

TW-EAV510

3G/4G/LTE
ADSL2+ / VDSL / EWAN
Wireless 802.11 b/g/n
VPN

User Manual

Copyright © TeleWell Oy

Table of Contents

| | |
|--|------------|
| Chapter 1: Introduction | 3 |
| Introduction to your Router | 3 |
| Features | 4 |
| Physical Interface | 7 |
| Package Contents | 7 |
| Device Description | 8 |
| Chapter 2: Basic Installation | 10 |
| Network Configuration | 11 |
| Factory Default Settings | 14 |
| Chapter 3: Configuration | 16 |
| Device Info | 16 |
| Summary | 17 |
| WAN | 18 |
| 3G/LTE Info | 19 |
| Statistics | 19 |
| Route | 22 |
| ARP | 23 |
| DHCP | 23 |
| VPN | 24 |
| Log | 25 |
| Advanced Setup | 26 |
| Layer 2 interface | 26 |
| WAN-Wide Area Network | 29 |
| 3G/LTE | 32 |
| LAN | 34 |
| NAT | 37 |
| Security | 41 |
| Parental Control | 43 |
| Quality of Service | 45 |
| Routing | 48 |
| DNS | 54 |
| Static ARP | 57 |
| DSL | 58 |
| SNR | 59 |
| UPnP | 59 |
| DNS Proxy | 60 |
| Print Server | 60 |
| DLNA | 65 |
| Storage Service | 65 |
| Interface Grouping | 69 |
| IP Tunnel | 70 |
| VPN | 73 |
| IPSec | 106 |
| Power Management | 109 |
| Multicast | 110 |
| Wireless | 111 |
| Wireless 2.4GHz and 5GHz | 111 |
| Diagnostics | 121 |
| Tools | 121 |
| Diagnostics | 122 |

| | |
|-------------------------|--|
| Management | 122 |
| Settings..... | 122 |
| System Log | 124 |
| SNMP Agent | 125 |
| TR- 069 Client | Virhe. Kirjanmerkkiä ei ole määritetty. |
| Alert..... | 126 |
| SMS Control..... | 127 |
| Internet Time..... | 128 |
| Access Control..... | 129 |
| Miscellaneous..... | 131 |
| Auto Reboot | 131 |
| Update Software | 132 |
| Reboot..... | 132 |

Chapter 1: Introduction

Introduction to your Router

The device is a fibre-ready ADSL2+/VDSL modem, an all-in-one advanced device integrating Wireles, Ethernet, 3G/4G/LTE, and NAS (Network Attached Storage) in one unit.

As well as being IPv6-capable, the device ADSL2+ router supports super fast fibre connections via dual-WAN connectivity through a Gigabit Ethernet WAN port. Also, it also has a USB port, allowing the device to act as a print server as well as a NAS (Network Attached Storage) device with DLNA (Digital Living Network Alliance). Moreover, the USB port can host a 3G/4G/LTE modem connecting to the 3G/4G/LTE network for Internet access. With an array of advanced features, the TeleWell TW-EAV510 delivers a future-proof solution for ADSL2+ connections, super fast FTTC and ultra-speed FTTH (Fibre-To-The-Home) network deployment and services.

Maximum wireless performance

With an integrated 802.11n Wireless Access Point, the router delivers up to 6 times the speed of an 802.11b/g/n network device.

- TW-EAV510 supports a data rate of up to 300Mbps and is also compatible with 802.11b/g/n equipment.

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

3G/4G/LTE Mobility and Always-on Connectivity

With 3G/4G/LTE-based Internet connection (requires an additional 3G/4G/LTE USB modem plugged into the built-in USB port), user can access internet through 3G/4G/LTE, whether you are seated at your desk or taking a cross-country trip. The auto fail-over feature ensures optimum connectivity and minimum interruption by quickly and smoothly connecting to a 3G/4G/ LTE network in the event that you ADSL/Fibre/Cable line fails. The TeleWell TW-EAV510 will then automatically reconnect to the ADSL/Fibre/Cable connection when it is restored, reducing connection costs. These features are perfect for office situations when a constant and smooth WAN connection is critical.

IPv6 supported

Internet Protocol version 6 (IPv6) is a version of the Internet Protocol that is designed to succeed IPv4. IPv6 has a vastly larger address space than IPv4. This results from the use of a 128-bit address, whereas IPv4 uses only 32 bits. The new address space thus supports 2^{128} (about 3.4×10^{38}) addresses. This expansion provides flexibility in allocating addresses and routing traffic and eliminates the primary need for network address translation (NAT), which gained widespread deployment as an effort to alleviate IPv4 address exhaustion. The device fully supports IPv6 (Internet Protocol Version 6), launched as the current IPv4 range is filling up, and IPv6 is gradually becoming the indispensable addressing system for savvy cloud computing users. Dual stack means the router is capable of running IPv4 and IPv6 in parallel during the transition period. With TeleWell IPv6 enabled devices, three major transition mechanisms such as Dual-Stack, Dual-Stack Lite, and 6RD (IPv6 rapid deployment) are supported to be adapted easily into service provider's IPv4/IPv6 network

Virtual AP

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

Web Based GUI

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

Firmware Upgradeable

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

Features

ADSL Compliance

- Compliant with ADSL+ / VDSL 2 Standard
- Full-rate ANSI T1.413 Issue 2
- G.dmt (ITU G.992.1)
- G.hs (ITU G.994.1)
- Compliant with ADSL2 Standard
- G.dmt.bis (ITU G.992.3)
- ADSL2 Annex M (ITU G.992.3 Annex M)
- G.dmt.bis plus (ITU G.992.5)
- ADSL2+ Annex M (ITU G.992.5 Annex M)

VDSL 2

- G.993g2 (VDSL2) protocol
- PTM and ATM mode including dual latency
- Both Annex A and Annex B including dual latency
- Profiles supported: 8a/b/c/d, 12 a/b, 17a and 30a (BCM6306 required)
- US0
- Diagnostics mode/DELT
- Bitswaps, SRA and SOS/ROC
- FEXT equalized UPBO
- Dying gasp
- INM
- PhyR and G.INP (framing type 1)
- G.vector
- Virtual Noise

Network Protocols and Features

- IPv4 or IPv4 / IPv6 Dual Stack
- NAT, static (v4/v6) routing and RIP-1 / 2
- IPv6 Stateless / Stateful Address Auto-configuration
- IPv6 Router Advertisement
- IPv6 over PPP
- DHCPv6
- IP Tunnel IPv6 in IPv4 (6RD)
- IP Tunnel IPv4 in IPv6 (DS-Lite)
- Universal Plug and Play (UPnP) Compliant
- Dynamic Domain Name System (DDNS)
- Virtual Server, DMZ and one-to-one NAT
- SNTP, DNS relay, IGMP snooping and IGMP proxy for video service
- MLD snooping and MLD proxy for video service
- Management based-on IP protocol, port number and address

Firewall

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

Quality of Service Control

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

ATM, PTM and PPP Protocols

- ATM Adaptation Layer Type 5 (AAL5)
- Multiple Protocol over ALL5 (RFC 268, formerly RFC 1483)
- Bridged or routed Ethernet encapsulation
- VC 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
- Virtual LAN (VLAN)
- Quality of Service (QoS)

Wireless LAN

- Compliant with
 - o TW-EAV510 v2:
 - IEEE 802.11 b/g/n standards
 - 2.4 radio band for wireless
 - Up to 300 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
- WDS repeater function support

USB Application Server

- 3G/4G/LTE dongle support
- DLNA media server
- Printer Server
- USB port x 1

Virtual Private Network (VPN)

- IKE key management
- DES, 3DES and AES encryption for IPSec
- L2TP over IPSec
- Pap/ Chap/ MS-CHAPv2 authentication for PPTP
- IPSec pass-through
- GRE tunnel
- Open VPN

Management

- Web-based GUI for remote and local management (IPv4/IPv6)
- Firmware upgrades and configuration data upload and download via web-based GUI
- Embedded Telnet server for remote and local management
- Supports DHCP server / client / relay
- Supports SNMP v1,v2, MIB-I and MIB-II
- TR-069 supports remote management
- Available Syslog
- Mail alert for WAN IP changed
- Auto failover and fallback
- Push Service

Physical Interface

- WLAN: 3 x 5 dBi internal antenna
- DSL: ADSL / VDSL port
- USB 2.0 port for DLNA, printer server and 3G/4G/LTE dongle
- Ethernet: 4-port 10/100 Mbps auto-crossover (MDI / MDI-X) Switch
- WAN: 10/100/1000 Mbps
- Factory default reset button
- WPS push button
- Power jack
- Power switch

Package Contents

- TW-EAV510
- Quick Start Guide
- RJ-45 Cat. 5e STP Ethernet cable
- RJ-11 ADSL/ telephone cable
- Power adapter
- Splitter / Micro-filter (Optional)

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.

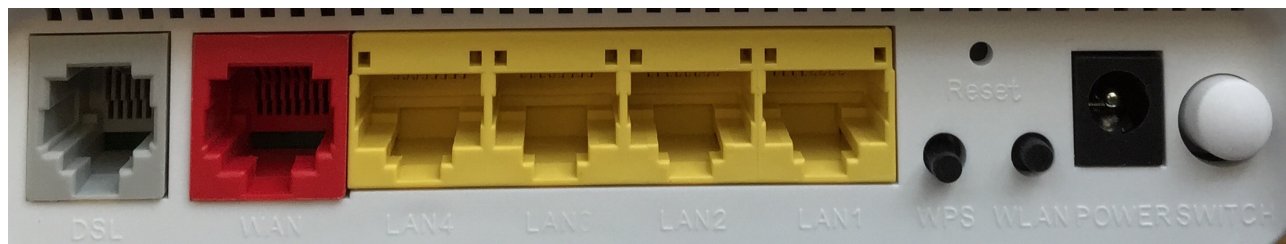
Only use the power adapter that comes with the package. Using a different voltage rating power adapter may damage the router.

Device Description

The Front LEDs

| LED | | Status | Meaning |
|-----|-------------------|----------------|--|
| 1 | Power | Red | Boot failure or in emergency mode |
| | | Green | System ready |
| 2 | Ethernet Port 1-4 | Green | Transmission speed hitting |
| | | Blinking | Data being transmitted/received |
| 3 | Wlan 2.4G | Green | Wireless connection established |
| | | Green blinking | Sending/receiving data |
| 4 | WPS 2.4G | Green blinking | WPS configuration being in progress |
| | | Off | WPS process completed or WPS is off |
| 5 | DSL / WAN | Green Blinking | DSL synchronizing or waiting for DSL synchronizing |
| | | Green | Successfully connected to an ADSL/VDSL DSLAM Sync |
| | | Off | DSL cable unplugged |
| 6 | Internet | Red | Obtaining IP failure |
| | | Green | Having obtained an IP address successfully |
| | | Off | Router in bridge mode or DSL connection not present. |
| 7 | USB | Green | USB activate on modem |
| | | Flashing green | Data is transmission |
| | | Off | Modem off or no device attached |

The Rear Ports



| Port | | Meaning |
|------|-------------------|--|
| 1 | Power Switch | Power ON / OFF switch. |
| 2 | Power | Connect the supplied power adapter to this jack. |
| 3 | RESET | After the device is powered on, press it 5 seconds or above: to restore to factory default settings (this is used when you cannot login to the router, e.g. forgot the password) |
| 4 | USB 1 | Connect the USB device (Printer, 3G/4G LTE USB modem) to this port. |
| 5 | WAN | Connect Ethernet cable for WAN connections |
| 6 | Ethernet (LAN1-4) | Connect a UTP Ethernet cable (Cat-5 or Cat-5e) to one of the four LAN ports when connecting to a PC or an office/home network. |
| 7 | DSL | Connect this port to the DSL network with the RJ-11 cable (telephone) provided. |

Cabling

One of the most common causes of problems is bad cabling or ADSL line(s). Make sure that all connected devices are turned on. On the front panel of your router is a bank of LEDs. Verify that the LAN Link and ADSL line LEDs are all lit. If they are not, verify if you are using the proper cables. If the error persists, you may have a hardware problem. In this case, you should contact technical support.

Make sure you have a line filter with all devices (e.g. telephones, fax machines, analogue modems) connected to the same telephone line and the wall socket (unless you are using a Central Splitter or Central Filter installed by a qualified and licensed electrician), and ensure that all line filters are correctly installed and the right way around. Missing line filters or line filters installed the wrong way around can cause problems with your ADSL connection, including causing frequent disconnections. If you have a back-to-base alarm system you should contact your security provider for a technician to make any necessary changes.

Chapter 2: 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.

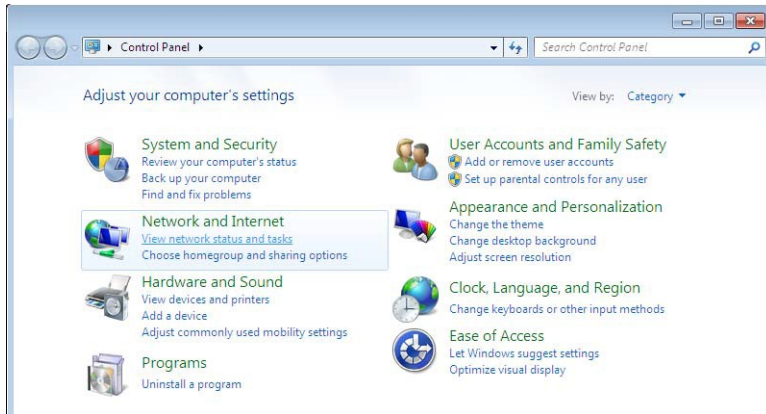
Please follow the following steps to configure your PC network environment.

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

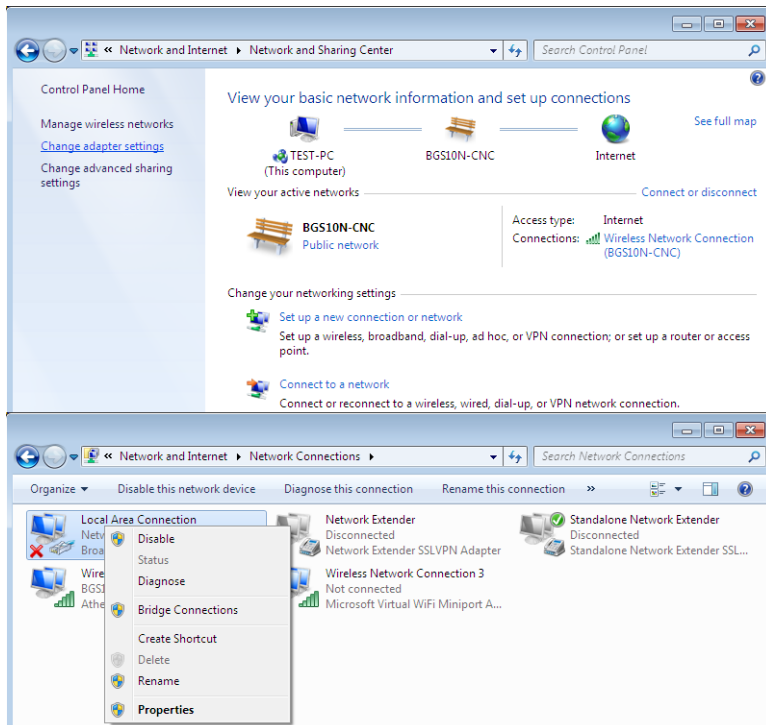
Go to Start. Click on Control Panel. Then click on Network and Internet.



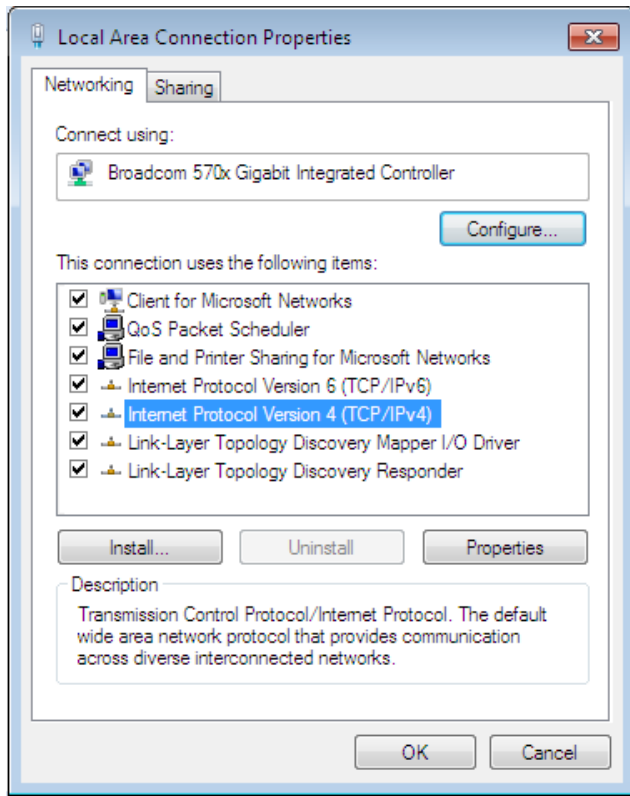
When the Network and Sharing Center window pops up, select and click on Change adapter settings on the left window panel.

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

IPv4:

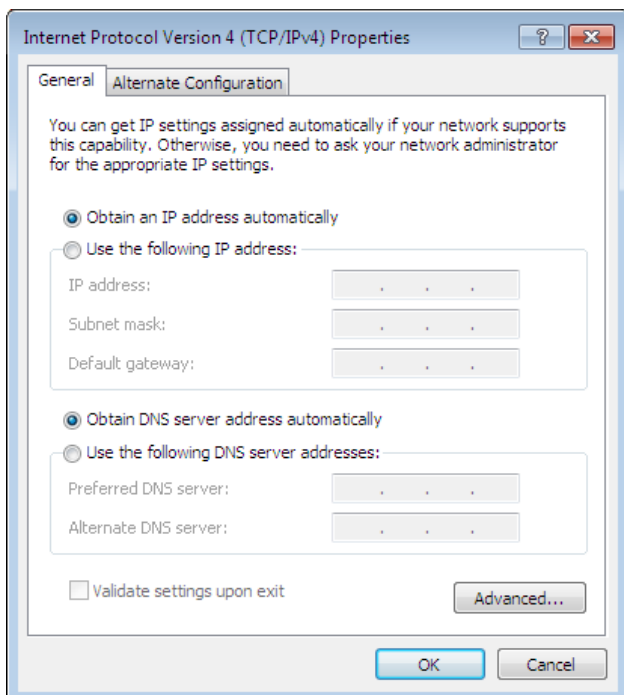


Select Internet Protocol Version 4 (TCP/IPv4) then click Properties



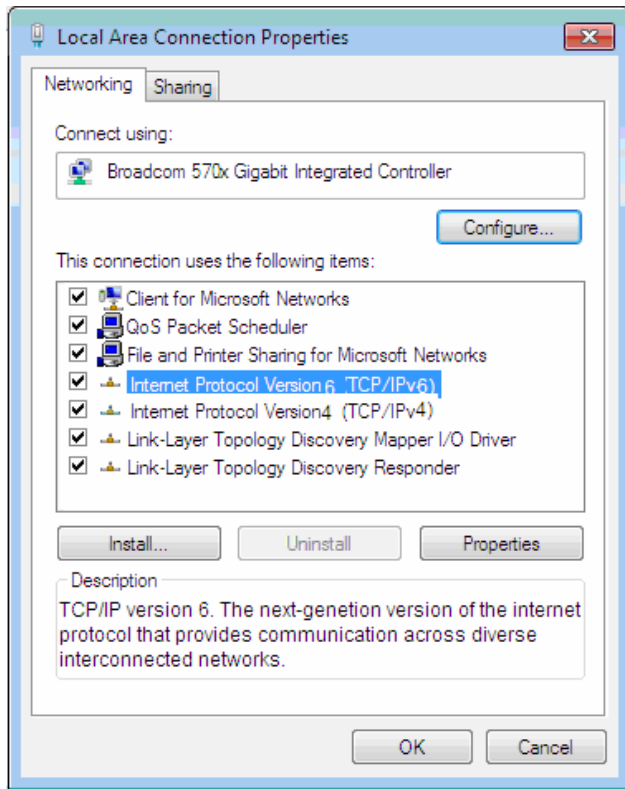
In the TCP/IPv4 properties window, select the Obtain an IP address automatically and Obtain DNS Server address automatically radio buttons. Then click OK to exit the setting.

Click OK again in the Local Area Connection Properties window to apply the new configuration.



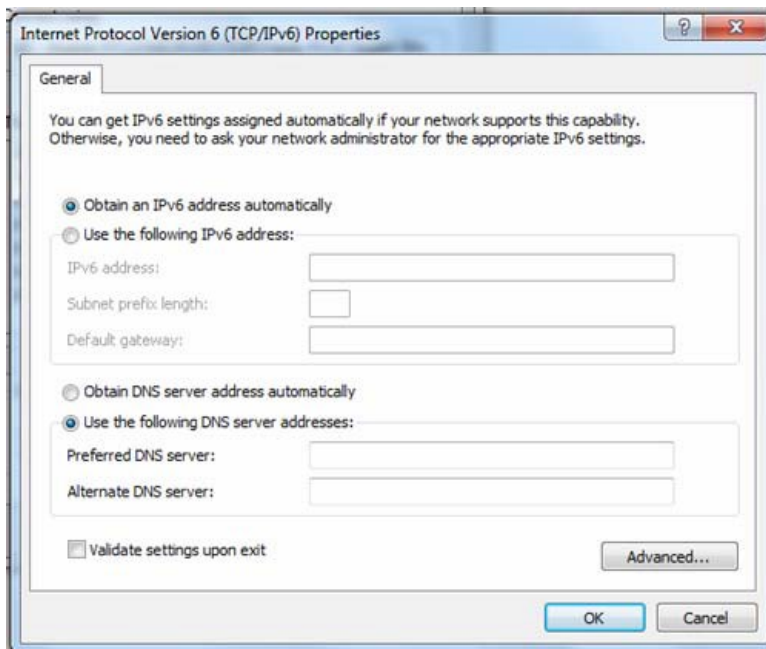
IPv6:

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)

Three user levels are provided by this router, namely Administrator, Remote and Local respectively. See Access Control .

Administrator

Username: admin Password: admin

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 5 seconds.

Device LAN IPv4 settings

- IPv4 Address: 192.168.0.254
- Subnet Mask: 255.255.255.0

Device LAN IPv6 settings

- IPv6 Address / prefix: Default is a link-local address and is different from each other as MAC address is different from one to one

DHCP server for IPv4

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

LAN and WAN Port Addresses

The parameters of LAN and WAN ports are pre-set in the factory. The default values are shown in the table.

IPv4

| LAN Port | | WAN Port |
|--------------------------------------|--|---|
| IPv4 address | 192.168.0.254 | The RFC1483 Bridged IP LLC function is enabled to automatically get the WAN IP address from the ISP |
| Subnet Mask | 255.255.255.0 | |
| DHCP server function | Enabled | |
| IP addresses for distribution to PCs | 100 IP addresses continuing from 192.168.0.100 through 192.168.0.199 | |

IPv6

| LAN Port | | WAN Port |
|----------------------|---|---|
| IPv6 address/prefix | Default is a link-local address and is different from each other as MAC address is different from one to one. | The RFC1483 Bridged IP LLC function is enabled to automatically get the WAN IP address from the ISP |
| DHCP server function | Enabled | |

Information from your ISP

Before configuring this device, you have to check with your ISP (Internet Service Provider) to find out what kind of service is provided.

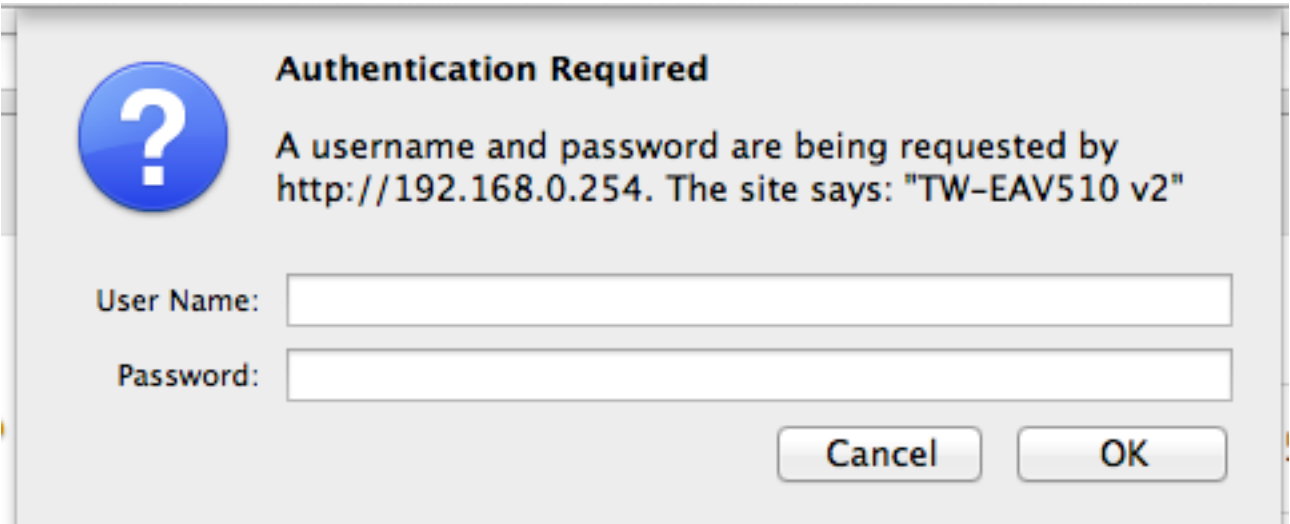
Gather the information as illustrated in the following table and keep it for reference.

| | |
|----------------|---|
| PPPoE(RFC2516) | VPI/VCI, VC / LLC-based multiplexing, Username, Password, Service Name, and Domain Name System (DNS) IP address (it can be automatically assigned by your ISP when you connect or be set manually). |
| DHCP Client | VPI/VCI, VC / LLC-based multiplexing, Domain Name System (DNS) IP address (it can be automatically assigned by your ISP when you connect or be set manually). |
| Pure Bridge | VPI/VCI, VC / LLC-based multiplexing to use Bridged Mode. |

Chapter 3: 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. The default root username and password are "admin" and "admin" respectively.



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

Once you have logged on to your TeleWell TW-EAV510 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:

Device Info

This Section gives users an easy access to the information about the working router and access to view the current status of the router.

Summary

The basic information about the device is provided here (the following is a configured screenshots to let users understand clearly).

