:

802.1p_Mark

Channel Mode: ▾

Enable Bridge: ☐

Bridge Mode: ▾

Enable NAPT: ☒

Enable QoS: ☐

Channel: ☒ Enable ☐ Disable

MTU:

Enable IGMP-Proxy: ☒

WAN IP Settings: Type: ☐ Fixed IP ☒ DHCP

Local IP Address:

Remote IP Address:

Subnet Mask:

IP Unnumbered ☐

Request DNS: ☒ Enable ☐ Disable

Primary DNS Server:

Secondary DNS Server:

Apply Changes

Delete

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

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.

ATM(ADSL) WAN

ATM(ADSL) WAN Configuration

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

VPI: VCI:





Encapsulation: ☒ LLC ☐ VC-Mux Channel Mode:

Enable NAPT: ☐ Enable QoS: ☐

Channel: ☒ Enable ☐ Disable

Enable IGMP-Proxy: ☐

Current ATM VC Table

Select	Interface	Mode	VPI	VCI	Encapsulation	NAPT	IGMP	Remote IP	UserName	Default Route	Status	Actions
<input type="radio"/>	ADSL_0	mer1483	0	33	LLC	on	on			on	Enabled	 
<input type="radio"/>	ADSL_1	mer1483	0	35	LLC	on	on			on	Enabled	 
<input type="radio"/>	ADSL_2	mer1483	0	100	LLC	on	on			on	Enabled	 

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

Enable NAT: 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 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.

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:	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Network Preference:	Use LTE module settings ▼
PIN Code:	<input type="text"/>
APN:	internet
Dial Number:	*99#
Authentication:	NONE ▼
Username:	<input type="text"/>
Password:	<input type="text"/>
Keep Alive:	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Time:	30 seconds [3-86400]
IP Address:	<input type="text"/> Empty means the 3G/LTE Primary DNS
MTU:	1500
NAPT:	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Default Route:	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
MTU:	1500
Extra_AT Command:	<input type="text"/>

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.

User Name: Enter the username that is provided by your ISP (optional).

Password: Enter the password that is provided by your ISP (optional).

Keep Alive: Enable/Disable keep alive function for 3G/4G LTE connection.

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 ▾

Assigned to Peer IP Address start from:

Local IP Address: 192.168.0.254

Apply

Server Account

Name:

Account: ☐ Disable ☒ Enable

Username:

Password:

Peer IP: optional, e.g. 10.0.0.1

Peer Subnet Mask: optional, e.g. 255.255.255

Add

PPTP Server Table

Select	Name	Enable	Username	Password
Delete Selected	Save			

PPTP Client

Name:

Server IP Address:

Username:

Password:

Authentication Type: CHAP ▾

Encryption Mode: NONE ▾

Default Gateway: ☐

Peer IP: optional, e.g. 10.0.0.1

Peer Subnet Mask: optional, e.g. 255.255.255

Add

PPTP Client Table

Select	Name	Interface	Server	Default Gateway	Peer Network	Action
Delete Selected						

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.

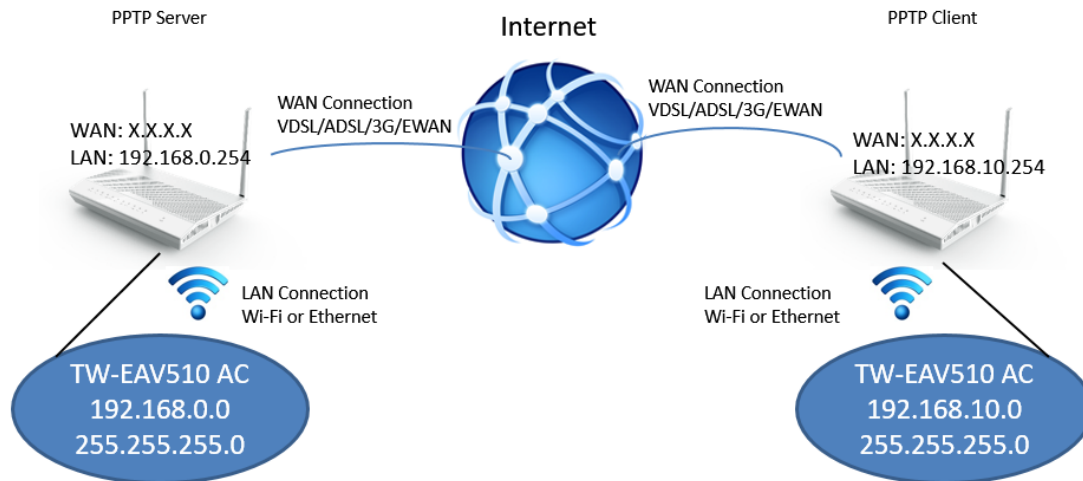
Peer IP: Enter the peer side LAN IP address for LAN to LAN type.

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.

PPTP Server

Authentication Type:	<input type="text" value="CHAP"/>	Encryption Mode:	<input type="text" value="NONE"/>
Assigned to Peer IP Address start from:	<input type="text" value="192.168.100.200"/>	Local IP Address:	<input type="text" value="192.168.0.254"/>
<input type="button" value="Apply"/>			

Server Account

Name:	<input type="text" value="admin"/>	Account:	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Username:	<input type="text" value="admin"/>	Password:	<input type="text" value="admin"/>
Peer IP:	<input type="text" value="optional, e.g. 10.0.0.1"/>	Peer Subnet Mask:	<input type="text" value="optional, e.g. 255.255.255.0"/>

PPTP Server Table

Select	Name	Enable	Username	Password
<input type="checkbox"/>	admin	<input checked="" type="checkbox"/>	admin	admin

TW-EAV510 AC (PPTP Client)

1. Go to **WAN -> VPN -> PPTP**, enable the PPTP VPN, Setting PPTP Client as below.

PPTP Client

Name:	<input type="text" value="admin"/>	Server IP Address:	<input type="text" value="36.229.14.220"/>
Username:	<input type="text" value="admin"/>	Password:	<input type="text" value="admin"/>
Authentication Type:	<input type="text" value="CHAP"/>	Encryption Mode:	<input type="text" value="NONE"/>
Default Gateway:	<input type="checkbox"/>		
Peer IP:	<input type="text" value="optional, e.g. 10.0.0.1"/>	Peer Subnet Mask:	<input type="text" value="optional, e.g. 255.255.255.255"/>

PPTP Client Table						
Select	Name	Interface	Server	Default Gateway	Peer Network	Action
<input type="button" value="Delete Selected"/>						

Click **Add** button to save account settings.

- 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.

