



TW-EAV510 AC

ADSL2+/VDSL2 WLAN 802.11ac

Router

User Manual

V: 2.53.d16

Directory

Introduction	1
Introduction to your Router	1
Features	3
Physical Interface.....	7
Package Contents	8
Device Description	9
Basic Installation	13
Factory Default Settings.....	18
Web Interface (Username and Password)	18
Device LAN IPv4 settings.....	18
DHCP server for IPv4	18
Configuration	18
Configuration via Web Interface	18
Status.....	21
Device	21
3G/4G/LTE Info	22
AP Neighbor	22
IPv6	23
VPN	23
PPTP	24
L2TP	25
IPSec.....	26
LAN Port	27
ARP.....	27
DHCP	28
System Log	29
LAN	31
WLAN.....	32
WLAN 2.4GHz / 5GHz.....	33
Basic Settings.....	33
Advanced Settings.....	34
Security.....	34
Access Control	37
Site Survey	39
WPS.....	39
Status.....	39
WAN.....	41
WAN Mode.....	41
Default Routing.....	41
Ethernet WAN	41
PTM(VDSL) WAN.....	44
ATM(ADSL) WAN.....	46
ATM Settings	49
DSL Settings.....	50
3G/4G LTE Settings	51
Services.....	53
DNS	53
Dynamic DNS	53

Firewall.....	55
ALG	55
IP/Port Filtering.....	55
MAC Filtering.....	56
Port Forwarding	57
URL Blocking	59
Domain Blocking	60
DMZ.....	60
DoS	61
UPnP	62
RIP	63
Samba	64
VPN	65
PPTP	65
How to for PPTP Server/Client	67
L2TP	76
How to for L2TP Server/Client.....	78
IPSec.....	78
How to for IPsec.....	82
GRE Settings	89
How to for GRE:	89
Advance	94
Bridging.....	94
Routing.....	95
SNMP	96
Bridge Grouping	97
IP QoS.....	99
QoS Policy.....	99
QoS Classification.....	100
Printer Server	102
IPv6	104
IPv6.....	104
RADVD	104
DHCPv6.....	105
MLD Proxy	105
MLD Snooping	105
IPv6 Routing.....	106
IP/Port Filtering.....	107
Diagnostics.....	108
Ping	108
ATM Loopback	109
DSL Tone.....	110
ADSL Connection	111
Management.....	112
Backup/Restore	112
Password	113
Firmware Upgrade.....	113
ACL.....	114
Time Zone.....	116
SMS Alert Settings	116

Statistics.....117

 Interface117

 DSL118

Language.....119

Reboot119

Logout.....119

Introduction

Introduction to your Router

The TW-EAV510 AC is a multi-service VDSL2 router. It features fiber-ready triple-WAN VDSL2 supports backward compatibility to ADSL2+ for a longer reach distance, an all-in-one advanced device including concurrent dual-band 802.11ac (5GHz) 867Mbps and 802.11n (2.4GHz) 300Mbps, Gigabit Ethernet, connections to 3G/4G LTE and NAS (Network Attached Storage) in one unit. As well as being IPv6-capable, the VDSL2 router supports superfast fiber connections via a Gigabit Ethernet WAN port. It also has two USB ports, allowing the device to act as a NAS (Network Attached Storage) device and FTP (File Transfer Protocol) access. Moreover, the USB port can host a 3G/4G LTE USB modem connecting to the 3G/4G LTE network for Internet access. With an array of advanced features, the router delivers a future-proof solution for VDSL2 connections, superfast FTTC and ultra-speed FTTH (Fiber-To-The-Home) network deployment and services.

Maximum wireless performance

Featured with simultaneous dual-band technology, the router can run both 2.4GHz and 5GHz frequency bands at the same time, offering ultra-fast wireless speeds of up to 867Mbps (5GHz) and 300Mbps (2.4GHz), and SSIDs on both bands. The TW-EAV510 AC, by adopting this state-of-the-art technology, allows for multiple-demand applications, such as streaming HD videos and multiplayer gaming simultaneously. 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.

3G/4G LTE mobility

With TW-EAV510 AC you can connect a 3G/4G LTE USB modem to its built-in USB port, allowing you to watch movies, download music or access e-mail no matter where you may be. You can even share your Internet connection with others, when away on business, at a show, or wherever there is mobile signal but no fixed line access.

Experience Gigabit WAN

The TW-EAV510 AC has four Gigabit LAN ports and one Giga Ethernet port as an Ethernet WAN port. This EWAN offers another broadband connectivity option for connecting to a cable, DSL, fiber modem.

Pathway to the Future

IPv6 (Internet Protocol Version 6), launched as the current IPv4 is getting filled up, gradually becomes the indispensable addressing system for the savvy cloud computing users. Equipped with IPv6, the router eagerly provides users a better working environment to work with, a shortcut to upgrade and a more efficient solution to save budget. For the customers during this transition period, dual stack (IPv4 and IPv6) feature enables the hosts a convenient way to reserve both address to smooth over this coexistent period.

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

- Compliant with VDSL2/ADSL2+ standards
- Triple-WAN ports for 3G/4G LTE, VDSL2/ADSL2+ fallback, Gigabit Ethernet WAN (EWAN) for broadband connectivity
- Simultaneous dual-band Wireless 867Mbps (5GHz) and 300Mbps (2.4GHz)
- Gigabit EWAN and LAN ports
- IPv6 ready (IPv4/IPv6 dual stacks)
- Fibre (FTTC/FTTP/FTTH) ready with high WAN throughput via EWAN port
- USB 3.0 port for NAS, Printer Server and 3G/4G/5G LTE USB modem
- QoS for traffic prioritization and bandwidth management
- Compliant with IEEE 802.11a/b/g/n and 802.11ac standards
- WPS (Wi-Fi Protected Setup) for easy setup
- Wireless security with WPA-PSK/WPA2-PSK
- Multiple wireless SSIDs with wireless guest access
- Secured IPSec VPN with powerful DES/ 3DES/ AES
- PPTP VPN with Pap/ Chap/ MS-CHAPv2 authentication
- L2TP
- IPSec
- GRE tunnel
- Supports Bridge Grouping
- SOHO firewall security
- Supports IPTV application
- Ideal for SOHO and office users

VDSL2/ADSL2+ Compliance

- Compliant with xDSL standard
- ITU-T G.993.2 (VDSL2)
- ITU-T G.998.4 (G.inp)
- ITU-T G.993.5 (G.vector)
- ITU-T G.992.3 (G.dmt.bis) Annex A, B, I, J, L and M.
- ITU-T G.992.5 (G.dmt.bis plus)
- Full-rate ANSI T1.413 Issue 2
- ITU-T G.992.1 (G.dmt) Annex A, B

- ITU-T G.992.2 (G.lite) Annex A, B
- Supports VDSL2 band plan: 997 and 998
- ADSL/2/2+ fallback modes
- Supports VDSL2 profiles: 8a, 8b, 8c, 8d, 12a, 12b, 17a, 30a and 35b.
- Supports ATM and PTM modes

Network Protocols and Features

- IPv4 or IPv4/IPv6 dual stack
- NAT, static (v4/v6) routing and RIP-1/2
- Pv6 stateless/stateful address auto-configuration
- IPv6 router advertisement
- IPv6 over PPP
- DHCPv6
- Universal Plug and Play (UPnP) compliant
- Dynamic Domain Name System (DDNS)
- Virtual Server (port forwarding) and DMZ
- SNTP, DNS relay, IGMP proxy and IGMP snooping for video service
- MLD proxy and MLD snooping for video service
- Management based on IP protocol, port number and address
- Supports Bridge Grouping

Firewall

- Built-in NAT firewall
- Stateful Packet Inspection (SPI)
- Prevents DoS attacks including Land Attack, Ping of Death, etc
- Remote access control for web based access
- Packet filtering - port, source IP address, destination IP address
- URL content filtering - string or domain name detection in URL string
- MAC filtering
- Password protection for system management

Virtual Private Network (VPN)

- PPTP Client / Server
- L2TP Client / Server

- IPSec
- GRE
- PPTP / L2TP / IPSec pass-through

Quality of Service Control

- Supports the DiffServ approach
- Traffic prioritization and bandwidth management based on IPv4/IPv6 protocol, port number and address

ATM and PPP Protocols

- Compliant with xDSL standard
- ATM Adaptation Layer Type 5 (AAL5)
- Multiple protocol over AAL5 (RFC 2684, formerly RFC 1483)
- Bridged or routed Ethernet encapsulation
- VC-based and LLC-based multiplexing
- PPP over Ethernet (PPPoE)
- PPP over ATM (RFC 2364)
- Classical IP over ATM (RFC 1577)
- MAC encapsulated routing (RFC 1483 MER)
- OAM F4/F5

IPTV Applications

- IGMP snooping and IGMP proxy
- MLD snooping and MLD proxy
- Bridge Grouping
- Supports VLAN MUX
- Quality of Service (QoS)

Wireless LAN

- Compliant with IEEE 802.11 a/ b/ g/ n/ac standards
- 2.4 GHz and 5GHz frequency range
- Up to 1200 (300+867) Mbps wireless operation rate
- 64 / 128 bits WEP supported for encryption
- WPS (Wi-Fi Protected Setup) for easy setup

- Supports WPS v2
- Wireless Security with WPA-PSK / WPA2-PSK support
- Multiple wireless SSIDs with wireless guest access

USB Application Server

- 3G/4G LTE USB modem
- Storage/NAS: FTP server, Samba server, Printer Server

Management

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

Physical Interface

- WLAN antennas: 2 external antennas
- DSL: VDSL/ADSL port
- Ethernet: 4-port 10/100/1000Mbps auto-crossover (MDI / MDI-X) Switch
- EWAN: 1 Gigabit Ethernet port as a WAN interface for broadband connectivity
- USB 2.0 and USB 3.0 for 3G/4G LTE USB modem
- USB 3.0 for storage service and 3G/4G LTE USB modem
- WLAN on/off button
- WPS push button
- Power jack
- Power switch
- Factory default reset button

Package Contents

- TeleWell TW-EAV510 AC ADSL2+/VDSL2 WLAN 802.11ac Router
- User Manual
- RJ-45 UTP 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.

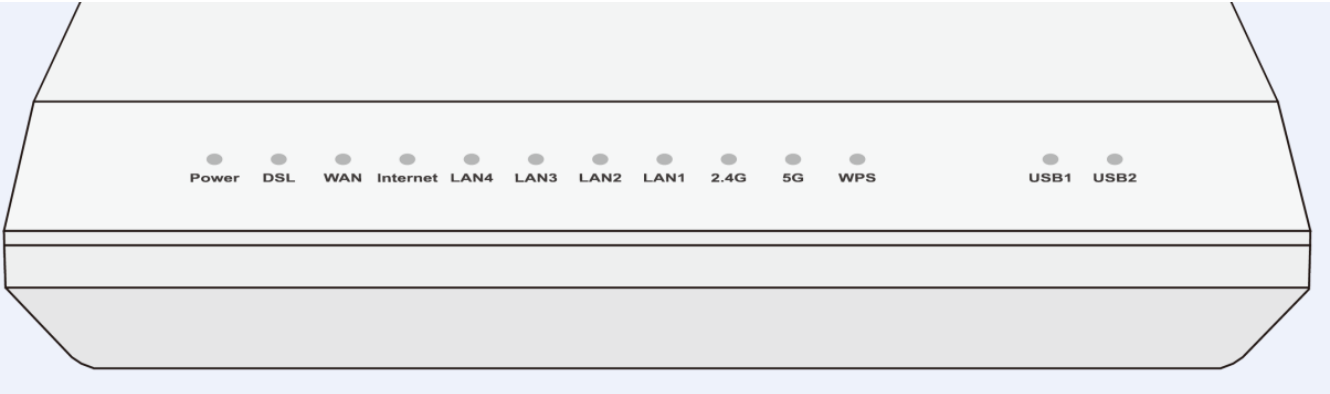
Avoid using this product and all accessories outdoors.

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

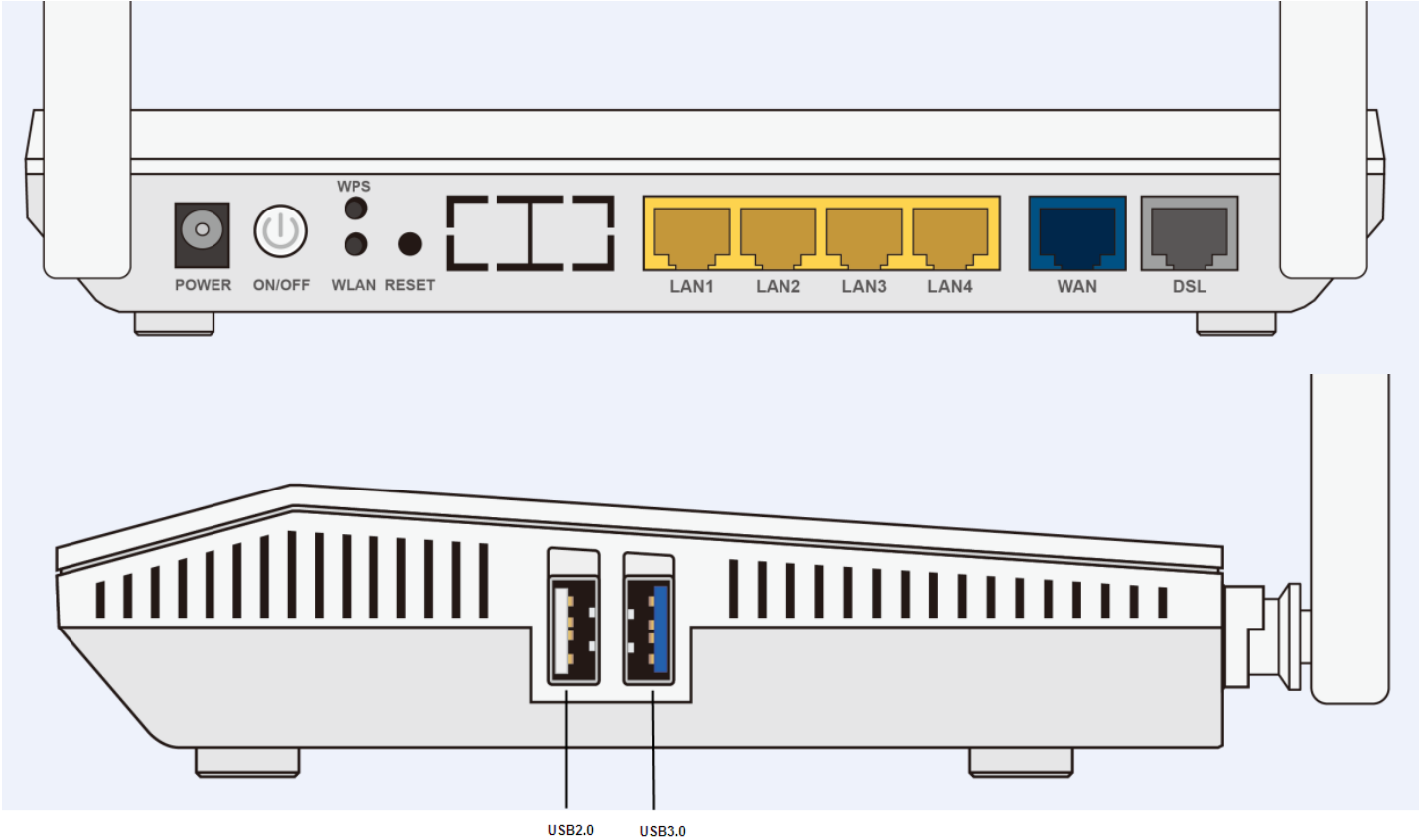
The Front LEDs



LED	Status	Meaning
Power	Green	System ready
	Off	Off
DSL	Green	xDSL Showtime Phase
	Green Blinking	xDSL Discovery/Training/Exchange Phase
	Off	No xDSL line connected
WAN	Green	Ethernet Link Up
	Green Blinking	Ethernet Link Up and traffic
	Off	Ethernet Link Down
Internet	Green	Device has a public IP via either static/ DHCP/ or IPCP
	Rapid Green Blinking	IP connected and traffic passing
	Off	IP or PPPoE session is idle and dropped, or DSL not connected
LAN1-4	Green	Ethernet Link Up
	Green Blinking	Ethernet Link Up and traffic
	Off	Ethernet Link Down
2.4G/5G	Green	WiFi is ready for using
	Green Blinking	Data being transmitted/received
	Rapid Green Blinking	There is STAs association connection and traffic
	Off	WiFi is disabled
WPS	Green Blinking	Running WPS Configuration
	Off	WPS Stop
USB1/2	On	USB device connected

	Off	USB device not connected
--	-----	--------------------------

The Rear Ports



Port	Meaning
POWER	Connect the supplied Power Adapter to this port.
ON/OFF	Power ON/OFF switch
WLAN	Press and release quickly to enable or disable the 2.4G and 5G Wi-Fi function
WPS	Press and release quickly to enable the WPS function
RESET	The RESET button is to designed to achieve two effects: 1. Press and hold it for 2-5 seconds to get FW/firmware upgrade from TeleWell server when internet is working. 2. Press and hold it for 5 seconds or above to restore to factory default settings.
LAN1~4	Connect a Ethernet cable to one of the LAN ports when connecting to a PC or an office/home network.
Gigabit WAN	Connect to Fibre/ Cable/ xDSL Modem with a RJ-45 cable, for broadband connectivity
DSL	Connect to the xDSL/ telephone network with RJ-11 cable(telephone)

USB(2.0/3.0)	Connect the USB device (Printer, USB storage, 3G/4G LTE USB modem) to the port. Note: USB 2.0 for 3G/4G LTE USB modem only USB 3.0 port for Printer, USB storage, 3G/4G LTE USB modem.
---------------------	--

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.

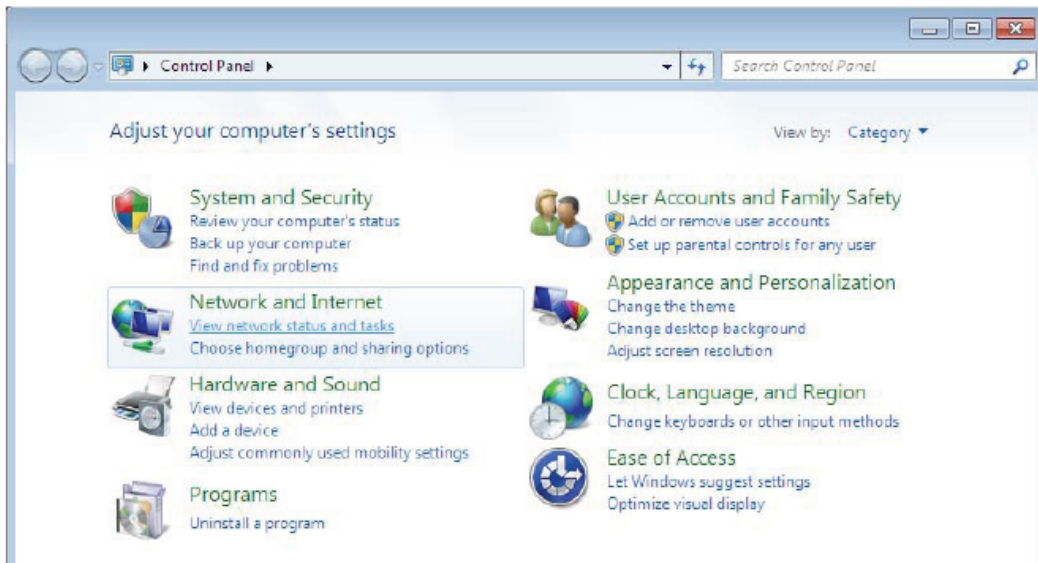
Please follow the following steps to configure your PC network environment.