Device Info

| | |
|-----------------------------|--------------------------------|
| Model Name: | TW-EAV510 |
| MAC Address: | 00:1e:ab:53:ef:b1 |
| Software Version: | 5.00.49 |
| DSL PHY and Driver Version: | A2pv6F039m.d25f |
| Wireless Driver Version: | 6.37.14.4803.cpe4.16L01A.0-kdb |
| Uptime: | 0D 0H 0M 47S |
| Date/Time: | Thu Jan 1 00:00:47 1970 |

This information reflects the current status of your WAN connection.

| | |
|--------------------------------|------------------------|
| Line Rate - Upstream (Kbps): | 0 |
| Line Rate - Downstream (Kbps): | 0 |
| 3G/LTE Operator Name: | |
| Frequency Band: | |
| 3G/LTE Signal Strength: | <div><div></div></div> |
| LAN IPv4 Address: | 192.168.0.254 |
| WAN IPv4 Address: | |
| Connection Time: | |
| Default Gateway: | |
| Primary DNS Server: | |
| Secondary DNS Server: | |
| LAN IPv6 ULA Address: | |
| WAN IPv6 Address: | |
| Default IPv6 Gateway: | |

Device Information

- Model Name:** Displays the model name.
- MAC Address:** Displays the MAC address.
- Software Version:** Firmware version.
- DSL PHY and Driver Version:** Display DSL PHY and Driver version.
- Wireless Driver Version:** Displays wireless driver version.
- Up-Time:** Displays the elapsed time since the device is on.
- Date/Time:** Displays the current exact date and time. Sync button is to synchronize the Date/Time with your PC time without regard to connecting to internet or not.

Line Rate – Upstream (Kbps): Displays Upstream line Rate in Kbps.

Line Rate – Downstream (Kbps): Displays Downstream line Rate in Kbps.

3G/LTE Operator Name: Displays the operator name

Frequency Band: Displays frequency Band

3G/LTE signal strength: Displays signal strength

LAN IPv4 Address: Displays the LAN IPv4 address.

LAN IPv6 Address: Displays the LAN IPv6 address. Default is a Link-Local address, but when connects to ISP, it will display the Global Address, like above figure.

Connection Time: Displays the elapsed time since ADSL connection is up.

Default gateway: Displays default gateway

Primary DNS Server: Displays IPV4 address of Primary DNS Server.

Secondary DNS Server: Displays IPV4 address of Secondary DNS Server.

LAN IPv6 ULA Address: Displays LAN IPV6 ULA address

WAN IPv6 Address: Displays WAN IPV6 address

Default IPv6 Gateway: Display the IPv6 Gateway and the obtained IPv6 address.

WAN

This table displays the information of the WAN connections, users can turn here for WAN connection information.

WAN Info

| Interface | Description | Type | VlanMuxId | IPv6 | Igmp Pxy | Igmp Src Enbl | MLD Pxy | MLD Src Enbl | NAT | Firewall | Status | IPv4 Address | IPv6 Address |
|-----------|----------------|--------|-----------|----------|----------|---------------|----------|--------------|---------|----------|--------------|---------------|--------------|
| atm0.1 | ipoe_0_0_33 | IPoE | Disabled | Disabled | Enabled | Enabled | Disabled | Disabled | Enabled | Enabled | Unconfigured | | |
| atm1.1 | ipoe_0_0_100 | IPoE | Disabled | Disabled | Enabled | Enabled | Disabled | Disabled | Enabled | Enabled | Unconfigured | | |
| atm2.2 | ipoe_0_0_35 | IPoE | Disabled | Disabled | Enabled | Enabled | Disabled | Disabled | Enabled | Enabled | Unconfigured | | |
| ptm0.1 | ipoe_0_1_1 | IPoE | Disabled | Disabled | Enabled | Enabled | Disabled | Disabled | Enabled | Enabled | Unconfigured | | |
| ptm0.3 | ipoe_0_1_1.252 | IPoE | 252 | Disabled | Enabled | Enabled | Disabled | Disabled | Enabled | Enabled | Unconfigured | | |
| eth4.1 | ipoe_eth4 | IPoE | Disabled | Disabled | Enabled | Enabled | Disabled | Disabled | Enabled | Enabled | Unconfigured | | |
| usbo3g0 | 3G_LTE0 | Direct | Disabled | Disabled | Disabled | Disabled | Disabled | Disabled | Enabled | Enabled | Connected | 10.188.20.198 | |
| pppo3g0 | 3G_LTE0 | PPP | Disabled | Disabled | Disabled | Disabled | Disabled | Disabled | Enabled | Enabled | Disabled | | |

Interface: The WAN connection interface.

Description: The description of this connection.

Type: The protocol used by this connection.

Status: To disconnect or connect the link.

IPv4 Address: The WAN IPv4 Address the device obtained.

IPv6 Address: The WAN IPv6 Address the device obtained.

3G/LTE Info

3G/LTE Info

| | |
|------------------|--|
| Status: | Up |
| Operator Name: | FI elisa elisa |
| Frequency Band: | LTE B3 Band & Frequency |
| Network Mode: | LTE |
| Signal Strength: | <div><div></div><div></div><div></div><div></div></div> -73dbm |
| Card Name: | TW-LTE/4G/3G + |
| Card Firmware: | BD_LTEMODEMV1.0.1B01 |

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

Operator Name: The operator name that the device is connected to.

Frequency Band: The frequency band that the device is connected to

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

Signal Strength: The signal strength bar indicates current 3G signal strength.

Card Name: The name of the 3G/LTE card.

Card Firmware: The current firmware for the 3G/LTE card.

Statistics

LAN

The table shows the statistics of LAN.

Statistics -- LAN

| Interface | Received | | | | | | | | Transmitted | | | | | | | |
|-----------------------|----------|------|------|-------|-----------|------|------|------|-------------|------|------|-------|-----------|------|------|------|
| | Total | | | | Multicast | | | | Total | | | | Multicast | | | |
| | Bytes | Pkts | Errs | Drops | Bytes | Pkts | Pkts | Pkts | Bytes | Pkts | Errs | Drops | Bytes | Pkts | Pkts | Pkts |
| LAN1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| LAN2 | 209548 | 1370 | 0 | 0 | 0 | 584 | 553 | 233 | 373263 | 666 | 0 | 4 | 0 | 21 | 636 | 9 |
| LAN3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| LAN4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| TW-EAV510-2.4GHz-EFB2 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| TW-EAV510-5GHz-EFB3 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Reset Statistics

Interface: List each LAN interface. P1-P4 indicates the four LAN interfaces.

Bytes: Display the Received and Transmitted traffic statistics in Bytes.

Packets: Display the Received and Transmitted traffic statistics in Packets.

Errors: Display the statistics of errors arising in Receiving or Transmitting data.

Drops: Display the statistics of drops arising in Receiving or Transmitting data.

Reset: Press this button to refresh the statistics.

WAN Service

The table shows the statistics of WAN.

Statistics -- WAN

| Interface | Description | Received | | | | | | | | Transmitted | | | | | | | |
|-----------|----------------|----------|------|------|-------|-----------|------|---------|-----------|-------------|------|------|-------|-----------|------|---------|-----------|
| | | Total | | | | Multicast | | Unicast | Broadcast | Total | | | | Multicast | | Unicast | Broadcast |
| | | Bytes | Pkts | Errs | Drops | Bytes | Pkts | Pkts | Pkts | Bytes | Pkts | Errs | Drops | Bytes | Pkts | Pkts | Pkts |
| atm0.1 | ipoe_0_0_33 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| atm1.1 | ipoe_0_0_100 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| atm2.2 | ipoe_0_0_35 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| ptm0.1 | ipoe_0_1_1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| ptm0.3 | ipoe_0_1_1.252 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| eth4.1 | ipoe_eth4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| usbo3g0 | 3G_LTE0 | 3222 | 29 | 0 | 0 | 0 | 0 | 0 | 0 | 7947 | 52 | 0 | 0 | 0 | 0 | 0 | 0 |
| pppo3g0 | 3G_LTE0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Reset Statistics

Interface: Display the connection interface.

Description: the description for the connection.

Bytes: Display the WAN Received and Transmitted traffic statistics in Bytes.

Packets: Display the WAN Received and Transmitted traffic statistics in Packets.

Errors: Display the statistics of errors arising in Receiving or Transmitting data.

Drops: Display the statistics of drops arising in Receiving or Transmitting data.

Reset: Press this button to refresh the statistics.

xTM

The Statistics-xTM screen displays all the xTM statistics

Interface Statistics

| Port Number | In Octets | Out Octets | In Packets | Out Packets | In OAM Cells | Out OAM Cells | In ASM Cells | Out ASM Cells | In Packet Errors | In Cell Errors |
|-------------|-----------|------------|------------|-------------|--------------|---------------|--------------|---------------|------------------|----------------|
|-------------|-----------|------------|------------|-------------|--------------|---------------|--------------|---------------|------------------|----------------|

Reset Statistics

Port Number: Shows number of the port for xTM.

In Octets: Number of received octets over the interface.

Out Octets: Number of transmitted octets over the interface.

In Packets: Number of received packets over the interface.

Out Packets: Number of transmitted packets over the interface.

In OAM Cells: Number of OAM cells received.

Out OAM Cells: Number of OAM cells transmitted.

In ASM Cells: Number of ASM cells received.

Out ASM Cells: Number of ASM cells transmitted.

In Packet Errors: Number of received packets with errors.

In Cell Errors: Number of received cells with errors.

Reset: Click to reset the statistics.

xDSL

Statistics -- xDSL

| | | |
|--------------------------|------------|----------|
| Mode: | | |
| Traffic Type: | | |
| Status: | | Disabled |
| Link Power State: | | |
| | | |
| | Downstream | Upstream |
| Line Coding(Trellis): | | |
| SNR Margin (0.1 dB): | | |
| Attenuation (0.1 dB): | | |
| Output Power (0.1 dBm): | | |
| Attainable Rate (Kbps): | | |
| Rate (Kbps): | | |
| | | |
| Super Frames: | | |
| Super Frame Errors: | | |
| RS Words: | | |
| RS Correctable Errors: | | |
| RS Uncorrectable Errors: | | |
| | | |
| HEC Errors: | | |
| OCD Errors: | | |
| LCD Errors: | | |
| Total Cells: | | |
| Data Cells: | | |
| Bit Errors: | | |
| | | |
| Total ES: | | |
| Total SES: | | |
| Total UAS: | | |

xDSL BER Test

Reset Statistics

Mode: Modulation protocol, including G.dmt, G.lite, T1.413, ADSL2, AnnexL, ADSL2+ and AnnexM.

Traffic Type: Transfer mode, here supports ATM and PTM.

Status: Show the status of DSL link.

Link Power State: Show link output power state.

Line Coding (Trellis): Trellis on/off.

SNR Margin (dB): Show the Signal to Noise Ratio (SNR) margin.

Attenuation (dB): This is estimate of average loop attenuation of signal.

Output Power (dBm): Show the output power.

Attainable Rate (Kbps): The sync rate you would obtain.

Rate (Kbps): Show the downstream and upstream rate in Kbps.

Super Frames: The total number of super frames.

Super Frame Errors: The total number of super frame errors.

RS Words: Total number of Reed-Solomon code errors.

RS Correctable Errors: Total number of RS with correctable errors.

RS Uncorrectable Errors: Total number of RS words with uncorrectable errors.

HEC Errors: Total number of Header Error Checksum errors.

OCD Errors: Total number of out-of-cell Delineation errors.

LCD Errors: Total number of Loss of Cell Delineation.

Total Cells: Total number of cells.

Data Cells: Total number of data cells

Bit Errors: Total number of bit errors.

Total ES: Total Number of Errored Seconds.

Total SES: Total Number of Severely Errored Seconds.

Total UAS: Total Number of Unavailable Seconds.

xDSL BER Test: Click this button to start a bit Error Rate Test. The ADSL Bit Error Rate (BER) test determines the quality of the ADSL connection. The test is done by transferring idle cells containing a known pattern and comparing the received data with this known pattern to check for any errors.

Select the Tested Time (sec), press Start to start test.

ADSL BER Test -- Running

The xDSL BER test is in progress.

Connection Speed

27447 Kbps

The test will run for

20 seconds

Stop

Close

When it is OK, the following test result window will appear. You can view the quality of ADSL connection. Here the connection is OK.

ADSL BER Test -- Result

The ADSL BER test completed successfully.

Test Time

20 seconds

Total Transferred Bits

0x000000001DA1F500

Error Ratio

0.00e+00

Close

Reset: Click this button to reset the statistics.

Route

Device Info -- Route

Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate
D - dynamic (redirect), M - modified (redirect).

| Destination | Gateway | Subnet Mask | Flag | Metric | Service | Interface |
|---------------|---------------|-----------------|------|--------|---------|-----------|
| 0.0.0.0 | 10.188.20.197 | 0.0.0.0 | UG | 0 | 3G_LTE0 | usbo3g0 |
| 10.188.20.196 | 0.0.0.0 | 255.255.255.252 | U | 0 | 3G_LTE0 | usbo3g0 |
| 192.168.0.0 | 0.0.0.0 | 255.255.255.0 | U | 0 | | br0 |

- Destination:** The IP address of destination network.
- Gateway:** The IP address of the gateway this route uses.
- Subnet Mask:** The destination subnet mask.
- Flag:** Show the status of the route.

i

U: Show the route is activated or enabled.

i

H (host): destination is host not the subnet.

i

G: Show that the outside gateway is needed to forward packets in this route.

- i R: Show that the route is reinstated from dynamic routing.
- i D: Show that the route is dynamically installed by daemon or redirecting.
- i M: Show the route is modified from routing daemon or redirect.

Metric: Display the number of hops counted as the Metric of the route.

Service: Display the service that this route uses.

Interface: Display the existing interface this route uses.

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. Here IPv6 Neighbor Table, listed with IPv6 address-MAC mapping, is supported.

Device Info -- ARP

| IP Address | Flags | HW Address | Device |
|---------------|----------|-------------------|---------|
| 10.188.20.197 | Complete | 02:50:f3:00:00:00 | usbo3g0 |
| 192.168.0.100 | Complete | 20:6a:8a:2a:5c:39 | br0 |

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.

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

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

Device: here refers to the physical interface, it is a concept to identify Clients from LAN or WAN. For example, the Clients in LAN, here displays "br0".

DHCP

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

Device Info -- DHCP Leases

| Hostname | MAC Address | IP Address | Expires In |
|----------|-------------------|---------------|----------------------------------|
| testi | 20:6a:8a:2a:5c:39 | 192.168.0.100 | 23 hours, 46 minutes, 33 seconds |

Host Name: The Host Name of DHCP client.

MAC Address: The MAC Address of internal DHCP client host.

IP Address: The IP address which is assigned to the host with this MAC address.

Expires in: Show the remaining time after registration.

VPN

The Server info and Client info Window shows the information about Server/Client connection.

Server Info

Device Info -- Server Info

| Name | Type | Enable | Status | Connection Type | Peer IP | Connected By | Action |
|------|------|--------|--------|-----------------|---------|--------------|--------|
|------|------|--------|--------|-----------------|---------|--------------|--------|

Name: The PPTP connection name.

Enable: Display the connection status with icons.

Status: The connection status.

Connection Type: Remote Access or LAN to LAN.

Peer IP: Display the remote network and subnet mask in LAN to LAN PPTP connection.

Connected By: Display the IP of remote connected client.

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

Client Info

Device Info -- Client Info

| Name | Type | Enable | Status | Connection Type | Remote Gateway | Peer IP | Client IP | Action |
|------|------|--------|--------|-----------------|----------------|---------|-----------|--------|
|------|------|--------|--------|-----------------|----------------|---------|-----------|--------|

Name: The PPTP connection name.

Enable: Display the connection status with icons.

Status: The connection status.

Connection Type: Remote Access or LAN to LAN.

Peer Network IP: Display the remote network and subnet mask in LAN to LAN PPTP connection.

Client: Assigned IP by PPTP server.

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

Refresh: Click this button to refresh the connection status.

GRE

Device Info -- GRE Info

| Name | Enable | Status | Remote Gateway |
|------|--------|--------|----------------|
|------|--------|--------|----------------|

- Name:** The GRE connection name.
- Enable:** Display the connection status with icons.
- Status:** The connection status, connected or disable.
- Remote Gateway:** The IP of remote gateway.

Log

System Log

Display system logs accumulated up to the present time. You can trace historical information with this function. And the log policy can be configured in Configure Log section.

System Log

| Date/Time | Facility | Severity | Message |
|----------------|----------|----------|--|
| Jan 1 00:00:14 | kern | warn | kernel: [FAP1] PSM : addr<0x80002000>, used <24320>, free <256>, total <24576> |
| Jan 1 00:00:14 | kern | warn | kernel: [FAP0] DQM : availableMemory 14660 bytes, nextByteAddress 0xE000489C |
| Jan 1 00:00:14 | kern | warn | kernel: [FAP1] DQM : availableMemory 14660 bytes, nextByteAddress 0xE000489C |
| Jan 1 00:00:14 | kern | warn | kernel: [FAP0] Initializing FAP4KE GSO LOOPBACK on fapIdx=0 ... |
| Jan 1 00:00:14 | kern | warn | kernel: [FAP1] FAP BPM Initialized. |
| Jan 1 00:00:14 | kern | warn | kernel: [FAP0] SWQ: HOST2FAP_GSO_LOOPBACK |
| Jan 1 00:00:14 | kern | warn | kernel: [FAP0] >>>>----- |
| Jan 1 00:00:14 | kern | warn | kernel: [FAP0] swq =80007ee0 msgSize =4 words , maxDepth=1024 |
| Jan 1 00:00:14 | kern | warn | kernel: [FAP0] qStart =a5c2c000 qEnd=a5c30000 |
| Jan 1 00:00:14 | kern | warn | kernel: [FAP0] rdPtr =a5c2c000 wrPtr=a5c2c000 count=0 |
| Jan 1 00:00:14 | kern | warn | kernel: [FAP0] processed =0 dropped =0 |
| Jan 1 00:00:14 | kern | warn | kernel: [FAP0] Associated DQM=18 dir HOST2FAP |
| Jan 1 00:00:14 | kern | warn | kernel: [FAP0] -----<<<< |
| Jan 1 00:00:14 | kern | warn | kernel: [FAP0] SWQ: FAP2HOST_GSO_LOOPBACK |
| Jan 1 00:00:14 | kern | warn | kernel: [FAP0] >>>>----- |
| Jan 1 00:00:14 | kern | warn | kernel: [FAP0] swq =80007ec0 msgSize =2 words , maxDepth=2048 |
| Jan 1 00:00:14 | kern | warn | kernel: [FAP0] qStart =a5c30000 qEnd=a5c34000 |
| Jan 1 00:00:14 | kern | warn | kernel: [FAP0] rdPtr =a5c30000 wrPtr=a5c30000 count=0 |
| Jan 1 00:00:14 | kern | warn | kernel: [FAP0] processed =0 dropped =0 |
| Jan 1 00:00:14 | kern | warn | kernel: [FAP0] Associated DQM=19 dir FAP2HOST |
| Jan 1 00:00:14 | kern | warn | kernel: [FAP0] -----<<<< |
| Jan 1 00:00:14 | kern | warn | kernel: [FAP0] FAP4KE GSO LOOPBACK Init Done... |
| Jan 1 00:00:14 | kern | warn | kernel: [FAP0] FAP BPM Initialized. |
| Jan 1 00:00:14 | kern | warn | kernel: ^[[0;36;44mBroadcom Packet Flow Cache HW acceleration enabled.^[[0m |

Refresh: Click to update the system log.

SMS Log

Displays tne sms messages sent

Advanced Setup

The function of each configuration sub-item is described in the following sections.

Layer 2 interface

This window is used to configure the ATM interface. You can add and delete ATM interface on this window.

If you are setting up the ATM interface for the first time, click the **Add** button.

DSL ATM Interface Configuration

Choose Add, or Remove to configure DSL ATM interfaces.

| Interface | Vpi | Vci | DSL Latency | Category | Peak Cell Rate(cells/s) | Sustainable Cell Rate(cells/s) | Max Burst Size(Bytes) | Min Cell Rate(cells/s) | Link Type | Connection Mode | IP QoS | MPAAL Prec/Alg/Wght | Remove |
|-----------|-----|-----|-------------|----------|-------------------------|--------------------------------|-----------------------|------------------------|-----------|-----------------|---------|---------------------|--------------------------|
| atm0 | 0 | 33 | Path0 | UBR | | | | | EoA | VlanMuxMode | Support | 8/WRR/1 | <input type="checkbox"/> |
| atm1 | 0 | 100 | Path0 | UBR | | | | | EoA | VlanMuxMode | Support | 8/WRR/1 | <input type="checkbox"/> |
| atm2 | 0 | 35 | Path0 | UBR | | | | | EoA | VlanMuxMode | Support | 8/WRR/1 | <input type="checkbox"/> |

Add

Remove

ATM Interface

The **ATM PVC** Configuration window allows you to set up ATM PVC configuration. Enter Virtual Path Identifier, and Virtual Channel Identifier. The VPI and VCI values should be provided by your ISP. This window also allows you to select DSL Link Type, PPPoA ,IPoA and EoA (EoA is for PPPoE, IPoE, and Bridge)

Use the drop-down menu to select the desired Encapsulation Mode.

Click the **Apply / Save** button to save.

ATM PVC Configuration

This screen allows you to configure a ATM PVC.

VPI: [0-255]
VCI: [32-65535]

Select DSL Latency

- ☒ Path0 (Fast)
☐ Path1 (Interleaved)

Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)

- ☒ EoA
☐ PPPoA
☐ IPoA

Encapsulation Mode:

Service Category:

Minimum Cell Rate: [cells/s] (-1 indicates no shaping)

Select Scheduler for Queues of Equal Precedence as the Default Queue

- ☒ Weighted Round Robin
☐ Weighted Fair Queuing

Default Queue Weight: [1-63]

Default Queue Precedence: [1-8] (lower value, higher priority)

VC WRR Weight: [1-63]

VC Precedence: [1-8] (lower value, higher priority)

PTM Interface

The **PTM Interface** Configuration window enables you to add, delete, or modify up to one VDSL WAN Layer 2 interface connections.

Click **PTM Interface** in the Layer2 Interface menu to open the VDSL(ptm) WAN Interface Configuration window

DSL PTM Interface Configuration

Choose Add, or Remove to configure DSL PTM interfaces.

| Interface | DSL Latency | PTM Priority | Conn Mode | IP QoS | Remove |
|-----------|-------------|--------------|-------------|---------|--------------------------|
| ptm0 | Path0 | Normal&High | VlanMuxMode | Support | <input type="checkbox"/> |

VDSL WAN Configuration

If you have selected to add or modify a VDSL interface connection, the VDSL WAN Configuration window opens. Click the **Apply/Save** button to save.

PTM Configuration

This screen allows you to configure a PTM flow.

Select DSL Latency

- ☒ Path0 (Fast)
☐ Path1 (Interleaved)

Select Scheduler for Queues of Equal Precedence as the Default Queue

- ☒ Weighted Round Robin
☐ Weighted Fair Queuing

Default Queue Weight: [1-63]

Default Queue Precedence: [1-8] (lower value, higher priority)

Default Queue Minimum Rate: [1-50000 Kbps] (-1 indicates no shaping)

Default Queue Shaping Rate: [1-50000 Kbps] (-1 indicates no shaping)

Default Queue Shaping Burst Size: [bytes] (shall be ≥ 1600)

WAN-Wide Area Network

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.

This window is used to configure the WAN interface. You can add and delete WAN interface on this window.

If you are setting up the WAN interface for the first time, click the **Add** button.

Wide Area Network (WAN) Service Setup

Choose Add, Remove or Edit to configure a WAN service over a selected interface.

| Interface | Description | Type | Vlan8021p | VlanMuxId | VlanTpid | Igmp Proxy | Igmp Source | NAT | Firewall | IPv6 | Mld Proxy | Mld Source | Remove | Edit |
|-----------|----------------|--------|-----------|-----------|----------|------------|-------------|---------|----------|----------|-----------|------------|--------------------------|------|
| atm0.1 | ipoe_0_0_33 | IPoE | N/A | N/A | N/A | Enabled | Enabled | Enabled | Enabled | Disabled | Disabled | Disabled | <input type="checkbox"/> | Edit |
| atm1.1 | ipoe_0_0_100 | IPoE | N/A | N/A | N/A | Enabled | Enabled | Enabled | Enabled | Disabled | Disabled | Disabled | <input type="checkbox"/> | Edit |
| atm2.2 | ipoe_0_0_35 | IPoE | N/A | N/A | N/A | Enabled | Enabled | Enabled | Enabled | Disabled | Disabled | Disabled | <input type="checkbox"/> | Edit |
| ptm0.1 | ipoe_0_1_1 | IPoE | N/A | N/A | N/A | Enabled | Enabled | Enabled | Enabled | Disabled | Disabled | Disabled | <input type="checkbox"/> | Edit |
| ptm0.3 | ipoe_0_1_1.252 | IPoE | 1 | 252 | 0x0 | Enabled | Enabled | Enabled | Enabled | Disabled | Disabled | Disabled | <input type="checkbox"/> | Edit |
| usbo3g0 | 3G_LTE0 | Direct | N/A | N/A | N/A | Disabled | Disabled | Enabled | Enabled | Disabled | Disabled | Disabled | | |
| ppp03g0 | 3G_LTE0 | PPP | N/A | N/A | N/A | Disabled | Disabled | Enabled | Enabled | Disabled | Disabled | Disabled | | |

Add

Remove

The **WAN Service Interface Configuration** window allows select a layer 2 interface for this service. Click the **Next** button to continue

WAN Service Interface Configuration

Select a layer 2 interface for this service

atm0/(0_0_33) ▼

Back

Next

This window allows you to select the appropriate connection type. The choices include PPP over ATM (PPPoA), PPP over Ethernet (PPPoE), IP over Ethernet (IPoE), IP over ATM (IPoA), and Bridging.

WAN Service Configuration – PPPoE

Click the PPP over Ethernet (PPPoE) radio button on this window. This window also allows you to use the drop-down menu to enable IPv6 service. Click the **Next** button to continue.

WAN Service Configuration

Select WAN service type:

- ☒ PPP over Ethernet (PPPoE)
☐ IP over Ethernet
☐ Bridging

☐ Allow as IGMP Multicast Source

Enter Service Description:

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.
For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.

Enter 802.1P Priority [0-7]:

Enter 802.1Q VLAN ID [0-4094]:

Select VLAN TPID:

Network Protocol Selection:

WAN Service Configuration – PPPoE

This window allows you to set the username and the password for your PPP connection. This information is obtained from your ISP. Additional settings on this window will also depend on your ISP. And you can input 2nd IP on this page. Click the **Next** button to continue.