PPTP Client Table						
Select	Name	Interface	Server	Default Gateway	Peer Network	Action
<input type="checkbox"/>	admin	ppp9_pptp0	36.229.14.220	off		<input type="button" value="Disconnect"/>
<input type="button" value="Delete Selected"/>						

- 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.

PPTP Configuration				
Interface	Protocol	IP Address	Gateway	Status
ppp9	PPP	192.168.100.200	192.168.0.254	up

LAN to LAN

TW-EAV510 (PPTP Server)

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

PPTP Server

Authentication Type:	CHAP ▼	Encryption Mode:	NONE ▼
Assigned to Peer IP Address start from:	192.168.100.200	Local IP Address:	192.168.0.254
<input type="button" value="Apply"/>			

Server Account

Name:	user	Account:	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Username:	user	Password:	user
Peer IP:	192.168.10.254	Peer Subnet Mask:	255.255.255.0
<input type="button" value="Add"/>			

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

PPTP Server Table				
Select	Name	Enable	Username	Password
<input type="checkbox"/>	user	<input checked="" type="checkbox"/>	user	user
<input type="button" value="Delete Selected"/>		<input type="button" value="Save"/>		

TW-EAV510 AC (PPTP Client)

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

PPTP Client

Name:	user	Server IP Address:	36.229.14.220
Username:	user	Password:	user
Authentication Type:	CHAP ▼	Encryption Mode:	NONE ▼
Default Gateway:	<input type="checkbox"/>		
Peer IP:	192.168.0.254	Peer Subnet Mask:	255.255.255.0
<input type="button" value="Add"/>			

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.

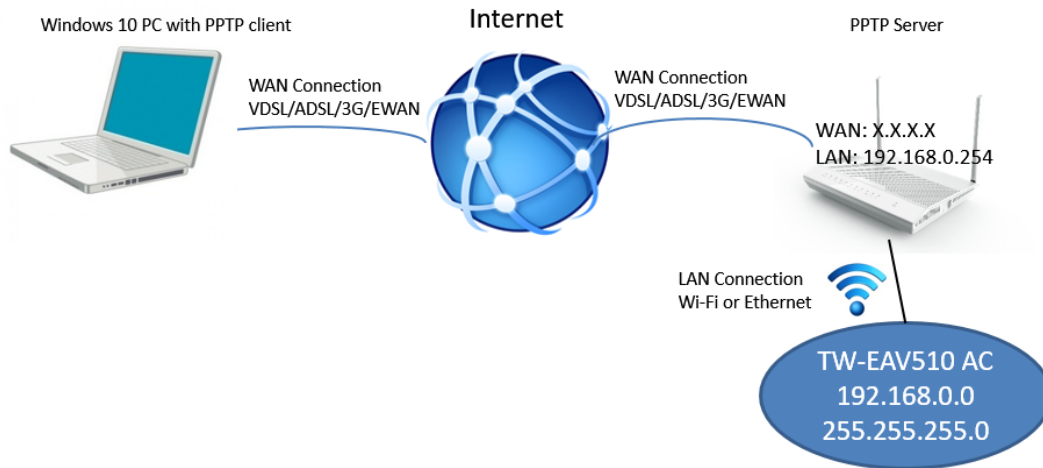
PPTP Client Table						
Select	Name	Interface	Server	Default Gateway	Peer Network	Action
<input type="checkbox"/>	user	ppp9_pptp0	36.229.14.220	off	192.168.0.254 255.255.255.0	<input type="button" value="Disconnect"/>
<input type="button" value="Delete Selected"/>						

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

PPTP Configuration				
Interface	Protocol	IP Address	Gateway	Status
ppp9	PPP	192.168.100.200	192.168.0.254	up

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.

PPTP Server

Authentication Type:	<input type="text" value="CHAP"/>	Encryption Mode:	<input type="text" value="NONE"/>
Assigned to Peer IP Address start from:	<input type="text" value="192.168.100.254"/>	Local IP Address:	<input type="text" value="192.168.0.254"/>
<input type="button" value="Apply"/>			

Server Account

Name:	<input type="text" value="admin"/>	Account:	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Username:	<input type="text" value="admina"/>	Password:	<input type="text" value="admin"/>
Peer IP:	<input type="text" value="optional, e.g. 10.0.0.1"/>	Peer Subnet Mask:	<input type="text" value="optional, e.g. 255.255.255."/>

PPTP Server Table

Select	Name	Enable	Username	Password
<input type="checkbox"/>	admin	<input checked="" type="checkbox"/>	admin	admin

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.

Change your networking settings



Set up a new connection or network

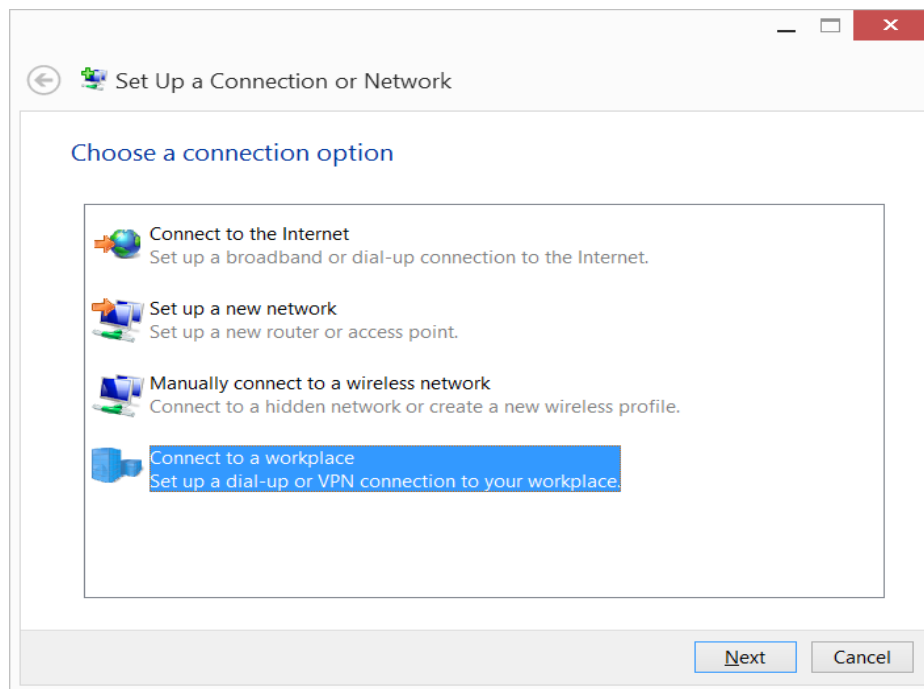
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.