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

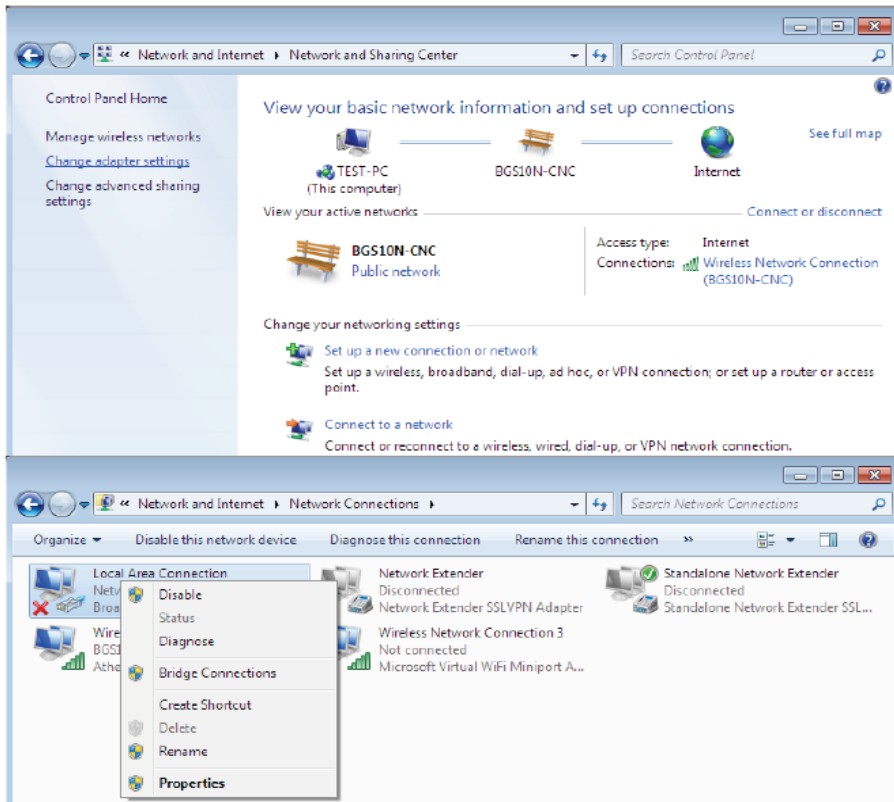
Go to Start. Click on Control Panel. Then click on Network and Internet.



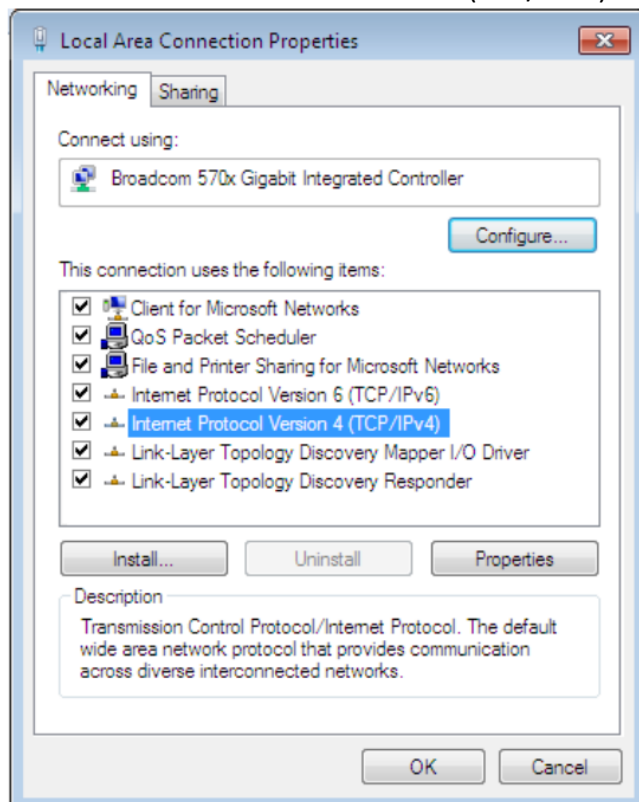
When the Network and Sharing Center window pops up, select and click on Change adapter settings on the left window panel.

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

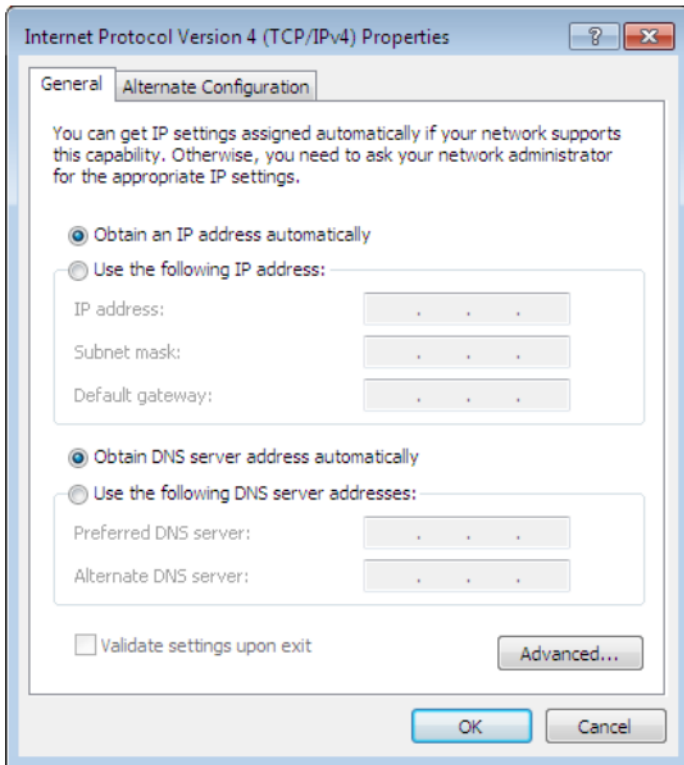
IPv4:



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

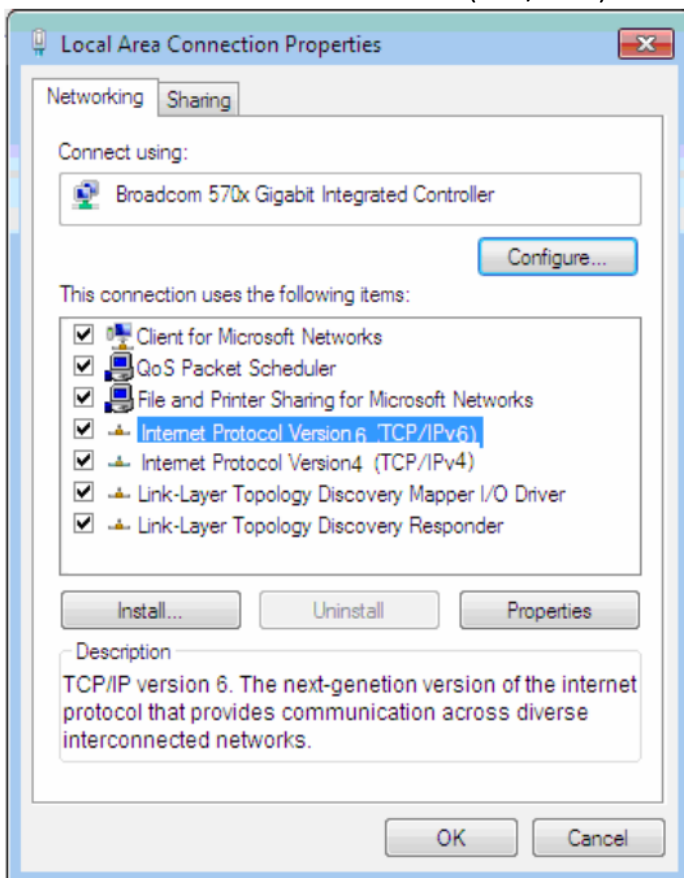


In the TCP/IPv4 properties window, select the Obtain an IP address automatically and Obtain DNS Server address automatically radio buttons. Then click OK to exit the setting. Click OK again in the Local Area Connection Properties window to apply the new configuration.

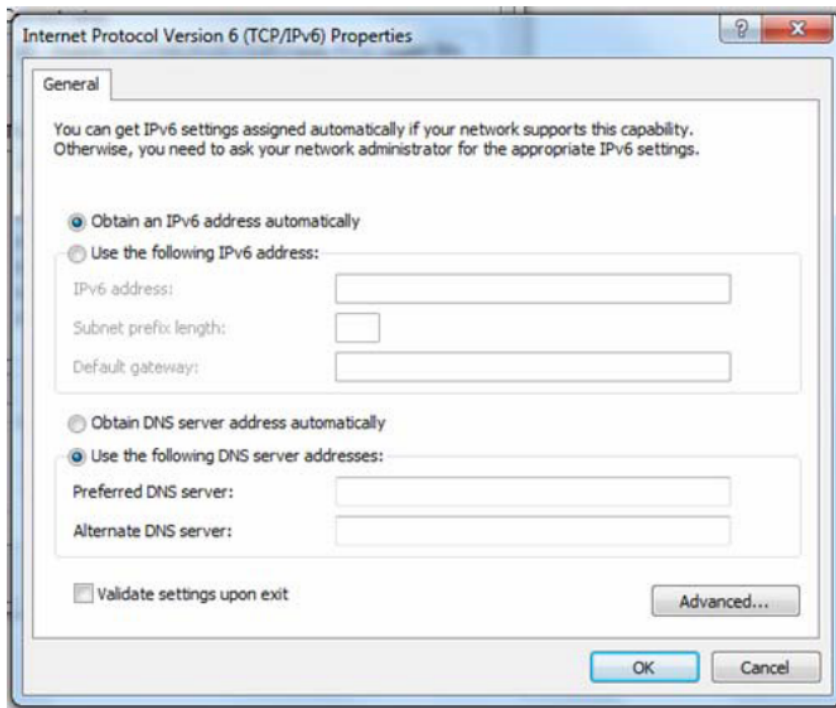


IPv6:

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

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

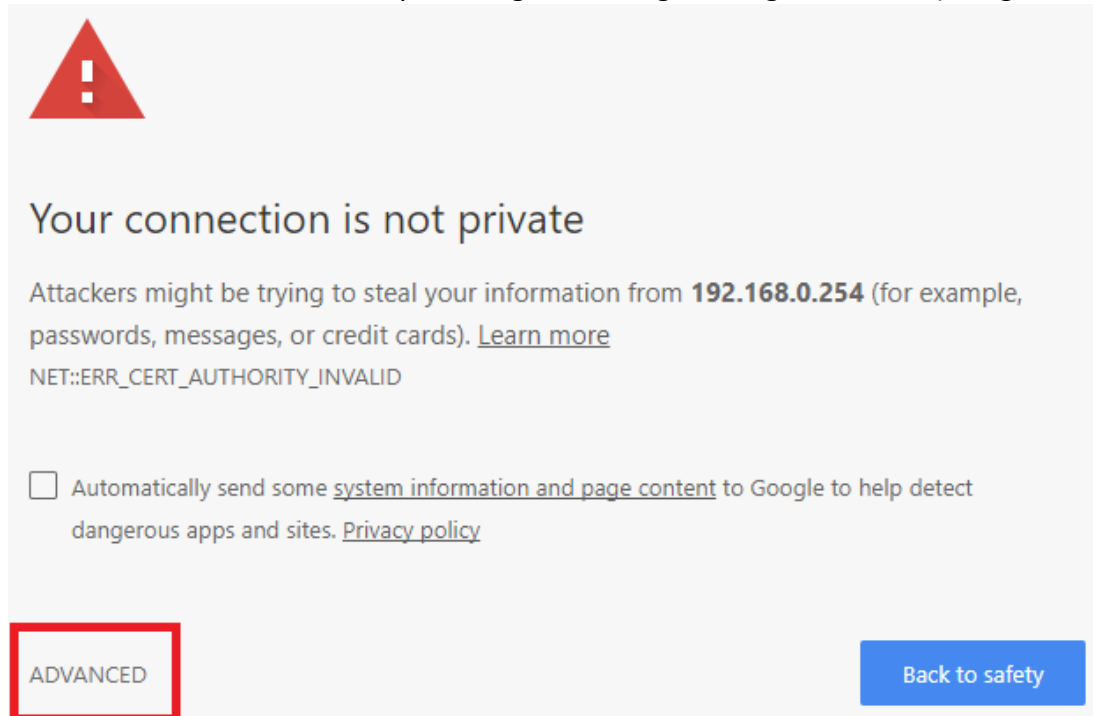
Open your web browser; enter the IP address of your router, which by default is 192.168.0.254, and click ok or press 'Enter' key on the keyboard, a login prompt window will appear.



Congratulations! You are now successfully logged in to the Firewall Router!

The TW-EAV510AC also supports 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 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 some basic settings of the device.

System	
Device Name	TW-EAV510 AC (b)
Uptime	13 min
Date/Time	Tue May 15 10:24:06 EEST 2018
Firmware Version	2.53.d16
DSP Version	v135k35B
CPU Usage	0%
Memory Usage	42%
Name Servers	139.175.1.1,8.8.8.8
IPv4 Default Gateway	ppp0
DSL	
Operational Status	G.dmt Annex A,SHOWTIME.
Upstream Speed	928 kbps
Downstream Speed	8000 kbps
LAN Configuration	
IP Address	192.168.0.254
Subnet Mask	255.255.255.0
DHCP Server	Enabled
MAC Address	00:04:ED:19:12:77

WAN Configuration						
Interface	VPI/VCI	Encapsulation	Protocol	IP Address	Gateway	Status
ppp0_vc0	0/33	LLC	PPPoE	59.104.108.29	59.104.108.1	up 00:11:08 Disconnect
ADSL1	0/100	LLC	mer1483			down
ADSL2	0/35	LLC	mer1483			down
PTM0	---	---	IPoE			down
EWAN	---	---	IPoE			down

3G Configuration				
Interface	Protocol	IP Address	Gateway	Status
4G	IPOE			n/a

[Refresh](#)

3G/4G/LTE Info

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

3G/4G LTE Status

3G/4G/LTE Status	
Status	3G/4G/LTE Card not found
Signal Strength	0 %
Network Name	N/A
Network Mode	N/A
Card Name	N/A
Card Firmware	N/A
Current TX Bytes / Packets	0 / 0
Current RX Bytes / Packets	0 / 0
Total TX Bytes / Packets	0 / 0
Total RX Bytes / Packets	0 / 0

Refresh

Status: The current status of the 3G/4G LTE connection.

Signal Strength: The signal strength bar and dBm value indicates the current 3G/4G-LTE signal strength. The front panel 3G/4G LTE Signal Strength LED indicates the signal strength as well.

Network Name: The name of the 3G/4G LTE network the router is connecting to.

Network Mode: The current operation mode for 3G/4G LTE module, it depends on service provider and card's limitation, GSM or UMTS.

Card Name: Given a name for the embedded 3G/4G LTE module.

Card Firmware: Current used FW in the 3G/4G LTE module.

Current Received (RX) /Transmitted (TX) Bytes: Current Rx/TX (receive/transmit) packets in Byte

Total Received (RX) /Transmitted (TX) Bytes: The total Rx/TX (receive/transmit) packets in Byte

Total Connection Time: The total of 3G/4G LTE dongle connection time since the 3G/4G LTE is up and running

AP Neighbor

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

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.

5GHz Wifi

SSID	BSSID	Channel	Type	Encryption	Signal
------	-------	---------	------	------------	--------

2.4GHz Wifi

SSID	BSSID	Channel	Type	Encryption	Signal
------	-------	---------	------	------------	--------

Refresh

IPv6

This page shows the current system status of IPv6.

IPv6 Status

This page shows the current system status of IPv6.

LAN Configuration

IPv6 Address	
IPv6 Link-Local Address	

Prefix Delegation

Prefix	
--------	--

WAN Configuration

Interface	VPI/VCI	Encapsulation	Protocol	IP Address	Status
-----------	---------	---------------	----------	------------	--------

Refresh

VPN

VPN status viewing section provides users IPsec, PPTP, L2TP VPN status.

PPTP

PPTP VPN Status

PPTP Server Status									
Name	Username	Connection Type	Peer Network IP	Peer Netmask	Status	Uptime	Connect By	Assigned IP Address	Action

PPTP Client Status							
Name	Username	Server	Connection Type	Peer Network IP	Peer Netmask	IP Address	Action

PPTP Server

Name: The PPTP connection name.

Connection Type: Remote Access or LAN to LAN.

Peer Network IP/Netmask: Display the remote (client side) network and subnet mask in LAN to LAN PPTP connection.

Status: The connection status, connected or not.

Uptime: The uptime.

Connected By: Display the IP of remotely connected client.

Assigned IP Address: The IP address to be assigned to PPTP Client

Action: Act to the connection. Click Drop button to disconnect the tunnel connection.

PPTP Client

Name: The PPTP connection name.

Server: The PPTP server IP.

Connection Type: Remote Access or LAN to LAN.

Peer Network IP/Netmask: Display the remote (server side) network and subnet mask.

IP Address: Assigned IP by PPTP server.

Action: Act to the connection. Click Disconnect button to disconnect the tunnel connection.

L2TP

L2TP VPN Status

L2TP Server Status									
Name	Username	Connection Type	Peer Network IP	Peer Netmask	Status	Uptime	Connect By	Assigned IP Address	Action

L2TP Client Status							
Name	Username	Server	Connection Type	Peer Network IP	Peer Netmask	IP Address	Action

L2TP Server

Name: The L2TP connection name.

Connection Type: Remote Access or LAN to LAN.

Peer Network IP/Netmask: Display the remote (client side) network and subnet mask in LAN to LAN L2TP connection.

Status: The connection status, connected or not.

Uptime: The uptime.

Connected By: Display the IP of remotely connected client.

Assigned IP Address: The IP address to be assigned to L2TP Client

Action: Act to the connection. Click Drop button to disconnect the tunnel connection.

L2TP Client

Name: The L2TP connection name.

Server: The L2TP server IP.

Connection Type: Remote Access or LAN to LAN.