PPP Username and Password

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username:
PPP Password:
PPPoE Service Name:
Authentication Method:

- ☐ Enable Fullcone NAT
☐ Dial on demand (with idle timeout timer)
☐ PPP IP extension
☐ Use Static IPv4 Address
☐ Enable PPP Debug Mode
☐ Bridge PPPoE Frames Between WAN and Local Ports

Igmp Proxy

- ☐ Igmp Proxy
☐ Igmp Source

MTU:

WAN Service Configuration – IPoE

This window allows you to configure the WAN IP settings. This information is obtained from your ISP. Click the **Next** button to continue

WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.
Note: If 'Obtain an IP address automatically' is chosen, DHCP will be enabled for PVC in IPoE mode.
If 'Use the following Static IP address' is chosen, enter the WAN IP address, subnet mask and interface gateway.

☒ Obtain an IP address automatically

Option 60 Vendor ID:

Option 61 IAID: (8 hexadecimal digits)

Option 61 DUID: (hexadecimal digit)

Option 125:

☒ Disable ☐ Enable

☐ Use the following Static IP address:

WAN IP Address:

WAN Subnet Mask:

WAN gateway IP Address:

MTU:

MAC Spoofing:

WAN Service Configuration – Bridging

Click the Bridge radio button on this window. Click the **Next** button to continue.

WAN Service Configuration

Select WAN service type:

☐ PPP over Ethernet (PPPoE)

☐ IP over Ethernet

☒ Bridging

☐ Allow as IGMP Multicast Source

☐ Allow as IGMP Multicast Source

☐ Allow as MLD Multicast Source

Enter Service Description:

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.
For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.

Enter 802.1P Priority [0-7]:

Enter 802.1Q VLAN ID [0-4094]:

Select VLAN TPID:

Select a TPID ▼

3G/LTE

3G/LTE settings

Select 3G/4G/LTE to configure the route to enjoy the mobility. By default the 3G/4G/LTE interface is on, user can edit the parameters to meet your own requirements.

3G/LTE Settings

☐ Enable WAN Failover:

Network Preference:

Use 3G/LTE dongle settings ▾

PIN Code:

Dialup Number:

APN Code:

Username:

Password:

Authentication Method:

AUTO ▾

☒ Enable Keep Alive

Time: seconds [1-86400]

IP Address: (Empty means the 3G/LTE Primary DNS)

MTU:

☒ Enable NAT

☒ Enable Firewall

Extra AT Command:

Apply/Save

Enable WAN Failover: If enabled, the 3G/LTE will work in failover mode and be brought up only when there is no active default route. In this mode, 3G/LTE work as a backup for the WAN connectivity. While if disabled, 3G/LTE serves as a normal interface, and can only be brought up when it has been configured to achieve a mobile connectivity.

Network preference: 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.

PIN code: PIN stands for Personal Identification Number. A PIN code is a numeric value used in certain systems as a password to gain access, and authenticate. In mobile phones a PIN code locks the SIM card until you enter the correct code. If you enter the PIN code incorrectly into the phone 3 times in a row, then the SIM card will be blocked and you will require a PUK code from your network/ service provider.

Dialup number.: The dial string to make a 3G/4G/LTE user internetworking call. It may provide by your mobile service provider.

APN code: An APN is similar to a URL on the WWW, it is what the unit makes a GPRS / UMTS call. The service provider is able to attach anything to an APN to create a data connection, requirements for APNs varies between different service providers. Most service providers have an internet portal which they use to

connect to a DHCP Server, thus giving you access to the internet i.e. some 3G operators use the APN 'internet' for their portal. The default value is "internet".

Username/Password: Enter the username and password provided by your service provider. The username and password are case sensitive.

Authentication Protocol: Default is Auto. Please consult your service provider on whether to use PAP, CHAP or MSCHAP.

Enable Keep Alive: Check Enable to allow the router to send message out

Time: 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.

MTU: MTU (Maximum Transmission Unit) is the size of the largest datagram that IP will attempt to send through the interface.

Enable NAT: Check to enable the NAT function.

Enable Firewall: Enable to drop all traffic from WAN side. If enabled, all incoming packets by default would be dropped, and please turn to IP Filtering Incoming to add allowing rules.

Extra AT command: Field can be entered AT command provided by 3G/LTE dongle manufacturer

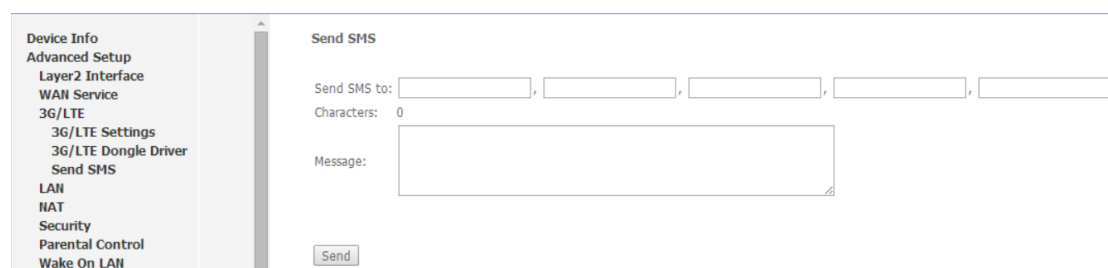
Send SMS

TW-EAV510 Series can support to send SMS when plug in the 3G/LTE dongle. You can access to the SMS sending page by two ways below.

Note:

The SIM card must support SMS service and it also depends on dongle you use, some of dongles may not support SMS when data connection is up.

1. Login to WEB GUI by using admin account and go to Advanced Setup -> 3G/LTE -> Send SMS. The administrator account can send SMS directly without password protection.



The screenshot shows the 'Send SMS' page in the router's web GUI. On the left is a sidebar menu with options: Device Info, Advanced Setup, Layer2 Interface, WAN Service, 3G/LTE, 3G/LTE Settings, 3G/LTE Dongle Driver, Send SMS (highlighted), LAN, NAT, Security, Parental Control, and Wake On LAN. The main content area is titled 'Send SMS' and contains a 'Send SMS to:' field with five input boxes, a 'Characters:' label with '0', a 'Message:' text area, and a 'Send' button.

2. Type URL address directly to access to Send SMS page.

URL: <http://192.168.0.254/sendsms.html>



The screenshot shows a web browser window with the address bar displaying 'http://192.168.0.254/sendsms.html'. The page content is titled 'Send SMS' and includes a 'Password:' field, a 'Send SMS to:' field with five input boxes, a 'Characters:' label with '0', a 'Message:' text area, and a 'Send' button.

This page doesn't require the login, but you must enter the password correctly to send SMS.
The password setting for SMS can be found at Management -> SMS Control -> SMS User. Enter the password you want and click Apply/Save button to save configuration.

SMS User

Password:

Apply/Save

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.

Local Area Network (LAN) Setup

Configure the Broadband Router IP Address and Subnet Mask for LAN interface. Group Name Default ▼

IP Address:

Subnet Mask:

☒ Enable IGMP Snooping

☐ Standard Mode

☒ Blocking Mode

Enable IGMP LAN to LAN Multicast: Disable ▼

(LAN to LAN Multicast is enabled until the first WAN service is connected, regardless of this setting.)

☐ Enable LAN side firewall

☐ Disable DHCP Server

☒ Enable DHCP Server

Start IP Address:

End IP Address:

Leased Time (hours):

Static IP Lease List: (Maximum entries: 32)

| MAC Address | IP Address | Remove |
|-------------|------------|--------|
|-------------|------------|--------|

Add

Remove

☐ Configure the second IP Address and Subnet Mask for LAN interface

Apply/Save

Parameters

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

Subnet Mask: the default Subnet mask on the router.

Enable 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."

When enabled, you will see two modes:

- i **Standard Mode:** In standard mode, multicast traffic will flood to all bridge ports when no client subscribes to a multicast group.
- i **Blocking Mode:** In blocking mode, the multicast data will be blocked when there are no client subscribes to a multicast group, it won't flood to the bridge ports.

Enable LAN side firewall: Enable to drop all traffic from the specified LAN group interface. After activating it, all incoming packets by default will be dropped, and the user on the specified LAN group interface can't access CPE anymore. But, you can still access the internet service. If user wants to manage the CPE, please turn to IP Filtering Incoming to add the allowing rules. Note that all incoming packets by default will be dropped if the LAN side firewall is enabled and user cannot manage this CPE from the specified LAN group.

DHCP Server

You can disable or enable the DHCP (Dynamic Host Configuration Protocol) server or enable the router's DHCP relay functions. The DHCP protocol allows your router to dynamically assign IP addresses to PCs on your network if they are configured to obtain IP addresses automatically.

Start IP Address: The start IP address of the range the DHCP Server used to assign to the Clients.

End IP Address: The end IP address of the range the DHCP Server used to assign to the Clients.

Leased Time (hour): The leased time for each DHCP Client.

Static IP List

The specified IP will be assigned to the corresponding MAC Address listed in the following table when DHCP Server assigns IP Addresses to Clients.

Press Add to the Static IP List.

Enter the MAC Address, IP Address, and then click Apply to confirm your settings. But the IP assigned should be outside the range of 192.168.0.100-192.168.0.199.

IPv6 Autoconfig

The IPv6 address composes of two parts, the prefix and the interface ID.

There are two ways to dynamically configure IPv6 address on hosts. One is "stateful" configuration, for example using DHCPv6 (which resembles its counterpart DHCP in IPv4.) In the stateful auto-configuration model, hosts obtain interface addresses and/or configuration information and parameters from a DHCPv6 server. The Server maintains a database that keeps track of which addresses have been assigned to which hosts.

The second way is "stateless" configuration. Stateless auto-configuration requires no manual configuration of hosts, minimal (if any) configuration of routers, and no additional servers. The stateless mechanism allows a host to generate its own addresses using a combination of locally available information (MAC address) and information (prefix) advertised by routers. Routers advertise prefixes that identify the subnet(s) associated with a link, while hosts generate an "interface identifier" that uniquely identifies an interface on a subnet. An address is formed by combining the two. When using stateless configuration, you needn't configure anything on the client.

IPv6 LAN Auto Configuration

Note: Stateful DHCPv6 is supported based on the assumption of prefix length less than 64. Interface ID does NOT support ZERO COMPRESSION '::.'. Please enter the complete information. For example: Please enter '0:0:0:2' instead of '::2'.

Static LAN IPv6 Address Configuration

Interface Address (prefix length is required):

IPv6 LAN Applications

☒ Enable DHCPv6 Server

☐ Stateless

☐ Stateful

Start interface ID:

End interface ID:

Leased Time (hours):

☒ Enable RADVD

☐ Enable ULA Prefix Advertisement

☐ Randomly Generate

☐ Statically Configure

Prefix:

Preferred Life Time (hours):

Valid Life Time (hours):

☒ Enable MLD Snooping

☐ Standard Mode

☒ Blocking Mode

Enable MLD LAN to LAN Multicast:

(LAN to LAN Multicast is enabled until the first WAN service is connected, regardless of this setting.)

Static LAN IPv6 Address Configuration

Interface Address / Prefix Length: Enter the static LAN IPv6 address.

IPv6 LAN application

Enable DHCPv6 Server: Check whether to enable DHCPv6 server.

Stateless: If selected, the PCs in LAN are configured through RA mode, thus, the PCs in LAN are configured through RA mode, to obtain the prefix message and generate an address using a combination of locally available information (MAC address) and information (prefix) advertised by routers, but they can obtain such information like DNS from DHCPv6 Server.

Stateful: if selected, the PCs in LAN will be configured like in IPv4 mode, thus obtain addresses and DNS information from DHCPv6 server.

Start interface ID: Enter the start interface ID. The IPv6 address composed of two parts, thus, the prefix and the interface ID. Interface is like the Host ID compared to IPv4.

End interface ID: Enter the end interface ID.

Note: Interface ID does NOT support ZERO COMPRESSION "::.". Please enter the complete information. For example: Please enter "0:0:0:2" instead of "::2".

Leased Time (hour): The leased time, similar to leased time in DHCPv4, is a time limit assigned to clients, when expires, the assigned ID will be recycled and reassigned.

Enable RADVD

Enable ULA Prefix Advertisement: Enable this parameter to include the ipv6 ULA address in the RA messages. ULA, unique local address, is an IPv6 address in the block fc00::/7. It is approximately the IPv6 counterpart of the IPv4 private address. They are not routable in the global IPv6 Internet.

The way that ULA prefix is generated.

i **Randomly Generated**

i **Statically Configured:** select to set manually in the following parameters.

Prefix: Set the prefix manually.

Preferred Life Time: The ULA prefix life time. When the time is over, the ULA prefix is invalid any more, -1 means no limit.

Valid Life Time: It is a time threshold, when the time is over, clients should obtain new IPv6 address from the router through RA; -1 means to be limitless.

Enable 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.

i **Standard Mode:** In standard mode, multicast traffic will flood to all bridge ports when no client subscribes to a multicast group.

i **Blocking Mode:** In blocking mode, the multicast data will be blocked when there is no client subscribes to a multicast group, it won't flood to the bridge ports.

NAT

NAT (Network Address Translation) feature translates a private IP to a public IP, allowing multiple users to access the Internet through a single IP account, sharing the single IP address. It is a natural firewall for the private network.

Virtual Servers

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 NAT is enabled.

Note: The maximum number of entries: 64.

It is virtual server listing table as you see, Click Add to move on.

The following configuration page will appear to let you configure.

NAT -- Virtual Servers

Select the service name, and enter the server IP address and click 'Apply/Save' to forward IP packets for this service to the specified server.
Note: The 'Internal Port End' cannot be modified directly. Normally, it is set to the same value as 'External Port End'. However, if you modify 'Internal Port Start', then 'Internal Port End' will be set to the same value as 'Internal Port Start'.

Remaining number of entries that can be configured:32

Use Interface

ipoe_0_0_33/atm0.1

Service Name:

Select a Service:

Select One

Custom Service:

Server IP Address:

192.168.0.

| External Port Start | External Port End | Protocol | Internal Port Start | Internal Port End |
|---------------------|-------------------|----------|---------------------|-------------------|
| | | TCP | | |
| | | TCP | | |
| | | TCP | | |
| | | TCP | | |
| | | TCP | | |
| | | TCP | | |
| | | TCP | | |
| | | TCP | | |
| | | TCP | | |
| | | TCP | | |
| | | TCP | | |
| | | TCP | | |
| | | TCP | | |
| | | TCP | | |

Apply/Save

- Use interface:

select from the drop-down menu the interface you want the virtual server(s) to apply.
- Server Name:

select the server name from the drop-down menu.
- Custom Service:

It is a kind of service to let users customize the service they want. Enter the user- defined service name here. It is a parameter only available when users select Custom Service in the above parameter.
- Server IP Address:

Enter your server IP Address here. User can select from the list box for quick setup.
- Protocol:

select the protocol this service used: TCP/UDP, TCP, UDP.
- External Port

i

Start:

Enter a port number as the external starting number for the range you want to give access to internal network.

i

End:

Enter a port number as the external ending number for the range you want to give access to internal network.
- Internal Port

i

Start:

Enter a port number as the internal staring number.

i

End:

Here it will generate automatically according to the End port number of External port and can't be modified.

Press Apply to conform, and the items will be list in the Virtual Servers Setup table.

Remove

If you don't need a specified Server, you can remove it. Check the check box beside the item you want to remove, then press Remove, it will be OK.

Port Triggering

Port triggering is a way to automate port forwarding with outbound traffic on predetermined ports ('triggering ports'), incoming ports are dynamically forwarded to the initiating host, while the outbound ports are in use. Port triggering triggers can open an incoming port when a client on the local network makes an outgoing connection on a predetermined port or a range of ports. Click Add to add a port triggering rule.

NAT -- Port Triggering

Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications. You can configure the port settings from this screen by selecting an existing application or creating your own (Custom application) and click 'Save/Apply' to add it.

Remaining number of entries that can be configured:32

Use Interface:

Application Name:

☒ Select an application:

☐ Custom application:

| Trigger Port Start | Trigger Port End | Trigger Protocol | Open Port Start | Open Port End | Open Protocol |
|----------------------|----------------------|----------------------------------|----------------------|----------------------|----------------------------------|
| <input type="text"/> | <input type="text"/> | <input type="text" value="TCP"/> | <input type="text"/> | <input type="text"/> | <input type="text" value="TCP"/> |
| <input type="text"/> | <input type="text"/> | <input type="text" value="TCP"/> | <input type="text"/> | <input type="text"/> | <input type="text" value="TCP"/> |
| <input type="text"/> | <input type="text"/> | <input type="text" value="TCP"/> | <input type="text"/> | <input type="text"/> | <input type="text" value="TCP"/> |
| <input type="text"/> | <input type="text"/> | <input type="text" value="TCP"/> | <input type="text"/> | <input type="text"/> | <input type="text" value="TCP"/> |
| <input type="text"/> | <input type="text"/> | <input type="text" value="TCP"/> | <input type="text"/> | <input type="text"/> | <input type="text" value="TCP"/> |
| <input type="text"/> | <input type="text"/> | <input type="text" value="TCP"/> | <input type="text"/> | <input type="text"/> | <input type="text" value="TCP"/> |
| <input type="text"/> | <input type="text"/> | <input type="text" value="TCP"/> | <input type="text"/> | <input type="text"/> | <input type="text" value="TCP"/> |
| <input type="text"/> | <input type="text"/> | <input type="text" value="TCP"/> | <input type="text"/> | <input type="text"/> | <input type="text" value="TCP"/> |

Use interface: Select from the drop-down menu the interface you want the port triggering rules apply to.

Application Name: Preinstalled applications or Custom Application user can customize the utility yourself.

Custom Application: It is a kind of service to let users themselves customizes the service they want. Enter the user-defined service name here.

Trigger Port

- i Start: Enter a port number as the triggering port starting number.
 - i End: Enter a port number as the triggering port ending number.
- Any port in the range delimited by the 'Start' and 'End' would be the trigger port.

Open port

- i Start: Enter a port number as the open port starting number.
 - i End: Enter a port number as the open port ending number.
- Any port in the range delimited by the 'Start' and 'End' would be the preset forwarding port or open port.

Protocol: select the protocol this service used:

Set up

An example of how port triggering works, when a client behind a NAT router connecting to Aim Talk, it is a TCP connection with the default port 4099.

When connecting to Aim Talk, the client typically makes an outgoing connection on port 4099 to the Aim Talk server, but when the computer is behind the NAT, the NAT silently drops this connection because it does not know which computer behind the NAT to send the request to connect.

So, in this case, port triggering in the router is working, when an outbound connection is attempted on port 4099 (or any port in the range set), it should allow inbound connections to that particular computer.

Select a Server Name from the drop-down menu, then the port will automatically appear, modify some as you like, or you can just leave it as default. Remember to enter your server IP Address.

Press Apply to conform, and the items will be list in the Virtual Servers Setup table.

Remove

If you don't need a specified Server, you can remove it. Check the check box beside the item you want to remove, and then press Remove.

DMZ Host

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

NAT -- DMZ Host

The Broadband Router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.

Enter the computer's IP address and click 'Apply' to activate the DMZ host.

Clear the IP address field and click 'Apply' to deactivate the DMZ host.

DMZ Host IP Address:

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

Using port mapping does have security implications, since outside users are able to connect to PCs on your network. For this reason you are advised to use specific Virtual Server entries just for the ports your application requires instead of simply using DMZ or creating a Virtual Server entry for "All" protocols, as doing so results in all connection attempts to your public IP address accessing the specified PC.

If you have disabled the NAT option in the WAN-ISP section, the Virtual Server function will hence be invalid. If the DHCP server option is enabled, you have to be very careful in assigning the IP addresses of the virtual servers in order to avoid conflicts. The easiest way of configuring Virtual Servers is to manually assign static IP address to each virtual server PC, with an address that does not fall into the range of IP addresses that are to be issued by the DHCP server. You can configure the virtual server IP address manually, but it must still be in the same subnet as the router

ALG

The ALG Controls enable or disable protocols over application layer.

ALG

Select the ALG below.

- ☒ SIP ALG Enabled
- ☒ FTP ALG Enabled
- ☒ H323 ALG Enabled
- ☒ PPTP ALG Enabled
- ☒ RTSP ALG Enabled
- ☒ TFTP ALG Enabled

Security

IP Filtering Outgoing / Incoming

IP filtering enables you to configure your router to block specified internal/external users (IP address) from Internet access, or you can disable specific service requests (Port number) to /from Internet. The relationship among all filters is “or” operation, which means that the router checks these different filter rules one by one, starting from the first rule. As long as one of the rules is satisfied, the specified action will be taken.

Outbound IP Filtering by default is set to forward all outgoing traffic from LAN to go through the router, but user can set rules to block the specific outgoing traffic.

Note: The maximum number of entries: 32.

Click Add button to enter the exact rule setting page.

Add IP Filter -- Outgoing

The screen allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.

| | |
|---|-----------------------------------|
| Filter Name: | <input type="text"/> |
| IP Version: | <input type="text" value="IPv4"/> |
| Protocol: | <input type="text"/> |
| Source IP address[/Prefix Length]: | <input type="text"/> |
| Source Port (port or port:port): | <input type="text"/> |
| Destination IP address[/Prefix Length]: | <input type="text"/> |
| Destination Port (port or port:port): | <input type="text"/> |

Filter Name: A user-defined rule name. User can select simply from the list box for the application for quick setup.

IP Version: Select the IP Version, IPv4 or IPv6.

Protocol: Set the traffic type (TCP/UDP, TCP, UDP, ICMP) that the rule applies to.

Source IP address: This is the Address-Filter used to allow or block traffic to/from particular IP address(es) featured in the IP range. If you leave empty, it means any IP address.

Source Port [port or port:port]: The port or port range defines traffic from the port (specific application) or port in the set port range blocked to go through the router. Default is set port from range 1 – 65535.

Destination IP address: Traffic from LAN with the particular traffic destination address specified in the IP range is to be blocked from going through the router, similarly set as the Source IP address above.

Destination Port [port or port: port]: Traffic with the particular set destination port or port in the set port range is to be blocked from going through the router. Default is set port from port range: 1 – 65535.

MAC Filtering

MAC Filtering is only effective on ATM PVCs configured in Bridged mode.

MAC Filtering Setup

MAC Filtering is only effective on ATM PVCs configured in Bridge mode. **FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching with any of the specified rules in the following table. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching with any of the specified rules in the following table.

MAC Filtering Policy For Each Interface:

WARNING: Changing from one policy to another of an interface will cause all defined rules for that interface to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.

| Interface | Policy | Change |
|-----------|-----------|--------------------------|
| atm0.2 | FORWARDED | <input type="checkbox"/> |
| atm1.2 | FORWARDED | <input type="checkbox"/> |
| atm2.1 | FORWARDED | <input type="checkbox"/> |
| ptm0.2 | FORWARDED | <input type="checkbox"/> |

Change Policy

Choose Add or Remove to configure MAC filtering rules.

| Interface | Protocol | Destination MAC | Source MAC | Frame Direction | Remove |
|-----------|----------|-----------------|------------|-----------------|--------|
|-----------|----------|-----------------|------------|-----------------|--------|

Add Remove

FORWARDED means that all MAC layer frames will be forwarded except those matching with any of the specified rules in the following table.

BLOCKED means that all MAC layer frames will be blocked except those matching with any of the specified rules in the following table.

By default, all MAC frames of the interface in Bridge Mode will be forwarded, you can check Change checkbox and then press Change Policy to change the settings to the interface.

For example, from above, the interface atm0.1 is of bridge mode, and all the MAC layer frames will be forward, but you can set some rules to let some item matched the rules to be blocked.

Click Add button to add the rules.

Add MAC Filter

Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect. Click 'Apply' to save and activate the filter.

Protocol Type:

Destination MAC Address:

Source MAC Address:

Frame Direction:

WAN Interfaces (Configured in Bridge mode only)

Save/Apply

Protocol type: Select from the drop-down menu the protocol that applies to this rule.
Destination /Source MAC Address: Enter the destination/source address.
Frame Direction: Select the frame direction this rule applies, both LAN and WAN: LAN <=>WAN, only **LAN to WAN**: LAN=>WAN, only WAN to LAN: WAN=>LAN.
WAN Interfaces: Select the interfaces configured in Bridge mode.

Intrusion detection

The router’s Intrusion Detection System (IDS) is used to detect hacker attacks and intrusion attempts from the Internet. If the IDS function of the firewall is enabled, inbound packets are filtered and blocked depending on whether they are detected as possible hacker attacks, intrusion attempts or other connections that the router determines to be suspicious.

Intrusion Detection

☒ Enable

ICMP Flood

Limit packet rate:

4

 / second

Limit Packet per second burst:

8

 / second

UDP Flood

Limit packet rate:

10

 / second

Limit Packet per second burst:

20

 / second

TCP Flood

Limit packet rate:

10

 / second

Limit Packet per second burst:

20

 / second

Apply/Save

Parental Control

Time Restriction

If you are setting up the MAC address blocking, click the **Add** button.

Access Time Restriction -- Maximum entries: 16

| Username | MAC | Mon | Tue | Wed | Thu | Fri | Sat | Sun | Start | Stop | Remove |
|--|-----|-----|-----|-----|-----|-----|-----|-----|-------|------|--------|
| <div><div>Add</div><div>Remove</div></div> | | | | | | | | | | | |

MAC address is a specially formatted text string (xx:xx:xx:xx:xx:xx) that uniquely identification of a device. This section will allow users to block devices with certain MAC addresses on the LAN. To configure for MAC address blocking, enter the username into the **Username** field, click **Browser's MAC Address** to have MAC address of the LAN device, or click **Other MAC Address** and enter a MAC address manually. Tick the checkboxes for the desired individual days of the week and enter desired **Start Blocking Time** and **End Blocking Time**. Click the **Save/Apply** button to save the configuration

Access Time Restriction

This page adds time of day restriction to a special LAN device connected to the Router.

User Name

☒ Browser's MAC Address

☐ Other MAC Address

(
xx:xx:xx:xx:xx:xx
)

Days of the week

| | | | | | | |
|-----------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| Mon | Tue | Wed | Thu | Fri | Sat | Sun |
| Click to select | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Start Blocking Time (hh:mm)

End Blocking Time (hh:mm)

Apply/Save

URL Filter

This window allows you to set up **URL Filter** on the Router. Choose URL List Type **Exclude** or **Include** first and click **Add** button.