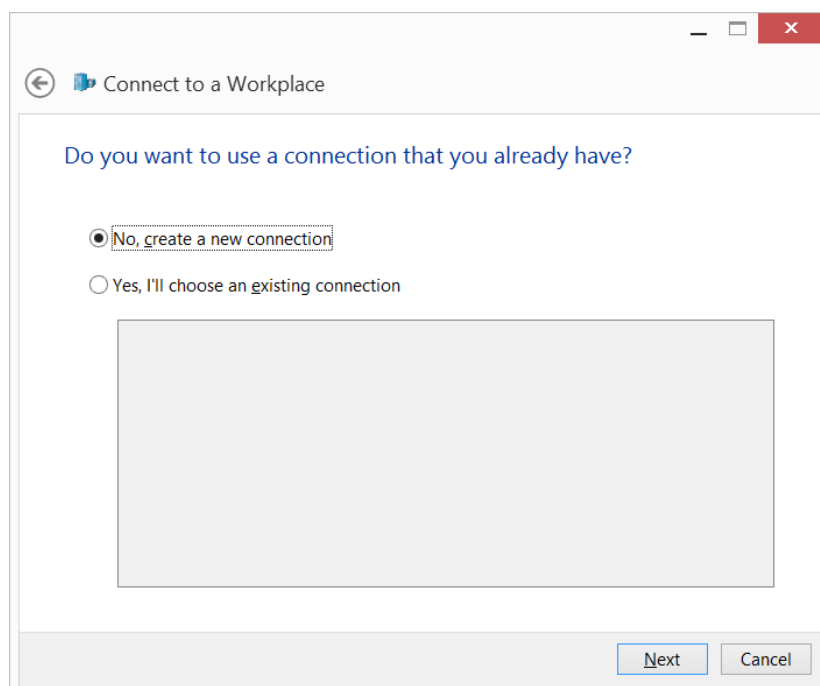
Troubleshoot problems

Diagnose and repair network problems, or get troubleshooting information.

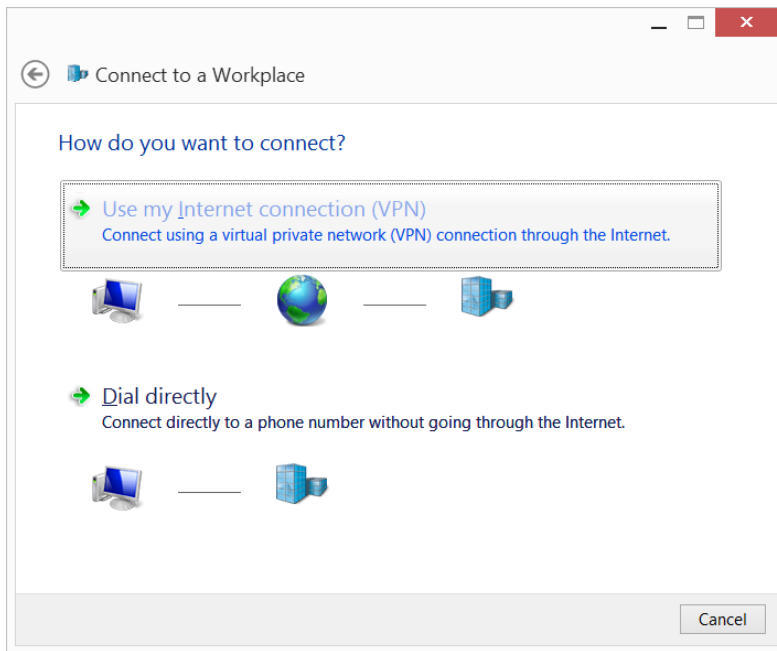
3. Select **Connect to a workplace**.



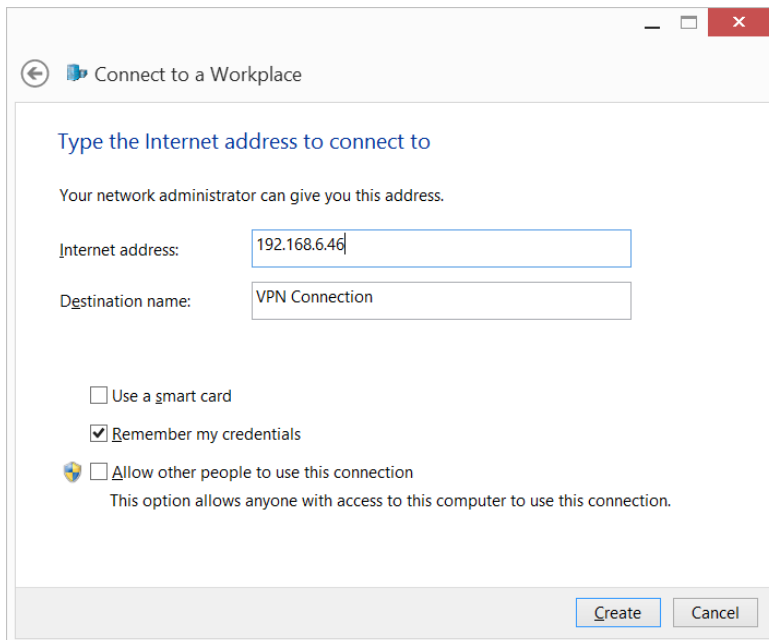
4. Select **No, create a new connection** and click **Next** button for next step.



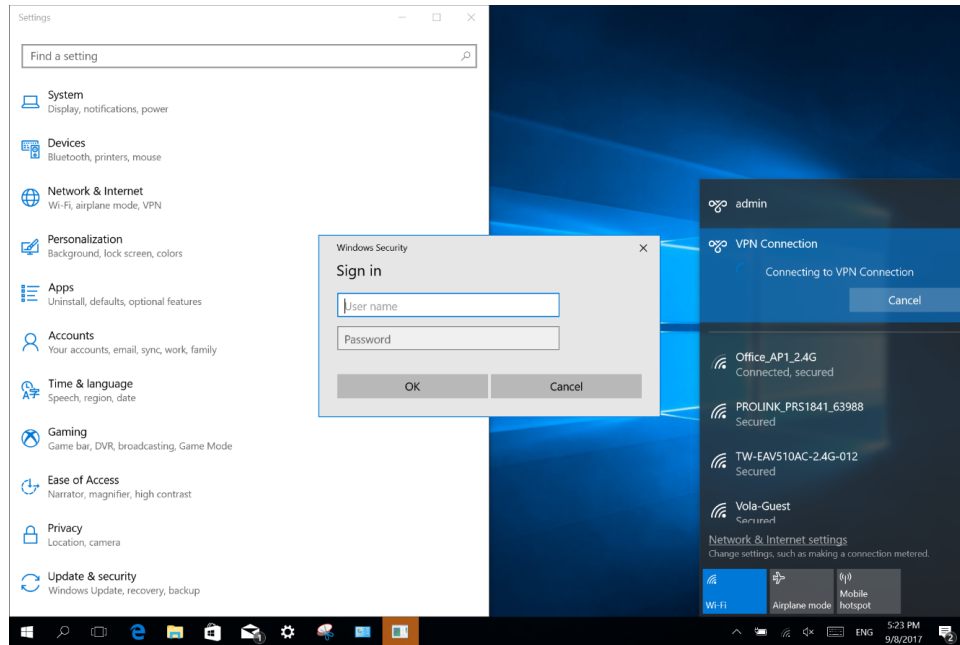
5. Select **Use my Internet connection (VPN)**.