Peer Network IP/Netmask: Display the remote (server side) network and subnet mask.

IP Address: Assigned IP by L2TP server.

Action: Act to the connection. Click Disconnect button to disconnect the tunnel connection.

IPSec

IPsec VPN Status

IPSec VPN Table							
Name	Active	Local Network	Remote Network	Remote Gateway IP	Connection State	Uptime	Action

- Name:** The IPSec connection name.
- Active:** Display the connection status.
- Local Subnet:** Display the local network.
- Remote Subnet:** Display the remote network.
- Remote Gateway:** The remote gateway address.
- Connection State:** Connection Status.
- Uptime:** The uptime for the tunnel.
- Action:** Act to the connection. Click Disconnect button to disconnect the tunnel connection.

LAN Port

This page shows if the LAN port is connected and the working status, rate, and duplex mode.

LAN Port Status

This page shows the current LAN Port status.

LAN Port Status	
LAN1	not-connected
LAN2	Up, 100Mb, Full
LAN3	not-connected
LAN4	not-connected

Refresh

ARP

This section displays the router’s ARP (Address Resolution Protocol) Table, which shows the mapping of Internet (IP) addresses to Ethernet (MAC) addresses. This is useful as a quick way of determining the MAC address of the network interface of your PCs to use with the router’s **Security – MAC Filtering** function.

User List

This table shows a list of learned MAC addresses.

IP Address	Flag	MAC Address	Mark
192.168.0.125	Complete	00:1E:8C:42:BD:15	

Refresh

ARP table

IP Address: Shows the IP Address of the device that the MAC address maps to.

Flag: Shows the current status of the ARP entries.

- ① Complete: the route resolving is processing well.
- ① M(Marked as permanent entry): the route is permanent.
- ① P (publish entry): publish this route item.

MAC Address: Shows the MAC address that is corresponded to the IP address of the device it is mapped to.

Mark: Show clearly the SSID (WLAN) the device is in.

DHCP

The DHCP Table lists the DHCP lease information for all IP addresses assigned by the DHCP server in the device.

Active DHCP Clients

This table shows the assigned IP address, MAC address and time expired for each DHCP leased client.

Host Name	IP Address	MAC Address	Expired Time (sec)	Mark
-----------	------------	-------------	--------------------	------

Refresh

Close

- Host Name:** The Host Name of DHCP client
- IP Address:** The IP address which is assigned to the host with this MAC address
- MAC Address:** The MAC Address of internal DHCP client host
- Expires in:** Show the remaining time after registration
- Mark:** Show clearly the SSID (WLAN) the device is in

System Log

Display system logs accumulated up to the present time. You can trace historical information with this function.

Log Configuring

System Log	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
System Log Reverse	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Log Level	Informational ▼
Display Level	Informational ▼
Mode	Local ▼
Server IP Address	<input type="text"/>
Server UDP Port	<input type="text"/>
<input type="button" value="Apply Changes"/>	
Save Log to File	<input type="button" value="Save..."/>
Clear Log	<input type="button" value="Reset"/>

System Log: Enable or disable this function.

System Log Reserve: Choose if to reverse the order of log item display, with the latest at the top.

Log level: Select your log level. The log level allows you to configure which types of events are logged. There are eight log levels from high to low are displayed below:

- ♦ **Emergency** = system is unusable
- ♦ **Alert** = action must be taken immediately
- ♦ **Critical** = critical conditions
- ♦ **Error** = error conditions
- ♦ **Warning** = warning conditions
- ♦ **Notice** = normal but significant conditions
- ♦ **Informational** = information events
- ♦ **Debugging** = debug-level messages

The gateway records all log events at the chosen level and above. For instance, if you set the log level to Critical, all critical, alert, and emergency events are logged, but none of the others are recorded

Display Level: Display the log according to the level you set when you view system log. Once you set the display level, the logs of the same or higher priority will be displayed.

Mode: Select the mode the system log adopted. Three modes: local, Remote and Both.

- ♦ **Local:** Select this mode to store the logs in the router's local memory.
- ♦ **Remote:** Select this mode to send the log information to a remote log server. Then you must assign the remote log server and port, 514 is often used.
- ♦ **Both:** Logs stored adopting above two ways.

Click **Apply changes** to submit.

Save Log to File: Download the log to your local PC.

Clear Log: Click to clear the current log from the screen.

Refresh: Click to update the system log.

System Log

Refresh

Date/Time	Facility	Level	Message
May 15 10:47:26	authpriv	err	boa[197]: login error from ::ffff:122.96.153.234 for invalid username
May 15 10:18:57	authpriv	info	boa[197]: login successful for hallinta from ::ffff:122.96.153.234
May 15 10:18:50	authpriv	info	boa[197]: logout successful from ::ffff:192.168.0.125
May 15 10:18:32	authpriv	err	boa[197]: login error from ::ffff:122.96.153.234 for using the same account with another user at the same time
Jan 1 02:02:24	daemon	info	syslog: 13[CFG] loading secrets from '/usr/local/strongswan/etc/ipsec.secrets'
Jan 1 02:02:24	daemon	info	syslog: 13[CFG] rereading secrets
Jan 1 02:02:24	daemon	info	dnsmasq[2337]: using local addresses only for domain wpad.Home
Jan 1 02:02:24	daemon	info	dnsmasq[2337]: using nameserver 139.175.1.1#53
Jan 1 02:02:24	daemon	info	dnsmasq[2337]: using nameserver 8.8.8.8#53
Jan 1 02:02:24	daemon	warn	dnsmasq[2337]: ignoring nameserver 127.0.0.1 - local interface
Jan 1 02:02:24	daemon	info	dnsmasq[2337]: using nameserver ::1#53
Jan 1 02:02:24	daemon	info	dnsmasq[2337]: reading /var/resolv.conf
Jan 1 02:02:24	daemon	info	dnsmasq[2337]: using local addresses only for domain wpad.Home
Jan 1	daemon	info	dnsmasq[2337]: using nameserver 139.175.1.1#53

Date/Time	Facility	Level	Message
May 18 05:29:22	daemon	info	dnsmasq[3427]: using nameserver 8.8.8.8#53
May 18 05:29:22	daemon	info	dnsmasq[3427]: compile time options: IPV6 GNU-getopt no-ISC-leasefile no-DBus no-I18N TFTP
May 18 05:29:22	daemon	info	dnsmasq[3427]: started, version 2.45 cachesize 150
May 18 05:29:22	daemon	info	dnsmasq[3379]: exiting on receipt of SIGTERM

(System Log Reserve Enabled)

LAN

A Local Area Network (LAN) is a shared communication system network where many computers are connected. This type of network is area defined and is usually limited to a confined region within a building.

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..

Interface Name	br0
IP Address	<input type="text" value="192.168.0.254"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
IGMP Snooping	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled
Ethernet to Wireless Blocking	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled

DHCP Settings

This page is used to configure DHCP Server and DHCP Relay.

DHCP Mode	<input type="radio"/> NONE <input type="radio"/> DHCP Relay <input checked="" type="radio"/> 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="192.168.0.199"/>	<input type="button" value="Show Client"/>
Max Lease Time	<input type="text" value="86400"/> seconds	(-1 indicates an infinite lease)
Domain Name	<input type="text" value="Home"/>	
Gateway Address	<input type="text" value="192.168.0.254"/>	
DNS option	<input checked="" type="radio"/> Use DNS Relay <input type="radio"/> Set Manually	

IP address: the IP address of the router. Default is 192.168.0.254.

Subnet Mask: the default Subnet mask on the router.

IGMP Snooping: Enable or disable the IGMP Snooping function. Without IGMP snooping, multicast traffic is treated in the same manner as broadcast traffic - that is, it is forwarded to all ports. With IGMP snooping, multicast traffic of a group is only forwarded to ports that have members of that group."

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.

Port Based Filter: Choose if DHCP server will drop DHCP packet from the designated port.

For example, if LAN3 is selected, PC on LAN3 will not obtain IP from the DHCP server. But PC on this port can be manually set IP.

Port-Based Filter

This page is used to configure the Port-Based Filtering.

Filter DHCP Discover packet

☐ LAN1

☐ LAN2

☒ LAN3

☐ LAN4

☐ TW-EAV510AC_5G_6688

☐ TW-EAV510AC_2.4G_6688

Apply Changes

Close

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

MAC-Based Assignment

This page is used to configure the static IP base on MAC Address. You can assign/delete the static IP. The Host MAC Address, please input a string with hex number. Such as 00-d0-59-c6-12-43. The Assigned IP Address, please input a string with digit. Such as 192.168.1.100 .

MAC Address (xx-xx-xx-xx-xx-xx)

Assigned IP Address (xxx.xxx.xxx.xxx)

Add IP

Edit

Delete Assigned IP

Close

MAC-Based Assignment Table			
Edit	MAC Address	Assigned IP Address	Select

WLAN

TW-EAV510 AC is a simultaneous dual-band (2.4G and 5G) wireless router supporting 11b/g/n/a/ac wireless standards. It allows multiple wireless users on 2.4G and 5G radio bands to surf the Internet, checking e-mail, watching video, listening to music over the Internet concurrently.

You can choose the optimum radio band wireless connection base on your environment.

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-EAV510AC_2.4G_1277

Channel Width

20/40MHz ▾

Control Sideband

Upper ▾

Channel Number

Auto ▾

Radio Power (%)

100% ▾

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.
- Radio Power:** 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)
Data Rate	<input type="text" value="Auto"/> ▼	
Preamble Type	<input checked="" type="radio"/> Long Preamble <input type="radio"/> Short Preamble	
Broadcast SSID	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	
Relay Blocking	<input type="radio"/> Enabled <input checked="" 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 Type	Root AP - TW-EAV510AC_2.4G_1277 ▼
-----------	-----------------------------------

Encryption	WPA2 ▼
Authentication Mode	<input type="radio"/> RADIUS <input checked="" type="radio"/> Pre-Shared Key
IEEE 802.11w	<input type="radio"/> None <input checked="" type="radio"/> Capable <input type="radio"/> Required
SHA256	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
WPA2 Cipher Suite	<input type="checkbox"/> TKIP <input checked="" type="checkbox"/> AES
Group Key Update Timer	3600
Pre-Shared Key Format	Passphrase ▼
Pre-Shared Key	●●●●●●●●●● Click here to display

Apply Changes

SSID choice: Apply the security settings to selected SSID.

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

◆ None

Encryption	NONE ▼
802.1x Authentication	<input type="checkbox"/>

802.1x Authentication: If to enable 802.1x authentication.

RADIUS Server IP Address: RADIUS(Remote Authentication Dial In User Service), Enter the IP address of RADIUS authentication server.

RADIUS Server Port: Enter the port number of RADIUS authentication server here.

RADIUS Password: Enter the password of RADIUS authentication server.

◆ WEP

Encryption	WEP ▼
802.1x Authentication	<input checked="" type="checkbox"/>
Authentication	<input type="radio"/> Open System <input type="radio"/> Shared Key <input checked="" type="radio"/> Auto
Key Length	<input checked="" type="radio"/> 64 Bits <input type="radio"/> 128 Bits
RADIUS Server IP Address	0.0.0.0
RADIUS Server Port	1812
RADIUS Server Password	

802.1x Authentication: If to enable 802.1x authentication.

Key Length: 64 Bits or 128 bits.

RADIUS Server IP Address: RADIUS(Remote Authentication Dial In User Service), Enter the IP address of RADIUS authentication server.

RADIUS Server Port: Enter the port number of RADIUS authentication server here.

RADIUS Password: Enter the password of RADIUS authentication server.

♦ WEP

Encryption	WEP ▼
802.1x Authentication	<input type="checkbox"/>
Authentication	<input type="radio"/> Open System <input type="radio"/> Shared Key <input checked="" type="radio"/> Auto
Key Length	64-bit ▼
Key Format	ASCII (5 characters) ▼
Encryption Key	*****

Authentication: Open, shared key or auto.

Key Length: 64 bits or 128 bits.

Key Format: ASCII or Hex.

Encryption Key: Enter the key to encrypt wireless data.

If you chose **WEP 64-bit**, then enter any 5 ASCII characters or 10 hexadecimal characters (0-9, A-F).

If you chose **WEP 128-bit**, then enter 13 ASCII characters or 26 hexadecimal characters (0-9, A-F).

♦ WPA

Encryption	WPA
Authentication Mode	<input type="radio"/> RADIUS <input checked="" type="radio"/> Pre-Shared Key
WPA Cipher Suite:	<input type="checkbox"/> TKIP <input checked="" type="checkbox"/> AES
Group Key Update Timer	3600
Pre-Shared Key Format	Passphrase
Pre-Shared Key	<input type="password"/> Click here to display

Authentication Mode: RADIUS and Pre-shared key. If RADIUS, please RADIUS(Remote Authentication Dial In User Service), Enter the IP address, port, password of RADIUS authentication server.

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.

◆ WPA2/WPA2 Mixed

Encryption	WPA2
Authentication Mode	<input type="radio"/> RADIUS <input checked="" type="radio"/> Pre-Shared Key
IEEE 802.11w	<input type="radio"/> None <input checked="" type="radio"/> Capable <input type="radio"/> Required
SHA256	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
WPA2 Cipher Suite	<input type="checkbox"/> TKIP <input checked="" type="checkbox"/> AES
Group Key Update Timer	3600
Pre-Shared Key Format	Passphrase
Pre-Shared Key	<input type="password"/> Click here to display

Authentication Mode: RADIUS and Pre-shared key. If RADIUS, please RADIUS(Remote Authentication Dial In User Service), Enter the IP address, port, password of RADIUS authentication server.

IEEE802.11w: If to enable IEEE802.11w. IEEE 802.11w is the Protected Management Frames standard

SHA256: Whether to enable SHA256 encryption.

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, wireless MAC Filter.

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. 00:E0:86:71:05:02)

Add Edit Reset

Current Access Control List

Edit	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	Type	Encryption	Signal
------	-------	---------	------	------------	--------

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.

Wi-Fi Protected Setup

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your WLAN client automatically synchronize its setting and connect to the Access Point in a minute without any hassle.

Disable WPS

☐

WPS Status

☒ Configured ☐ UnConfigured

Auto-lock-down state

Unlocked

Unlock

Self-PIN Number

12345670

Regenerate PIN

Push Button Configuration

Start PBC

Apply Changes

Reset

Current Key Info

Authentication	Encryption	Key
WPA2 PSK	AES	822e54a9acd77d85

Client PIN Number

Start PIN

Status

This page shows the current configuration of WiFi module.

WLAN Status

This page shows the WLAN current status.

WLAN Configuration	
Mode	AP
Band	2.4 GHz (B+G+N)
SSID	TW-EAV510AC_2.4G_1277
Channel Number	1
Encryption	WPA2
BSSID	00:04:ED:19:12:78
Associated Clients	0

WAN

A WAN (Wide Area Network) is a computer network that covers a broad geographical area (eg. Internet) that is used to connect LAN and other types of network systems.

WAN Mode

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

WAN Mode

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

WAN Mode

☒ ATM

☒ Ethernet

☒ PTM

Submit

Default Routing

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

Default Routing Gateway Priority

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

4G
PTM0
ADSL1
ADSL2
EWAN
ppp0_vc0

↑

↓

Enable Multi-Path Routing Load Balancing ☐

(All WAN interfaces must have different gateway IP address.)

Apply Changes

Ethernet WAN

The page is used to configure the parameters and protocol for the Ethernet WAN port. The device offers four popular methods for connecting WAN - Ethernet WAN (broadband) seen below, VDSL, see [PTM \(VDSL\) WAN](#) and ADSL, see [ATM \(ADSL\) WAN](#) and 3G/4G LTE, see [3G/4G LTE Settings](#).

Ethernet WAN

This page is used to configure the parameters for EthernetWAN

WAN Interface	<input type="text" value="nas0_0"/>		
Enable VLAN	<input type="checkbox"/>		
VLAN ID	<input type="text"/>	802.1p_Mark	<input type="text"/>
Channel Mode	<input type="text" value="IPoE"/>		
Enable Bridge	<input type="checkbox"/>		
Bridge Mode	<input type="text" value="Bridged Ethernet (Transparent Bridging)"/>		
Enable NAPT	<input checked="" type="checkbox"/>	Enable QoS	<input checked="" type="checkbox"/>
Admin Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
MTU	<input type="text" value="1500"/>		
IGMP Proxy	<input checked="" type="checkbox"/> Enable		

WAN IP Settings	
Type	<input type="radio"/> Fixed IP <input checked="" type="radio"/> DHCP
Local IP Address	<input type="text"/>
Remote IP Address	<input type="text"/>
Subnet Mask	<input type="text"/>
Request DNS	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Primary DNS Server	<input type="text"/>
Secondary DNS Server	<input type="text"/>
IP Unnumbered <input type="checkbox"/>	

WAN Interface: 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 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.

PTM(VDSL) WAN

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

PTM WAN

This page is used to configure the parameters for PTMWAN

WAN Interface

ptm0_0

Enable VLAN

☐

VLAN ID

802.1p_Mark

Channel Mode

IPoE

Enable Bridge

☐

Bridge Mode

Bridged Ethernet (Transparent Bridging)

Enable NAPT

☒

Enable QoS

☒

Admin Status

☒ Enable ☐ Disable

MTU

1500

IGMP Proxy

☒ Enable

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

- WAN Interface:** 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.

ATM(ADSL) WAN

The page is used to configure the parameters and protocol for the ADSL WAN port. There are three pre-set ADSL connections, users can edit  or add your own ADSL rules.

But note, edit when your channel mode (protocol) is in line with one of the pre-set rules, or please add new ones.




Click  to delete the undesired ADSL rules.

DSL WAN Configuration

This page is used to configure the parameters for WAN Mode

VPI/VCI	<input type="text" value="0"/> / <input type="text" value=""/>	Encapsulation	<input checked="" type="radio"/> LLC <input type="radio"/> VC-Mux
Channel Mode	<input type="text" value="1483 Bridged"/>	Enable NAPT	<input type="checkbox"/>
Enable NAPT	<input type="checkbox"/>	Enable QoS	<input type="checkbox"/>
Admin Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
IGMP Proxy	<input type="checkbox"/> Enable		

Current ATM VC Table

Select	Interface	Mode	VPI	VCI	Encapsulation	NAPT	IGMP	IP Address	Remote IP	Subnet Mask	UserName	Default Route	Status	Actions
<input type="radio"/>	ADSL0	mer1483	0	33	LLC	on	on					on	Enabled	
<input type="radio"/>	ADSL1	mer1483	0	100	LLC	on	on					on	Enabled	
<input type="radio"/>	ADSL2	mer1483	0	35	LLC	on	on					on	Enabled	

<input type="checkbox"/> Enable Auto-PVC Search	<input type="button" value="Apply"/>
VPI <input type="text" value="0"/> VCI <input type="text" value=""/>	<input type="button" value="Add"/> <input type="button" value="Delete"/>

Current Auto-PVC Table:

PVC	VPI	VCI
-----	-----	-----

VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit.