Url Filter -- Please select the list type first then configure the list entries.
Maximum entries: 100

URL List Type:
☐ Exclude
☐ Include

| | | |
|---------|------|--------|
| Address | Port | Remove |
|---------|------|--------|

Add
Remove

Enter the URL address and port number then click **Apply / Save** to add the entry to the URL filter.

Parental Control -- URL Filter Add

Enter the URL address and port number then click 'Apply/Save' to add the entry to the URL filter.

URL Address:

Port Number:
(
Default 80 will be applied if leave blank.
)

Apply/Save

Wake On LAN

Wake on LAN (WOL, sometimes WoL) is an Ethernet computer networking standard that allows a computer to be turned on or woken up remotely by a network message.

Configure Wake On LAN

Name:

MAC Address: or select from Selection ▼

Wake Up: ☐

Name: Enter identification for the host.

MAC address: Enter MAC address or select the computer that you want to wake up or turn on remotely.

Quality of Service

QoS or Quality of Service allows your Router to help prioritize the data packet flow in your Router and network. This is very important for time sensitive applications such as VoIP where it may help prevent dropped calls. Large amounts of non-critical data can be scaled so as not to affect these prioritized sensitive real-time programs.

To access the **QoS – Queue Management Configuration** window, click the **Quality of Service** button in the **Advanced Setup** directory.

This window allows you to set up QoS on the Router. When you are finished, click on the **Save/Apply** button.

QoS -- Queue Management Configuration

If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier. Click 'Apply/Save' button to save it.

Note: If Enable Qos checkbox is not selected, all QoS will be disabled for all interfaces.

Note: The default DSCP mark is used to mark all egress packets that do not match any classification rules.

☐ Enable QoS

Apply/Save

Qos Queue

Click the **Add** button to add a QoS Queue Configuration table entry.

QoS Queue Setup

In ATM mode, maximum queues: 16
In PTM mode, maximum queues: 8
For each Ethernet interface, maximum queues: 4
For each Ethernet WAN interface, maximum queues: 8
To add a queue, click the **Add** button.
To remove queues, check their remove-checkboxes, then click the **Remove** button.
The **Enable** button will scan through every queues in the table. Queues with enable-checkbox checked will be enabled. Queues with enable-checkbox un-checked will be disabled.
The enable-checkbox also shows status of the queue after page reload.
Note that if WMM function is disabled in Wireless Page, queues related to wireless will not take effects.

The QoS function has been disabled. Queues would not take effects.

| Name | Key | Interface | Qid | Prec/Alg/Wght | DSL Latency | PTM Priority | Shaping Rate(bps) | Min Bit Rate(bps) | Burst Size(Bytes) | Enable | Remove |
|--------------------|-----|------------------|-----|---------------|-------------|--------------|-------------------|-------------------|-------------------|--------------------------|--------|
| WMM Voice Priority | 1 | TW-EAV510-BR0001 | 8 | 1/SP | | | | | | Enabled | |
| WMM Voice Priority | 2 | TW-EAV510-BR0001 | 7 | 2/SP | | | | | | Enabled | |
| WMM Video Priority | 3 | TW-EAV510-BR0001 | 6 | 3/SP | | | | | | Enabled | |
| WMM Video Priority | 4 | TW-EAV510-BR0001 | 5 | 4/SP | | | | | | Enabled | |
| WMM Best Effort | 5 | TW-EAV510-BR0001 | 4 | 5/SP | | | | | | Enabled | |
| WMM Background | 6 | TW-EAV510-BR0001 | 3 | 6/SP | | | | | | Enabled | |
| WMM Background | 7 | TW-EAV510-BR0001 | 2 | 7/SP | | | | | | Enabled | |
| WMM Best Effort | 8 | TW-EAV510-BR0001 | 1 | 8/SP | | | | | | Enabled | |
| Default Queue | 33 | atm0 | 1 | 8/WRR/1 | Path0 | | | | | <input type="checkbox"/> | |
| Default Queue | 34 | atm1 | 1 | 8/WRR/1 | Path0 | | | | | <input type="checkbox"/> | |
| Default Queue | 35 | atm2 | 1 | 8/WRR/1 | Path0 | | | | | <input type="checkbox"/> | |
| Default Queue | 36 | ptm0 | 1 | 8/WRR/1 | Path0 | Low | | | | <input type="checkbox"/> | |

Add Enable Remove

This window allows you to configure a QoS queue entry and assign it a specific network interface.

Click the **Apply / Save** button to save and activate the filter.

QoS Queue Setup

This screen allows you to configure a QoS queue and add it to a selected layer2 interface.

Name:

Enable:

Enable ▼

Interface:

▼

Apply/Save

QoS Classification

Choose **Add** or **Remove** to configure network traffic classes.

QoS Classification Setup -- Maximum entries: 32

To add a rule, click the **Add** button.
To remove rules, check their remove-checkboxes, then click the **Remove** button.
The **Enable** button will scan through every rules in the table. Rules with enable-checkbox checked will be enabled. Rules with enable-checkbox un-checked will be disabled.
The enable-checkbox also shows status of the rule after page reload.
If you disable WMM function in Wireless Page, classification related to wireless will not take effects.

The QoS function has been disabled. Classification rules would not take effects.

| | | CLASSIFICATION CRITERIA | | | | | | | | | | | CLASSIFICATION RESULTS | | | | | |
|------------|-------|-------------------------|------------|--------------|--------------|----------------------|----------------------|----------|---------|---------|------------|--------------|------------------------|-----------|-------------|------------------|--------|--------|
| Class Name | Order | Class Intf | Ether Type | SrcMAC/ Mask | DstMAC/ Mask | SrcIP/ Prefix Length | DstIP/ Prefix Length | Protocol | SrcPort | DstPort | DSCP Check | 802.1P Check | Queue Key | DSCP Mark | 802.1P Mark | Rate Limit(kbps) | Enable | Remove |
| Add | | Enable | | Remove | | | | | | | | | | | | | | |

Use this window to create a traffic class rule to classify the upstream traffic, assign a queue that defines the precedence and the interface, and optionally overwrite the IP header DSCP byte. A rule consists of a class name and at least one condition. Please remember that all of the specified conditions on this window must be met for the rule to take effect.

Click the **Apply / Save** button to save and activate this rule.

Add Network Traffic Class Rule

This screen creates a traffic class rule to classify the ingress traffic into a priority queue and optionally mark the DSCP or Ethernet priority of the packet.
Click 'Apply/Save' to save and activate the rule.

Traffic Class Name:

Rule Order:

Last ▾

Rule Status:

Enable ▾

Specify Classification Criteria (A blank criterion indicates it is not used for classification.)

Class Interface:

LAN ▾

Ether Type:

▾

Source MAC Address:

Source MAC Mask:

Destination MAC Address:

Destination MAC Mask:

Specify Classification Results (A blank value indicates no operation.)

Specify Class Queue (Required):

▾

- Packets classified into a queue that exit through an interface for which the queue is not specified to exist, will instead egress to the default queue on the interface.

Mark Differentiated Service Code Point (DSCP):

▾

Mark 802.1p priority:

▾

Set Rate Limit:

[Kbits/s]

Apply/Save

QoS Port Shaping

Enter both Shaping Rate and Burst Size and on specify Ethernet port. Click the **Apply / Save** button to save and activate this rule.

QoS Port Shaping Setup

QoS port shaping supports traffic shaping of Ethernet interface.
If "Shaping Rate" is set to "-1", it means no shaping and "Burst Size" will be ignored.

| Interface | Type | Shaping Rate (Kbps) | Burst Size (bytes) |
|-----------|------|---------------------------------|--------------------------------|
| EWAN | WAN | <input type="text" value="-1"/> | <input type="text" value="0"/> |
| LAN1 | LAN | <input type="text" value="-1"/> | <input type="text" value="0"/> |
| LAN2 | LAN | <input type="text" value="-1"/> | <input type="text" value="0"/> |
| LAN3 | LAN | <input type="text" value="-1"/> | <input type="text" value="0"/> |
| LAN4 | LAN | <input type="text" value="-1"/> | <input type="text" value="0"/> |

Routing

Default Gateway

Routing -- Default Gateway

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 removing all and adding them back in again.

Selected Default Gateway Interfaces

eth4.1
atm0.1
atm1.1
ptm0.1
atm2.2
ptm0.3
usb03g0
ppp03g0




Available Routed WAN Interfaces

Select a preferred wan interface as the system default IPv6 gateway.

Selected WAN Interface

WAN port: Select the port this gateway applies to.

To set Default Gateway and Available Routed WAN Interface. This interfaces are the ones you have set in

WAN section, here select the one you want to be the default gateway by moving the interface via  or



. And select a Default IPv6 Gateway from the drop-down menu.

Note: Only one default gateway interface 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.

Static Route

With static route feature, you can control the routing of all the traffic across your network. With each routing rule created, you can specifically assign the destination where the traffic will be routed.

Click Add to create static routing.

Routing -- Static Route Add

Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click 'Apply/Save' to add the entry to the routing table.

| | |
|---------------------------------------|--|
| IP Version: | <input type="text" value="IPv4"/> |
| Destination IP address/Prefix Length: | <input type="text"/> |
| Interface: | <input type="text"/> |
| Gateway IP Address: | <input type="text"/> |
| Metric: | <input type="text"/> (optional: metric number should be greater than or equal to zero) |

IP Version: Select the IP version, IPv4 or IPv6.

Destination IP Address / Prefix Length: Enter the destination IP address and the prefix length. For IPv4, the prefix length means the number of '1' in the submask, it is another mode of presenting submask. One IPv4 address, 192.168.1.0/24, submask is 255.255.255.0. While in IPv6, IPv6 address composes of two parts, thus, the prefix and the interface ID, the prefix is like the net ID in IPv4, and the interface ID is like the host ID in IPv4. The prefix length is to identify the net ID in the address. One IPv6 address, 3FFE:FFFF:0:CD30:0:0:0:0 / 64, the prefix is 3FFE:FFFF:0:CD3.

Interface: Select an interface this route associated.

Gateway IP Address: Enter the gateway IP address.

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

Click Apply to apply this route and it will be listed in the route listing table.

In listing table you can remove the one you don't want by checking the checking box and press Remove button.

Policy Routing

Here users can set a route for the host (source IP) in a LAN interface to access outside through a specified Default Gateway or a WAN interface.

Click Add to create a policy route.

Policy Routing Setup

Enter the policy name, policies, and WAN interface then click 'Apply/Save' to add the entry to the policy routing table.
Note: If selected 'IPoE' as WAN interface, default gateway must be configured.

Policy Name:

Physical LAN Port:

Source IP:

Use Interface

Default Gateway IP:

Policy Name: User-defined name. **Physical LAN Port:** Select the LAN port. **Source IP:** Enter the Host Source IP.

Physical LAN Port: Select LAN port which you want to use

Source IP:

Use interface: Select the WAN interface which you want the Source IP to access outside through.

Default Gateway: Enter the default gateway which you want the Source IP to access outside through.

Click Apply to apply your settings. And the item will be listed in the policy Routing listing table. Here if you want to remove the route, check the remove checkbox and press Remove to delete it.

Load Sharing

The TW-EAV510 supports multiple WAN media interface, like DSL, EWAN and 3G/LTE. Load sharing function is great feature to help you to make load sharing on each interface.

The Load Sharing setting page can be found at **Advanced Setup -> Routing -> Load Sharing**.

Load Sharing -- Maximum entries: 7

| Name | Physical LAN Port | Physical WAN Port | Protocol | SrcIP/Prefix Length | SrcPort | DstIP/Prefix Length | DstPort | Remove | Edit |
|------|-------------------|-------------------|----------|---------------------|---------|---------------------|---------|--------|------|
|------|-------------------|-------------------|----------|---------------------|---------|---------------------|---------|--------|------|

Click **Add** button to add new load sharing rule.

Load Sharing

| | |
|---|--------------------------------------|
| Name: | <input type="text"/> |
| Physical LAN Port: | <input type="text"/> |
| Physical WAN Port: | <input type="text" value="DSL"/> |
| Protocol: | <input type="text" value="TCP/UDP"/> |
| Source IP address[/Prefix Length]: | <input type="text"/> |
| Source Port (port or port:port): | <input type="text"/> |
| Destination IP address[/Prefix Length]: | <input type="text"/> |
| Destination Port (port or port:port): | <input type="text"/> |

Name: The name for the rule.

Physical LAN Port: You can specify the physical LAN port, like Ethernet Port 1 or Wireless and make all traffic from this specified port to specified WAN port. If leave it empty, it means all LAN ports.

Physical WAN Port: Specify the WAN port for the outgoing traffic.

Protocol: Specify the protocol of outgoing traffic. If leave it empty, it means all protocols

Source IP address[/Prefix Length]: Specify the source IP of outgoing traffic. If leave it empty, it will not check source IP address.

Source Port (port or port:port): Specify the source port of outgoing traffic. If leave it empty, it will not check source port.

Destination IP address[/Prefix Length]: Specify the destination IP of outgoing traffic. If leave it empty, it will not check destination IP address.

Destination Port (port or port:port): Specify the destination port of outgoing traffic. If leave it empty, it will not check destination port.

Note: If the specified WAN interface is down, then all traffic will just follow the default route for Internet access.

Example 1: BitTorrent Usage

Normally, the PC which runs BitTorrent will allocate all bandwidth and we can make one specify LAN port for BitTorrent. In this case, the main connection is DSL and we use EWAN for BitTorrent.

Load Sharing

| | |
|---|---|
| Name: | <input type="text" value="BitTorrent"/> |
| Physical LAN Port: | <input type="text" value="LAN1"/> |
| Physical WAN Port: | <input type="text" value="EWAN"/> |
| Protocol: | <input type="text"/> |
| Source IP address[/Prefix Length]: | <input type="text"/> |
| Destination IP address[/Prefix Length]: | <input type="text"/> |

Example 2: Video Streaming Usage

Most video streaming are use UDP packet for transmission. In this case, the main connection is LTE and use DSL for video streaming.

Load Sharing

| | |
|---|--|
| Name: | <input type="text" value="Video_Streaming"/> |
| Physical LAN Port: | <input type="text"/> |
| Physical WAN Port: | <input type="text" value="DSL"/> |
| Protocol: | <input type="text" value="UDP"/> |
| Source IP address[/Prefix Length]: | <input type="text"/> |
| Source Port (port or port:port): | <input type="text"/> |
| Destination IP address[/Prefix Length]: | <input type="text"/> |
| Destination Port (port or port:port): | <input type="text"/> |

If you know the port number that will be used for UDP traffic, you can also fill in the port number on it.

Load Sharing

| | |
|---|--|
| Name: | <input type="text" value="Video_Streaming"/> |
| Physical LAN Port: | <input type="text" value=""/> |
| Physical WAN Port: | <input type="text" value="DSL"/> |
| Protocol: | <input type="text" value="UDP"/> |
| Source IP address[/Prefix Length]: | <input type="text" value=""/> |
| Source Port (port or port:port): | <input type="text" value=""/> |
| Destination IP address[/Prefix Length]: | <input type="text" value=""/> |
| Destination Port (port or port:port): | <input type="text" value="1000:2000"/> |

Example 3: Game playing usage

Online game is getting more popular and it always need most stable connection like EWAN or DSL. If we don't know the online game server IP address, we can just specify the source IP. In this case, the specified IP address can have guarantee connection for game playing.

Load Sharing

| | |
|---|--|
| Name: | <input type="text" value="Game"/> |
| Physical LAN Port: | <input type="text" value=""/> |
| Physical WAN Port: | <input type="text" value="DSL"/> |
| Protocol: | <input type="text" value=""/> |
| Source IP address[/Prefix Length]: | <input type="text" value="192.168.0.100"/> |
| Destination IP address[/Prefix Length]: | <input type="text" value=""/> |

If you know the IP address of online game server, you can just change the settings as below. It applies to all game players at LAN side.

Load Sharing

| | |
|---|---|
| Name: | <input type="text" value="Game"/> |
| Physical LAN Port: | <input type="text" value=""/> |
| Physical WAN Port: | <input type="text" value="DSL"/> |
| Protocol: | <input type="text" value=""/> |
| Source IP address[/Prefix Length]: | <input type="text" value=""/> |
| Destination IP address[/Prefix Length]: | <input type="text" value="123.123.10.5"/> |

RIP

RIP, Router Information Protocol, is a simple Interior Gateway Protocol (IGP). RIP has two versions, RIP-1 and RIP-2.

Routing -- RIP Configuration

Note: If selected interface has NAT enabled, only Passive mode is allowed.

To activate RIP for the WAN Interface, select the desired RIP version and operation and place a check in the 'Enabled' checkbox. To stop RIP on the WAN Interface, uncheck the 'Enabled' checkbox. Click the 'Apply/Save' button to star/stop RIP and save the configuration.

| Interface | Version | Operation | Enabled |
|-----------|---------|-----------|--------------------------|
| atm0.1 | 2 ▼ | Passive ▼ | <input type="checkbox"/> |
| atm1.1 | 2 ▼ | Passive ▼ | <input type="checkbox"/> |
| atm2.2 | 2 ▼ | Passive ▼ | <input type="checkbox"/> |
| ptm0.1 | 2 ▼ | Passive ▼ | <input type="checkbox"/> |
| ptm0.3 | 2 ▼ | Passive ▼ | <input type="checkbox"/> |
| eth4.1 | 2 ▼ | Passive ▼ | <input type="checkbox"/> |
| usbo3g0 | 2 ▼ | Passive ▼ | <input type="checkbox"/> |

Apply/Save

- Interface:** the interface the rule applies to.
- Version:** select the RIP version, there are two versions, RIP-1 and RIP-2.
- Operation:** RIP has two operation mode.
- i Passive: only receive the routing information broadcasted by other routers and modifies its routing table according to the received information.
 - i Active: working in this mode, the router sends and receives RIP routing information and modifies routing table according to the received information.
- Enable:** check the checkbox to enable RIP rule for the interface.

Note: RIP can't be configured on the WAN interface which has NAT enabled (such as PPPoE). Click

Apply to apply your settings.

DNS

DNS server

DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

DNS Server Interfaces can have multiple WAN interfaces served as system dns servers 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 removing all and adding them back in again.

☒ Select DNS Server Interface from available WAN interfaces:

Selected DNS Server
Interfaces

Available WAN Interfaces

The screenshot shows a configuration window with two list boxes. The left list box, titled 'Selected DNS Server Interfaces', contains the following items: ptm0.1, eth4.1, atm0.1, atm1.1, atm2.2, ptm0.3, usb03g0, and ppp03g0. The right list box, titled 'Available WAN Interfaces', is currently empty. Between the two list boxes are two buttons: a right-pointing arrow (->) and a left-pointing arrow (<-).

☐ Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

IPv4

Two ways to set an IPv4 DNS server

- i Select DNS server from available WAN interfaces: Select a desirable WAN interface as the IPv4 DNS server.
- i Use the following Static DNS IP address: To specify DNS server manually by entering your primary and secondary DNS server addresses.

IPv6:

IPv6 DNS Server's operation is similar to IPv4 DNS server. There are two modes to get DNS server address: Auto and Static mode.

Obtain IPv6 DNS info from a WAN interface

- I WAN Interface selected: Select one configured IPv6 WAN connection from the drop-down menu to be as an IPv6 DNS.

Use the following Static IPv6 DNS address

- I Primary IPv6 DNS Server / Secondary IPv6 DNS Server: Type the specific primary and secondary IPv6 DNS Server address.

Static DNS

Static DNS is a concept relative to Dynamic DNS; in static DNS system, the IP mapped is static without change.

You can map the specific IP to a user-friendly domain name. In LAN, you can map a PC to a domain name for convenient access. Or you can set some well-known Internet IP mapping item so your router will response quickly for your DNS query instead of querying from the ISP's DNS server.

Static DNS Configuration

Hostname:

IP Address:

Apply/Save

Host Name: Type the domain name (host name) for the specific IP.

IP Address: Type the IP address bound to the set host name above. Click Add to save your settings.

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 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.

Here users can register different WAN interfaces with different DNS(es).

Click Add to register a WAN interface with the exact DNS.

Add Dynamic DNS

D-DNS provider

DynDNS.org ▼

Hostname

Selected Interfaces

->

<-

Available WAN Interfaces

ipoe_0_0_33/atm0.1
ipoe_0_0_100/atm1.1
ipoe_0_0_35/atm2.2
ipoe_0_1_1/ptm0.1
ipoe_0_1_1.252/ptm0.3
ipoe_eth4/eth4.1
3G_LTE0/usbo3g0
3G_LTE0/pppo3g0

Username

Password

Update Period

Hours ▼

Apply/Save

You will first need to register and establish an account with the Dynamic DNS provider using their website, for example <http://www.dyndns.org/>

D-DNS Server: Select the DDNS service you have established an account with.

Host Name, Username and Password: Enter your registered domain name and your username and password for this service.

Selected WAN Interface: Select the Interface that is bound to the registered Domain name.

Static ARP

ARP (Address Resolution Protocol) is a TCP/IP protocol that allows the resolution of network layer addresses into the link layer addresses. And “Static ARP” here allows user to map manually the layer-3 MAC (Media Access Control) address to the layer-2 IP address of the device.

Static ARP Configuration

IP Address:

MAC Address:

Apply/Save

IP Address: Enter the IP of the device that the corresponding MAC address will be mapped to.

MAC Address: Enter the MAC address that corresponds to the IP address of the device. Click Add to confirm the settings.

DSL

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

Select the modulation below.

- ☒ G.Dmt Enabled
- ☒ G.lite Enabled
- ☒ T1.413 Enabled
- ☒ ADSL2 Enabled
- ☒ AnnexL Enabled
- ☒ ADSL2+ Enabled
- ☒ AnnexM Enabled
- ☒ VDSL2 Enabled

Select the phone line pair below.

- ☒ Inner pair
- ☐ Outer pair

Capability

- ☒ Bitswap Enable
- ☐ SRA Enable

PhyR

- ☐ Upstream
- ☒ Downstream

Apply/Save

Select the profile below.

- ☒ 8a Enabled
- ☒ 8b Enabled
- ☒ 8c Enabled
- ☒ 8d Enabled
- ☒ 12a Enabled
- ☒ 12b Enabled
- ☒ 17a Enabled

US0

- ☒ Enabled

Modulation: There are 7 modes “G.Dmt”, “G.lite”, “T1.413”, “ADSL2”, “AnnexL”, “ADSL2+”, “AnnexM” that user can select for this connection.

Phone line pair: This is for reserved only. You can choose "Inner Pair" or "Outer Pair".

Capability: There are 2 options “Bitswap Enable” and “SRA Enable” that user can select for this connection.

- i Bitswap Enable: Allows bitswaping function.
- i SRA Enable: Allows seamless rate adaptation.

PhyR: A new technology to control impulse and noise to improve the BER and DSL data quality.

Click Apply to confirm the settings.

SNR

Signal-to-noise ratio (often abbreviated SNR or S/N) is a measure used in science and engineering that compares the level of a desired signal to the level of background noise. It is defined as the ratio of signal power to the noise power.

SNR Setting

This field can be adjusted to affect the SNR value so as to achieve the highest possible sync speed.

Note: A value set too low may affect stability, a balance needs to be achieved between speed and stability.

There are no set values recommended as each ADSL line will be different. A value of 6 is a good starting point, this is the target SNR, from here you can gradually reduce values to achieve the highest possible sync speed whilst still maintaining stability. e.g 5,4...
1 is the lowest possible value.

SNR: dB (Auto: -1)

SNR: Change the value to adjust the DSL link rate, more suitable for an advanced user.

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.

Both the user's Operating System and the relevant application must support UPnP in addition to the router.

UPnP Configuration

Note: UPnP is activated only when there is a live WAN service with NAT enabled.

☐ Enable UPnP

UPnP:

- i Enable: Check to enable the router's UPnP functionality.

DNS Proxy

DNS proxy is used to forward request and response message between DNS Client and DNS Server. Hosts in LAN can use router serving as a DNS proxy to connect to the DNS Server in public to correctly resolve Domain name to access the internet.

DNS Proxy Configuration

☒ Enable DNS Proxy

Host name of the Broadband Router:

TeleWell

Domain name of the LAN network:

Home

Apply/Save

Enable DNS Proxy: Select whether to enable or disable DNS Proxy function, default is enabled.
Host name of the Broadband Router: Enter the host name of the router. Default is home.gateway.
Domain name of the LAN network: Enter the domain name of the LAN network. home.gateway.

Print Server

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 This allows you to print from any location on your network.

Note: Only USB printers are supported

Setup of the printer is a 3 step process (for example)
Connect the printer to the 's USB port
Enable the print server on the TW-EAV510
Install the printer drivers on the PC you want to print from

Print Server settings

This page allows you to enable / disable printer support.

☒ Enable on-board print server.

Printer name

Example:

The settings for Windows

Select a shard printer by name

<http://192.168.0.254:631/printers/TW-EAV510AC>

The settings for MAC

Select a shard printer by name

Address: 192.168.0.254

Protocol: Internet Printing Protocol - IPP

Queue: printers/TW-EAV510AC

Use: Please choose your printer here. The router doesn't support Generic PostScript Printer.