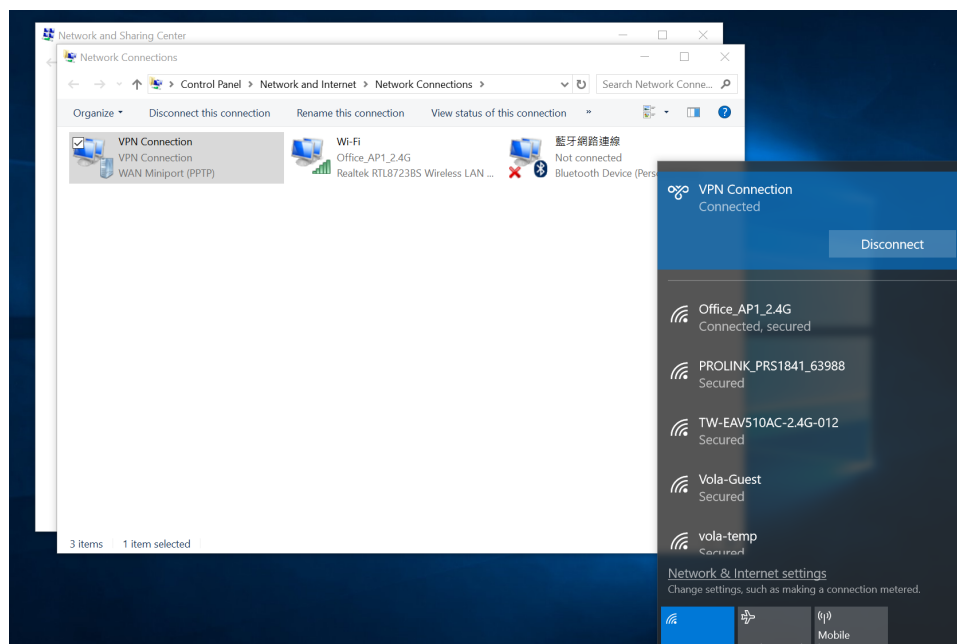
6. Enter the PPTP Server address/domain to field named **Internet address**. Please make sure your domain name address is work correctly if you are use domain name instead of IP address. Click **Create** button finish the PPTP client settings on Windows.



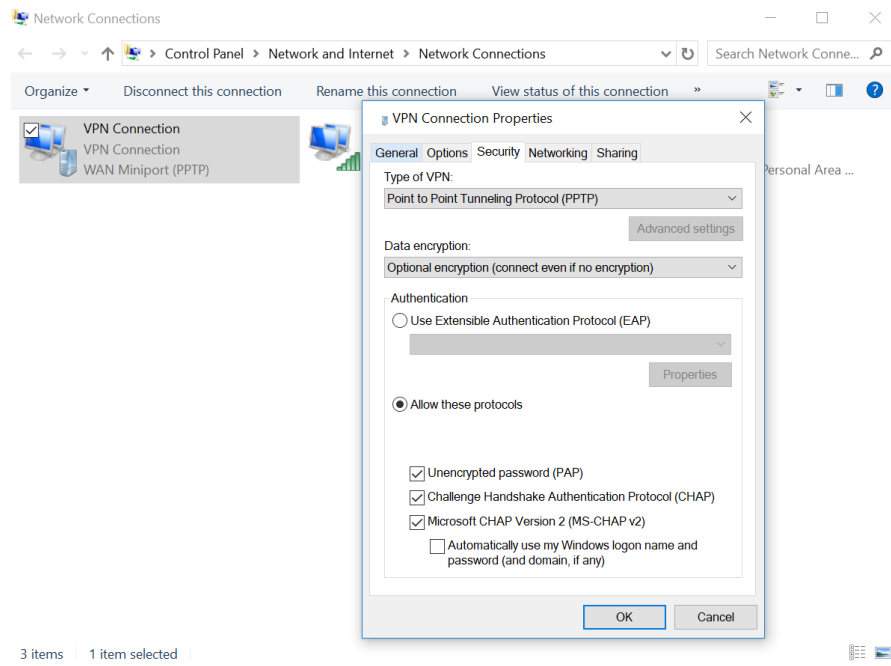
7. Enter the **username** and **password** that set on TW-EAV510/510AC's PPTP Server and click **OK** button to connect to PPTP Server.



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 VPN: ☒ Disable ☐ Enable

L2TP Server

Authentication Type: Encryption Mode:
Tunnel Authentication ☐ Secret Key:
Assigned to Peer IP Address start from: Local IP Address:

Server Account

Name: Account: ☐ Disable ☒ Enable
Username: Password:
Peer IP: Peer Subnet Mask:

L2TP Server Table

Select	Name	Enable	Username	Password
<input type="button" value="Delete Selected"/>	<input type="button" value="Save"/>			

L2TP Client

Name: Server IP Address:
Username: Password:
Tunnel Authentication ☐ Secret Key:
Authentication Type: Encryption Mode:
Default Gateway: ☐
Peer IP: Peer Subnet Mask:

L2TP Client Table

Select	Name	Server	tunnel Auth	PPP Auth	Default Gateway	Peer Network	Action
<input type="button" value="Delete Selected"/>							

L2TP VPN: Enable/Disable L2TP function.

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.