VPI: Virtual Path Identifier. The valid range for the VPI is 0 to 255. Enter the VPI assigned to you. This field may already be configured.

VCI: Virtual Channel Identifier. The valid range for the VCI is 1 to 65535. Enter the VCI assigned to you. This field may already be configured.

Encapsulation: Select in the Mode field, select LLC, VC-Mux.

Channel Mode: You can choose 1483 Bridged, 1483 MER, PPPoE, PPPoA, 1483 Routed or 1577 Routed.

Enable NAPT: Select it to enable Network Address Port Translation (NAPT) function which allows multiple users to access the Internet through a single IP account by sharing the single IP address. If you do not select it and you want to access the Internet normally, you must add a route on the uplink equipment. Otherwise, the access to the Internet fails. Normally, it is enabled.

Admin Status: Activate/Enable or disable the connection.

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

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

Now, let's add a PPPoE ADSL connection.

VPI/VCI

0

/

33

Encapsulation

☒ LLC

☐ VC-Mux

Channel Mode

PPPoE

Enable NAPT

☒

Enable QoS

☐

Admin Status

☒ Enable

☐ Disable

IGMP Proxy

☒ Enable

PPP Settings

User Name

t0083328

Password

••••••••

Type

Continuous

Idle Time (sec)

Add

Modify

VPI/VCI: if not sure, please [Enable Auto-PVC Search](#).

PPP Settings:

Username/Password: Please input the PPP dial-up account.

Type: To determine the duration of a dial-up connection.

- ♦ **Continuous:** Select this option when you want your connection up all the time.
- ♦ **Connect on Demand:** Select it when you don't want the connection up all the time and specify an idle time-out in the Max Idle Timeout field.
- ♦ **Manual:** Select this mode if you want to connect manually.

Idle Time(min): If set the type to Connect on Demand, you need to enter the idle timeout time. Within the preset minutes, if the router does not detect the flow of the user, the router automatically disconnects the PPP connection.

Click Add the put it in the **Current ATM VC Table**.

Select	Interface	Mode	VPI	VCI	Encapsulation	NAPT	IGMP	IP Address	Remote IP	Subnet Mask	UserName	Default Route	Status	Actions
<input type="radio"/>	ppp0_vc0	PPPoE	0	33	LLC	on	on				t0083328	on	Enabled	

Check the connection status in Status > Device page.

WAN Configuration						
Interface	VPI/VCI	Encapsulation	Protocol	IP Address	Gateway	Status
ppp0_vc0	0/33	LLC	PPPoE	203.67.167.198	203.67.167.1	up 00:03:41 <div>Disconnect</div>

Enable Auto-PVC Search

This feature is used to configure pvc auto detection. Here you can add/delete items in auto pvc search table.

☐ Enable Auto-PVC Search

Apply

VPI 0

VCI

Add

Delete

Current Auto-PVC Table:

PVC	VPI	VCI
-----	-----	-----

Apply: When ADSL is up and you are not sure about your VPI/VCI. Press Apply to auto-search PVCs, which are to be shown in the current auto-PVC table.

Current Auto-PVC Table:

PVC	VPI	VCI
0	0	35
1	8	35
2	0	43
3	0	51
4	0	59
5	8	43
6	8	51
7	8	59

VPI/VCI: Enter the VPI/VCI needs to be added to the Current Auto-PVC Table by pressing Add button or deleted from the table by pressing Delete button.

ATM Settings

This page is used to configure the ATM parameters. Here you may change the setting for QoS, PCR,CDVT, SCR and MBS.

ATM Settings

This page is used to configure the parameters for the ATM of your Device. Here you may change the setting for VPI, VCI, QoS etc...

VPI

VCI

QoS

UBR

PCR

CDVT

SCR

MBS

Apply Changes

Undo

Current ATM VC Table

Select	VPI	VCI	QoS	PCR	CDVT	SCR	MBS
<input type="radio"/>	0	33	UBR	6000	0	---	---
<input type="radio"/>	0	100	UBR	6000	0	---	---
<input type="radio"/>	0	35	UBR	6000	0	---	---

The ATM QoS types include CBR (Constant Bit Rate), VBR (Variable Bit Rate) and UBR (Unspecified Bit Rate). These QoS types are all controlled by the parameters specified below, including PCR, SCR and MBS.

Select CBR to specify fixed (always-on) bandwidth for voice or data traffic. Select UBR for applications that are non-time sensitive, such as e-mail. Select VBR for burst traffic and bandwidth sharing with other applications.

PCR: Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells.

CDVT: CDVT (Cell Delay Variation Tolerance), is often associated with PCR to indicate how much jitter is allowed.

SCR: The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted.

MBS: Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535

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

G.INP Option

☐ Enabled

G.Vector Option

☒ Enabled

VDSL2 Profile

☒ 8a
☒ 8b
☒ 8c
☒ 8d
☒ 12a
☒ 12b
☒ 17a
☒ 30a
☐ 35b

DSL 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 WAN	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Mode	4G LTE only ▼
Use PPP	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
IPv6 for this service	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
PIN Code	<input type="text"/>
APN	internet
Dial Number	*99#
Authentication	NONE ▼
User Name	<input type="text"/>
Password	<input type="text"/>
Connection Type	Continuous ▼
Keep Alive	<input checked="" type="checkbox"/> Enable <input type="text" value="30"/> seconds [1-86400]
Target Address	8.8.8.8
NAPT	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Firewall	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Default Route	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
MTU	1500

3G/4G LTE WAN: Enable/Disable the 3G/4G LTE dongle detection function.

Mode: There are 6 options of phone service standards: GSM 2G only, UTMS 3G only, GSM 2G preferred, UMTS 3G preferred, Automatic, and Use 3G/LTE 3g dongle settings. If you are uncertain what services are available to you, and then please select Automatic.

IPv6 for this service: If to enable IPv6.

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).

Connection: Default set to Continuous to keep an always-on 3G/4G-LTE connection.

- ♦ **Connect on Demand:** If you want to make UMTS/GPRS call only when there is a packet requesting access to the Internet (i.e. when a program on your computer attempts to access the Internet). In this mode, you must set Idle Timeout value at same time. Click on Connect on Demand, the Idle Timeout field will display.

Idle Timeout: Auto-disconnect the broadband firewall gateway when there is no activity on the line for a predetermined period of time. Default is 60 mins.

- ♦ **Continuous:** keep an always-on 3G/4G-LTE connection

Keep Alive: Check Enable to allow the router to send message out every 7 seconds (can be changed base on need) to prevent the connection being dropped by ISP.

IP Address: The IP address is used to “ping”, and router will ping the IP to find whether the connection is still on.

- ♦ **Manual:** Select this mode if you want to connect manually.

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.

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, TZO, No-IP or dy.fi. Here you can Add/Remove to configure Dynamic DNS.

Enable

☒

DDNS Provider

DynDNS.com ▾

Hostname

Interface

Any ▾

DynDns/No-IP Settings

User Name

Password

TZO/dy.fi Settings

Email

Key

Add

Modify

Remove

Dynamic DNS Table

Select	State	Hostname	User Name	Service	Status
--------	-------	----------	-----------	---------	--------

- Enable:** Select this check box to activate Dynamic DNS.
- DNS Provider:** Select from drop-down menu for the appropriate service provider, for example: DynDNS.org.
- Hostname:** Type the domain name registered at your Dynamic DNS provider.
- Interface:** The interface applies DDNS, and is associated with the hostname..

DynDns Settings

Username: Your registered name.

Password: Your registered password.

TZO Settings:

Email: Your registered email.

Key: Your registered key.

Click Add to confirm your DDNS rules.

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

h323

☒ Enable ☐ Disable

rtsp

☒ Enable ☐ Disable

sip

☒ Enable ☐ Disable

pptp

☒ Enable ☐ Disable

Apply Changes

VPN pass-through (L2TP/PPTP) is a feature of routers which allows VPN client on a private network to establish outbound VPNs unhindered.

FTP ALG enabled allows FTP clients behind an NAT to establish a connection on the port of FTP Server.

Enable the H.323/SIP ALG when H.323/SIP SIP phone needs ALG to pass through the NAT. Disable the SIP ALG when H.323/SIP phone includes NAT-Traversal algorithm.

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

Source IP Address

Destination IP Address

Protocol

TCP

Subnet Mask

Subnet Mask

Rule Action

☒ Deny ☐ Allow

Port

Port

Add

Edit

Current Filter Table

Edit	Direction	Protocol	Source IP Address	Source Port	Destination IP Address	Destination Port	Rule Action	Select
------	-----------	----------	-------------------	-------------	------------------------	------------------	-------------	--------

Delete Selected

Delete All

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 for bridge mode

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

Outgoing Default Action

Incoming Default Action

☐ Deny

☒ Allow

☐ Deny

☒ Allow

Apply Changes

Direction

Source MAC Address

Destination MAC Address

Rule Action

Outgoing

☒ Deny

☐ Allow

Add

Edit

Current Filter Table

Edit	Direction	Source MAC Address	Destination MAC Address	Rule Action	Select
------	-----------	--------------------	-------------------------	-------------	--------

Delete Selected

Delete All

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

Direction: Specify the direction of traffic.

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

Rule Action: Specify what action will be applied to this rule.

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

Application FTP Server

Enable ☒

Comment	Local IP	Local Port	Protocol	Remote IP	Public Port	Interface
FTP Server		21 ~ 21	TCP ▾		21 ~ 21	Any ▾
		~	▾			Any ▾
		~	▾			Any ▾
		~	▾			Any ▾
		~	▾			Any ▾
		~	▾			Any ▾
		~	▾			Any ▾
		~	▾			Any ▾
		~	▾			Any ▾
		~	▾			Any ▾
		~	▾			Any ▾
		~	▾			Any ▾
		~	▾			Any ▾
		~	▾			Any ▾
		~	▾			Any ▾
		~	▾			Any ▾

Current Port Forwarding Table

Edit	Comment Local	IP Address	Protocol	Local Port	Enable	Remote Host	Public Port	Interface	Select
<input type="button" value="Delete Selected"/>	<input type="button" value="Delete All"/>								

Port Forwarding: Choose if to enable Port Forwarding feature. And Apply Changes to save the setting.

Application: You can select the common application type, for example, **AUTH**, **FTP** or **TFTP**.

Enable: To activate the rule or not.

Comment: user-defined description for the rule.

Local IP/Port: Set the local IP and port (range) for the application(local server). The local IP is in the same network segment with LAN IP address of the router.

Protocol: Choose the transport layer protocol that the service uses. You can choose **TCP**, **UDP** or **Both**.

Remote IP/Public Port: Set the remote/external IP and port (range) for the application.

WAN Interface: Choose the WAN interface that will apply virtual server.

Examples of well-known and registered port numbers are shown below. For further information, please see IANA's website at <http://www.iana.org/assignments/port-numbers>

Well-known and Registered Ports

Port Number	Protocol	Description
21	TCP	FTP Control
22	TCP & UDP	SSH Remote Login Protocol
23	TCP	Telnet
25	TCP	SMTP (Simple Mail Transfer Protocol)
53	TCP & UDP	DNS (Domain Name Server)
69	UDP	TFTP (Trivial File Transfer Protocol)
80	TCP	World Wide Web HTTP
110	TCP	POP3 (Post Office Protocol Version 3)
443	TCP & UDP	HTTPS
1503	TCP	T.120
1720	TCP	H.323
7070	UDP	RealAudio

Example: How to setup Port Forwarding for port 21 (FTP server)

If you have a FTP server on your LAN network and want others to access it through WAN.

Step 1: Assign a static IP to your local computer that is hosting the FTP server.

Step 2: Login to the Gateway to **Virtual Server**.

FTP server uses TCP protocol with port 21.

Enter "21" to Public Port and LAN Port. And specify the external IP. The router will accept port 21 requests from the designated external IP.

Enter the static IP assigned to the local PC that is hosting the FTP server. Ex: 192.168.0.102

The router will forward port 21 request to the specific LAN PC (ex:192.168.0.102) in the network.

Comment	Local IP	Local Port	Protocol	Remote IP	Public Port	Interface
FTP Server	192.168.0.102	21 ~ 21	TCP	59.104.108.177	21 ~ 21	Any
						Any

Current Port Forwarding Table

Edit	Comment Local	IP Address	Protocol	Local Port	Enable	Remote Host	Public Port	Interface	Select
<input checked="" type="checkbox"/>	FTP Server	192.168.0.102	TCP	21	Enable	59.104.108.177	21	Any	<input type="checkbox"/>

URL Blocking

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

URL Blocking

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

Apply Changes

FQDN

Add

Edit

URL Blocking Table

Edit	FQDN	Select
------	------	--------

Delete Selected

Delete All

Keyword

Add

Edit

Keyword Filtering Table

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

Delete Selected

Delete All

FQDN Blocking: To block the URL request with a matched FQDN. If a URL request is matched with listed items, the request will be dropped. Add restricted FQDN to the URL blocking table.

Keywords Filtering: Allow blocking against specific keywords within a particular URL (e.g.to block any image called “advertisement.gif”). When enabled, your specified keywords list will be checked to see if any keywords are present in URLs accessed to determine if the connection attempt should be blocked.

Domain Blocking

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

Domain Blocking Configuration

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

Domain Blocking

☒ Disable ☐ Enable

Apply Changes

Domain

Add

Edit

Domain Blocking Configuration

Edit

Domain

Select

Delete Selected

Delete All

Domains Blocking: Enter the domain to be blocked.

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.

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

0.0.0.0

Apply Changes

DMZ: If to enable DMZ.

DMZ Host IP Address: Enter the IP Address of a host that you want to be a DMZ host. Select from the list box to quick set the DMZ.

DoS

This page helps user to setup protection for DOS attack.

DoS Configuration

DoS (Denial-of-Service) attack which is launched by hacker aims to prevent legal user from taking normal services. In this page you can configure to prevent some kinds of DOS attack.

☒ **Enable DoS Block**

<input type="checkbox"/> Whole System Flood: SYN	<input type="text" value="500"/>	packets/second
<input type="checkbox"/> Whole System Flood: FIN	<input type="text" value="500"/>	packets/second
<input type="checkbox"/> Whole System Flood: UDP	<input type="text" value="500"/>	packets/second
<input type="checkbox"/> Whole System Flood: ICMP	<input type="text" value="500"/>	packets/second
<input type="checkbox"/> Per-Source IP Flood: SYN	<input type="text" value="500"/>	packets/second
<input type="checkbox"/> Per-Source IP Flood: FIN	<input type="text" value="500"/>	packets/second
<input type="checkbox"/> Per-Source IP Flood: UDP	<input type="text" value="500"/>	packets/second
<input type="checkbox"/> Per-Source IP Flood: ICMP	<input type="text" value="500"/>	packets/second
<input type="checkbox"/> TCP/UDP PortScan	<input type="text" value="Low"/>	Sensitivity
<input type="checkbox"/> ICMP Smurf		
<input type="checkbox"/> IP Land		
<input type="checkbox"/> IP Spoof		
<input type="checkbox"/> IP TearDrop		
<input type="checkbox"/> PingOfDeath		
<input type="checkbox"/> TCP Scan		
<input type="checkbox"/> TCP SynWithData		
<input type="checkbox"/> UDP Bomb		
<input type="checkbox"/> UDP EchoChargen		

Select All

Clear

☐ **Enable Source IP Blocking**

Block Interval (seconds)

Apply Changes

UPnP

UPnP offers peer-to-peer network connectivity for PCs and other network devices, along with control and data transfer between devices. UPnP offers many advantages for users running NAT routers through UPnP NAT Traversal, and on supported systems makes tasks such as port forwarding much easier by letting the application control the required settings, removing the need for the user to control advanced configuration of their device.

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

WAN Interface

ppp0

Apply Changes

UPnP: Select this checkbox to activate UPnP. Be aware that anyone could use an UPnP application to open the web configuration’s login screen without entering the TW-EAV510AC-B IP address.

WAN Interface: The interface UPnp is applied to.

Press **Apply Changes** to apply your settings.

RIP

Enable this Routing Information protocol for the router to communicate with other rip-enable devices.

RIP Configuration

Enable the RIP if you are using this device as a RIP-enabled Device to communicate with others using the Routing Information Protocol. This page is used to select the interfaces on your device is that use RIP, and the version of the protocol used.

RIP

☒ Disable ☐ Enable

Apply Changes

Interface

br0

Receive Mode

NONE

Send Mode

NONE

Add Edit

RIP Config Table

Edit	Interface	Receive Mode	Send Mode	Select
------	-----------	--------------	-----------	--------

Delete Selected Delete All

RIP: Select **Enable**, the router communicates with other RIP-enabled devices.

Interface: Choose the router interface that uses RIP.

Receive Mode: Choose the interface RIP version that receives RIP messages. You can choose **RIP1**, **RIP2**, or **Both**.

- Choose **RIP1** indicates the router receives RIP v1 messages.
- Choose **RIP2** indicates the router receives RIP v2 messages.
- Choose **Both** indicates the router receives RIP v1 and RIP v2 messages.

Send Mode: The working mode for sending RIP messages. You can choose **RIP1** or **RIP2**.

- Choose **RIP1** indicates the router broadcasts RIP1 messages only.
- Choose **RIP2** indicates the router multicasts RIP2 messages only.

Add: Click it to add the RIP interface to the **Rip Configuration List**.

Delete: Select a row in the **Rip Configuration List** and click it to delete the row.

Samba

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

Samba Configuration

This page let user to config Samba. (Only USB 3.0 port)

Samba	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Server String	<input type="text" value="Samba Server"/>
<input type="button" value="Apply Changes"/>	

Samba: Enable/Disable the Samba server. And security on/off

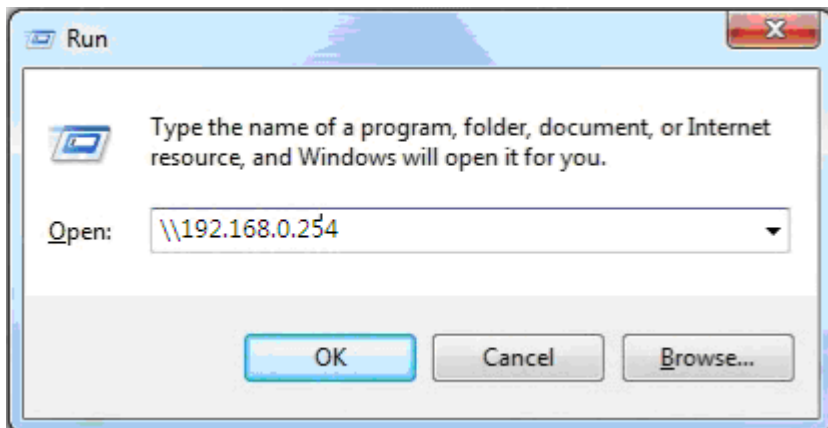
User id is :hallinta

Password: wifi key number

Server String: Descriptive string for the Samba server

How to access Samba

On a connected PC, go directly to Start > Run, enter [\\192.168.0.254](#).