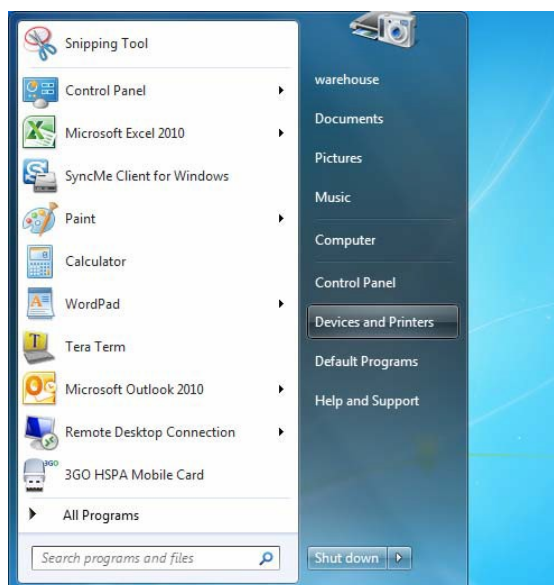
Enable on-board Print Server: Check Enable to activate the print server

Printer Name: Enter the Printer name, for example, OfficePrinter

Click Apply

Set up of Printer client (Windows 7)

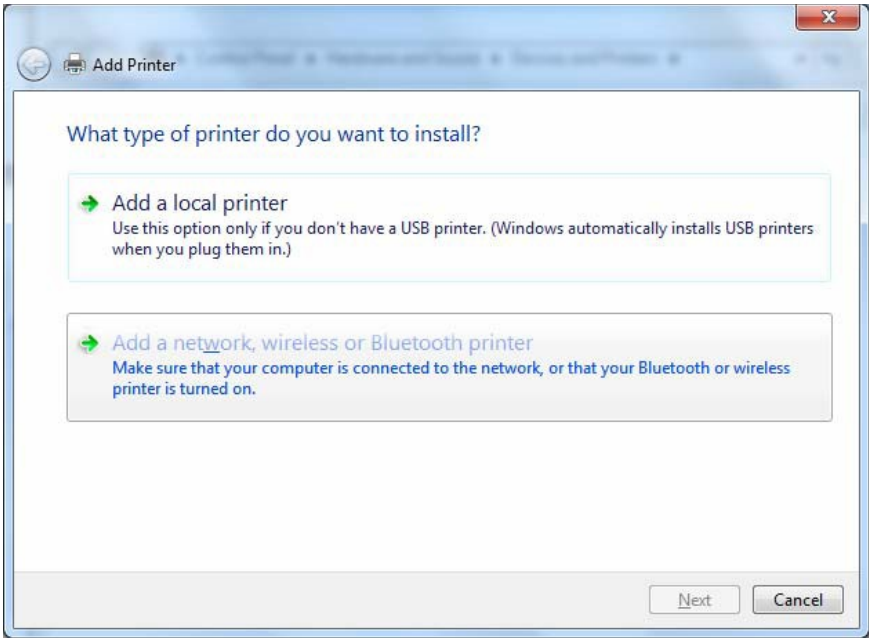
Step 1: Click Start and select "Devices and Printers"



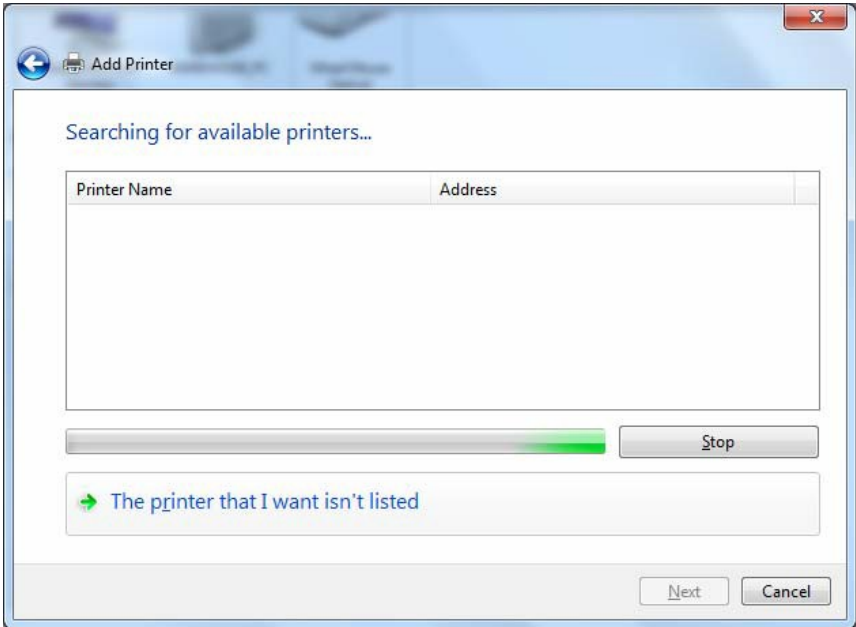
Step 2: Click "Add a Printer".



Step 3: Click "Add a network, wireless or Bluetooth printer



Step 4: Click "The printer that I want isn't listed"

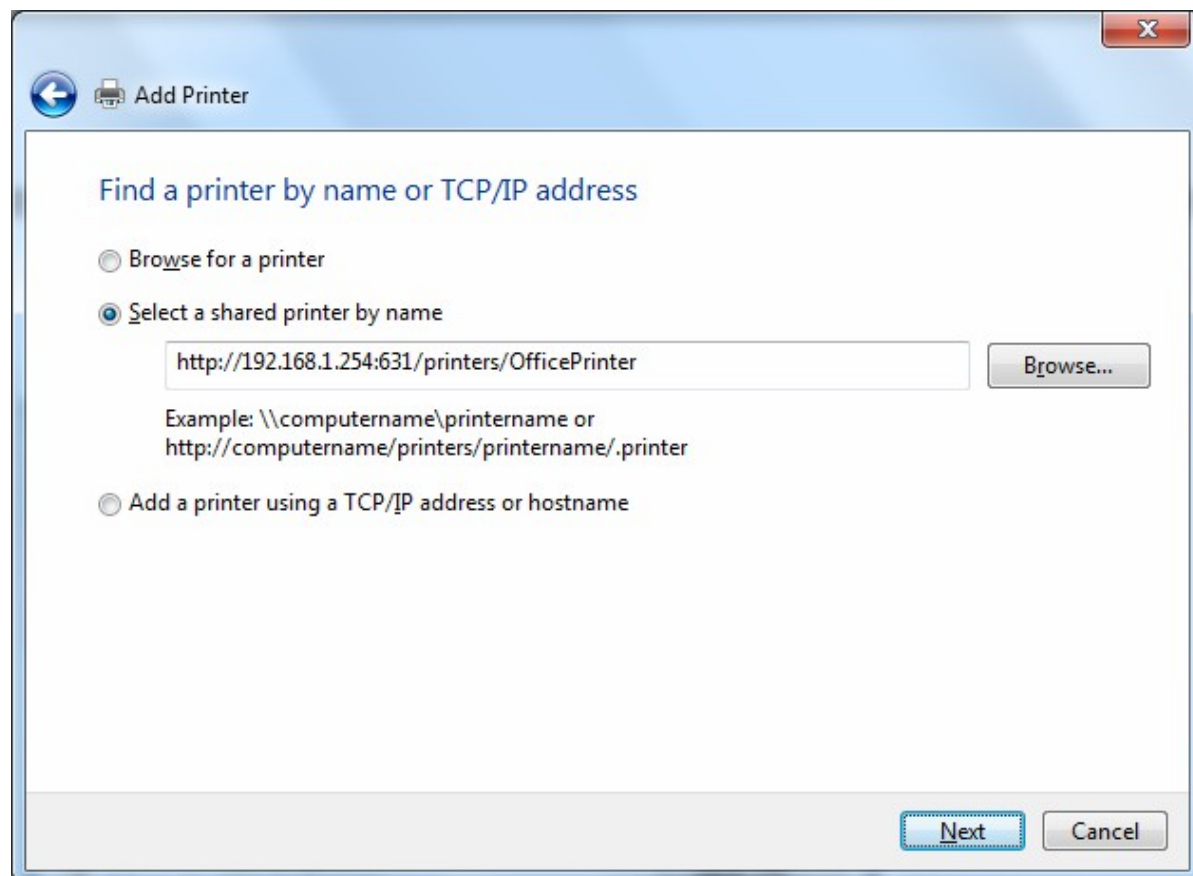


Step 5: Select “Select a shared printer by name”

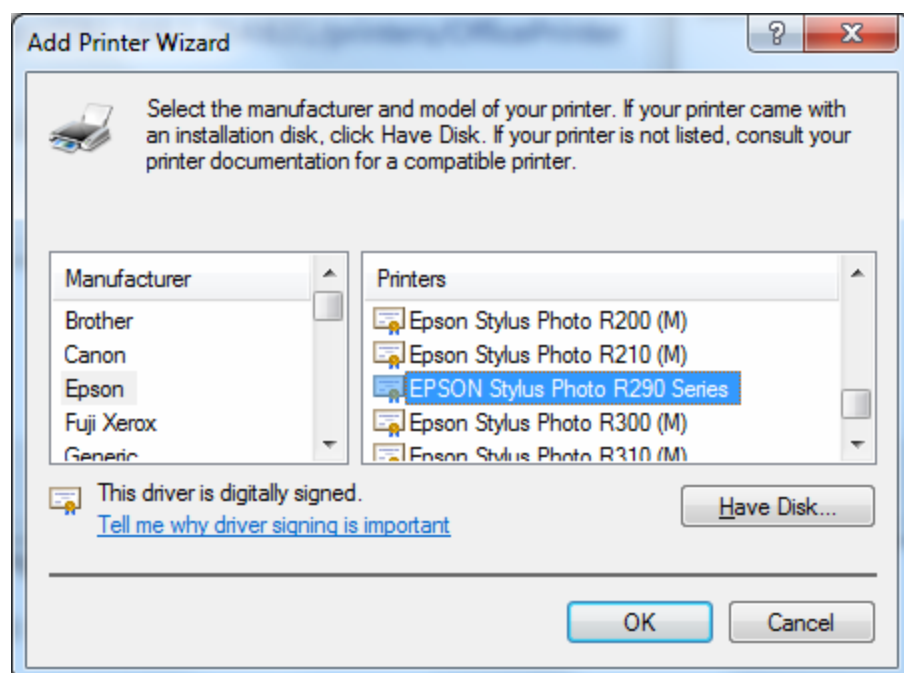
Enter http://- LAN-IP:631/printers/printer-name or. Make sure printer’s name is the same as what you set in the earlier

For Example: http://192.168.0.254:631/printers/OfficePrinter

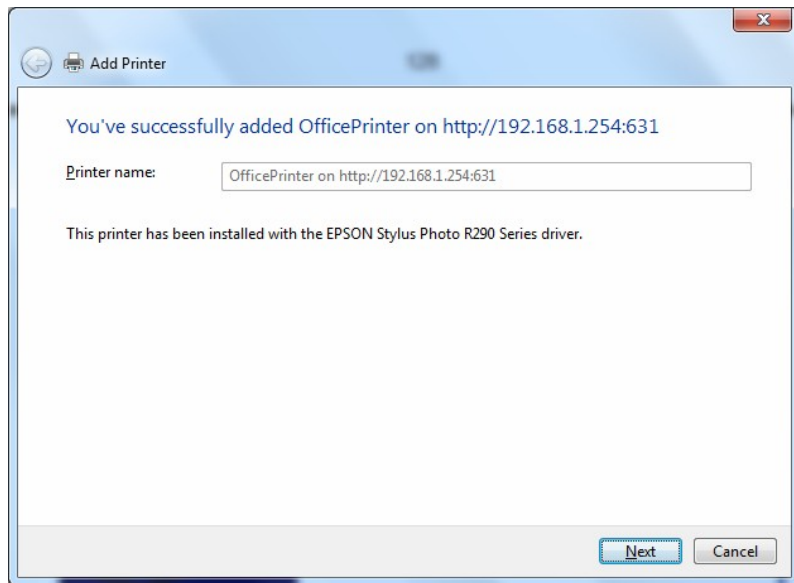
OfficePrinter is the Printer Name we setup earlier



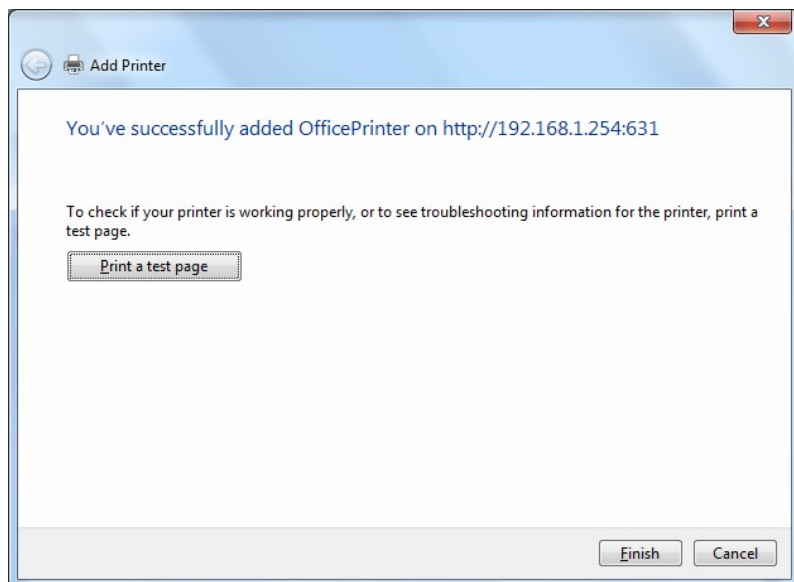
Step 6: Click “Next” to add the printer driver. If your printer is not listed and your printer came with an installation disk, click “Have Disk” find it and install the driver.



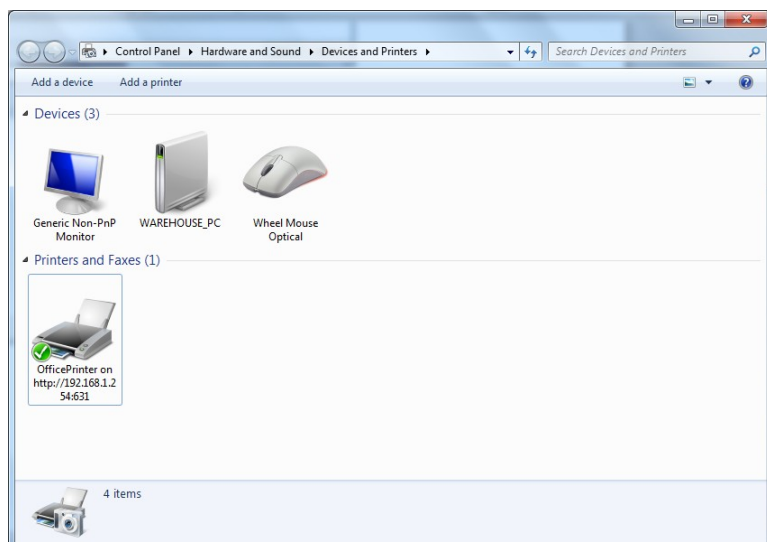
Step 7: Click “Next”



Step 8: Click “Next” and you are done



You will now be able to see your printer on the Devices and Printers Page



Storage Service

The Storage service allows you to use Storage devices with modem to be more easily accessed .

| Volumename | FileSystem | Total Space | Used Space | Unmount |
|------------|------------|-------------|------------|--|
| disk1_1 | fat | 3810 | 1064 | <input type="button" value="Unmount"/> |

Volume Name: Display the storage volume name

FileSystem: Display the storage device's file system format, well-known is FAT.

Total Space: Display the total space of the storage, with unit MB.

Used Space: Display the remaining space of each partition, unit MB.

Unmount: Click Unmount button if you want to uninstall the USB device. Please Note that first click Unmount before you uninstall your USB storage.

User Account

Users here can add user accounts for access to the storage, in this way users can access the network sharing storage with the specified account, and again protect their own data.

Default user admin.

Click Add button, enter the user account-adding page:

Storage User Account Setup

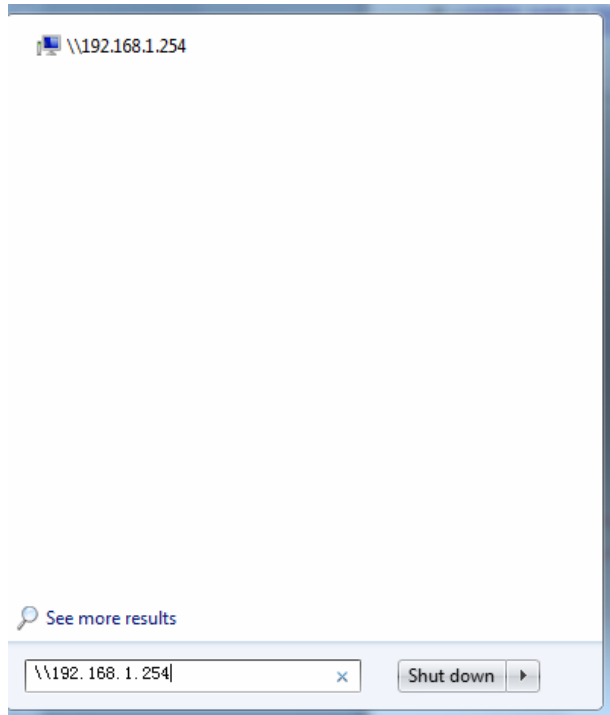
In the boxes below, enter the user name, password and volume name on which the home directory is to be created.

| | |
|-------------------|--------------------------|
| Username: | <input type="text"/> |
| Password: | <input type="password"/> |
| Confirm Password: | <input type="password"/> |
| Volumename: | <input type="text"/> |

- Username:** user-defined name, but simpler and more convenient to remember would be favorable.
- Password:** Set the password.
- Confirm Password:** Reset the password for confirmation.
- Volume Name:** Set Volume name, as to create access to the volume of the specified partition of the storage.

Accessing mechanism of Storage:

In your computer, Click Start > Run, enter [\\192.168.0.254](#)

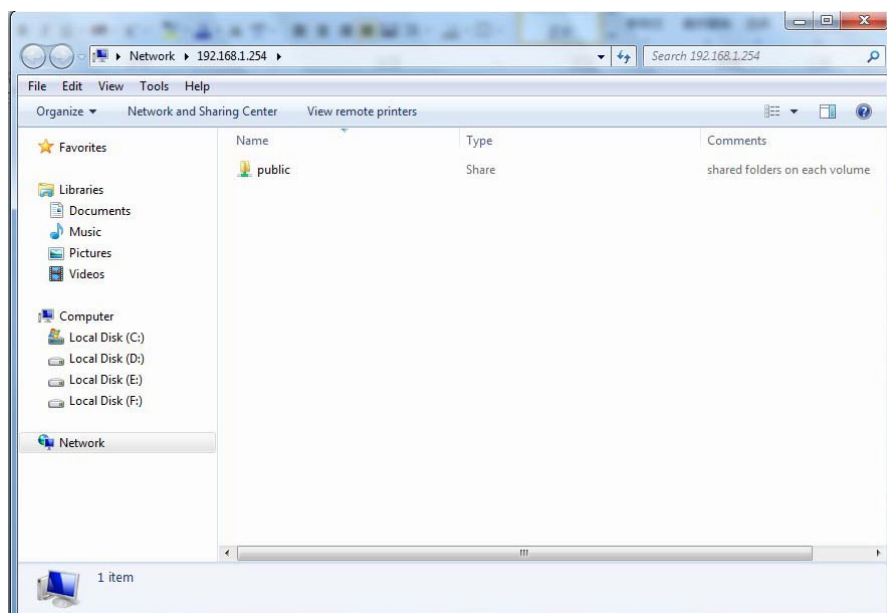


When accessing the network storage, you can see a folder named “public”, users should have the account to enter, and the account can be set at the User Accounts section.

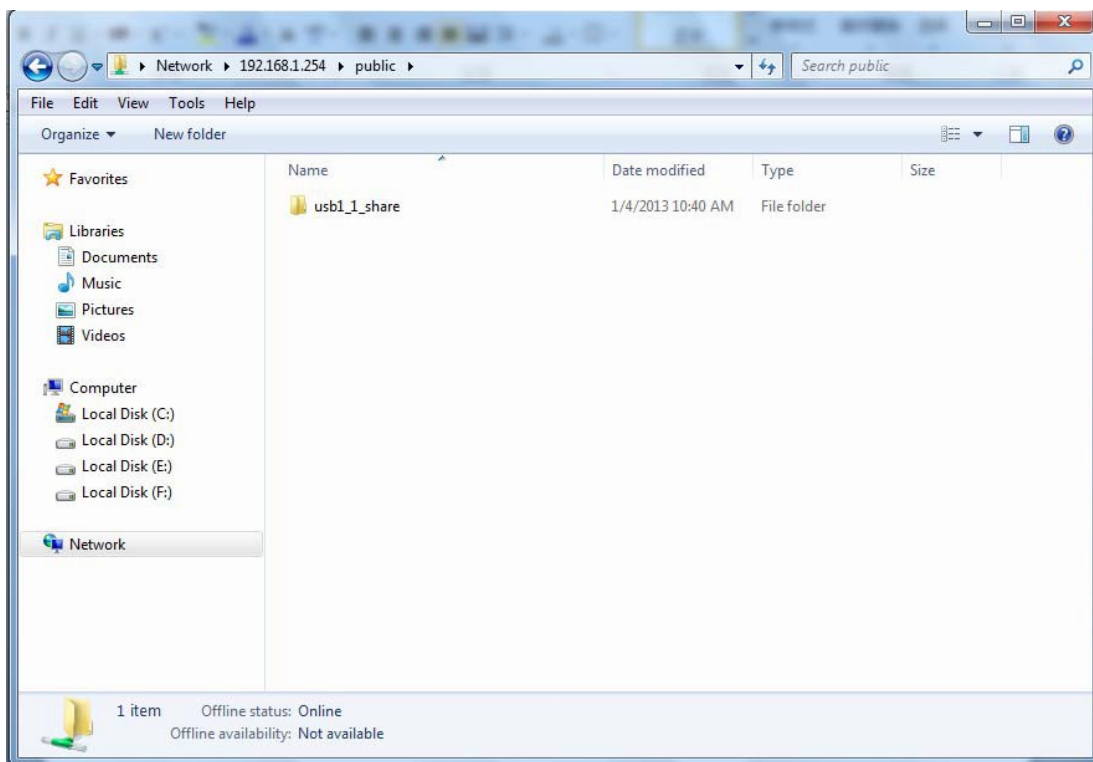
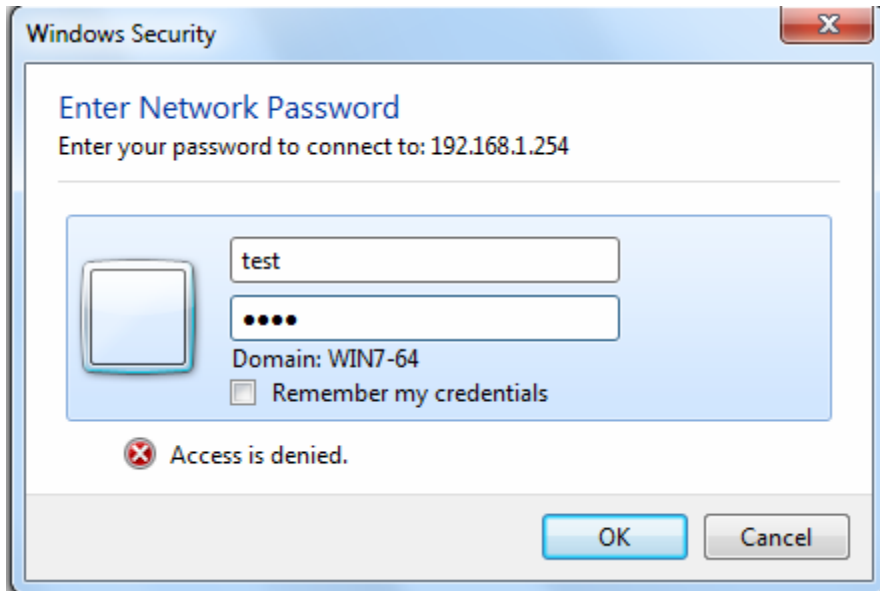
When first logged on to the network folder, you will see the “public” folder.

Public: The public sharing space for each user in the USB Storage.

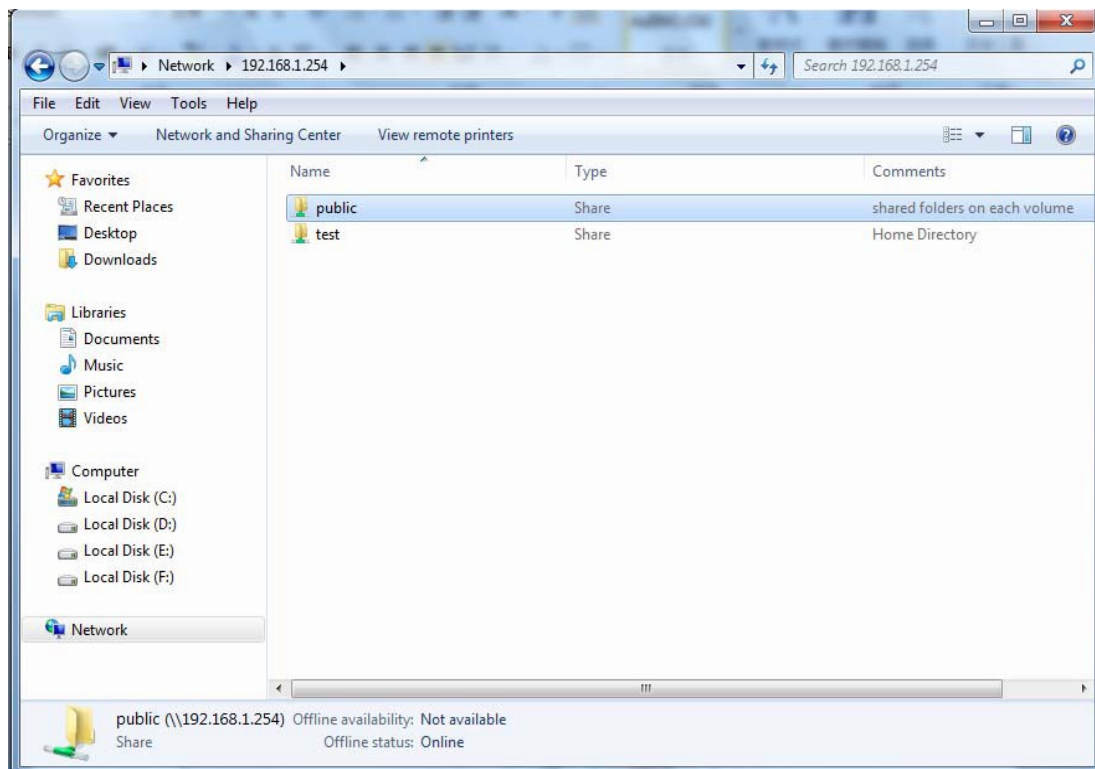
When user register a USB account and log successfully, a private folder (the same name as the user account registered) exclusive for each user is established. Go on to see the details.



Access the folder public.



When successfully accessed, the private folder of each user is established, and user can see from the following picture. The test fold in the picture is the private space for each user.



Interface Grouping

Interface grouping is a function to group interfaces, known as VLAN. A Virtual LAN, commonly known as a VLAN, 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. A VLAN has the same attributes as a physical LAN, but it allows for end stations to be grouped together even if they are not located on the same network switch.

Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button.

Interface Grouping -- Maximum entries: 16

Interface Grouping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.

☐ Enable Isolation

| Group Name | Remove | WAN Interface | LAN Interfaces | DHCP Vendor IDs |
|------------|--------|---------------|-----------------------|-----------------|
| Default | | atm0.1 | LAN1 | |
| | | atm1.1 | LAN2 | |
| | | atm2.2 | LAN3 | |
| | | eth4.1 | LAN4 | |
| | | ptm0.1 | TW-EAV510-2.4GHz-EFB2 | |
| | | ptm0.3 | TW-EAV510-5GHz-EFB3 | |

Enable Isolation: If enabled, devices in one group are not able to access those in the other group.