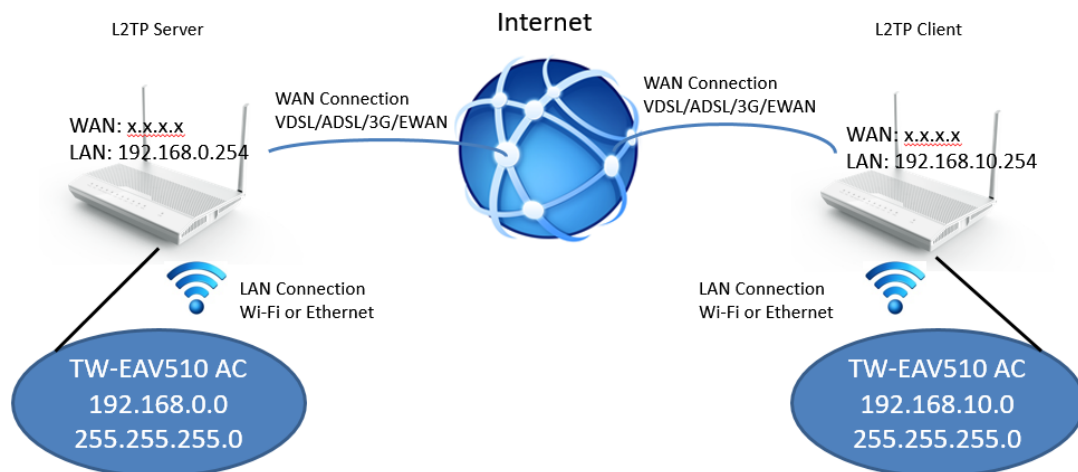
Peer IP: Enter the peer side LAN IP address for LAN to LAN type.

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)

- Go to **WAN -> VPN -> L2TP**, enable the L2TP VPN
- Setup L2TP Server and press **Apply** button
- Add new user account, don't need input Peer IP/ Peer Subnet Mask.

L2TP VPN: ☐ Disable ☒ Enable

L2TP Server

Authentication Type: Encryption Mode:

Tunnel Authentication ☒ Secret Key:

Assigned to Peer IP Address start from: Local IP Address:

Server Account

Name: Account: ☐ Disable ☒ Enable

Username: Password:

Peer IP: Peer Subnet Mask:

L2TP Server Table				
Select	Name	Enable	Username	Password
<input type="checkbox"/>	admin	<input checked="" type="checkbox"/>	admin	admin

Click **Add** button to save changes.

TW-EAV510 AC (L2TP Client)

- Go to **WAN -> VPN -> L2TP**, enable the L2TP VPN, Setting L2TP Client as below.

L2TP Client

Name: Server IP Address:

Username: Password:

Tunnel Authentication ☒ Secret Key:

Authentication Type: Encryption Mode:

Default Gateway: ☐

Peer IP: Peer Subnet Mask:

Click **Add** button to save account settings.

- 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.

L2TP Client Table							
Select	Name	Server	tunnel Auth	PPP Auth	Default Gateway	Peer Network	Action
<input type="checkbox"/>	admin	36.229.14.220	Challenge	CHAP	off		Disconnect
Delete Selected							

- 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.

L2TP Configuration				
Interface	Protocol	Local IP Address	Remote IP Address	Status
ppp11	PPP	172.166.0.201	192.168.0.254	up
Refresh				

LAN to LAN

TW-EAV510 (L2TP Server)

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

L2TP Server

Authentication Type:	CHAP ▼	Encryption Mode:	NONE ▼
Tunnel Authentication	<input checked="" type="checkbox"/>	Secret Key	12345678
Assigned to Peer IP Address start from:	172.166.0.200	Local IP Address:	192.168.0.254
Apply			

Server Account

Name:	user	Account:	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Username:	user	Password:	user
Peer IP:	192.168.10.254	Peer Subnet Mask:	255.255.255.0
Add			

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

L2TP Server Table				
Select	Name	Enable	Username	Password
<input type="checkbox"/>	user	<input checked="" type="checkbox"/>	user	user
Delete Selected	Save			

TW-EAV510 AC (L2TP Client)

- 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.

L2TP Client

Name:	<input type="text" value="user"/>	Server IP Address:	<input type="text" value="36.229.14.220"/>
Username:	<input type="text" value="user"/>	Password:	<input type="text" value="user"/>
Tunnel Authentication:	<input checked="" type="checkbox"/>	Secret Key:	<input type="text" value="12345678"/>
Authentication Type:	<input type="text" value="CHAP"/>	Encryption Mode:	<input type="text" value="NONE"/>
Default Gateway:	<input type="checkbox"/>	Peer Subnet Mask:	<input type="text" value="255.255.255.0"/>
Peer IP:	<input type="text" value="192.168.0.254"/>		
<input type="button" value="Add"/>			

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.

L2TP Client Table							
Select	Name	Server	tunnel Auth	PPP Auth	Default Gateway	Peer Network	Action
<input type="checkbox"/>	user	36.229.14.220	Challenge	CHAP	off	192.168.0.254 255.255.255.0	<input type="button" value="Connect"/>
<input type="button" value="Delete Selected"/>							

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.

L2TP Configuration				
Interface	Protocol	Local IP Address	Remote IP Address	Status
ppp11	PPP	172.166.0.200	192.168.0.254	up

IPSec

This page is for setting IPSec connection.

IPSec Configuration

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

Remote:

IPSec gateway address
LAN IP address
Subnet Mask

Local:

WAN IP address
LAN IP address
Subnet Mask

Security Option:

Encapsulation Type
Pre-Shared Key
Advanced Options ☒

IKE Phase 1:

Mode
IKE Algorithm
Encryption Algorithm
Integrity Algorithm
Select Diffie-Hellman Group

IKE Phase 2:

Security Algorithm
Encryption Algorithm
Integrity Algorithm
Select Diffie-Hellman Group

Key Life Time

Enable	State	Type	IPSec gateway address	Remote Network	WAN IP address	Local Network	Mode
<input type="button" value="Delete Selected"/>	<input type="button" value="Enable"/>	<input type="button" value="Disable"/>					

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.

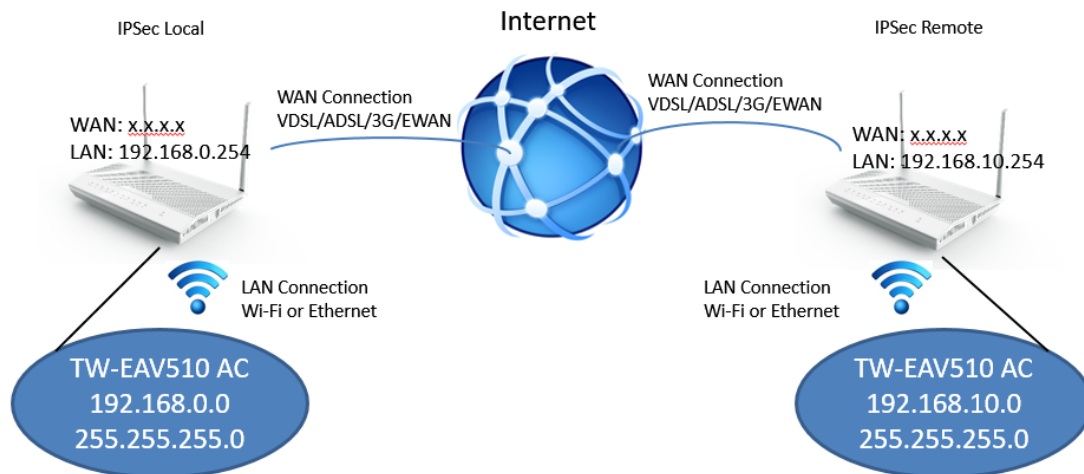
Select Diffie-Hellman Group: Select the group that will be used for tunnel connection.