VPN

A **virtual private network (VPN)** is a private network that interconnects remote (and often geographically separate) networks through primarily public communication infrastructures such as the Internet. VPNs provide security through tunneling protocols and security procedures such as encryption. For example, a VPN could be used to securely connect the branch offices of an organization to a head office network through the public Internet.

PPTP

The **Point-to-Point Tunneling Protocol (PPTP)** is a Layer2 tunneling protocol for implementing virtual private networks through IP network. PPTP uses an enhanced GRE (Generic Routing Encapsulation) mechanism to provide a flow- and congestion-controlled encapsulated datagram service for carrying PPP packets. In the Microsoft implementation, the tunneled PPP traffic can be authenticated with PAP, CHAP, Microsoft CHAP V1/V2.

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

Auth. Type

PAP

Peer Address

start from:

Local Address

Apply

Encryption Mode

NONE

Server Account

Name

Username

Connection Type

☒ Remote Access ☐ LAN to LAN

Peer Network IP

Add

Edit

Tunnel Password

Peer Netmask

☐ Disable ☒ Enable

PPTP Server Table

Edit	Name	Enable	Username	Connection Type	Peer Network IP	Peer Netmask	Select
------	------	--------	----------	-----------------	-----------------	--------------	--------

Delete Selected

Save

PPTP Client

Name

Username

Auth. Type

PAP

Connection Type

☒ Remote Access ☐ LAN to LAN

Peer Network IP

Default Gateway

☐

Add

Edit

Server Address

Password

Encryption Mode

NONE

Peer Netmask

PPTP Client Table

Edit	Interface	Server	Connection Type	Peer Network IP	Peer Netmask	Action	Select
------	-----------	--------	-----------------	-----------------	--------------	--------	--------

Delete Selected

PPTP VPN: Enable/Disable PPTP function.

PPTP Server

Auth. Type: Setup the authentication type for client - Chap/Pap, Pap, Chap or MS-CHAPv2 Encryption. When using PAP, the password is sent unencrypted, whilst CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that an intruder has not replaced the client. When passed the authentication with MS-CHAPv2, the MPPE encryption is supported.

Encryption Mode: Available when using MS-CHAPv2 authentication mode. The data can be encrypted by MPPE/MPPC algorithm

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 virtual interface.

Server Account

Name: Enter the name for this account profile.

Tunnel: Enable/Disable this tunnel.

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 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.

Auth.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.

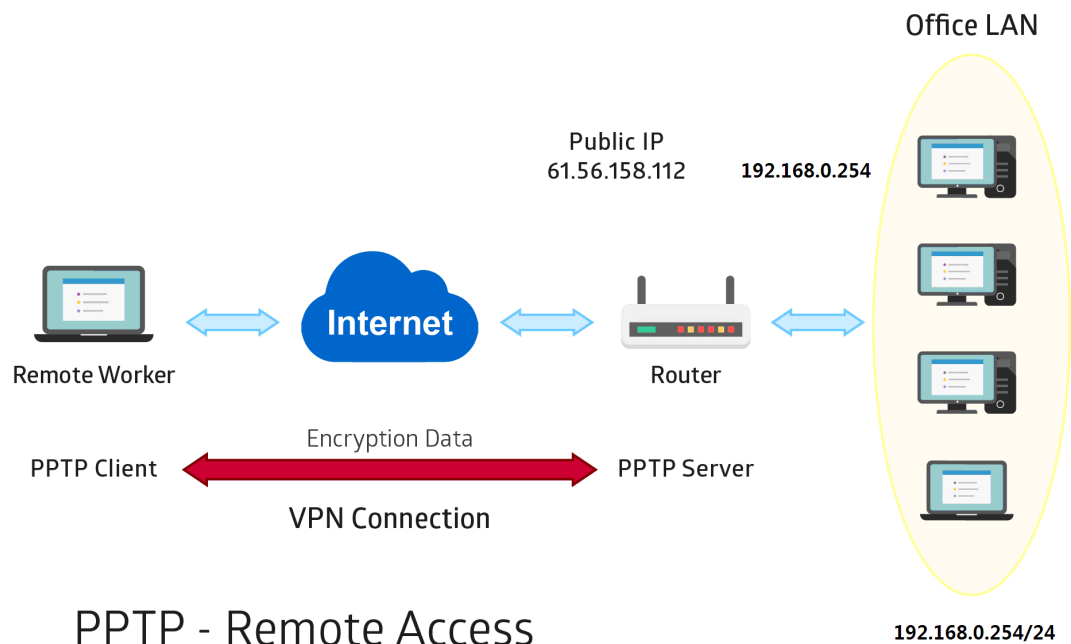
Peer IP: Enter the peer side LAN IP address for LAN to LAN type.

Peer Subnet Mask: Enter the peer side LAN subnet mask for LAN to LAN type.

How to for PPTP Server/Client

Example: PPTP Remote Access connection

A remote worker establishes a PPTP VPN connection with the head office using Microsoft's VPN Adapter. The TW-EAV510 AC router is installed in the head office, connected to a couple of PCs and Servers.



Configuring PPTP server in the office

1. Set the PPTP Server

Item		Description
Authentication Type	MS-CHAPv2 MPPE	Authentication type
Peer Address	Starting from 192.168.100.2	IP pool for PPTP clients
Local Address(virtual address)	192.168.100.254	Virtual gateway address from PPTP clients
Username	test	authenticate user name
Passwrod	test	authenticate user password
Conneciton Type	Remote Access	Remote access

PPTP VPN

☐ Disable

☒ Enable

PPTP Server

Auth. Type

MS-CHAPV2

Encryption Mode

MPPE

Peer Address

start from: 192.168.100.2

Local Address

192.168.100.254

Apply

Server Account

Name

test

Tunnel

☐ Disable

☒ Enable

Username

test

Password

test

Connection Type

☒ Remote Access

☐ LAN to LAN

Peer Network IP

Peer Netmask

Add

Edit

PPTP Server Table

Edit	Name	Enable	Username	Connection Type	Peer Network IP	Peer Netmask	Select
<div><input checked="" type="radio"/></div>	test	<div><input checked="" type="checkbox"/></div>	test	Remote Access			<div><input type="checkbox"/></div>

Delete Selected

Save

Client Side: Windows series

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

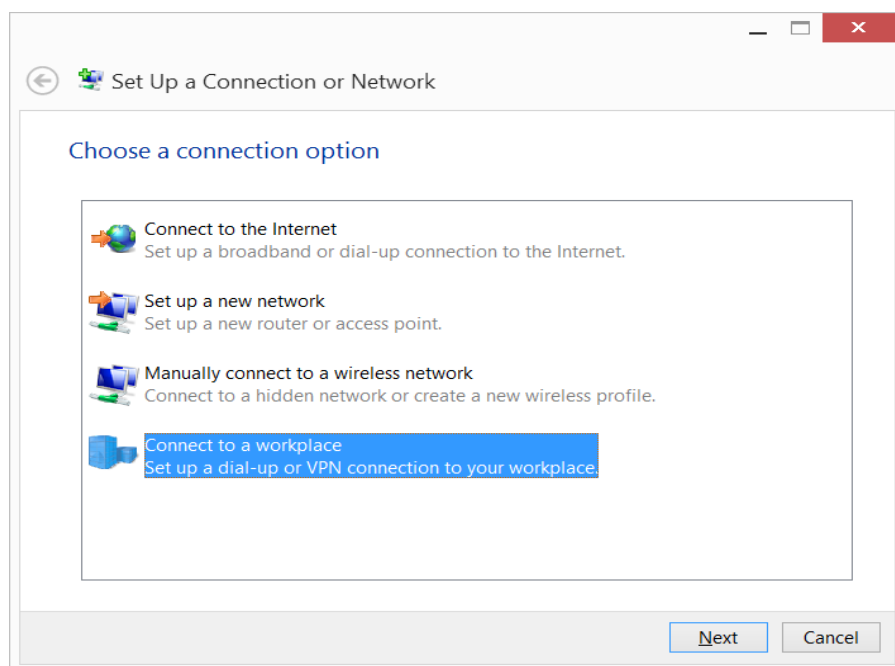
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.



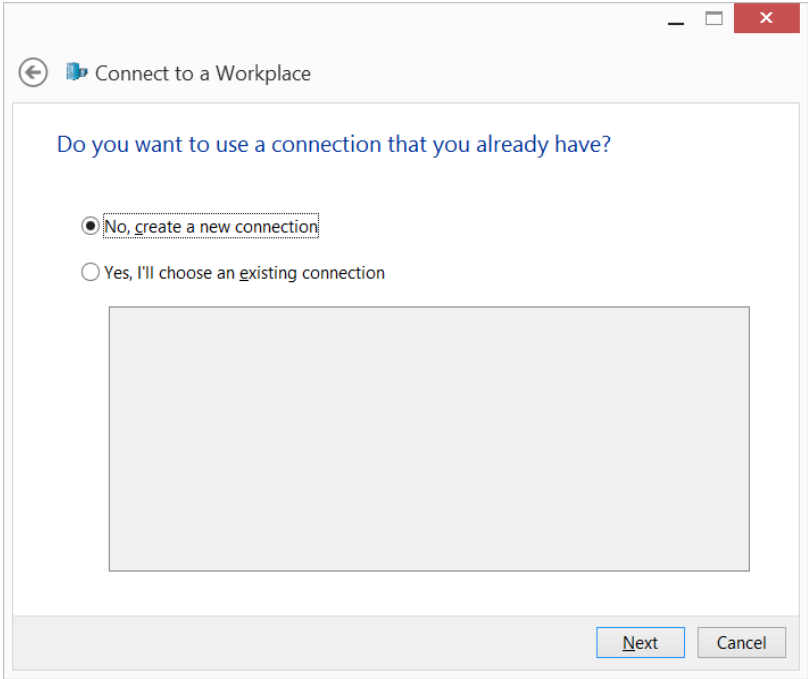
Troubleshoot problems

Diagnose and repair network problems, or get troubleshooting information.

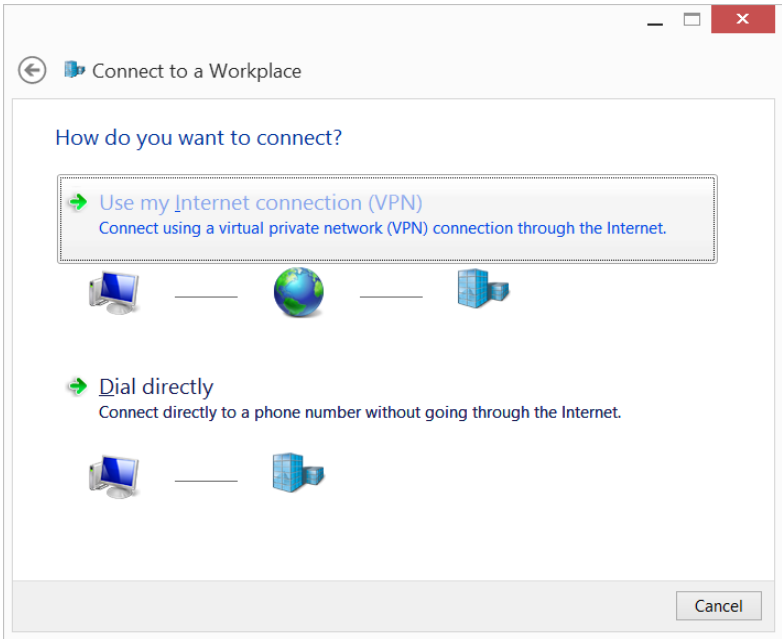
3. Select **Connect to a workplace**.



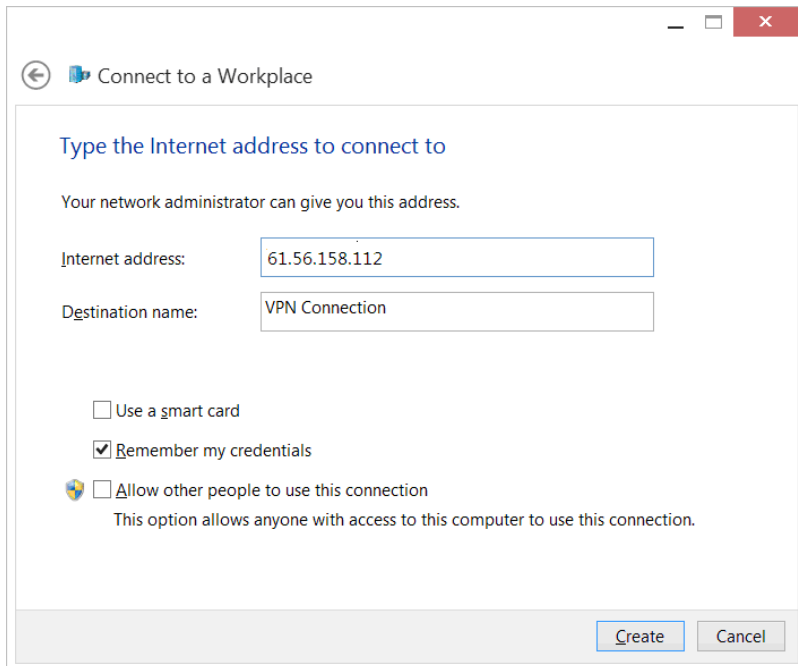
4. Select **No, create a new connection** and click **Next** button for next step.



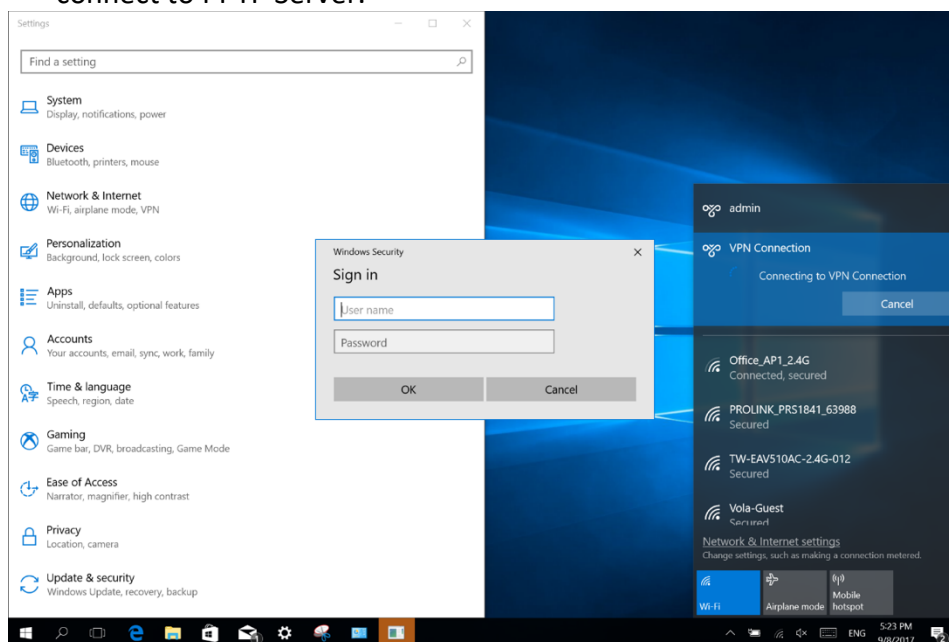
5. Select **Use my Internet connection (VPN)**.



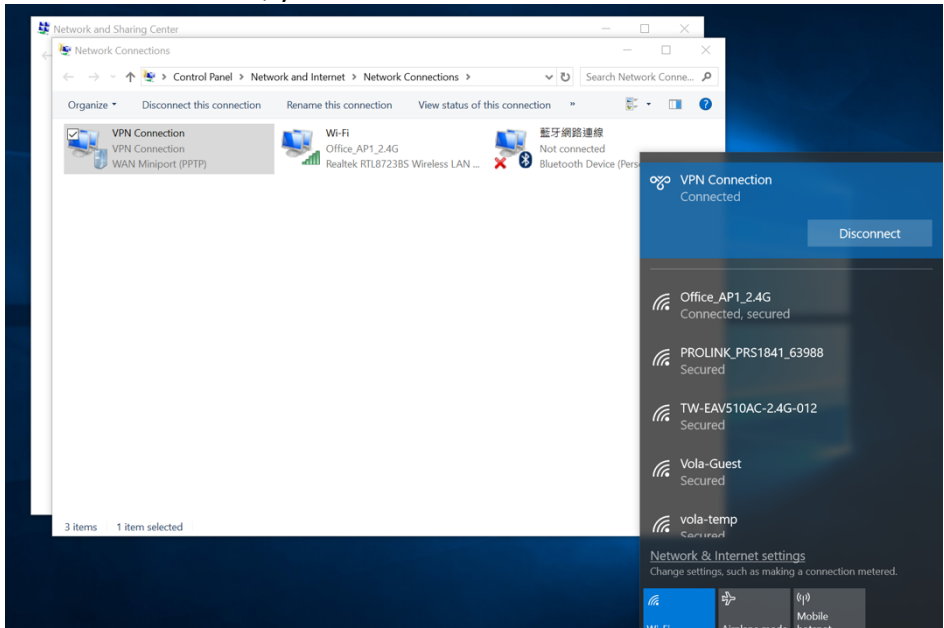
6. Enter the PPTP Server address/domain to field named **Internet address**. Please make sure your domain name address is work correctly if you are use domain name instead of IP address. Click **Create** button finish the PPTP client settings on Windows.



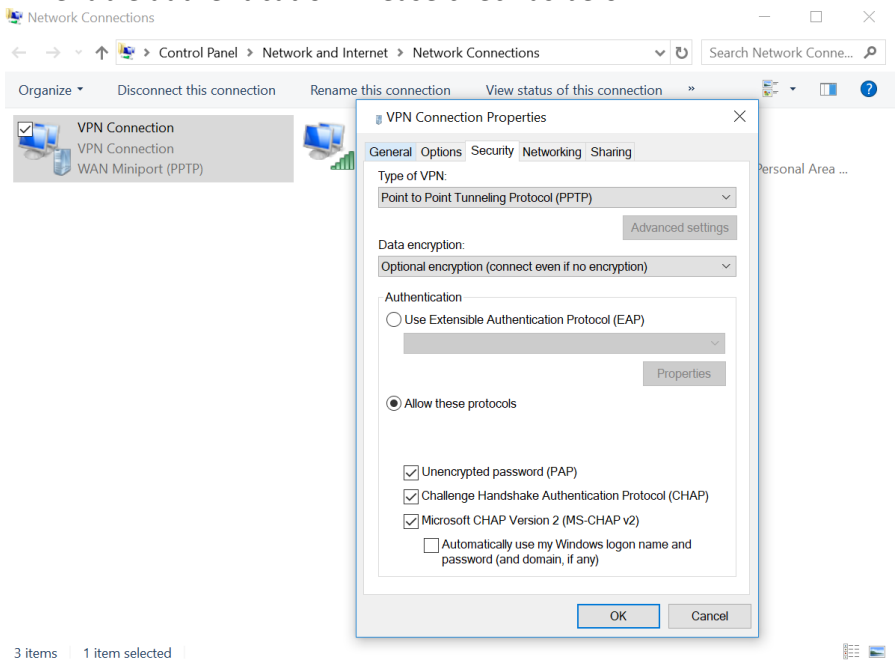
7. Enter the **username** and **password** that set on TW-EAV510 AC's PPTP Server and click **OK** button to connect to PPTP Server.