Click Add to add groups.

IMPORTANT If a vendor ID is configured for a specific client device, please **REBOOT** the client device attached to the modem to allow it to obtain an appropriate IP address.

Group Name:

Grouped WAN Interfaces



Available WAN Interfaces

ipoe_0_0_33/atm0.1
ipoe_0_0_100/atm1.1
ipoe_0_0_35/atm2.2
ipoe_0_1_1/ptm0.1
ipoe_0_1_1.252/ptm0.3
ipoe_eth4/eth4.1

Grouped LAN Interfaces



Available LAN Interfaces

LAN1
LAN2
LAN3
LAN4
TW-EAV510-2.4GHz-EFB2
TW-EAV510-5GHz-EFB3

Automatically Add Clients With
the following DHCP Vendor IDs

Group Name: Type a group name.

Grouped WAN Interfaces: Select from the box the WAN interface you want to applied in the group.

Grouped LAN Interfaces: Select the LAN interfaces you want to group as a single group from Available LAN Interfaces.

Automatically Add Clients with following DHCP Vendor IDs: Enter the DHCP Vendor IDs for which you want the Clients automatically added into the group. DHCP vendor ID (DHCP 60) is an Authentication for DHCP Messages.

Click Apply to confirm your settings and your added group will be listed in the Interface Grouping table.

If you want to remove the group, check the box as the following and press Remove.

IP Tunnel

An IP Tunnel is an Internet Protocol (IP) network communication channels between two networks of different protocols. It is used to transport another network protocol by encapsulation of its packets.

IP Tunnels are often used to connect two disjoint IP networks that do not have a native routing path to each other, via an underlying routable protocol across an intermediate transport network, like VPN.

Another prominent use of IP Tunnel is to connect islands of IPv6 installations across the IPv4 internet.

IPv6inIPv4

6in4 is an Internet transition mechanism for migrating from IPv4 to IPv6. 6in4 uses tunneling to encapsulate IPv6 traffic over explicitly configured IPv4 links. The 6in4 traffic is sent over the IPv4 Internet inside IPv4 packets whose IP headers have the IP Protocol number set to 41. This protocol number is specifically designated for IPv6 capsulation.

6RD:

6RD is a mechanism to facilitate IPv6 rapid deployment across IPv4 infrastructures of internet service providers (ISPs).

It is derived from 6to4, a preexisting mechanism to transporting IPv6 packets over IPv4 infrastructure network, with the significant change that it operates entirely within the enduser's ISP network, thus avoiding the major architectural problems inherent in the original design of 6to4.

Click Add button to manually add the 6in4 rules.

IP Tunneling -- 6in4 Tunnel Configuration

Currently, only 6rd configuration is supported.

| | |
|---|------------------------|
| Tunnel Name | <input type="text"/> |
| Mechanism: | 6RD ▼ |
| Associated WAN Interface: | <input type="text"/> ▼ |
| Associated LAN Interface: | LAN/br0 ▼ |
| <input checked="" type="radio"/> Manual <input type="radio"/> Automatic | |
| IPv4 Mask Length: | <input type="text"/> |
| 6rd Prefix with Prefix Length: | <input type="text"/> |
| Border Relay IPv4 Address: | <input type="text"/> |
| <input type="button" value="Apply/Save"/> | |

Tunnel Name: User-defined name.

Mechanism: Here only 6RD.

Associated WAN Interface: The applied WAN interface with the set tunnel, thus when there are packets from/to the WAN interface, the tunnel would be used to transport the packets.

Associated LAN Interface: Set the linked LAN interface with the tunnel.

Manually configured or **automatically** configured. If manually, please fill out the following 6rd parameters.

IPv4 Mask Length: Specify the length of IPv4 address carried in IPv6 prefix, for example, 0 means to carry all the 32 bits of IPv4 address while 8 carries 24 bits of the IPv4 address.

6rd Prefix with Prefix Length: Enter the 6rd prefix and prefix length you uniquely designate to 6rd by the ISP(The 6rd prefix and prefix length are to replace the standard 6to4 prefix 2002::/16 by an IPv6 prefix that belongs to the ISP-assigned.)

Border Relay IPv4 Address: The IPv4 address of the border relay. The relay is used to unwrap capsulated IPv4 packets into IPv6 packets and send them to the IPv6 network.

IPv4inIPv6

4in6 refers to tunneling of IPv4 in IPv6. It is an inherent internet interoperation mechanism allowing IPv4 to be used in an IPv6 only network.

4in6 uses tunneling to encapsulate IPv4 traffic over configured IPv6 tunnels. 4in6 tunnels are usually manually configured but they can be automated using protocols such as TSP to allow easy connection to a tunnel broker.

DS – Lite

DS –Lite, or Dual-Stack Lite, is designed to let an ISP omit the deployment of any IPv4 address to the customer's CPE. Instead, only global IPv6 addresses are provided (Regular Dual-Stack Lite deploys global addresses for both IPv4 and IPv6).

The CPE distributes private IPv4 addresses for the LAN clients, the same as a NAT device. The subnet information is chosen by the customer, identically to the NAT model. However, instead of performing the NAT itself, the CPE encapsulates the IPv4 packet inside an IPv6 packet.

Click Add button to manually add the 4in6 rules.

IP Tunneling -- 4in6 Tunnel Configuration

Currently, only DS-Lite configuration is supported.

| | |
|---|------------------------|
| Tunnel Name | <input type="text"/> |
| Mechanism: | DS-Lite ▼ |
| Associated WAN Interface: | <input type="text"/> ▼ |
| Associated LAN Interface: | LAN/br0 ▼ |
| <input checked="" type="radio"/> Manual <input type="radio"/> Automatic | |
| AFTR: | <input type="text"/> |
| <input type="button" value="Apply/Save"/> | |

Tunnel Name: User-defined tunnel name.

Mechanism: It is the 4in6 tunnel operation technology. Please select DS-Lite.

Associated WAN Interface: The applied WAN interface with the set tunnel, and when there are packets from/to the WAN interface, the tunnel would be used to transport the packets.

Associated LAN Interface: Specify the linked LAN interface with the tunnel.

VPN

Note: Please make sure that both LAN side networks are in different subnet.

PPTP Server

Make “**Enable PPTP Server**” checkbox checked. And you will see the page as below:

PPTP Server

☒ Enabled PPTP Server

☒ Enable MPPE

Assigned to Peer IP Address start from: 192.168.20.

Inactivity Timeout (minutes) [0-120]:

Apply/Save

Enabled PPTP Server: Make it checked to enable PPTP Server function.

Enable MPPE: Enable the Microsoft Point-to-Point Encryption (MPPE) encrypts data in Point-to-Point Tunneling Protocol (PPTP) virtual private network (VPN) connections when checked. Your PPTP client must support MPPE if checked.

Assigned to Peer IP Address start from: Enter the IP that will be assigned to remote client. The pool range is the value you entered + 3 (192.168.20.10~192.168.20.13), totally 4 IP addresses. Please make this pool out of DHCP Server Pool.

Inactivity Timeout (minutes) [0-120]: Check the traffic in PPTP tunnel and disconnect the connection if no traffic after period of value you set. Default is 0 and keeps always on without checking.

Account

Account

Maximum entries: 4

| Name | Enable | Username | Connection Type | Peer IP | Peer Netmask | Remove | Edit |
|------|--------|----------|-----------------|---------|--------------|--------|------|
|------|--------|----------|-----------------|---------|--------------|--------|------|

Add

Remove

Click **Add** button to add new user. Totally support up to 4 users.

Configure Account

Name:

☒ Enable

Username:

Password:

Connection Type: ☐ Remote Access ☒ LAN TO LAN

Peer IP:

Peer Netmask:

Name: The name for user profile.

Enable: Enable/Disable this account.

Username: The name will be used for authentication.

Password: The password will be used for authentication.

Connection Type: Setup connection to Remote Access or LAN to LAN.

Remote Access - Limited your remote PPTP Client as one of clients at local network. The remote client can have full access to local network, but any clients at local network cannot access to remote client's network.

LAN to LAN - The clients at both local/remote network can access each other.

Peer IP: Enter the remote network's IP address.

Peer Netmask: Enter the remote network's netmask.

Account

Maximum entries: 4

| Name | Enable | Username | Connection Type | Peer IP | Peer Netmask | Remove | Edit |
|-------|--------|----------|-----------------|-------------|---------------|-------------------------------------|-------------------------------------|
| test1 | Enable | test1 | LAN TO LAN | 192.168.0.0 | 255.255.255.0 | <input checked="" type="checkbox"/> | <input type="button" value="Edit"/> |

Make Remove checkbox checked and click **Remove** button to remove user or click **Edit** button to edit the details of user.

Client

PPTP Client

Maximum entries: 4

| Name | Local Gateway Interface | Remote Gateway | Username | MPPE | Connection Type | Peer IP | Peer Netmask | Enable | Remove | Edit |
|------|-------------------------|----------------|----------|------|-----------------|---------|--------------|--------|--------|------|
|------|-------------------------|----------------|----------|------|-----------------|---------|--------------|--------|--------|------|

Click **Add** button to add a new PPTP Client connection.

Configure PPTP Client

| | |
|---|---|
| Name: | <input type="text" value="Office"/> |
| <input checked="" type="checkbox"/> Enable | |
| Local Gateway Interface: | <input type="text" value="ipoe_eth4/eth4.1"/> |
| Remote Gateway: | <input type="text" value="10.0.0.254"/> |
| Username: | <input type="text" value="test1"/> |
| Password: | <input type="password" value="*****"/> |
| <input checked="" type="checkbox"/> Enable MPPE | |
| Connection Type: | <input type="radio"/> Remote Access <input checked="" type="radio"/> LAN TO LAN |
| Peer IP: | <input type="text"/> |
| Peer Netmask: | <input type="text"/> |

Name: The name for PPTP Client profile.

Enable: Enable/Disable this profile.

Local Gateway Interface: Select the correct WAN interface that will be used to access to remote network.

Remote Gateway: Enter the IP/Domain address of remote PPTP Server.

Username: The name will be used for authentication.

Password: The password will be used for authentication.

Enable MPPE: Enable the Microsoft Point-to-Point Encryption (MPPE) encrypts data in Point-to-Point Tunneling Protocol (PPTP) virtual private network (VPN) connections when checked. Your PPTP Server must support MPPE if checked.

Connection Type: Setup connection to Remote Access or LAN to LAN.

Remote Access - Make your router as one of clients at remote network. You can have full access to remote network, but remote network cannot access to any client at your local network.

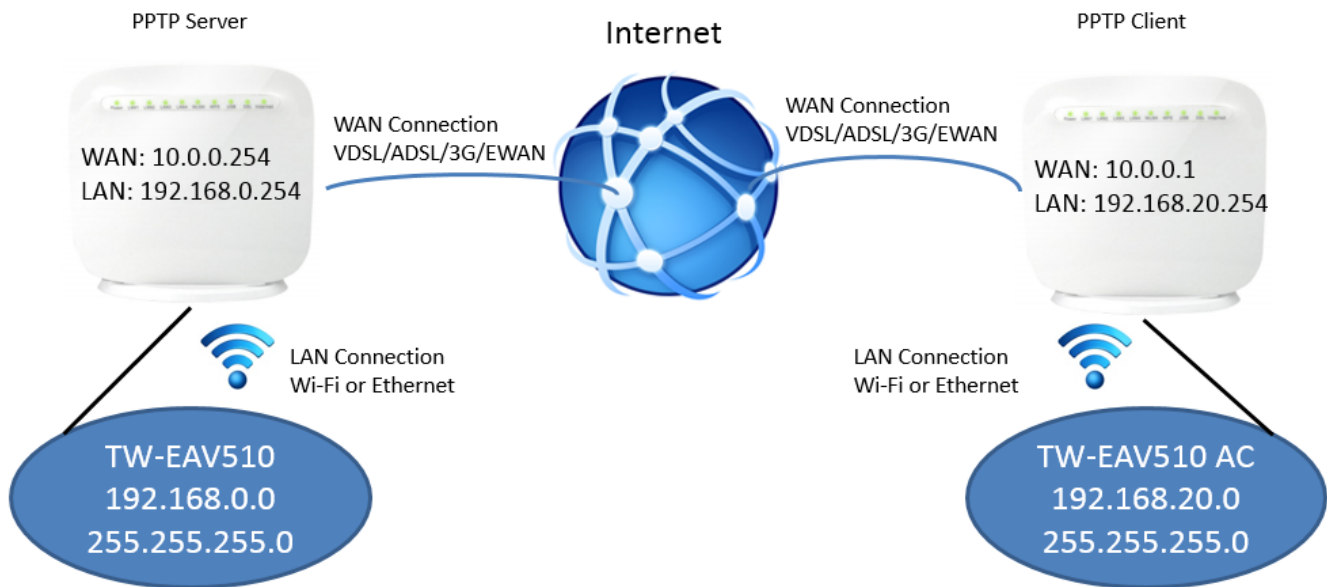
LAN to LAN - The clients at both local/remote network can access each other.

Peer IP: Enter the remote network's IP address.

Peer Netmask: Enter the remote network's netmask.

PPTP Example 1

TW-EAV510 is activated as PPTP Server and TW-EAV510 AC is activated as PPTP Client.



REMOTE ACCESS

TW-EAV510 (PPTP Server)

1. Go to **Advanced Setup** -> **VPN** -> **PPTP**, enable the PPTP Server and do the settings as below. Click **Apply/Save** button to save changes.

PPTP Server

☒ Enabled PPTP Server

☒ Enable MPPE

Assigned to Peer IP Address start from: 192.168.0.100

Inactivity Timeout (minutes) [0-120]: 0

Apply/Save

2. Go to **Advanced Setup** -> **VPN** -> **Account**, add a new user for login.

Configure Account

Name:

☒ Enable

Username:

Password:

Connection Type: ☒ Remote Access ☐ LAN TO LAN

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

Account

Maximum entries: 4

| Name | Enable | Username | Connection Type | Peer IP | Peer Netmask | Remove | Edit |
|------|--------|----------|-----------------|---------|--------------|--------------------------|-------------------------------------|
| test | Enable | test | Remote Access | | | <input type="checkbox"/> | <input type="button" value="Edit"/> |

TW-EAV510 AC (PPTP Client)

1. Go to **Advanced Setup** -> **VPN** -> **PPTP Client**, click **Add** button to add a new PPTP connection.

Configure PPTP Client

Name:

☒ Enable

Local Gateway Interface:

Remote Gateway:

Username:

Password:

☒ Enable MPPE

Connection Type: ☒ Remote Access ☐ LAN TO LAN

Click **Apply/Save** button to save account settings.

PPTP Client

Maximum entries: 4

| Name | Local Gateway Interface | Remote Gateway | Username | MPPE | Connection Type | Peer IP | Peer Netmask | Enable | Remove | Edit |
|-----------|-------------------------|----------------|----------|--------|-----------------|---------|--------------|-------------------------------------|--------------------------|-------------------------------------|
| PPTP-Test | eth4.1 | 10.0.0.254 | test | Enable | Remote Access | | | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="button" value="Edit"/> |

2. Go to **Device Info -> VPN -> Client Info** to check connection status. You can also click **Disconnect** button to disconnect the PPTP connection.

Device Info -- Client Info

| Name | Enable | Status | Connection Type | Remote Gateway | Peer IP | Client IP | Action |
|-----------|---------|-----------|-----------------|----------------|---------------|---------------|---|
| PPTP-Test | Enabled | Connected | Remote Access | 10.0.0.254 | 192.168.0.254 | 192.168.0.100 | <input type="button" value="Disconnect"/> |

When **Status** shows **Connected**, you can now access to remote network.

Below is Server Info for reference.

Device Info -- Server Info

| Name | Enable | Status | Connection Type | Peer IP | Connected By | Action |
|------|---------|-----------|-----------------|---------------|--------------|---|
| test | Enabled | Connected | Remote Access | 192.168.0.100 | 10.0.0.1 | <input type="button" value="Disconnect"/> |

LAN to LAN

TW-EAV510 (PPTP Server)

1. Go to **Advanced Setup -> VPN -> PPTP**, enable the PPTP Server and do the settings as below. Click **Apply/Save** button to save changes.

PPTP Server

☒ Enabled PPTP Server

☒ Enable MPPE

Assigned to Peer IP Address start from: 192.168.0.

Inactivity Timeout (minutes) [0-120]:

2. Go to **Advanced Setup -> VPN -> Account**, add a new user for login. The different with Remote Access is you need to enter peer network information.

Configure Account

Name:

☒ Enable

Username:

Password:

Connection Type: ☐ Remote Access ☒ LAN TO LAN

Peer IP:

Peer Netmask:

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

Account

Maximum entries: 4

| Name | Enable | Username | Connection Type | Peer IP | Peer Netmask | Remove | Edit |
|------|--------|----------|-----------------|--------------|---------------|--------------------------|-------------------------------------|
| test | Enable | test | LAN TO LAN | 192.168.20.0 | 255.255.255.0 | <input type="checkbox"/> | <input type="button" value="Edit"/> |

TW-EAV510 AC (PPTP Client)

1. Go to **Advanced Setup** -> **VPN** -> **PPTP Client**, click **Add** button to add a new PPTP connection. For LAN to LAN, you need to enter peer network information.

Configure PPTP Client

Name:

☒ Enable

Local Gateway Interface:

Remote Gateway:

Username:

Password:

☒ Enable MPPE

Connection Type: ☐ Remote Access ☒ LAN TO LAN

Peer IP:

Peer Netmask:

Click **Apply/Save** button to save account settings.

PPTP Client

Maximum entries: 4

| Name | Local Gateway Interface | Remote Gateway | Username | MPPE | Connection Type | Peer IP | Peer Netmask | Enable | Remove | Edit |
|-----------|-------------------------|----------------|----------|--------|-----------------|-------------|---------------|-------------------------------------|--------------------------|------|
| PPTP-Test | eth4.1 | 10.0.0.254 | test | Enable | LAN TO LAN | 192.168.0.0 | 255.255.255.0 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | Edit |

2. Go to **Device Info -> VPN -> Client Info** to check connection status. You can also click **Disconnect** button to disconnect the PPTP connection.

Device Info -- Client Info

| Name | Enable | Status | Connection Type | Remote Gateway | Peer IP | Client IP | Action |
|-----------|---------|-----------|-----------------|----------------|-------------|---------------|------------|
| PPTP-Test | Enabled | Connected | LAN TO LAN | 10.0.0.254 | 192.168.0.0 | 192.168.0.100 | Disconnect |

When **Status** shows **Connected**, both local and remote network can access each other.

Below is Server Info for reference.

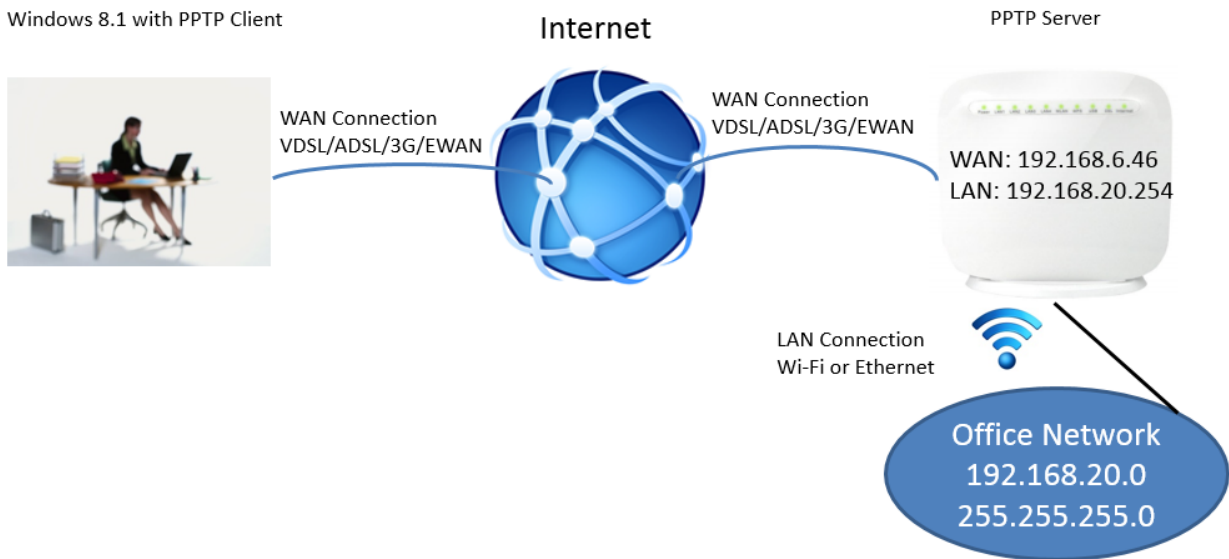
Device Info -- Server Info

| Name | Enable | Status | Connection Type | Peer IP | Connected By | Action |
|------|---------|-----------|-----------------|--------------|--------------|------------|
| test | Enabled | Connected | LAN TO LAN | 192.168.20.0 | 10.0.0.1 | Disconnect |

PPTP Example 2

TW-EAV510 is activated as PPTP Server and Windows 8.1 is activated as PPTP Client for Remote Access.

Windows 8.1 with PPTP Client



TW-EAV510 (PPTP Server)

- 1. Go to **Advanced Setup -> VPN -> PPTP**, enable the PPTP Server and do the settings as below. Click **Apply/Save** button to save changes.

PPTP Server

☒ Enabled PPTP Server

☒ Enable MPPE

Assigned to Peer IP Address start from: 192.168.20.

Inactivity Timeout (minutes) [0-120]:

Apply/Save

- 2. Go to **Advanced Setup -> VPN -> Account**, add a new user for login.

Configure Account

Name:

☒ Enable

Username:

Password:

Connection Type: ☒ Remote Access ☐ LAN TO LAN

Apply/Save

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

Account

Maximum entries: 4

| Name | Enable | Username | Connection Type | Peer IP | Peer Netmask | Remove | Edit |
|------|--------|----------|-----------------|---------|--------------|--------------------------|------|
| Test | Enable | test | Remote Access | | | <input type="checkbox"/> | Edit |

Add Remove

Windows 8/8.1 (PPTP Client)

- 1. Go to **Control Panel -> View network status and tasks**, click **Setup a new connection or network** to add a new PPTP connection.

Change your networking settings



Set up a new connection or network

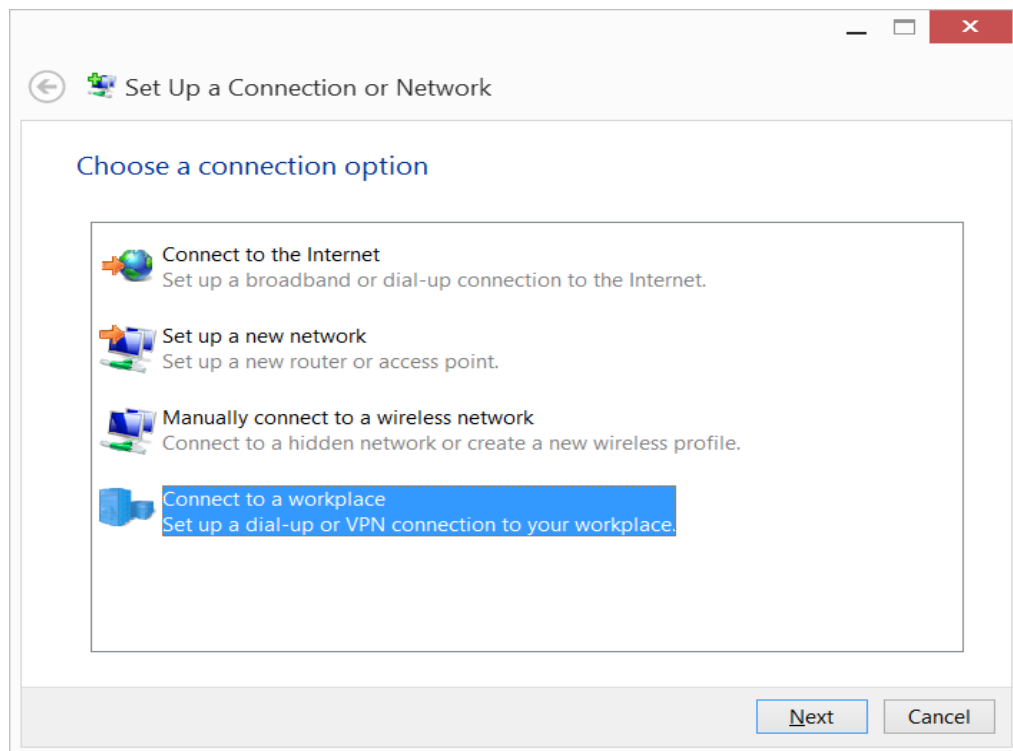
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.



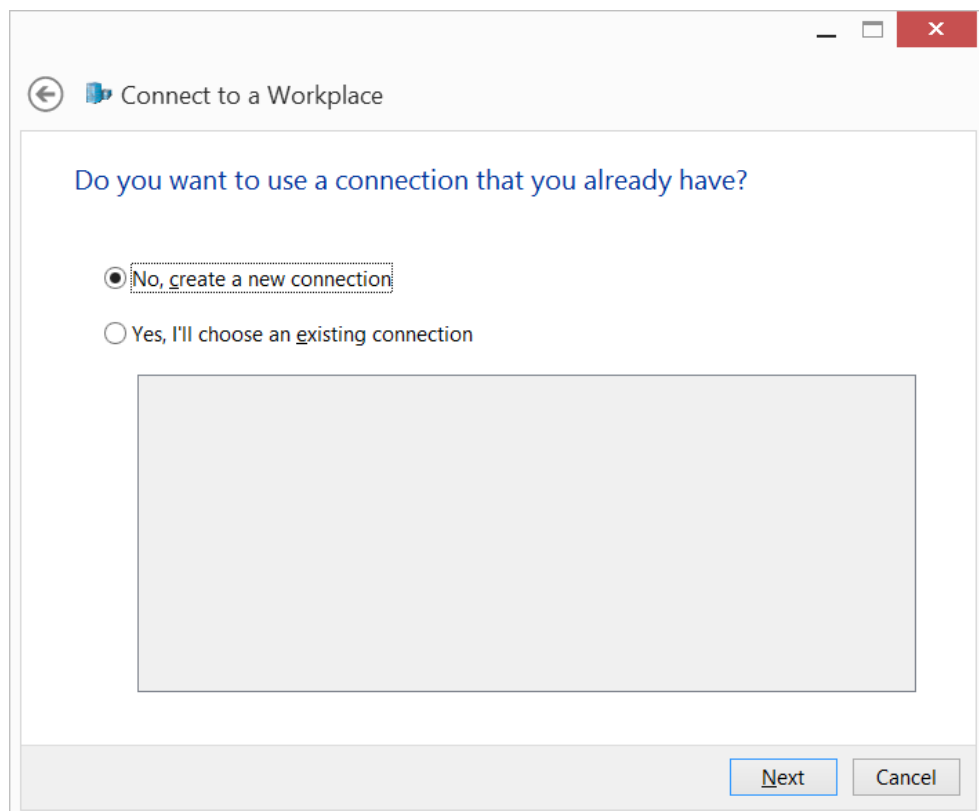
Troubleshoot problems

Diagnose and repair network problems, or get troubleshooting information.