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.

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

Remote:	
IPSec gateway address	36.229.14.220
LAN IP address	192.168.0.254
Subnet Mask	255.255.255.0
Local:	
WAN IP address	0.0.0.0
LAN IP address	0.0.0.0
Subnet Mask	255.255.255.0
Security Option:	
Encapsulation Type	ESP
Pre-Shared Key	psk12345678
Advanced Options	<input type="checkbox"/>
<input type="button" value="Add / Save"/>	

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.

Key Life Time								
	Enable	State	Type	IPSec gateway address	Remote Network	WAN IP address	Local Network	Mode
<input type="checkbox"/>	Enable	Established	AUTO	36.229.14.220	192.168.0.254	0.0.0.0	192.168.10.254	ESP
<input type="button" value="Delete Selected"/>				<input type="button" value="Enable"/>	<input type="button" value="Disable"/>			

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.

Remote:

IPSec gateway address

LAN IP address

Subnet Mask

Local:

WAN IP address

LAN IP address

Subnet Mask

Security Option:

Encapsulation Type

Pre-Shared Key

Advanced Options ☐

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.

Key Life Time								
	Enable	State	Type	IPSec gateway address	Remote Network	WAN IP address	Local Network	Mode
<input type="checkbox"/>	Enable	Established	AUTO	36.225.80.226	192.168.10.254	0.0.0.0	192.168.0.254	ESP
<input type="button" value="Delete Selected"/>				<input type="button" value="Enable"/>	<input type="button" value="Disable"/>			

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.

Administrator: Command Prompt

```
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

Pinging 192.168.10.100 with 32 bytes of data:
Request timed out.
Reply from 192.168.10.100: bytes=32 time=16ms TTL=126
Reply from 192.168.10.100: bytes=32 time=11ms TTL=126
Reply from 192.168.10.100: bytes=32 time=12ms 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 = 11ms, Maximum = 16ms, Average = 13ms

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.oy
    Link-local IPv6 Address . . . . . : fe80::f109:45a5: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:

Port Number:

Tunnel Subnet:

Tunnel Mask:

Cipher Encryption:

HMAC Authentication:

Enable LZO: ☐

Apply

Certificate Authority (CA):