8. After connected, you can access remote network now.



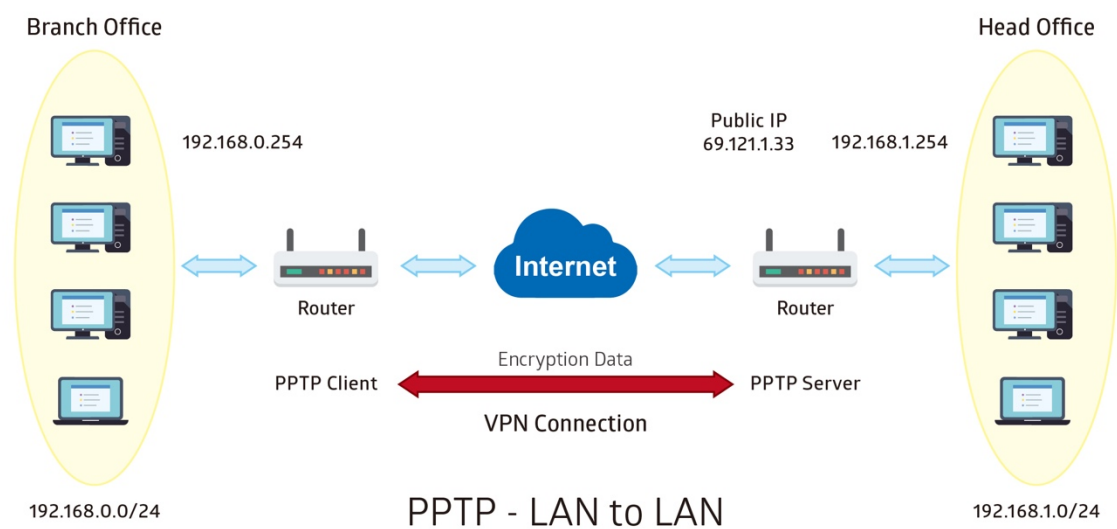
9. If you have problem connect with PPTP VPN via PC, please check **Control Panel -> Network and Internet -> Network and Sharing Center**, click **Change adapter settings** on left side, would show VPN Connection then right click to select **Properties -> Security**. Choose **Type of VPN** to **Point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



Example: PPTP LAN-to-LAN connection

The branch office establishes a PPTP VPN tunnel with head office to connect two private networks over the Internet. The routers are installed in the head office and branch offices accordingly.

Note: Both office LAN networks must be in different subnets with the LAN-LAN application.



Configuring PPTP server in the office

Set the PPTP Server

Item		Description
Name	test	Give a name of PPTP connection
Authentication Type	MS-CHAPv2 MPPE	Authentication type
Peer Address	Starting from 192.168.100.2	IP pool for PPTP clients
Local Address(virtual address)	192.168.100.254	Virtual gateway address from PPTP clients
Username	test	authenticate user name
Passwrod	test	authenticate user password
Conneciton Type	LAN-to-LAN	Connection type
Peer Network IP	192.168.0.0	Remote access network
Peer Netmask	255.255.255.0	

PPTP VPN

☐ Disable ☒ Enable

PPTP Server

Auth. Type

MS-CHAPV2

Peer Address

start from: 192.168.100.2

Local Address

192.168.100.254

Apply

Encryption Mode

MPPE

Server Account

Name

test

Username

test

Connection Type

☐ Remote Access ☒ LAN to LAN

Peer Network IP

192.168.0.0

Add

Edit

Tunnel

☐ Disable ☒ Enable

Password

test

Peer Netmask

255.255.255.0

PPTP Server Table

Edit	Name	Enable	Username	Connection Type	Peer Network IP	Peer Netmask	Select
<input checked="" type="checkbox"/>	test	<input checked="" type="checkbox"/>	test	LAN to LAN	192.168.0.0	255.255.255.0	<input type="checkbox"/>

Delete Selected

Save

74

Configuring PPTP client in the branch office

Item		Description
Name	test	Give a name of PPTP connection
Authentication Type	MS-CHAPv2 MPPE	Authentication type
Server Address	69.121.1.33	Remote server IP
Username	test	authenticate user name
Passwrod	test	authenticate user password
Conneciton Type	LAN-to-LAN	Connection type
Peer Network IP	192.168.1.0	Remote access network
Peer Netmask	255.255.255.0	

PPTP Client

Name

test

Username

test

Auth. Type

MS-CHAPV2

Connection Type

Remote Access

LAN to LAN

Peer Network IP

192.168.1.0

Default Gateway

Server Address

69.121.1.33

Password

test

Encryption Mode

MPPE

Peer Netmask

255.255.255.0

Add

Edit

PPTP Client Table

Edit	Interface	Server	Connection Type	Peer Network IP	Peer Netmask	Action	Select
	ppp9_pptp0	69.121.1.33	LAN to LAN	192.168.1.0	255.255.255.0	Connect	<input type="checkbox"/>

L2TP

L2TP, Layer 2 Tunneling Protocol is a tunneling protocol used to support virtual private networks (VPNs). It does not provide any encryption or confidentiality by itself; it relies on an encryption protocol that it passes within the tunnel to provide.

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

Auth. Type

PAP

Encryption Mode

NONE

Tunnel Authentication

☐

Secret

Peer Address

start from

Local Address

Apply

Server Account

Name

Username

Connection Type

☒ Remote Access ☐ LAN to LAN

Peer Network IP

Tunnel Password

Peer Netmask

Add

Edit

L2TP Server Table

Edit	Name	Enable	Username	Connection Type	Peer Network IP	Peer Netmask	Select
Delete Selected		Save					

L2TP Client

Name

Username

Tunnel Authentication

☐

Auth. Type

PAP

PPP Connection Type

Persistent

MTU

Connection Type

☒ Remote Access ☐ LAN to LAN

Peer Network IP

Server Address

Password

Secret

Encryption Mode

NONE

Idle Time (min)

Default Gateway

☐

Peer Netmask

Add

Edit

L2TP Client Table

Edit	Name	Server	Connection Type	Peer Network IP	MTU	Default Gateway	Action	Select
Delete Selected								

L2TP VPN: Enable/Disable L2TP function.

L2TP Server

Auth. 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 virtual interface.

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 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

Please Refer to PPTP.

IPSec

Internet Protocol Security (IPSec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPsec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session.

IPSec is an end-to-end security scheme operating in the Internet Layer of the Internet Protocol Suite. It can be used in protecting data flows between a pair of security gateways (*network-to-network*), or between a security gateway and a host (*network-to-host*).

IPSec VPN Table									
Select	Connection Name	Active	Protocol	Local Port	Remote Port	Local Network	Remote Network	Remote Security Gateway	Edit
<div><div>Add New Connection</div><div>Delete Selected</div><div>Enable</div><div>Disable</div></div>									

Click **Add New Connection** to create IPsec connections.

IPsec VPN Configuration

IPsec Settings

Connection Name	<input type="text"/>	Active	<input checked="" type="radio"/> Yes <input type="radio"/> No
Application	NONE <input type="button" value="v"/>	This is only for quick set, not save	
WAN Interface	Any <input type="button" value="v"/>		
Remote Gateway IP	<input type="text"/>	*	
Protocol	Any <input type="button" value="v"/>		
Local Port	<input type="text"/>	Remote Port	<input type="text"/>
	*		*
Local Network	Subnet <input type="button" value="v"/>		
Local IP Address	<input type="text"/>	Subnet Mask	<input type="text"/>
	*		*
Remote Network	Subnet <input type="button" value="v"/>		
Remote IP address	<input type="text"/>	Subnet Mask	<input type="text"/>
	*		*
IKE Mode	Main <input type="button" value="v"/>	Pre-Shared Key	<input type="text"/>
Local ID Type	Default(Local WAN IP) <input type="button" value="v"/>	ID Content	<input type="text"/>
			**
Remote ID Type	Default(Local WAN IP) <input type="button" value="v"/>	ID Content	<input type="text"/>
			**
Connection Mode	<input checked="" type="radio"/> Tunnel <input type="radio"/> Transport		

Phase 1

Encryption Algorithm	DES <input type="button" value="v"/>	Authentication Algorithm	MD5 <input type="button" value="v"/>
Diffie-Hellman Group	MODP1024(DH2) <input type="button" value="v"/>	SA Lifetime	480 min(s)

Phase 2

IPsec Proposal	<input checked="" type="radio"/> ESP <input type="radio"/> AH		
Encryption Algorithm	DES <input type="button" value="v"/>	Authentication Algorithm	MD5 <input type="button" value="v"/>
Perfect Forward Secrecy	None <input type="button" value="v"/>	SA Lifetime	60 min(s)
Keep Alive	NONE <input type="button" value="v"/>	Detection Interval	30 seconds
DPD Timeout	150 seconds (180 at least)		

Note * : ((0/0.0.0.0 means any))

Note ** : FQDN with @ as first character means don't resolve domain name.

IPsec Connection Setting

Connection Name: A given name for the connection (e.g. **connection to office**).

Active: Select **Yes** to activate the tunnel.

WAN Interface: Select the existing WAN interface for the IPsec connection, when you select 3G/4G-LTE interface, the IPsec tunnel would via this interface to connect to the remote peer.

Remote Gateway IP: The WAN IP address of the remote VPN gateway that is to be connected, establishing a VPN tunnel.

Protocol: Set the protocol and the local/remote port.

Local Network: Set the IP address or subnet of the local network.

- ▶ **Single IP Address:** The IP address of the local host, for establishing an IPsec connection between a security gateway and a host (*network-to-host*).

- ▶ **Subnet:** The subnet of the local network, for establishing an IPSec tunnel between a pair of security gateways (*network-to-network*)

Remote Network: Set the IP address or subnet of the remote network.

- ▶ **Single IP:** The IP address of the local host, for establishing an IPSec connection between a security gateway and a host (*network-to-host*). If the remote peer is a host, select Single Address.
- ▶ **Subnet:** The subnet of the local network, for establishing an IPSec tunnel between a pair of security gateways (*network-to-network*), If the remote peer is a network, select Subnet.

IKE Mode: IKE, Internet Key Exchange, is the mechanism to negotiate and exchange parameters and keys between IPSec peers to establish security associations(SA). Select Main or Aggressive mode.

Pre-Shared Key: This is for the Internet Key Exchange (IKE) protocol, a string from 4 to 128 characters. Both sides should use the same key. IKE is used to establish a shared security policy and authenticated keys for services (such as IPSec) that require a key. Before any IPSec traffic can be passed, each router must be able to verify the identity of its peer. This can be done by manually entering the pre-shared key into both sides (router or hosts).

Local ID Type and Remote ID Type: When the mode of IKE is aggressive, Local and Remote peers can be identified by other IDs.

IDContent: Enter IDContent the name you want to identify when the Local and Remote Type are Domain Name; Enter IDContent IP address you want to identify when the Local and Remote Type are IP addresses

Phase 1

Encryption Algorithm: Select the encryption algorithm from the drop-down menu. There are several options: DES and AES (128, 192 and 256). 3DES and AES are more powerful but increase latency.

- ▶ **DES:** Stands for Data Encryption Standard, it uses 56 bits as an encryption method.
- ▶ **3DES:** Stands for Triple Data Encryption Standard, it uses 168 (56*3) bits as an encryption method.
- ▶ **AES:** Stands for Advanced Encryption Standards, you can use 128, 192 or 256 bits as encryption method.

Authentication Algorithm: Authentication establishes the integrity of the datagram and ensures it is not tampered with in transmission. There are 3 options: Message Digest 5 (MD5) and Secure Hash Algorithm (SHA1, SHA256). SHA1 is more resistant to brute-force attacks than MD5. However, it is slower.

- ▶ **MD5:** A one-way hashing algorithm that produces a 128-bit hash.
- ▶ **SHA1:** A one-way hashing algorithm that produces a 160-bit hash.

Diffie-Hellman Group: It is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communication channel (i.e. over the Internet). MODP stands for Modular Exponentiation Groups.

SA Lifetime: Specify the number of minutes that a Security Association (SA) will stay active before new encryption and authentication key will be exchanged. It is used to issue an initial connection request for a new VPN tunnel. The range can be from 5 to 15,000 minutes, and the default is 480 minutes.

Phase 2

IPSec Proposal: Select the IPSec security method. There are two methods of verifying the authentication information, AH(Authentication Header) and ESP(Encapsulating Security Payload). Use ESP for greater

security so that data will be encrypted and the data origin be authenticated but using AH data origin will only be authenticated but not encrypted.

Encryption Algorithm: Select the encryption algorithm from the drop-down menu. There are several options: DES and AES (128, 192 and 256). 3DES and AES are more powerful but increase latency.

- ▶ **DES:** Stands for Data Encryption Standard, it uses 56 bits as an encryption method.
- ▶ **3DES:** Stands for Triple Data Encryption Standard, it uses 168 (56*3) bits as an encryption method.
- ▶ **AES:** Stands for Advanced Encryption Standards, you can use 128, 192 or 256 bits as encryption method.

Authentication Algorithm: Authentication establishes the integrity of the datagram and ensures it is not tampered with in transmission. There are 3 options: Message Digest 5 (MD5) and Secure Hash Algorithm (SHA1, SHA256). SHA1 is more resistant to brute-force attacks than MD5. However, it is slower.

- ▶ **MD5:** A one-way hashing algorithm that produces a 128-bit hash.
- ▶ **SHA1:** A one-way hashing algorithm that produces a 160-bit hash.

Perfect Forward Secrecy: It is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communication channel (i.e. over the Internet). MODP stands for Modular Exponentiation Groups.

SA Lifetime: Specify the number of minutes that a Security Association (SA) will stay active before new encryption and authentication key will be exchanged. To negotiate and establish secure authentication. The range can be from 5 to 15,000 minutes, and the default is 60 minutes. A short SA time increases security by forcing the two parties to update the keys. However, every time the VPN tunnel re-negotiates, access through the tunnel will be temporarily disconnected.

Keep Alive:

- ▶ **None:** The default setting is None. To this mode, it will not detect the remote IPSec peer has been lost or not. It only follows the policy of Disconnection time after no traffic, which the remote IPSec will be disconnected after the time you set in this function.
- ▶ **DPD:** Dead peer detection (DPD) is a keeping alive mechanism that enables the router to be detected lively when the connection between the router and a remote IPSec peer has lost. Please be noted, it must be enabled on the both sites.

Detection Interval: The period cycle for dead peer detection.

Idle Timeout: Auto-disconnect the IPSec connection after DPD Timeout.

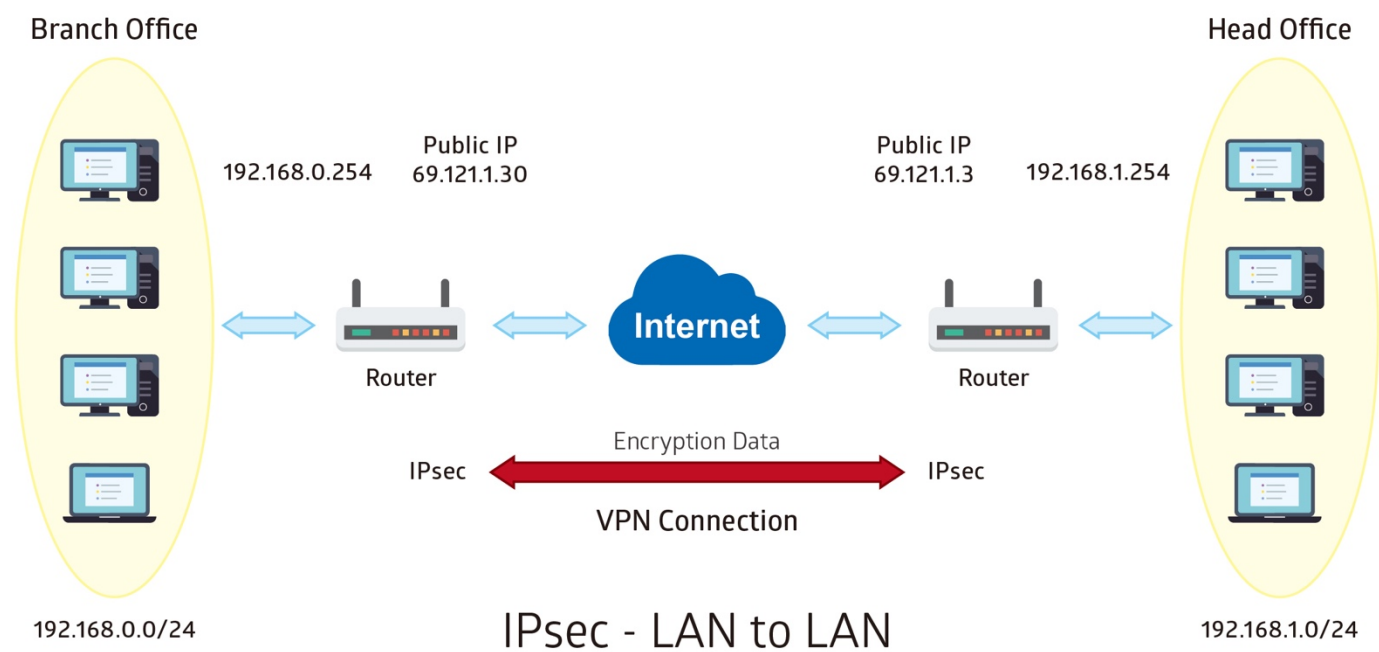
Click **SAVE** to submit the settings.

How to for IPsec

1. LAN-to-LAN connection

Two TW-EAV510 AC routers want to setup a secure IPsec VPN tunnel. Both are with enabled IPsec function.

Note: The IPsec Settings shall be consistent between the two routers.