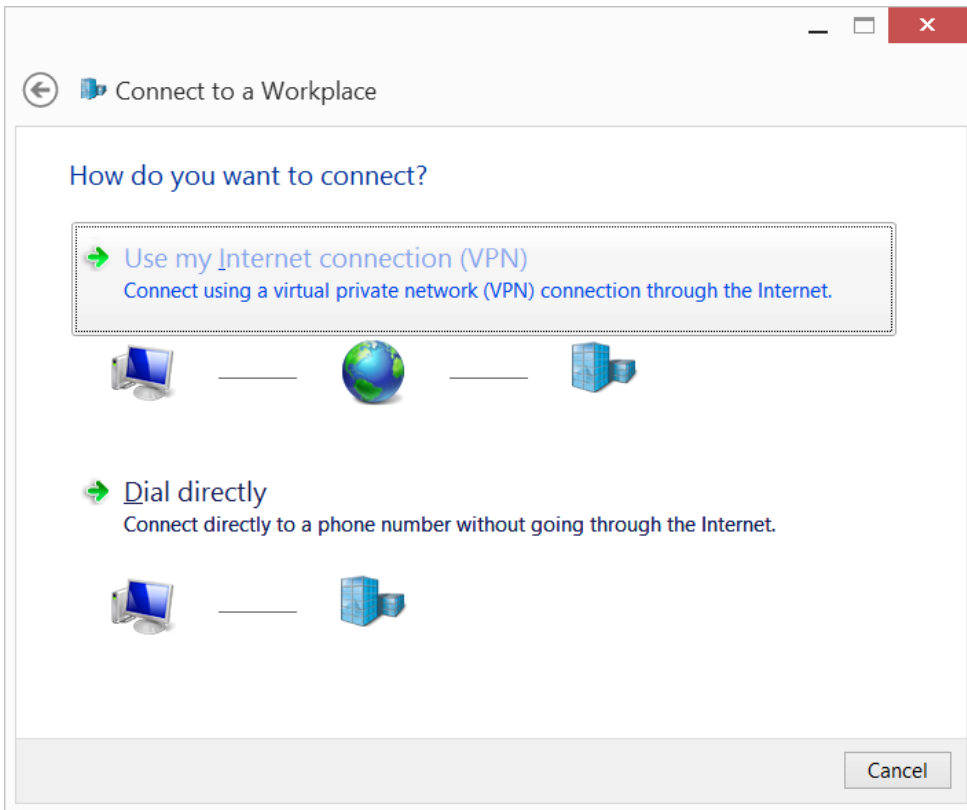
2. Select **Connect to a workplace**.



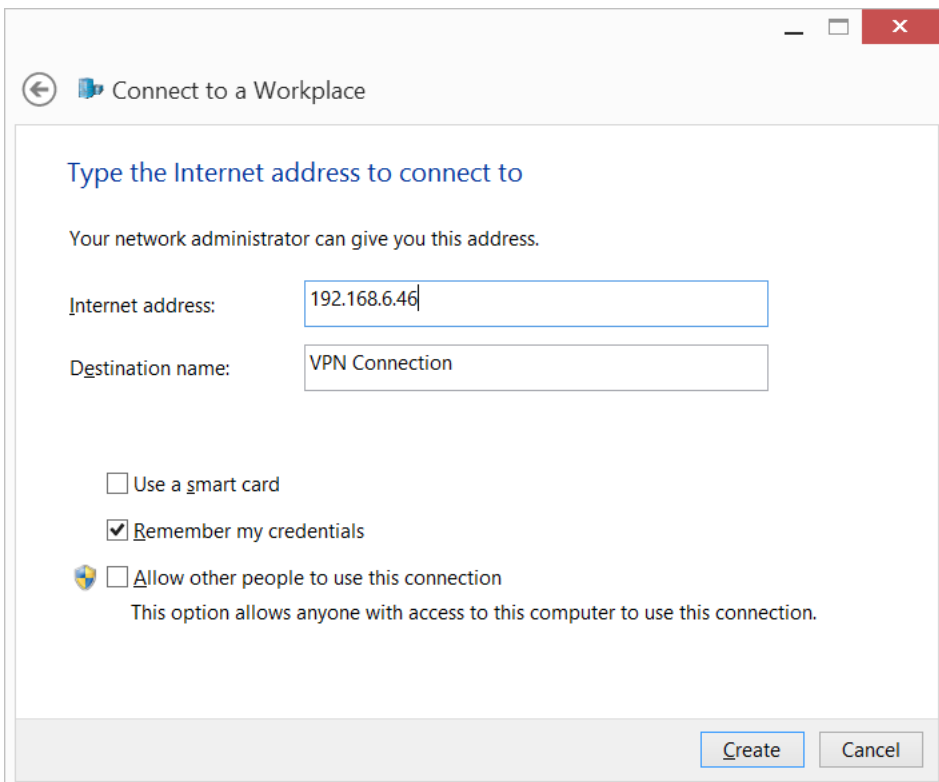
3. Select **No, create a new connection** and click **Next** button for next step.



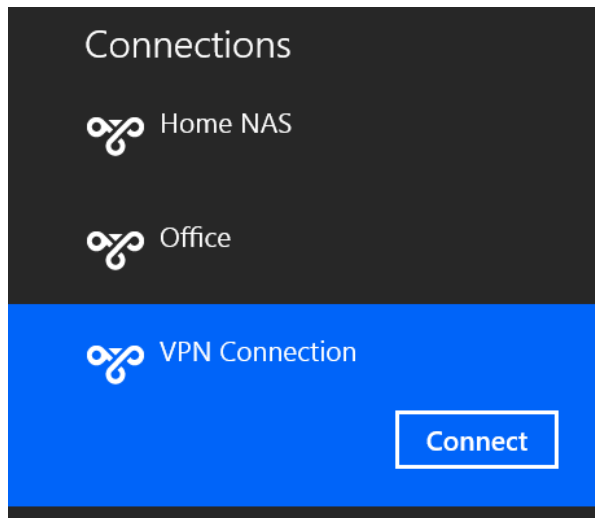
4. Select **Use my Internet connection (VPN)**.



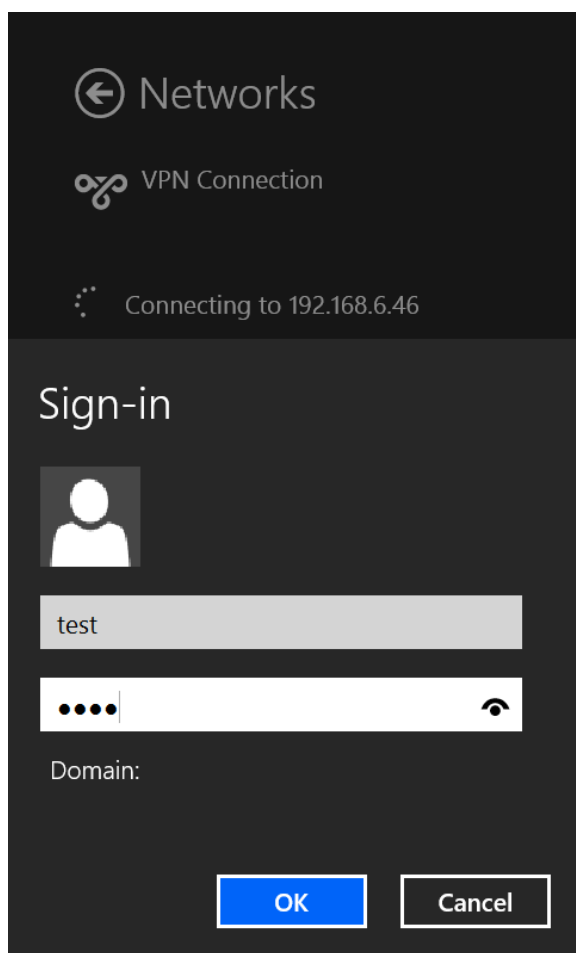
5. Enter the PPTP Server address/domain to field named **Internet address**. Please make sure your domain name address is work correctly if you are use domain name instead of IP address. Click **Create** button finish the PPTP client settings on Windows 8.1.



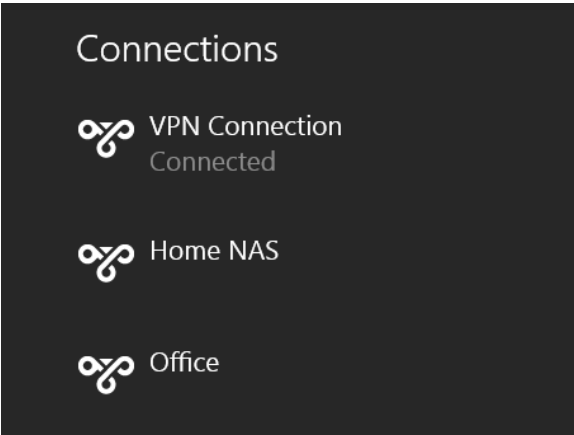
- Click the Network icon at the lower right corner. You can find the **VPN Connection** that we just created under **Connections**, click **Connect** button to enter the username and password.



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



Connected



Once connected, you can also see the connection status as below on TW-EAV510/510AC’s WEB GUI.

Device Info -- Server Info

| Name | Enable | Status | Connection Type | Peer IP | Connected By | Action |
|------|---------|-----------|-----------------|---------------|--------------|-----------------------------|
| Test | Enabled | Connected | Remote Access | 192.168.20.10 | 192.168.6.32 | <button>Disconnect</button> |

L2TP Server

Note: Please make sure that both LAN side networks are in different subnet.

Make “**Enable L2TP Server**” checkbox checked. And you will see the page as below:

L2TP Server

☒ Enabled L2TP Server

Assigned to Peer IP Address start from:

Inactivity Timeout (minutes) [0-120]:

☒ Tunnel Authentication

Secret:

Apply/Save

- Enabled L2TP Server:** Make it checked to enable L2TP Server function.
- Assigned to Peer IP Address start from:** Enter the IP that will be assigned to remote client. The pool range is the value you entered + 3 (192.168.20.10~192.168.20.13), totally 4 IP addresses. Please make this pool out of DHCP Server Pool and PPTP assigned IP address pool.
- Inactivity Timeout (minutes) [0-120]:** Check the traffic in L2TP tunnel and disconnect the connection if no traffic after period of value you set. Default is 0 and keeps always on without checking.
- Tunnel Authentication:** Make it checked to enable L2TP tunnel authentication. (Optional)

Secret: Once the **Tunnel Authentication** is checked, you can enter the authentication key here.

Note: Both Server and Client must use the same tunnel authentication secret key otherwise the connection 85

cannot be established.

Account

Account

Maximum entries: 4

| Name | Enable | Username | Connection Type | Peer IP | Peer Netmask | Remove | Edit |
|------|--------|----------|-----------------|---------|--------------|--------|------|
|------|--------|----------|-----------------|---------|--------------|--------|------|

Add

Remove

Click **Add** button to add new user. Totally support up to 4 users for both PPTP and L2TP.

Configure Account

Name:

test1

☒ Enable

Username:

test1

Password:

.....

Connection Type:

☐ Remote Access

☒ LAN TO LAN

Peer IP:

192.168.20.0

Peer Netmask:

255.255.255.0

Apply/Save

- Name:** The name for user profile.
- Enable:** Enable/Disable this account.
- Username:** The name will be used for authentication.
- Password:** The password will be used for authentication.
- Connection Type:** Setup connection to Remote Access or LAN to LAN.
- Remote Access** - Limited your remote L2TP Client as one of clients at local network. The remote client can have full access to local network, but any clients at local network cannot access to remote client's network.
 - LAN to LAN** - The clients at both local/remote network can access each other.
- Peer IP:** Enter the remote network's IP address.
- Peer Netmask:** Enter the remote network's netmask.

Account

Maximum entries: 4

| Name | Enable | Username | Connection Type | Peer IP | Peer Netmask | Remove | Edit |
|-------|--------|----------|-----------------|--------------|---------------|--------------------------|------|
| test1 | Enable | test1 | LAN TO LAN | 192.168.20.0 | 255.255.255.0 | <input type="checkbox"/> | Edit |

Add

Remove

Make Remove checkbox checked and click **Remove** button to remove user or click **Edit** button to edit the details of user.

Client

Go to **Advanced Setup -> VPN -> Client**.

Client

Maximum entries: 4

| Name | Type | Local Gateway Interface | Remote Gateway | Username | MPPE | Connection Type | Peer IP | Peer Netmask | Enable | Remove | Edit |
|------|------|-------------------------|----------------|----------|------|-----------------|---------|--------------|--------|--------|------|
| | | | | | | | | | | | |

Click **Add** button to add a new L2TP Client connection.

Configure Client

Name:

☒ Enable

Type: ☐ PPTP ☒ L2TP

Local Gateway Interface:

Remote Gateway:

Username:

Password:

Connection Type: ☐ Remote Access ☒ LAN TO LAN

Peer IP:

Peer Netmask:

☒ Tunnel Authentication

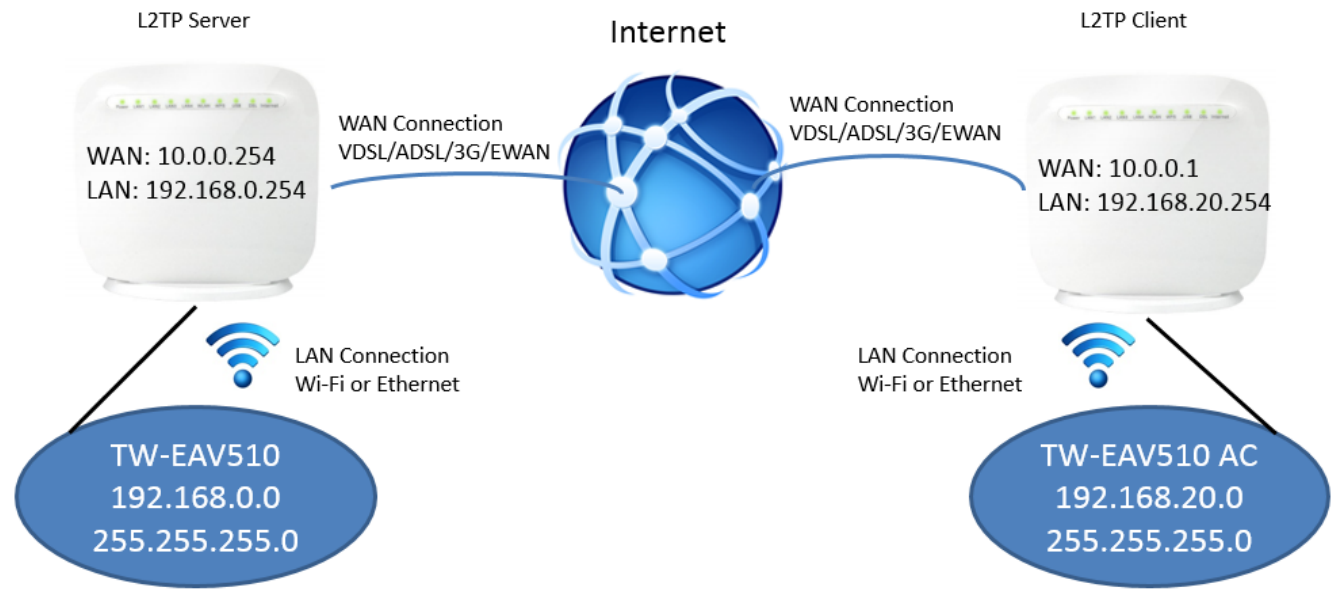
Secret:

- Name:** The name for L2TP Client profile.
- Enable:** Enable/Disable this profile.
- Type:** Setup the connection type to L2TP.
- Local Gateway Interface:** Select the correct WAN interface that will be used to access to remote network.
- Remote Gateway:** Enter the IP/Domain address of remote L2TP Server.
- Username:** The name will be used for authentication.
- Password:** The password will be used for authentication.
- Connection Type:** Setup connection to Remote Access or LAN to LAN.
- Remote Access** - Make your router as one of clients at remote network. You can have full access to remote network, but remote network cannot access to any client at your local network.
 - LAN to LAN** - The clients at both local/remote network can access each other.
- Peer IP:** Enter the remote network's IP address.
- Peer Netmask:** Enter the remote network's netmask.
- Tunnel Authentication:** Make it checked to enable L2TP tunnel authentication. (Optional)
- Secret:** Once the **Tunnel Authentication** is checked, you can enter the authentication key here.

Note: Both Server and Client must use the same tunnel authentication secret key otherwise the connection cannot be established.

L2TP Example

TW-EAV510 is activated as L2TP Server and TW-EAV510 AC is activated as L2TP Client.



REMOTE ACCESS

TW-EAV510 (L2TP Server)

Go to **Advanced Setup** -> **VPN** -> **L2TP Server**, enable the L2TP Server and do the settings as below. Click **Apply/Save** button to save changes.

L2TP Server

☒ Enabled L2TP Server

Assigned to Peer IP Address start from: 192.168.0.10

Inactivity Timeout (minutes) [0-120]: 0

☒ Tunnel Authentication

Secret: 12345678

Go to **Advanced Setup** -> **VPN** -> **Account**, add a new user for login.

Configure Account

Name:

☒ Enable

Username:

Password:

Connection Type: ☒ Remote Access ☐ LAN TO LAN

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

Account

Maximum entries: 4

| Name | Enable | Username | Connection Type | Peer IP | Peer Netmask | Remove | Edit |
|------|--------|----------|-----------------|---------|--------------|--------------------------|-------------------------------------|
| test | Enable | test | Remote Access | | | <input type="checkbox"/> | <input type="button" value="Edit"/> |

TW-EAV510 AC (L2TP Client)

Go to **Advanced Setup** -> **VPN** -> **Client**, click **Add** button to add a new L2TP connection.

Configure Client

Name:

☒ Enable

Type: ☐ PPTP ☒ L2TP

Local Gateway Interface:

Remote Gateway:

Username:

Password:

Connection Type: ☒ Remote Access ☐ LAN TO LAN

☒ Tunnel Authentication

Secret:

Click **Apply/Save** button to save account settings.

Client

Maximum entries: 4

| Name | Type | Local Gateway Interface | Remote Gateway | Username | MPPE | Connection Type | Peer IP | Peer Netmask | Enable | Remove | Edit |
|-----------|------|-------------------------|----------------|----------|---------|-----------------|---------|--------------|-------------------------------------|--------------------------|-----------------------|
| L2TP-Test | l2tp | eth4.1 | 10.0.0.254 | test | Disable | Remote Access | | | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <button>Edit</button> |

Add Enable Remove

Go to **Device Info** -> **VPN** -> **Client Info** to check connection status. You can also click **Disconnect** button to disconnect the L2TP connection.

Device Info -- Client Info

| Name | Type | Enable | Status | Connection Type | Remote Gateway | Peer IP | Client IP | Action |
|-----------|------|---------|-----------|-----------------|----------------|---------------|--------------|-----------------------------|
| L2TP-Test | l2tp | Enabled | Connected | Remote Access | 10.0.0.254 | 192.168.0.254 | 192.168.0.10 | <button>Disconnect</button> |

When **Status** shows **Connected**, you can now access to remote network.

Below is Server Info for reference.

Device Info -- Server Info

| Name | Type | Enable | Status | Connection Type | Peer IP | Connected By | Action |
|------|------|---------|-----------|-----------------|--------------|--------------|-----------------------------|
| test | l2tp | Enabled | Connected | Remote Access | 192.168.0.10 | 10.0.0.1 | <button>Disconnect</button> |

LAN TO LAN

TW-EAV510 (L2TP Server)

Go to **Advanced Setup** -> **VPN** -> **L2TP Server**, enable the L2TP Server and do the settings as below. Click **Apply/Save** button to save changes.

L2TP Server

☒ Enabled L2TP Server

Assigned to Peer IP Address start from: 192.168.0.

Inactivity Timeout (minutes) [0-120]:

☒ Tunnel Authentication

Secret:

Apply/Save

Go to **Advanced Setup** -> **VPN** -> **Account**, add a new user for login. The different with Remote Access is you 90

need to enter peer network information.

Configure Account

Name:

test

☒ Enable

Username:

test

Password:

....

Connection Type:

☐ Remote Access

☒ LAN TO LAN

Peer IP:

192.168.20.0

Peer Netmask:

255.255.255.0

Apply/Save

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

Account

Maximum entries: 4

| Name | Enable | Username | Connection Type | Peer IP | Peer Netmask | Remove | Edit |
|------|--------|----------|-----------------|--------------|---------------|--------------------------|------|
| test | Enable | test | LAN TO LAN | 192.168.20.0 | 255.255.255.0 | <input type="checkbox"/> | Edit |

Add Remove

TW-EAV510 AC (L2TP Client)

Go to **Advanced Setup** -> **VPN** -> **Client**, click **Add** button to add a new L2TP connection. For LAN to LAN, you need to enter peer network information.

Configure Client

Name:

☒ Enable

Type: ☐ PPTP ☒ L2TP

Local Gateway Interface:

Remote Gateway:

Username:

Password:

Connection Type: ☐ Remote Access ☒ LAN TO LAN

Peer IP:

Peer Netmask:

☒ Tunnel Authentication

Secret:

Click **Apply/Save** button to save account settings.

Client

Maximum entries: 4

| Name | Type | Local Gateway Interface | Remote Gateway | Username | MPPE | Connection Type | Peer IP | Peer Netmask | Enable | Remove | Edit |
|-----------|------|-------------------------|----------------|----------|---------|-----------------|-------------|---------------|-------------------------------------|--------------------------|-------------------------------------|
| L2TP-Test | l2tp | eth4.1 | 10.0.0.254 | test | Disable | LAN TO LAN | 192.168.0.0 | 255.255.255.0 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="button" value="Edit"/> |

Go to **Device Info -> VPN -> Client Info** to check connection status. You can also click **Disconnect** button to disconnect the L2TP connection.

Device Info -- Client Info

| Name | Type | Enable | Status | Connection Type | Remote Gateway | Peer IP | Client IP | Action |
|-----------|------|---------|-----------|-----------------|----------------|-------------|--------------|---|
| L2TP-Test | l2tp | Enabled | Connected | LAN TO LAN | 10.0.0.254 | 192.168.0.0 | 192.168.0.11 | <input type="button" value="Disconnect"/> |

When **Status** shows **Connected**, both local and remote network can access each other.

Below is Server Info for reference.

Device Info -- Server Info

| Name | Type | Enable | Status | Connection Type | Peer IP | Connected By | Action |
|------|------|---------|-----------|-----------------|--------------|--------------|---|
| test | l2tp | Enabled | Connected | LAN TO LAN | 192.168.20.0 | 10.0.0.1 | <input type="button" value="Disconnect"/> |

OpenVPN

Note: Please make sure that both LAN side networks are in different subnet.

Enable OpenVPN Server Function

Go to **Advanced Setup -> VPN -> OpenVPN -> OpenVPN Server**, make **“Enable OpenVPN Server”** checkbox checked. And you will see the page as below:

OpenVPN Server

☒ Enabled OpenVPN Server

Protocol:

TCP ▾

Port Number:

443

Tunnel Subnet:

10.8.0.0

Tunnel Mask:

255.255.255.0

Cipher Encryption:

BF-CBC ▾

HMAC Authentication:

SHA1 ▾

☒ Enabled LZO data compression

Apply/Save

CA

Generate CA

-----BEGIN CERTIFICATE-----
MIIDvDCCAYWgAwIBAgIJANeg5nRroR8HMA0GCSqGSIb3DQEBBQUAMIGBMCQswCQYD
VQQGEwJGSTELMAKGA1UECBMCRkkxCzAJBgNVBACkIAZSBRMRkwFwYDVQQKEwB3d3cu
dGVzZXdlbGwuY29tMRkwFwYDVQLExB3d3cudGVzZXdlbGwuY29tMRwwGyYDVQQD
ExN3d3cudGVzZXdlbGwuY29tIENBMRA4wHAYJKoZIhvcNAQkBFG9jYUB0ZWxld2Vs
bC5jb20wHhcNMTAwMTAxMDAwMDE2WhcNMTEkxMjMwMDAwMDE2WjCBmzELMAKGA1UE
BhMCRkkxCzAJBgNVBAGTAKZJMQuSwCQYDVQQHEwJQQTETZMBcGA1UEChMQd3d3LnRl
bGV3ZWxsLmNvbTEZMBCGA1UECxMQd3d3LnRlbGV3ZWxsLmNvbTECMBoGA1UEAUMT
d3d3LnRlbGV3ZWxsLmNvbSBBDQTEeMBwGCsqGSIb3DQEQJARYPY2FAdGVzZXdlbGwu
Y29tMIGfMA0GCSqGSIb3DQEBAAUAA4GNADCBiQKBggQDLDRUuyZkwyDDIIADf1BL
tyXvTeCK+veKRuNkfIw9HExBx8ZFMDDKz3nUKPUjBPHSWC3Z1v1A3J6ZyytXb/xbj
YnBgFjTLVegKHqIkjZ6sbtlW0XGX8Jq7knGpwU23ez9ovlMIDfUsN0YFKb3DM27/
EHDoD+veXbuP/5Ir4qfASwIDAQABo4IBBDCCAQAwhHQYDVR00OBByEFGS+yI1V1gT6
o1jm7pgCf2TJCx3AMIHQBGnvHSMegcgwgclAFGS+yI1V1gT6o1jm7pgCf2TJCx3A
oYGhpIGeMIGBMCQswCQYDVQQGEwJGSTELMAKGA1UECBMCRkkxCzAJBgNVBACkIAZS
BRMRkwFwYDVQQKEwB3d3cudGVzZXdlbGwuY29tMRkwFwYDVQLExB3d3cudGVzZXdl
bGwuY29tMRwwGyYDVQQDEwN3d3cudGVzZXdlbGwuY29tIENBMRA4wHAYJKoZIhvcN
AQkBFG9jYUB0ZWxld2Vs bC5jb22CCQDRI0Z0a6EfBzAMBGNVHRMEBTADAQH/MA0G
CSqGSIb3DQEBBQUAA4GBAG+j8ysMUZSA3Z8Rc3k5ioHhTnMvditi8seap4c8XT5S1
A2yqLyBaQqVvzUJZz/rIYIPes7yx0uyoZC1ukTtLRWnr4kyXyjFouxZGbnCyGvX

Send CA To E-mail:

Send

Enabled OpenVPN Server: Make it checked to enable OpenVPN Server function.