```
-----BEGIN CERTIFICATE-----
MIIDKzCCAaOgAwIBAgIJA3K16zgVcJEZMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIB
BAHwMCE15Um91dGVyMB4XDTE4MTAxNzIxMTM1M1oXDTI4MTAxNDIxMTM1M1owEzER
MA8GA1UEAwITX15b3V0ZXIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIB
AQCuDFrQxSBdm13c+ifoUnvVB1Ejn0F1NEdowoh/uv9/mVwvcM1WQaj5ynvk+4n7
PLKrbeg8+u09YeqkI068tyTar5RlhBYf5xQUmOk8071U5VYv6zILKzuwBe2XH/7K
VoghmlIip1bgrinaKVxNuH1bgbIrhmlfdOECZyUkKCVwbBrurqc4je0R3VfoRpTo
qNxQNALxQht0EichCdAY9vt78IzmVkd1Vy4MOG3hbwFtVUN/tLFjG0gqK4bnyNv
vwNblNUq1C1xDG1NNuAtJK62F2rUpNhlLZbPJRizA6/2Keg6kMhKgLzZszQEx480
vyHnkAt1ljL5iDR13Ijv9tXNAgMBAAGjgYEWfzAdBgNVHQ4EFgQUJwSmfLVmsX0+
ScUEgNzow5C9V9kwQwYDVR0fjBDwwOoAUJwSmfLVmsX0+ScUEgNzow5C9V9mhF6QV
MBMxETAPBgNVBAMCE15Um91dGVyggkAkrXrOBVwRkwdAYDVR0TBAlUwAwEB/zAL
BgNVHQ8EBAMCAQYwDQYJKoZIhvcNAQELBQADggEBAGKMFYnRgirMor55jn8EqVz
b2mAYuUltrTimsn3jnActEuoC5xp+m+EIFpnC9/ZmAsXh5XCXq6HB1ZKEbbJKZr
JqPpTCfDCs6+PMKi0H0UeevxnXRc1DCQg0B10mjfleaR2ozvwBU32sTD8SS1P+uy
xfQgxMpdTFense52txB61ZEq5zp2L7zh5mPDyy9k3Yurek8AK/2vUbMkcgK4hPjN
gewc9BGWk81mQmElwpoNRu9HXCrx6C1RyOKOSwsgqtrOt4COn1bzKk61mcpBHoIsFI
y4mqzgYnqxOb+gIbu9HzF3xNubxY/agDFL/KaPGTOpGD/VRMMbq52S0ZRWISI=
-----END CERTIFICATE-----
```

OpenVPN Account

Name:

Username:

Password:

Add

Openvpn Account Table			
Select	Name	Username	Password
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: ☐ Disable ☒ Enable

Apply

OpenVPN Client

Name:

Server IP:

Protocol:

Port Number:

Username:

Password:

Cipher Encryption:

HMAC Authentication:

LZO: ☐

Default Gateway: ☐

Server CA:

Add

Openvpn Client							
Select	Enable	Name	Server	Username	Password	CA	Default Gateway
<input type="button" value="Delete"/>							

OpenVPN Trusted CA

Name:	<input type="text"/>
	<div>-----BEGIN CERTIFICATE----- -----END CERTIFICATE-----</div>
CA:	

Add

Trusted CA List		
Select	Name	Subject
<input type="button" value="Delete"/>		

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

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.

Outgoing Default Action

☐ Deny ☒ Allow

Incoming Default Action

☒ Deny ☐ Allow

Apply Changes

Direction:

Outgoing ▾

Protocol:

TCP ▾

Source IP Address:

Subnet Mask:

Port:

-

Destination IP Address:

Subnet Mask:

Port:

-

Rule Action

☒ Deny ☐ Allow

Add

Modify

Current Filter Table							
Select	Direction	Protocol	Source IP Address	Source Port	Destination IP Address	Destination Port	Rule Action
<div><div>Delete Selected</div><div>Delete All</div></div>							

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 ☐ Deny ☒ Allow

Source MAC Address:

Ex: 0011aabbccdd

Current Filter Table

Select	Source MAC Address
--------	--------------------

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.

Port Forwarding:

Disable

Enable

Apply Changes

Enable

Application:

Active Worlds

Comment	Local IP	Local Port from	Local Port to	Protocol	Remote IP	Remote Port from	Remote Port to	Interface
				Both ▾				Any ▾
				Both ▾				Any ▾
				Both ▾				Any ▾
				Both ▾				Any ▾
				Both ▾				Any ▾
				Both ▾				Any ▾
				Both ▾				Any ▾
				Both ▾				Any ▾
				Both ▾				Any ▾
				Both ▾				Any ▾
				Both ▾				Any ▾
				Both ▾				Any ▾
				Both ▾				Any ▾
				Both ▾				Any ▾
				Both ▾				Any ▾

Add

Modify

Current Port Forwarding Table

Select	Enable	Comment	IP Address	Local Port	Protocol	Remote Host	Public Port	Interface
--------	--------	---------	------------	------------	----------	-------------	-------------	-----------

Delete Selected

Delete All

URLBlocking

This page is used to configure the Blocked FQDN(Such as tw.yahoo.com) and filtered keyword. Here you can add/delete FQDN and filtered keyword.

URL Blocking: ☒ Disable ☐ Enable

FQDN:

URL Blocking Table:

Select	FQDN
--------	------

Keyword:

Keyword Filtering Table:

Select	Filtered Keyword
--------	------------------

Domain Blocking

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

Domain BlockingConfiguration

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

Domain Blocking: ☒ Disable ☐ Enable

Domain:

Domain BlockingConfiguration:

Select	Domain
--------	--------

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.

DMZ Host:

☒ Disable ☐ Enable

DMZ Host IP Address:

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

☐ Per-Source IP Flood: SYN

☐ Per-Source IP Flood: FIN

☐ Per-Source IP Flood: UDP

☐ Per-Source IP Flood: ICMP

☐ TCP/UDP PortScan

☐ ICMP Smurf

☐ IP Land

☐ IP TearDrop

☐ PingOfDeath

☐ TCP Scan

☐ TCP SynWithData

☐ UDP Bomb

☐ UDP EchoChargen

packets/second

packets/second

packets/second

packets/second

packets/second

packets/second

packets/second

packets/second

▼

Sensitivity

☐ Enable Source IP Blocking

Block Interval (seconds)

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.

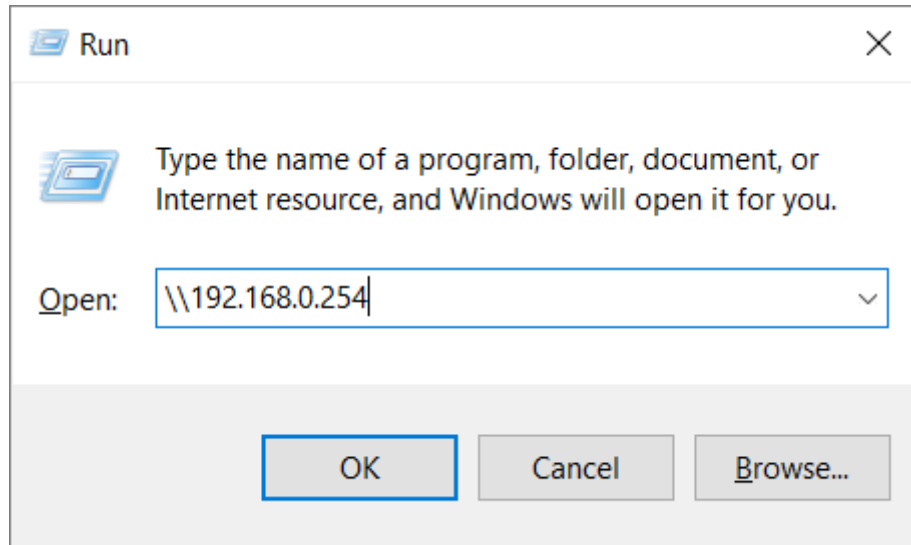
Server String: Descriptive string for the Samba server

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)

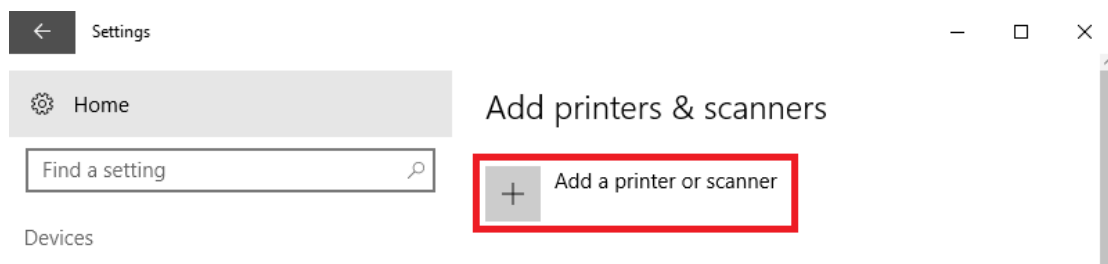
This page is used to show printer URL(s).

<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.

←  Add Printer

Find a printer by other options

☐ My printer is a little older. Help me find it.

☒ Select a shared printer by name

☐ Add a printer using a TCP/IP address or hostname

☐ Add a Bluetooth, wireless or network discoverable printer

☐ Add a local printer or network printer with manual settings

http://192.168.0.254:631/printers/lp0

Browse...

Example: \\computername\printername or
http://computername/printers/printername/.printer

Next

Cancel

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.

IP Address	MAC Address
192.168.1.2	50-e5-49-5f-7f-d5

Refresh

Routing

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

Routing Configuration

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

Enable:

☒

Destination:

Subnet Mask:

Next Hop:

Metric:

Interface:

Any

▼

Add Route

Update

Delete Selected

Show Routes

Static Route Table						
Select	State	Destination	Subnet Mask	Next Hop	Metric	Interface

- 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:	<input type="text" value="v2"/>
Query Interval:	<input type="text" value="125"/>
Query Response Interval:	<input type="text" value="10"/>
Last Member Query Interval:	<input type="text" value="10"/>
Robustness Value:	<input type="text" value="2"/>

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.