Head Office Side:

Item		Description
Connection Name	H-to-B	Name for IPSec tunnel
Remote Secure Gateway	69.121.1.30	IP address of the Branch office gateway
Access Netork		
Local Access Range	Subnet	Head Office network
Local Netwrok IP Address	192.168.1.0	
Local Netwrok Netmask	255.255.255.0	
Remote Access Range	Subnet	Branch office network
Remote Netwrok IP Address	192.168.0.0	
Remote Netwrok Netmask	255.255.255.0	
IPSec Proposal		
IKE Mode	Main	Security Plan
Pre-Shared Key	1234567890	
Phase 1 Encryption	DES	
Phase 1 Authentication	MD5	
Phase 1 Diffie-Hellman Group	MODP 1024(group2)	
Phase 2 Proposal	ESP	
Phase 2 Authentication	MD5	
Phase 2 Encryption	DES	
Prefer Forward Security	MODP 1024(group2)	

Connection Name	<input type="text" value="H-to-B"/>	Active	<input checked="" type="radio"/> Yes <input type="radio"/> No
Application	<input type="text" value="NONE"/> <small>This is only for quick set, not save</small>		
WAN Interface	<input type="text" value="ppp0"/>		
Remote Gateway IP	<input type="text" value="69.121.1.30"/> *		
Protocol	<input type="text" value="Any"/>		
Local Port	<input type="text" value="0"/> *	Remote Port	<input type="text" value="0"/> *
Local Network	<input type="text" value="Subnet"/>		
Local IP Address	<input type="text" value="192.168.1.0"/> *	Subnet Mask	<input type="text" value="255.255.255.0"/> *
Remote Network	<input type="text" value="Subnet"/>		
Remote IP address	<input type="text" value="192.168.0.0"/> *	Subnet Mask	<input type="text" value="255.255.255.0"/> *
IKE Mode	<input type="text" value="Main"/>	Pre-Shared Key	<input type="text" value="1234567890"/>
Local ID Type	<input type="text" value="Default(Local WAN IP)"/>	ID Content	<input type="text" value="**"/>
Remote ID Type	<input type="text" value="Default(Local WAN IP)"/>	ID Content	<input type="text" value="**"/>
Connection Mode	<input checked="" type="radio"/> Tunnel <input type="radio"/> Transport		

Phase 1

Encryption Algorithm	<input type="text" value="DES"/>	Authentication Algorithm	<input type="text" value="MD5"/>
Diffie-Hellman Group	<input type="text" value="MODP1024(DH2)"/>	SA Lifetime	<input type="text" value="480"/> min(s)

Phase 2

IPSec Proposal	<input checked="" type="radio"/> ESP <input type="radio"/> AH		
Encryption Algorithm	<input type="text" value="DES"/>	Authentication Algorithm	<input type="text" value="MD5"/>
Perfect Forward Secrecy	<input type="text" value="None"/>	SA Lifetime	<input type="text" value="60"/> min(s)
Keep Alive	<input type="text" value="DPD"/>	Detection Interval	<input type="text" value="30"/> seconds
DPD Timeout	<input type="text" value="180"/> seconds (180 at least)		

Branch Office Side:

Item		Description
Connection Name	B-to-H	Name for IPSec tunnel
Remote Secure Gateway	69.121.1.3	IP address of the Branch office gateway
Access Netork		
Local Access Range	Subnet	Branch Office network
Local Netwrok IP Address	192.168.0.0	
Local Netwrok Netmask	255.255.255.0	
Remote Access Range	Subnet	Head office network
Remote Netwrok IP Address	192.168.1.0	
Remote Netwrok Netmask	255.255.255.0	
IPSec Proposal		
IKE Mode	Main	Security Plan
Pre-Shared Key	1234567890	
Phase 1 Encryption	DES	
Phase 1 Authentication	MD5	
Phase 1 Diffie-Hellman Group	MODP 1024(group2)	
Phase 2 Proposal	ESP	
Phase 2 Authentication	MD5	
Phase 2 Encryption	DES	
Prefer Forward Security	MODP 1024(group2)	

Connection Name	B-to-H	Active	<input checked="" type="radio"/> Yes <input type="radio"/> No
Application	NONE	This is only for quick set, not save	
WAN Interface	ppp0		
Remote Gateway IP	69.121.1.3	*	
Protocol	Any		
Local Port	0	Remote Port	0
Local Network	Subnet		
Local IP Address	192.168.0.0	Subnet Mask	255.255.255.0
Remote Network	Subnet		
Remote IP address	192.168.1.0	Subnet Mask	255.255.255.0
IKE Mode	Main	Pre-Shared Key	1234567890
Local ID Type	Default(Local WAN IP)	ID Content	**
Remote ID Type	Default(Local WAN IP)	ID Content	**
Connection Mode	<input checked="" type="radio"/> Tunnel <input type="radio"/> Transport		

Phase 1

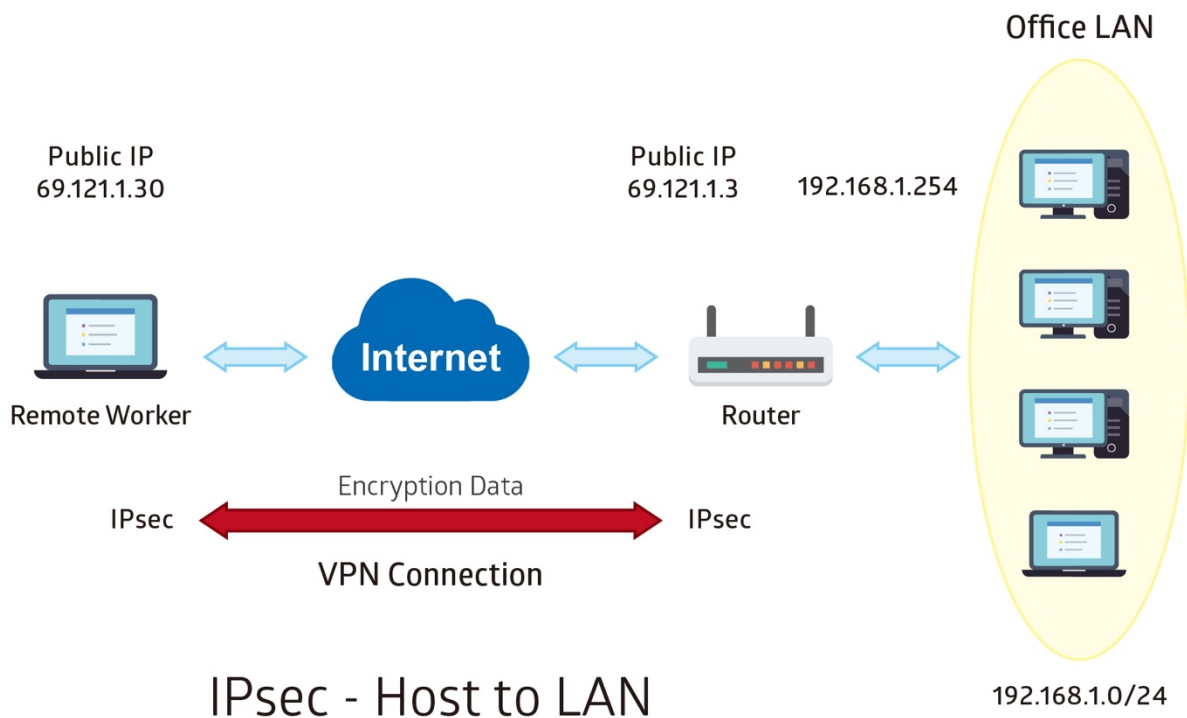
Encryption Algorithm	DES	Authentication Algorithm	MD5
Diffie-Hellman Group	MODP1024(DH2)	SA Lifetime	480 min(s)

Phase 2

IPSec Proposal	<input checked="" type="radio"/> ESP <input type="radio"/> AH		
Encryption Algorithm	DES	Authentication Algorithm	MD5
Perfect Forward Secrecy	None	SA Lifetime	60 min(s)
Keep Alive	DPD	Detection Interval	30 seconds
DPD Timeout	180 seconds (180 at least)		

2. Host to LAN

Router servers as VPN server, and host should install the IPsec client to connect to head office through IPsec VPN.



Head Office Side:

Item		Description
Connection Name	H-to-H	Name for IPSec tunnel
Remote Secure Gateway	69.121.1.30	IP address of the Branch office gateway
Access Netork		
Local Access Range	Subnet	Head Office network
Local Netwrok IP Address	192.168.1.0	
Local Netwrok Netmask	255.255.255.0	
Remote Access Range	Signal IP	Host
Remote Netwrok IP Address	69.121.1.30	
Remote Netwrok Netmask	255.255.255.255	
IPSec Proposal		
IKE Mode	Main	Security Plan
Pre-Shared Key	1234567890	
Phase 1 Encryption	DES	
Phase 1 Authentication	MD5	
Phase 1 Diffie-Hellman Group	MODP 1024(group2)	
Phase 2 Proposal	ESP	
Phase 2 Authentication	MD5	
Phase 2 Encryption	DES	
Prefer Forward Security	MODP 1024(group2)	

Connection Name	<input type="text" value="H-to-H"/>	Active	<input checked="" type="radio"/> Yes <input type="radio"/> No
Application	<input type="text" value="NONE"/> <small>This is only for quick set, not save</small>		
WAN Interface	<input type="text" value="ppp0"/>		
Remote Gateway IP	<input type="text" value="69.121.1.30"/> *		
Protocol	<input type="text" value="Any"/>		
Local Port	<input type="text" value="0"/> *	Remote Port	<input type="text" value="0"/> *
Local Network	<input type="text" value="Subnet"/>		
Local IP Address	<input type="text" value="192.168.1.0"/> *	Subnet Mask	<input type="text" value="255.255.255.255"/> *
Remote Network	<input type="text" value="Single IP address"/>		
Remote IP address	<input type="text" value="69.121.1.30"/> *	Subnet Mask	<input type="text" value="255.255.255.255"/> *
IKE Mode	<input type="text" value="Main"/>	Pre-Shared Key	<input type="text" value="1234567890"/>
Local ID Type	<input type="text" value="Default(Local WAN IP)"/>	ID Content	<input type="text" value="**"/>
Remote ID Type	<input type="text" value="Default(Local WAN IP)"/>	ID Content	<input type="text" value="**"/>
Connection Mode	<input checked="" type="radio"/> Tunnel <input type="radio"/> Transport		

Phase 1

Encryption Algorithm	<input type="text" value="DES"/>	Authentication Algorithm	<input type="text" value="MD5"/>
Diffie-Hellman Group	<input type="text" value="MODP1024(DH2)"/>	SA Lifetime	<input type="text" value="480"/> min(s)

Phase 2

IPSec Proposal	<input checked="" type="radio"/> ESP <input type="radio"/> AH		
Encryption Algorithm	<input type="text" value="DES"/>	Authentication Algorithm	<input type="text" value="MD5"/>
Perfect Forward Secrecy	<input type="text" value="None"/>	SA Lifetime	<input type="text" value="60"/> min(s)
Keep Alive	<input type="text" value="DPD"/>	Detection Interval	<input type="text" value="30"/> seconds
DPD Timeout	<input type="text" value="180"/> seconds (180 at least)		

GRE Settings

In terms of how to use GRE here, it needs to be associated with Bridge Grouping.

GRE Configuration

This page is used to configure the parameters for GRE.

GRE

☐ Enabled ☒ Disabled

Apply Changes

Name

Admin Status

☐

CheckSum

☐

Sequencing

☐

Key

☐

DSCP

GRE Endpoint

GRE Backup Endpoint

802.1Q VLAN ID

(0-4092),empty means no VLAN tag

Upstream Bandwidth

kbps,empty mean no limitation

Downstream Bandwidth

kbps,empty mean no limitation

Add

Modify

Remove

GRE Table

Select	State	Name	EndPoint	Back EndPoint	DSCP	VLAN ID	UP Rate	Down Rate
--------	-------	------	----------	---------------	------	---------	---------	-----------

GRE: Choose to enable or disable the GRE feature. Press **Apply Changes** to submit your changes.

Name: A given name for identification for GRE tunnel.

Admin Status: Choose to enable or disable this tunnel.

Sequencing: Enable to serialize all incoming and outgoing packets.

CheckSum: Enable to generate/require checksums for tunneled packets

Key: Enable to sets the key to use in both directions.

DSCP: Differentiated Services Code Point (DSCP), it is the first 6 bits in the ToS byte. DSCP Marking allows users to classify the traffic of the application to be executed according to the DSCP value.

GRE Endpoint: Set the remote gateway address.

GRE Backup Endpoint: a backup address for remote gateway.

802.11Q VLAN ID: Set the VLAN ID for this GRE tunnel.

Upstream/Downstream Bandwidth: Specify the upstream/downstream bandwidth in kbps.

How to for GRE:

1. Set a route WAN

Ethernet WAN

This page is used to configure the parameters for EthernetWAN

WAN Interface	<input type="text" value="nas0_0"/>		
Enable VLAN	<input type="checkbox"/>		
VLAN ID	<input type="text"/>	802.1p_Mark	<input type="text"/>
Channel Mode	<input type="text" value="IPoE"/>		
Enable Bridge	<input type="checkbox"/>		
Bridge Mode	<input type="text" value="Bridged Ethernet (Transparent Bridging)"/>		
Enable NAPT	<input checked="" type="checkbox"/>	Enable QoS	<input checked="" type="checkbox"/>
Admin Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
MTU	<input type="text" value="1500"/>		
IGMP Proxy	<input checked="" type="checkbox"/> Enable		

WAN IP Settings

Type	<input checked="" type="radio"/> Fixed IP <input type="radio"/> DHCP		
Local IP Address	<input type="text" value="172.16.1.10"/>		
Remote IP Address	<input type="text" value="172.16.1.102"/>		
Subnet Mask	<input type="text" value="255.255.255.0"/>	IP Unnumbered	<input type="checkbox"/>
Request DNS	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
Primary DNS Server	<input type="text"/>		
Secondary DNS Server	<input type="text"/>		

2. Create a GRE Tunnel

GRE Configuration

This page is used to configure the parameters for GRE.

GRE

☒ Enabled ☐ Disabled

Apply Changes

Name

GRETunnel1

Admin Status

☒

CheckSum

☒

Sequencing

☒

Key

☒ 200

DSCP

AF12(001100) ▾

GRE Endpoint

172.16.1.102

GRE Backup Endpoint

172.16.1.103

802.1Q VLAN ID

100 (0-4092),empty means no VLAN tag

Upstream Bandwidth

1024 kbps,empty mean no limitation

Downstream Bandwidth

2048 kbps,empty mean no limitation

Add

Modify

Remove

GRE Table

Select	State	Name	EndPoint	Back EndPoint	DSCP	VLAN ID	UP Rate	Down Rate
<input checked="" type="radio"/>	Enable	GRETunnel1	172.16.1.102	172.16.1.103	0x30	100	1024	2048

3. Map LAN interface(s) on the GRE tunnel with Bridge 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 arrows of the ports.
 - 3. Click 'Apply Changes' button to save the changes.

Note that the selected interfaces will be removed from their existing groups and added to the new group.

Grouped Interfaces

->

<-

Available Interfaces

LAN3
LAN4
TW-EAV510AC_5G_6688
TW-EAV510AC_2.4G_6688
ptm0_0
vc3
gret0
gret0.100

Select	Interfaces
Default	LAN1, LAN2, LAN3, LAN4, TW-EAV510AC_5G_6688, TW-EAV510AC_2.4G_6688, ptm0_0, vc3, gret0, gret0.100
<input checked="" type="radio"/>	

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 arrows of the ports.
 - 3. Click 'Apply Changes' button to save the changes.

Note that the selected interfaces will be removed from their existing groups and added to the new group.

Grouped Interfaces

gret0.100
LAN4
TW-EAV510AC_5G_6688

->

<-

Available Interfaces

LAN1
LAN2
LAN3
TW-EAV510AC_2.4G_6688
ptm0_0
vc3
gret0

Select	Interfaces
Default	LAN1, LAN2, LAN3, LAN4, TW-EAV510AC_5G_6688, TW-EAV510AC_2.4G_6688, ptm0_0, vc3, gret0, gret0.100
<input checked="" type="radio"/>	

Select	Interfaces
Default	LAN1, LAN2, LAN3, TW-EAV510AC_2.4G_6688, ptm0_0, vc3, gret0
<input type="radio"/>	LAN4, TW-EAV510AC_5G_6688, gret0.100

4. Disable DHCP assignment for the LAN interfaces.

Port-Based Filter

This page is used to configure the Port-Based Filtering.

Filter DHCP Discover packet

☐ LAN1

☐ LAN2

☐ LAN3

☒ LAN4

☒ TW-EAV510AC_5G_6688

☐ TW-EAV510AC_2.4G_6688

Apply Changes

Close

Advance

Bridging

This page is used to configure the bridge parameters. You can change the settings or view some information on the bridge and its attached ports.

Bridging Configuration

This page is used to configure the bridge parameters. Here you can change the settings or view some information on the bridge and its attached ports.

Ageing Time	<input type="text" value="7200"/>	(seconds)
802.1d Spanning Tree	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled	
<div><input type="button" value="Apply Changes"/> <input type="button" value="Show MACs"/></div>		

Ageing Time: If the host is idle for 7200 seconds (default value), its entry is deleted from the bridge table.

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.

SNMP

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. The router serves as a SNMP agent that allows a manager station to manage and monitor the router through the network.

SNMP Configuration

This page is used to configure the SNMP. Here you may change the settings for system description, trap ip address, community name, etc..

SNMP	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
System Description	<input type="text" value="System Description"/>
System Contact	<input type="text" value="System Contact"/>
SystemName	<input type="text" value="TW-EAV510 AC (b)"/>
System Location	<input type="text" value="System Location"/>
System Object ID	<input type="text" value="1.3.6.1.4.1.16972"/>
Trap IP Address	<input type="text" value="192.168.1.254"/>
Community name (read-only)	<input type="text" value="public"/>
Community name (write-only)	<input type="text" value="public"/>

Enable SNMP: Enable to activate SNMP function.

System Description: User-defined system description.

System Name: User-defined system name.

System location: User-set location.

Trap IP Address: Enter the IP of the server receiving the trap message (when some exception occurs) sent by this SNMP agent.

Community name(read-only): Type the Get Community, which is the password for the incoming Get-and-GetNext requests from the management station.

Community name(write-only): Type the Set Community, which is the password for incoming Set requests from the management station.

Bridge Grouping

Bridge/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.

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 'Apply Changes' button to save the changes.

Note that the selected interfaces will be removed from their existing groups and added to the new group.

Grouped Interfaces

Available Interfaces

→

←

Select	Interfaces
Default	LAN1, LAN2, LAN3, LAN4, TW-EAV510AC_5G_6688, TW-EAV510AC_2.4G_6688
<input type="radio"/>	
<input type="radio"/>	
<input type="radio"/>	
<input type="radio"/>	

Apply Changes

Grouped Interfaces: Group interfaces into one group. Interfaces listed in this box are one group.

Available Interfaces: Select the interfaces you want to be put single group from **Available Interfaces**. Interfaces listed here can be LAN interfaces, wireless interfaces, GRE Tunnels, Bridged WAN interfaces.

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.