Interface Grouping Configuration

To manipulate a mapping group:

1. Select a group from the table.
2. Select interfaces from the available/grouped interface list and add it to the grouped/available interface list using the arrow buttons to manipulate the required mapping of the ports.
3. Click the 'Apply Changes' button to save the changes.

Note: The selected interfaces will be removed from their existing groups and added to the new group. Only WAN interface with pure bridge setting will be shown here.

Grouped Interfaces

Available Interfaces

->

<-

Select	Interface
Default	LAN1, LAN2, LAN3, LAN4, WLAN 5G, WLAN 2.4G
<input type="radio"/>	
<input type="radio"/>	
<input type="radio"/>	
<input type="radio"/>	

Apply Changes

IP QoS

QoS Policy

IP QoS Configuration

IP QoS

☐ Disable

☒ Enable

QoS Queue Config

This page is used to configure the QoS policy and Queue. If select PRIO of policy, the lower numbers imply 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'

Policy: ☒ PRIO ☐ WRR

Queue	Policy	Priority	Weight	Enable
Q1	PRIO	1	--	<input type="checkbox"/>
Q2	PRIO	2	--	<input type="checkbox"/>
Q3	PRIO	3	--	<input type="checkbox"/>
Q4	PRIO	4	--	<input type="checkbox"/>

QoS Bandwidth Config

This part is used to configure the bandwidth of different type 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: ☒ Disable ☐ Enable

Total Bandwidth Limit: 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

QoS Classification

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

Mark				Classification Rules					
ID	Name	VLAN ID	DSCP Mark	802.1p	Queue	WanIf	Rule Detail	Delete	Edit
<div><div>Add</div><div>Apply Changes</div></div>									

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

Add QoS Classification Rules

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

RuleName:

Assign IP Precedence/DSCP/802.1p

VLAN ID (1~4095):

Precedence:

Queue 1 ▼

DSCP:

▼

802.1p:

▼

Specify Traffic Classification Rules

IP QoS Rule by type: ☐ Port ☐ Ethery Type ☐ IP/Protocol ☐ MAC Address

WAN:

Any ▼

Apply Changes

- 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

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 RADVD's configuration of your device.

MaxRtrAdvInterval:

MinRtrAdvInterval:

AdvManagedFlag: ☒ off ☐ on

AdvOtherConfigFlag: ☐ off ☒ on

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 $0.75 * \text{MaxRtrAdvInterval}$.

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 ☒ DHCPv6Server(Auto)

Auto Config by Prefix Delegation for DHCPv6 Server:

DHCPv6 Mode: Set to **DHCPv6Server(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 Proxy Configuration

This page be used to configure MLD Proxy.

MLD Proxy: ☒ Disable ☐ Enable

WAN Interface:

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 be used to configure MLD Snooping.

MLD Snooping: ☒ Disable ☐ Enable

Apply Changes

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:

ppp0 ▾

Add RouteUpdateDelete SelectedDelete AllShow 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.

Outgoing Default Action ☐ Deny ☒ Allow

Incoming Default Action ☒ Deny ☐ Allow

Direction: **Protocol:** **Rule Action** ☒ Deny ☐ Allow

Source Interface ID:

Destination Interface ID:

Source Port:

Destination Port:

Current Filter Table:

Select	Direction	Protocol	Source Interface ID	Source Port	Destination Interface ID	Destination Port	Rule Action
--------	-----------	----------	---------------------	-------------	--------------------------	------------------	-------------

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:

Restore Settings from File:

Reset Settings to Default:

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.

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

No file selected.

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!

ACL Capability: ☐ Disable ☒ Enable

Enable: ☒
Interface:
IP Address: 0.0.0.0 -> Allows connections from anywhere.
Subnet Mask: 0.0.0.0 -> Allows connections from anywhere.

ServiceName LAN
Any ☐
TELNET ☐
HTTP ☐
HTTPS ☐
PING ☒

ACL Table					
Select	State	Interface	IP Address	Services	Port
<input type="radio"/>	Enable	LAN	0.0.0.0/0	web,https,ping	80,443
<input type="radio"/>	Enable	WAN	0.0.0.0/0	ping	

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.

Current Time :

Year

1970

Mon

1

Day

1

Hour

8

Min

57

Sec

59

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.

Configure Schedule

Time Schedule

1.

☐ Sun

☐ Mon

☐ Tue

☐ Wed

☐ Thu

☐ Fri

☐ Sat

00

:

00

Clear

2.

☐ Sun

☐ Mon

☐ Tue

☐ Wed

☐ Thu

☐ Fri

☐ Sat

00

:

00

Clear

Apply

Statistics

Interface

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

Interface Statisitcs

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

Interface	Rx pkt	Rx err	Rx drop	Tx pkt	Tx err	Tx drop
LAN PORT1	0	0	0	0	0	0
LAN PORT2	741	0	0	1040	0	0
LAN PORT3	0	0	0	0	0	0
LAN PORT4	0	0	0	0	0	0
WLAN 2.4G	520	0	0	0	0	0
WLAN 5G	0	0	0	0	0	0
ADSL_0	0	0	0	0	0	0
ADSL_1	0	0	0	0	0	0
ADSL_2	0	0	0	0	0	0
VDSL_0	0	0	0	0	0	0
VDSL_1	0	0	0	0	0	0
EWAN_0	1	0	0	6	0	0
USB 3G/4G	0	0	0	3	0	0

Refresh

Reset Statistics

DSL

This page shows more details of your xDSL line.

DSL Statistics

Mode	VDSL2-30A Annex A
TPS-TC	PTM
Latency	Fast
Status	SHOWTIME.
Power Level	L0
Uptime	00:15:49
G.Vector	Off

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

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:

English ▼

Update selected language

Reboot

Click the *Reboot* button to reboot the device immediately.

Reboot

This page is used to reboot your system.

Reboot

Logout

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

Logout

This page is used to logout from the Device.

Logout

Tiedostonimi: 20181112 TW-EAV510 AC-LTE CAT 6 WLAN 802.11ac Router User
Manual V1.9(WEB).docx

Hakemisto: /Users/Markku/Library/Containers/com.microsoft.Word/Data/Documents

Malli: /Users/Markku/Library/Group Containers/UBF8T346G9.Office/User
Content.localized/Templates.localized/Normal.dotm

Otsikko:

Aihe:

Tekijä: Markku Åberg

Avainsanat:

Kommentit:

Luontipäivä: 5.12.2018 13.48.00

Version numero: 2

Viimeksi tallennettu: 5.12.2018 13.48.00

Viimeksi tallentanut: TeleWell Markku

Kokonaismuokkausaika: 1 Minuutti

Viimeksi tulostettu: 5.12.2018 13.48.00

Viimeisestä täydestä tulostuksesta

Sivuja: 86

Sanoja: 6 700 (noin)

Merkkejä: 54 277 (noin)