1. Create bridged WAN interfaces or GRE tunnels.

DSL WAN Configuration

This page is used to configure the parameters for WAN Mode

VPI/VCI

8 / 35

Channel Mode

1483 Bridged

Enable NAPT

Admin Status

Enable

Disable

IGMP Proxy

Enable

Encapsulation

LLC

VC-Mux

Enable QoS

Add

Modify

Current ATM VC Table

Select	Interface	Mode	VPI	VCI	Encapsulation	NAPT	IGMP	IP Address	Remote IP	Subnet Mask	UserName	Default Route	Status	Actions
<input type="radio"/>	ppp0_vc0	PPPoE	0	33	LLC	on	on				t0083328	on	Enabled	
<input checked="" type="radio"/>	ADSL3	br1483	8	35	LLC								Enabled	

2. Classify interfaces into one group. Click Apply Changes to save.

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 of the ports.
 3. Click 'Apply Changes' button to save the changes.

Note that the selected interfaces will be removed from their existing groups and added to the new group.

Grouped Interfaces

TW-EAV510AC_5G_6688

LAN4

vc3

Available Interfaces

LAN1

LAN2

LAN3

TW-EAV510AC_2.4G_6688

ptm0_0

->

<--

Select	Interfaces
Default	LAN1, LAN2, LAN3, LAN4, TW-EAV510AC_5G_6688, TW-EAV510AC_2.4G_6688, ptm0_0, vc3
<input checked="" type="radio"/>	
<input type="radio"/>	
<input type="radio"/>	
<input type="radio"/>	

Apply Changes

Select	Interfaces
Default	LAN1, LAN2, LAN3, TW-EAV510AC_2.4G_6688, ptm0_0
<input type="radio"/>	LAN4, TW-EAV510AC_5G_6688, vc3

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:

1024 Kb

Apply Changes

IP QoS: Enable/Disable the IP QoS function.

Policy: Specify the policy for queue.

Policy: The Queue Scheduling Algorithm, here supporting WRR (Weighted Round Robin) and PRIO (Priority).

- WRR: Weighted Round Robin, used to alternate each WRR queue to ensure that every queue can enjoy its due service time (resource) in accordance with its weight.
- PRIO: Strict Priority; it always sends the packets in queue with higher priority, and under this circumstance, the packets in lowest-priority queue may be delayed for quite a long time.

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	Order	DSCP Mark	802.1p	Queue	WanIf	Rule Detail	Delete	Edit	State

Add

Apply Changes

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

Add QoS Classification Rules

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

Rule Name

Rule Order

Precedence

DSCP

802.1p

IP QoS Rule by type

WAN

rule_

Queue 1

☐ Port

☐ Ethery Type

☐ IP/Protocol

☐ MAC Address

Any

Apply Changes

- Rule Name:** Enter the rule name.
- Rule Order:** Rule Index.
- Precedence:** Specify which Queue the packets matching the QoS conditions are to be classified into.

Please notice that only when the packet fulfill every detailed conditions set below, then this packet will be remarked as the priority queue of each rule.

DSCP: Select the DSCP mark to be a QoS classification condition.

802.1p: Specify the 802.1p value.

WAN: Specify which WAN interface will be applied.

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

- ♦ **Port**

Physical Port

Physical Port: LAN ports to be monitored.

- ♦ **Ethery Type**

Ethernet Type 0x

Ethernet Type: EtherType is a two-octet field in an Ethernet frame. It is used to indicate which protocol is encapsulated in the payload of the frame. Specify the Ethernet Type of packets to be monitored.

♦ IP/Protocol

Protocol	<input type="text"/>	▼
DSCP	<input type="text"/>	▼
Source IP	<input type="text"/>	
Source Mask	<input type="text"/>	
Destination IP	<input type="text"/>	
Destination Mask	<input type="text"/>	
Source Port	<input type="text"/>	<input type="text"/>
Destination Port	<input type="text"/>	<input type="text"/>

Source IP/Port: The source IP/Port of packets to be monitored.

Destination IP/Port: The destination IP/Port of packets to be monitored.

♦ MAC Address

Source MAC	<input type="text"/>
Destination MAC	<input type="text"/>

Source/Destination MAC: The Source/Destination MAC of packets to be monitored.

Printer Server

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

The Print Server feature allows you to share a printer on your network by connecting a USB cable from your printer to the USB port on the TW-EAV510 AC. This allows you to print from any location on your network.

Note: Only USB printers are supported

Setup of the printer is a 2 step process

1. Connect the printer to the router 's USB port
2. Install the printer drivers on the PC you want to print from

Printer URL(s)

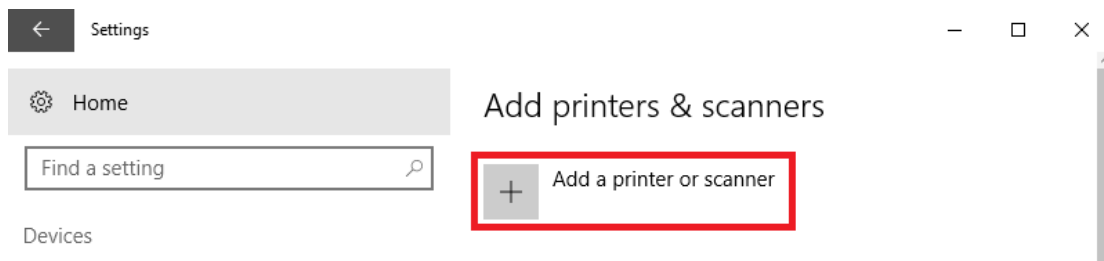
This page is used to show printer URL(s).

<http://192.168.0.254:631/printers/lp0>

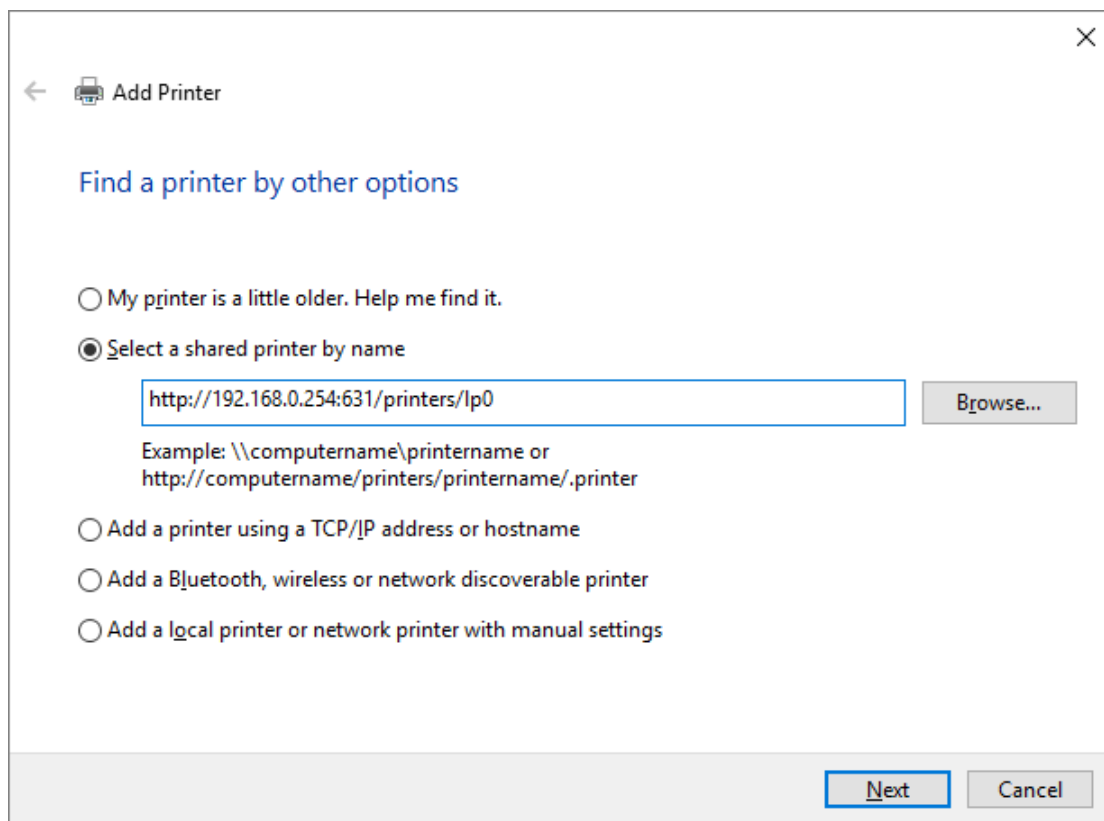
Refresh

Printer installation on Windows 10

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



2. Select "Select a shared printer by name", copy the printer URL that shows on device WEB GUI (Advanced -> Printer) and past it here.



3. Click *Next* button and follow the instruction by Windows 10.

IPv6

IPv6

IPv6 Configuration

This page be 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

600

MinRtrAdvInterval

198

AdvManagedFlag

☒ off

☐ on

AdvOtherConfigFlag

☐ off

☒ on

Apply Changes

- MaxRtrAdvInterval:** The maximum time allowed between sending unsolicited multicast router advertisements from the interface, in seconds. It 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 and DHCPv6 Relay.

DHCPv6 Mode

☐ NONE

☐ DHCP Relay

☐ DHCP Server(Manual)

☒ DHCP Server(Auto)

Auto Config by Prefix Delegation for DHCPv6 Server.

Show Client

Apply Changes

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

MLD Proxy

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

MLD Proxy Configuration

This page be used to configure MLD Proxy.

MLD Proxy

☒ Disable

☐ Enable

WAN Interface

▼

Apply Changes

MLD Proxy: Enable or disable the MLD Proxy function.
WAN Interface: Set the upstream interface for MLD Proxy. The WAN interface must has 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

Any ▾

Add Route

Update

Delete Selected

Delete All

Show Routes

Static IPv6 Route Table

Select	State	Destination	Next Hop	Metric	Interface
--------	-------	-------------	----------	--------	-----------

Enable: Checked to enable static route function.

Destination: Enter the destination IPv6 address.

Next Hop: Specify the gateway IPv6 address for routing to next network.

Metric: Metric is a policy for router to commit router, to determine the optimal route. Enter one number greater than or equal to 0.

Interface: Select an interface this route associated.

IP/Port Filtering

IPv6 IP/Port Filtering

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

Outgoing Default Action

Incoming Default Action

☐ Deny

☒ Allow

☒ Deny

☐ Allow

Apply Changes

Direction

Protocol

Rule Action

Source Interface ID

Destination Interface ID

Source Port

Destination Port

Outgoing

TCP

☒ Deny

☐ Allow

-

-

Add

Edit

Current Filter Table

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

Delete Selected

Delete All

- 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

Host: Enter your host IP/domain name to ping to test the connectivity between the host and your router.

PING 8.8.8.8 (8.8.8.8): 56 data bytes

64 bytes from 8.8.8.8: icmp_seq=0

64 bytes from 8.8.8.8: icmp_seq=1

64 bytes from 8.8.8.8: icmp_seq=2

--- ping statistics ---

3 packets transmitted, 3 packets received.

Back

ATM Loopback

The router is equipped to perform connectivity verification by the use of the ATM OAM loopback capability for both VP and VC connections. This page is used to perform the VCC loopback function to check the connectivity of the VCC.

ATM Loopback Diagnostics - Connectivity Verification

Connectivity verification is supported by the use of the ATM OAM loopback capability for both VP and VC connections. This page is used to perform the VCC loopback function to check the connectivity of the VCC.

Select PVC

☒ 0/33 ☐ 0/100 ☐ 0/35

Flow Type

☐ F4 Segment ☐ F4 End-to-End
☒ F5 Segment ☐ F5 End-to-End

Loopback Location ID

FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

Go !

DSL Tone

The frequency band of ADSL is split up into 256 separate tones, each spaced 4.3125 kHz apart.

With each tone carrying separate data, the technique operates as if 256 separate modems were running in parallel. The tone range is from 0 to 31 for upstream and from 32 to 255 for downstream.

DSL Tone Diagnostics

DSL Tone Diagnostics. Only ADSL2/ADSL2+/VDSL2 support this function.

Start

	Downstream	Upstream
Hlin Scale		
Loop Attenuation(dB)		
Signal Attenuation(dB)		
SNR Margin(dB)		
Attainable Rate(Kbps)		
Output Power(dBm)		

Tone Number	H.Real	H.Image	SNR	QLN	Hlog
0					
1					
2					
3					
4					
5					
6					
7					

ADSL Connection

The router is capable of testing your WAN connection. Run Diagnostic Test to proceed.

ADSL Connection Diagnostics

The Device is capable of testing your connection. The individual tests are listed below. If a test displays a fail status, click 'Go' button again to make sure the fail status is consistent.

Select the ADSL Connection

ppp0

Go

Select the ADSL Connection

ppp0

Go

ADSL Connection Check	
Test ADSL Synchronization	PASS
Test ATM OAM F5 Segment Loopback	FAIL
Test ATM OAM F5 End-to-end Loopback	FAIL
Test ATM OAM F4 Segment Loopback	FAIL
Test ATM OAM F4 End-to-end Loopback	FAIL

Internet Connection Check	
Test PPP Server Connection	PASS
Test Authentication with ISP	PASS
Test the assigned IP Address	PASS
Ping Default Gateway	PASS
Ping Primary Domain Name Server	PASS

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	<input type="button" value="Backup..."/>	
Restore Settings from File	<input type="button" value="Choose File"/> No file chosen	<input type="button" value="Restore"/>
Reset Settings to Default	<input type="button" value="Reset"/>	

Click **Backup**, a window appears, click save, and then browse the location where you want to save the backup file

Click **Choose File**. Browse and Select the backup file. Then in the above page, click **Restore**.

Reset Settings to Default: Press Reset button to restart the device with factory default settings.

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. Empty user name and password will disable the protection.

User Name

hallinta ▼

Old Password

New Password

Confirmed Password

Apply Changes

Reset

- Old Password:** The old password for the user.
- New Password:** Enter new password.
- Confirm Password:** Enter new password again for confirmation.

Firmware Upgrade

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

Clicking “**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 upgrade the firmware to the newer version. Please note that do not power off the device during the upload because this make the system unbootable.

☐ Upload firmware with default configuration

Choose File

No file chosen

Upgrade

Upgrade (Auto)

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

ACL

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

ACL Configuration

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

ACL Capability

☐ Disable ☒ Enable

Apply Changes

Enable

☒

Interface

LAN

IP Address

Subnet Mask

Service Name

LAN

Any

☐

TELNET

☐

FTP

☐

TFTP

☐

HTTP

☐

HTTPS

☐

SNMP

☐

PING

☒

Add

Edit

ACL Table

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

ACL Capability: The router’s all service will be opened and can be accessed by any direction if set to disable. Default is enable. Press **Apply Changes** to save the changes.

Enable: To activate the ACL Rule.

Interface: LAN or WAN, to determine the rule is workable for LAN or WAN.

IP Address/Subnet Mask: The IP or IP range to be monitored. 0.0.0.0 means any IP.

Services Name: List all services to be monitored. Choose a service or services that you want to give access to all the secure IP clients.

Click **Add** to add the ACL rule to the ACL Table. **Note:** If ACL is enabled, only the IP address in the ACL Table can access CPE.

Example on how to configure ACL, Here we are going to establish two frequently used rules to illustrate.

1. Set up a rule to allow only clients from LAN to have access to all embedded applications (HTTP, HTTPS, Ping, etc). Under this situation, clients from WAN cannot access the router even from Ping. Click Add to add rule.

Enable

Interface

IP Address

Subnet Mask

☒

LAN

0.0.0.0

0.0.0.0

Service Name

LAN

Any

☐

TELNET

☐

FTP

☐

TFTP

☐

HTTP

☒

HTTPS

☒

SNMP

☐

PING

☒

Add

Edit

ACL Table

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

2. An ACL rule to open Ping to WAN side. Click Add to add rule.

Enable

Interface

IP Address

Subnet Mask

☒

WAN

0.0.0.0

0.0.0.0

Service Name

WAN

WAN Port

TELNET

☐

23

FTP

☐

21

TFTP

☐

HTTP

☐

80

HTTPS

☐

443

SNMP

☐

PING

☒

Add

Edit

ACL Table

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

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.

Time Zone Select

Europe/Helsinki (UTC+02:00) ▼

Enable Daylight Saving Time

☒

Enable SNTP Client Update

☒

WAN Interface

Any ▼

SNTP Server

☒ 130.149.17.8 - Europe ▼

☐ 220.130.158.52 (Manual Setting)

Apply Changes

Refresh

SMS Alert Settings

SMS, Short Message Service, is to inform clients the information clients subscribe. TW-EAV510 AC offers SMS alert sending clients alert messages when a default route change is detected.

SMS Alert Settings

This page is used to configure the parameters for your SMS alert.

Default Route Change Alert

Recipient's Number

Apply Changes

Reset

Recipient's Number (Default Route Change Alert): Enter the Recipient's number that will receive the alert message when a default route change is detected.

Statistics

Interface

This page shows the statistics (Receive/Transmit packets, Receive/Transmit errors, Receive/Transmit drops) 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
LAN1	0	0	0	0	0	0
LAN2	3665	0	0	1782	0	0
LAN3	0	0	0	0	0	0
LAN4	0	0	0	0	0	0
TW-EAV510AC_5G_6688	0	0	0	0	0	0
TW-EAV510AC_2.4G_6688	65222	0	0	0	0	0
ppp0_vc0	5704	0	0	609	0	0
ADSL1	0	0	0	4415	0	0
ADSL2	0	0	0	4415	0	0
PTM0	0	0	0	0	0	0
EWAN	0	0	0	0	0	0
4G	0	0	0	0	0	0

Refresh

Reset Statistics

DSL

This page shows more DSL Synchronization details.

DSL Statistics

Mode	G.dmt Annex A	
TPS-TC	ATM	
Latency	Interleave	
Status	SHOWTIME.	
Power Level	L0	
Uptime	01:39:00	
G.Vector	Off	

	Downstream	Upstream
Trellis	On	On
SNR Margin (dB)	20.0	7.0
Attenuation (dB)	0.0	0.0
Output Power (dBm)	0.0	12.5
Attainable Rate (Kbps)	11948	0
G.INP	Off	Off
Rate (Kbps)	8000	928
R (number of check bytes in RS code word)	2	8
N (RS codeword size)	253	248
L (number of bits in DMT frame)	2024	248
S (RS code word size in DMT frame)	1.00	8.00
D (interleaver depth)	16	2
Delay (msec)	4.00	4.00
INP (DMT frame)	0.063	0.258
FEC errors	0	0
OH Frame	344520	344520
OH Frame errors	0	0
Total ES	0	0
Total SES	0	0
Total UAS	31	0
Total LOSS	—	—
Last Link Rate	0	0
Full Init	0	
Failed Full Init	0	
Synchronized time(Second)	5853	
Synchronized number	1	

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 **Commit and Reboot** button to reboot the device immediately with the current settings.

Commit and Reboot

This page is used to commit changes to system memory and reboot your system.

Commit and Reboot

Logout

This page will force the user logout immediately by clicking Logout button. Simultaneous access to the router is not allowed. One user at a time

Logout

This page is used to logout from the Device.

Logout