Protocol: Select the protocol for OpenVPN. It can be TCP or UDP.

Port Number: Enter the port number for OpenVPN, default is 443.

Tunnel Subnet: The IP subnet for tunnel interface, the system will generate the IP for clients automatically.

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

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

Authentication: Select the authentication way.

Enabled LSO data compression: Make it checked to enable data compression.

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

Send CA to E-mail: Fill in the E-Mail address and click **Send** button. The system will send the generated CA to the address. You can just copy and paste to your OpenVPN client once you get it via mail.

Note: All clients must use the CA that generated from TW-EAV510/AC, otherwise the connection cannot be established.

Setup OpenVPN account for OpenVPN Server

Go to **Advanced Setup -> VPN -> Account**.

Account

Maximum entries: 4

| Name | Enable | Username | Connection Type | Peer IP | Peer Netmask | Remove | Edit |
|------|--------|----------|-----------------|---------|--------------|--------|------|
|------|--------|----------|-----------------|---------|--------------|--------|------|

Click **Add** button to add new user. Totally support up to 4 users for both PPTP, L2TP and OpenVPN.

Configure Account

| | |
|--|---|
| Name: | <input type="text" value="test1"/> |
| <input checked="" type="checkbox"/> Enable | |
| Username: | <input type="text" value="test1"/> |
| Password: | <input type="password" value="....."/> |
| Connection Type: | <input type="radio"/> Remote Access <input checked="" type="radio"/> LAN TO LAN |
| Peer IP: | <input type="text" value="192.168.20.0"/> |
| Peer Netmask: | <input type="text" value="255.255.255.0"/> |

Name: The name for user profile.

Enable: Enable/Disable this account.

Username: The name will be used for authentication.

Password: The password will be used for authentication.

Connection Type: Setup connection to Remote Access or LAN to LAN.

Remote Access - Limited your remote OpenVPN Client as one of clients at local network. The remote client can have full access to local network, but any clients at local network cannot access to remote client's network.

LAN to LAN - The clients at both local/remote network can access each other.

Peer IP: Enter the remote network's IP address.

Peer Netmask: Enter the remote network's netmask.

Remove/Edit user

Account

Maximum entries: 4

| Name | Enable | Username | Connection Type | Peer IP | Peer Netmask | Remove | Edit |
|-------|--------|----------|-----------------|--------------|---------------|--------------------------|----------------------|
| test1 | Enable | test1 | LAN TO LAN | 192.168.20.0 | 255.255.255.0 | <input type="checkbox"/> | Edit |

Add Remove

Make Remove checkbox checked and click **Remove** button to remove user or click **Edit** button to edit the details of user.

Setup OpenVPN Client

Go to **Advanced Setup** -> **VPN** -> **OpenVPN** -> **Trusted CA**

Trusted CA (Certificate Authority) Certificates

Add, View or Remove certificates from this page. CA certificates are used by you to verify peers' certificates.
Maximum entries: 4

| Name | Subject | Type | Action |
|------|---------|------|--------|
|------|---------|------|--------|

Import Certificate

Click **Import Certificate** button. The content of Certificate can be got from Server side or your mailbox if you did use function **Send CA to E-mail** on TW-EAV510/AC OpenVPN setting page. Click **Apply** button to save your CA. The TW-EAV510/AC can support multiple CAs.

Import CA certificate

Enter certificate name and paste certificate content.

Certificate Name:

Test

Certificate:

V00GEwJGSTE~~LM~~AKGA1UECBMCRk~~k~~x~~C~~zA~~J~~BgNVBAcTAK5BMRkwFwYDVQOQ~~E~~x~~B~~3d3cu
dGVsZXdlbGw~~u~~yY29tMRkwFwYDVQOQ~~E~~x~~B~~3d3cudGVsZXdlbGw~~u~~yY29tMR~~w~~gGyYDVQOQ~~E~~
ExN3d3cudGVsZXdlbGw~~u~~yY29tIENBMRA4W~~H~~AYJKoZiHvcNAQ~~B~~Fg9jYUB0Z~~W~~xl2V~~s~~
bC5jb20wHhcNMTAwMTAxMDA0NTI4WhcNMTkxMjIwMDA0NTI4WjCBmzELMAkGA1UE
BhMCRk~~k~~xx~~C~~zA~~J~~BgNVBAcTAKZJM0s~~Q~~COYDVQOQ~~E~~wJ0QTEZMBcGA1UEChM~~o~~d3d3LnRl
bGV3Z~~W~~xsLnMvN~~b~~TEZMBcGA1UEChM~~o~~d3d3LnRlbgV3Z~~W~~xsLnMvN~~b~~TECBMBoGA1UEA~~x~~MT
d3d3LnRlbgV3Z~~W~~xsLnMvN~~b~~TSBDOQTEeMBwGCSqGSIb3DQEJLmY~~P~~Y2FAdG~~V~~sZXdlbGw~~u~~
Y29tMTGfMA0GC~~S~~qGSIb3DQEBAQUAAAGNADCBiQK~~B~~gQDUi~~y~~ks4JY~~C~~9cymymC~~x~~gK1P
At211mafmycN/hwi6B1kij3QKqN~~Q~~v/5dJ~~s~~X6Jdh/v1N~~x~~VE1O~~y~~xx+gCC~~K~~OxTz~~v~~b4T~~v~~
kHO7McUJ4czH0p1RyLhU94c6HCAkTMDbt8wQGF~~C~~5+qG~~P~~0qkyj3vV2TNO~~R~~zEAdDny0~~D~~
G4Gq8I2cs2XUuK~~V~~37U1uHwIDAQABo4IBDDCCAQAuHQYDV~~R~~QOBBEY~~F~~BFkFzFvXIGI
x67bes5c2AB8PvbqMIHOBgNVHSM~~E~~gcgwgcWAFBukFzFvXIGIx67bes5c2AB8Pvbq
oYGhpTGeMTGbM0s~~Q~~COYDVQOQ~~E~~wJGSTE~~LM~~AKGA1UECBMCRk~~k~~x~~C~~zA~~J~~BgNVBAcTAK5B
MRkwFwYDVQOQ~~E~~x~~B~~3d3cudGVsZXdlbGw~~u~~yY29tMRkwFwYDVQOQ~~E~~x~~B~~3d3cudGVsZXdlb
bGw~~u~~yY29tMR~~w~~gGyYDVQOQ~~E~~ExN3d3cudGVsZXdlbGw~~u~~yY29tIENBMRA4W~~H~~AYJKoZiHvcN
AQB~~B~~Fg9jYUB0Z~~W~~xl2V~~s~~bC5jb22CQCQ0ag1gn0shGzAMBgNVHRMBETADAQH/MA0G
CSqGSIb3DQE~~B~~BQUAA4GBAE0Wi4aUJT0VwMQV~~k~~qJqFYhe6BfvHtf/R6w97B4ihq6g
/F/SA117Hz7aR9HSLNn9Rjhr6k+Q7NMxUrsF1fl~~h~~qf2p1dR~~K~~75w21wNbU~~x~~feuxerL
aEYIwGQ~~W~~qxjThqz14v1fjZUJO773ZtMabTgeUoM7qcTFAbvJa+CYT~~x~~wk1NtRpEd
-----END CERTIFICATE-----

Apply

Once it is done, you can see the settings as below. You can also click **View** button to check imported CA

or **Remove** button to remove the CA.

Trusted CA (Certificate Authority) Certificates

Add, View or Remove certificates from this page. CA certificates are used by you to verify peers' certificates.
Maximum entries: 4

| Name | Subject | Type | Action |
|------|--|------|---|
| Test | C=FI/ST=FI/L=NA/O=www.telewell.fi/OU=www.telewell.fi/CN=www.telewell.fi CA/emailAddress=ca@telewell.fi | ca | <button>View</button> <button>Remove</button> |

Import Certificate

Go to **Advanced Setup -> VPN -> OpenVPN -> OpenVPN Client**

OpenVPN Client

Maximum entries: 4

| Name | Local Gateway Interface | Remote Gateway | Username | Protocol | Port Number | Cipher Encryption | HMAC Authentication | LZO | CA Profile | Enable | Remove | Edit |
|------|-------------------------|----------------|----------|----------|-------------|-------------------|---------------------|-----|------------|--------|--------|------|
|------|-------------------------|----------------|----------|----------|-------------|-------------------|---------------------|-----|------------|--------|--------|------|

Add Enable Remove

Click **Add** button to add a new OpenVPN Client connection.

OpenVPN Client

| | |
|--|---|
| Name: | <input type="text" value="Office"/> |
| <input checked="" type="checkbox"/> Enable | |
| Local Gateway Interface: | <input type="text" value="ipoe_eth2/eth2.1"/> |
| Remote Gateway: | <input type="text" value="10.0.0.254"/> |
| Username: | <input type="text" value="test1"/> |
| Password: | <input type="password" value="*****"/> |
| Protocol: | <input type="text" value="TCP"/> |
| Port Number: | <input type="text" value="443"/> |
| Cipher Encryption: | <input type="text" value="BF-CBC"/> |
| HMAC Authentication: | <input type="text" value="SHA1"/> |
| <input checked="" type="checkbox"/> Enabled LZO data compression | |
| CA Profile: | <input type="text" value="Test"/> |

Apply/Save

Name: The name for OpenVPN Client profile.

Enable: Enable/Disable this profile.

Local Gateway Interface: Select the correct WAN interface that will be used to access to remote network.

Remote Gateway: Enter the IP/Domain address of remote OpenVPN Server.

Username: The name will be used for authentication. **Password:** The password will be used for authentication. **Protocol:** Select the protocol for OpenVPN. It can be TCP or UDP.

Port Number: Enter the port number for OpenVPN, default is 443.

Cipher Encryption: Select the encryption method.

HMAC Authentication: Select the authentication way.

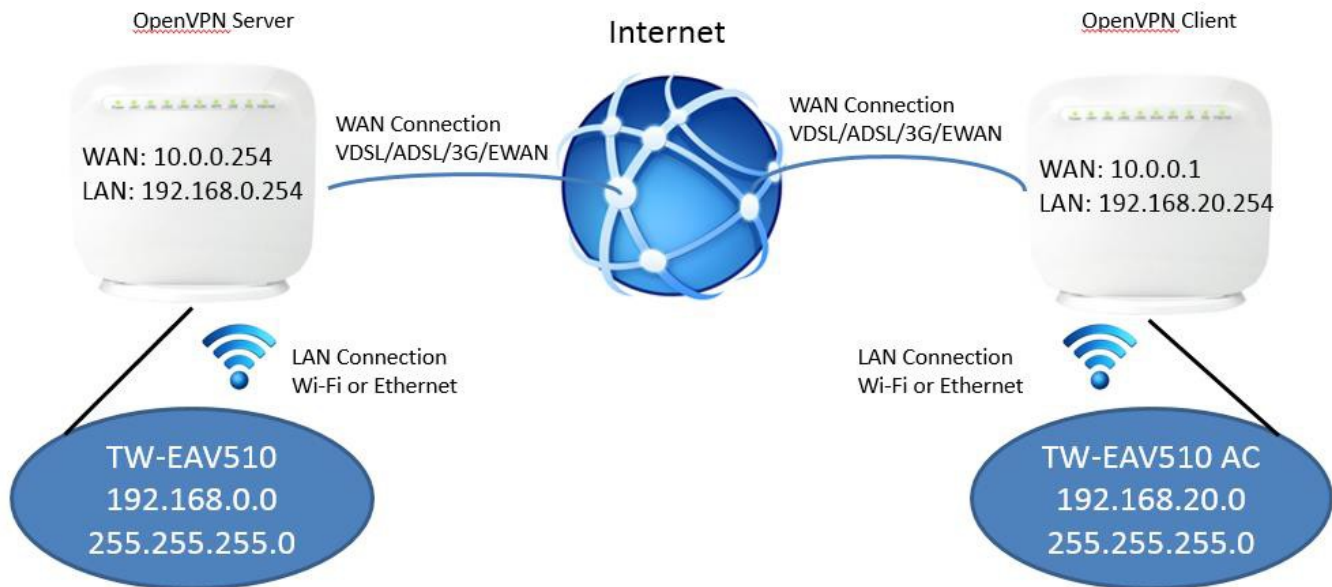
Enabled LSO data compression: Make it checked to enable data compression.

CA Profile: Select one of imported CA for OpenVPN connection.

Note: All clients must use the CA that generated from TW-EAV510/AC, otherwise the connection cannot be established.

Example 1

TW-EAV510 is activated as OpenVPN Server and TW-EAV510 AC is activated as OpenVPN Client.



Remote Access

TW-EAV510 (OpenVPN Server)

1. Go to **Advanced Setup -> VPN -> OpenVPN -> OpenVPN Server**, enable the OpenVPN Server and do the settings as below. Click **Apply/Save** button to save changes.

☒ Enabled OpenVPN Server

Protocol: TCP

Port Number: 443

Tunnel Subnet: 10.8.0.0

Tunnel Mask: 255.255.255.0

Cipher Encryption: BF-CBC

HMAC Authentication: SHA1

☒ Enabled LZO data compression

Apply/Save

[illegible]

Send CA To E-mail:

- ## Configure Account

| | |
|--|---|
| Name: | <input type="text" value="test"/> |
| <input checked="" type="checkbox"/> Enable | |
| Username: | <input type="text" value="test"/> |
| Password: | <input type="password" value="...."/> |
| Connection Type: | <input checked="" type="radio"/> Remote Access <input type="radio"/> LAN TO LAN |
| <input type="button" value="Apply/Save"/> | |

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

Account

Maximum entries: 4

| Name | Enable | Username | Connection Type | Peer IP | Peer Netmask | Remove | Edit |
|------|--------|----------|-----------------|---------|--------------|--------------------------|-------------------------------------|
| test | Enable | test | Remote Access | | | <input type="checkbox"/> | <input type="button" value="Edit"/> |

Add Remove

TW-EAV510 AC (OpenVPN Client)

1. Go to **Advanced Setup -> VPN -> OpenVPN -> Trusted CA**, click Import Certificate button to add a new CA.

Trusted CA (Certificate Authority) Certificates

Add, View or Remove certificates from this page. CA certificates are used by you to verify peers' certificates.
Maximum entries: 4

| Name | Subject | Type | Action |
|------|---------|------|--------|
|------|---------|------|--------|

Import Certificate

2. Setup a name for importing certificate and paste the CA to **Certificate** field. Click **Apply** button to save your CA.

Import CA certificate

Enter certificate name and paste certificate content.

Certificate Name:

Test CA

```
-----BEGIN CERTIFICATE-----
MIIDrjCCAxegAwIBAgIJAMdMBDEBCqzKMA0GCSqSgSIb3DQEBlBOUAMIGXMQswCQYD
VQQGEwJSTELMakGA1UECBMCRkxkxCzAJBGNvBACAk5BRGRWfGyDVQQKEw93d3cudG
VGVSZkd1bGwuzmkxGDAWBGNVBABTAD3d3dy50ZWxld2VsbC5maTEybmBkGA1UEAXMA
d3d3LnRlbGV3ZlwxLmZpIENBMR0wGyWJKoZIhvcNAQkBFgs5YUB0ZWxld2VsbC5m
aTAeFw0xMDAxMDEwMDI4MTthaFw0xOTEyMzAwMDI4MTthaMIGXMQswCQYDVQQGEwJG
STELMakGA1UECBMCRkxkxCzAJBGNvBACAk5BRGRWfGyDVQQKEw93d3cudGVSZkd1
bGwuzmkxGDAWBGNVBABTAD3d3dy50ZWxld2VsbC5maTEybmBkGA1UEAXMSd3d3LnRl
bGV3ZlwxLmZpIENBMR0wGyWJKoZIhvcNAQkBFgs5YUB0ZWxld2VsbC5maTBCEzAN
BgqhkhIG9w0BAEQFAAOBjYAQAwgYKKCGYEaUKHu5YpduQHd+SL33d9NS12MVX8ezOfI
EiPt8qhvhvcsUSv+MlwPKII1Xcqolzf+kQw36iDRcgIYZD=QPtNjfvFuNiBOPXWO3W
yHua+dxjl1Scqseg+y3oMBth034H8VRClpl1fanTUowxAWC0dkJaMnQu46CpUnz
0IamZUQSULkUwEAFAAACw/zCB/DAdBgNVHQ4EEGQUFIQAEwNB1U9c986ZLSy38Jjn1P
q34wgcnwGA1UdIAwSBDCXBwYAUFIOQAEwNB1U9c986ZLSy38Jjn1Paq36hgz2kgZowgc
CzABGwNBAYTAkZJMOMSQDVQOIEwJGSTELMakGA1UEBjMCTExGDAWBGNVBABTAD3d3dy
50ZWxld2VsbC5maTEYMBYGA1UECjMPd3d3LnRlbGV3ZlwxLmZpMRswGQYD
VQODEwJ3d3cudGVSZkd1bGwuzmkxGQOEwHTAbBgqhkhIG9w0BCQEWDMNhOHRlbGV3
ZlwxLmZpPggekAx0wMF4EKRoQwDAYDRVZLTBAUWAawEB/zANBgqhkhIG9w0BAQIFAABO
gQA7njkt+gODM9csSYhmGe2Ud8y+UV62VluVuNSIf1ccQvvaWe9X07y3pqdQNIdo
5Cc54Amurwm/DX+vYzw7n7S+vsvgnFqZatVRra+aOSbcvPAj5wFMHS/xTng+IKXSImQ
```

Certificate:

Apply

Note: The CA contents must between wording “-----BEGIN CERTIFICATE-----” and “-----END CERTIFICATE-----”, they cannot be deleted.

3. Once the CA import successfully, you will see the page as below.

Trusted CA (Certificate Authority) Certificates

Add, View or Remove certificates from this page. CA certificates are used by you to verify peers' certificates.
Maximum entries: 4

| Name | Subject | Type | Action |
|---------|--|------|--|
| Test_CA | C=FI/ST=FI/L=NA/O=www.telewell.fi/OU=www.telewell.fi/CN=www.telewell.fi CA/emailAddress=ca@telewell.fi | ca | <div> View Remove </div> |

Import Certificate

- Go to **Advanced Setup -> VPN -> OpenVPN -> OpenVPN Client**, click **Add** button to add a new OpenVPN connection.

OpenVPN Client

Name:

☒ Enable

Local Gateway Interface:

Remote Gateway:

Username:

Password:

Protocol:

Port Number:

Cipher Encryption:

HMAC Authentication:

☒ Enabled LZO data compression

CA Profile:

Click **Apply/Save** button to save account settings.

OpenVPN Client

Maximum entries: 4

| Name | Local Gateway Interface | Remote Gateway | Username | Protocol | Port Number | Cipher Encryption | HMAC Authentication | LZO | CA Profile | Enable | Remove | Edit |
|--------------|-------------------------|----------------|----------|----------|-------------|-------------------|---------------------|--------|------------|-------------------------------------|--------------------------|-------------------------------------|
| OpenVPN-Test | eth4.1 | 10.0.0.254 | test | TCP | 443 | BF-CBC | SHA1 | Enable | Test_CA | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="button" value="Edit"/> |

- Go to **Device Info -> VPN -> Client Info** to check connection status. You can also click **Disconnect** button to disconnect the OpenVPN connection.

Device Info -- Client Info

| Name | Type | Enable | Status | Connection Type | Remote Gateway | Peer IP | Client IP | Action |
|--------------|---------|---------|-----------|-----------------|----------------|----------|-----------|---|
| OpenVPN-Test | OpenVPN | Enabled | Connected | | 10.0.0.254 | 10.8.0.1 | 10.8.0.6 | <input type="button" value="Disconnect"/> |

When **Status** shows **Connected**, you can now access to remote network.

Below is Server Info for reference.

Device Info -- Server Info

| Name | Type | Enable | Status | Connection Type | Peer IP | Connected By | Action |
|------|---------|---------|-----------|-----------------|---------|--------------|--------|
| test | OpenVPN | Enabled | Connected | Remote Access | | 10.8.0.6 | |

LAN to LAN

TW-EAV510 (OpenVPN Server)

1. Go to **Advanced Setup -> VPN -> OpenVPN -> OpenVPN Server**, enable the OpenVPN Server and do the settings as below. Click **Apply/Save** button to save changes.

OpenVPN Server

☒ Enabled OpenVPN Server

Protocol:

TCP ▾

Port Number:

443

Tunnel Subnet:

10.8.0.0

Tunnel Mask:

255.255.255.0

Cipher Encryption:

BF-CBC ▾

HMAC Authentication:

SHA1 ▾

☒ Enabled LZO data compression

Apply/Save

CA

-----BEGIN CERTIFICATE-----
MIIDvDCCAYWgAwIBAgIJALRqDWcK6yEbMA0GCSqGSIb3DQEBBQUAMIGBMQswCQYD
VQQGEwJGSTEIMAKGA1UECBMCRkxkCzA3BgNVBACIAk5BRMRkwFwYDVQQKEExB3d3cu
dGVsZXdlbGwuy29tMRkwFwYDVQLLEB3d3cudGVsZXdlbGwuy29tMRwwGgYDVQQDD
ExN3d3cudGVsZXdlbGwuy29tIENBMHRAwHAYJKoZIhvcNAQkBFG9jYUBOZlxl2VsbC
5jcjb20wHicNMHTAwMTAxMDA0NTI14WhcNMHTkxMjMwMDA0NTI14WjCBmzELMAKGA1
UECBMCRkxkCzA3BgNVBAGTAkZJMqSwCQYDVQQHEwJQTEZMBcGA1UEChMQd3d3LnRl
bGV3ZWxsLmNvbTEZMBcGA1UECxMQd3d3LnRlRlbGV3ZWxsLmNvbTETMBcGA1UEAxMT
d3d3LnRlRlbGV3ZWxsLmNvbSBDOQTETeMBWGCSqGSIsb3DQEJARYPY2FAdGVsZXdlbGw
y29tMHIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBggQDUiYks4JYC9cmymCxBKLP
At211mafmycN/hwI6BIkj3QKqNQv/5d3sX6Jdh/vINxVE10yx+xCCKCoXtzvb4Tv
kHQ7mCuJ4czH0pIRYLuk4c6HCKTMDbt8wQGfc5+qGp0kkyj3vV2TNqrEzATDnyOd
GE4Gq87cs2XUuKV37u1H9wIDAQABoA1BBDDCCAQAwhQYDVROB0BEYFBukFzfVXIgi
x67bes5c2AB8PvbqMIHQBgNVHSMEgcgwgcWAFBukFzfVXIgiX67bes5c2AB8Pvbq
oYGhpIGeMIGbMQswCQYDVQQGEwJGSTEIMAKGA1UECBMCRkxkCzA3BgNVBACIAk5B
MRkwFwYDVQQKEExB3d3cudGVsZXdlbGwuy29tMRkwFwYDVQLLEB3d3cudGVsZXdl
bGwuy29tMRwwGgYDVQQDEExN3d3cudGVsZXdlbGwuy29tIENBMHRAwHAYJKoZIhvcN
AQkBFG9jYUBOZlxl2VsbC5jcjb22CCQC0ag1nGshgzAMBGNVHRMEBTADAQH/MA0G
CSqGSIb3DQEBBQUAA4GBAE0W14auJT0VmwMQvkQjQfyHe6BfvHtf/R6w97B4ihq6G
/F/SAA17Hz7aR9HSLNn9Rjhr6k+Q7NmXuRsFlfwqf2p1dRK75w2IwnblUXfeuXerL

Generate CA

Send CA To E-mail:

Send

2. Go to **Advanced Setup** -> **VPN** -> **Account**, add a new user for login. The different with Remote Access is you need to enter peer network information.

Configure Account

| | |
|--|---|
| Name: | <input type="text" value="test"/> |
| <input checked="" type="checkbox"/> Enable | |
| Username: | <input type="text" value="test"/> |
| Password: | <input type="password" value="••••"/> |
| Connection Type: | <input type="radio"/> Remote Access <input checked="" type="radio"/> LAN TO LAN |
| Peer IP: | <input type="text" value="192.168.20.0"/> |
| Peer Netmask: | <input type="text" value="255.255.255.0"/> |
| <input type="button" value="Apply/Save"/> | |

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

Account

Maximum entries: 4

| Name | Enable | Username | Connection Type | Peer IP | Peer Netmask | Remove | Edit |
|------|--------|----------|-----------------|--------------|---------------|--------------------------|-------------------------------------|
| test | Enable | test | LAN TO LAN | 192.168.20.0 | 255.255.255.0 | <input type="checkbox"/> | <input type="button" value="Edit"/> |

Add

Remove

TW-EAV510 AC (OpenVPN Client)

5. Go to **Advanced Setup -> VPN -> OpenVPN -> Trusted CA**, click Import Certificate button to add a new CA.

Trusted CA (Certificate Authority) Certificates

Add, View or Remove certificates from this page. CA certificates are used by you to verify peers' certificates.
Maximum entries: 4

| Name | Subject | Type | Action |
|------|---------|------|--------|
|------|---------|------|--------|

Import Certificate

7. Setup a name for importing certificate and paste the CA to **Certificate** field. Click **Apply** button to save your CA.

Import CA certificate

Enter certificate name and paste certificate content.

Certificate Name:

Test CA

Certificate:

```
-----BEGIN CERTIFICATE-----
MIIDrjCCAXegAwIBAgIJAMdMDBeBcqzKMA0GCSqGSIb3DQEBBQUAMIGXMQswCQYD
VQGEwJGSTELMAKGAIUECBMCRkKxCzAJBgNVBACkA55MRGwFgYDVQQKEwE93d3cud
dGv5ZXd1bGwuzmKxGDAwBgNVBAsTD3d3dy50ZWxld2VsbC5maTEyBMBGGA1UEAxM
d3d3LnRlbGv3ZlXw5LmZpIENBR09GwYjYkoZlIhvcNAQKBG9G5YU0B0ZWxld2VsbC5m
aTAeFw0xMDAxMDEwMDI4MThaFw0xOTYyMzAwMDI4MThaIGXMQswCQYDVQGEwJG
STELMAKGAIUECBMCRkKxCzAJBgNVBACkA55MRGwFgYDVQQKEwE93d3cudGv5ZXd1
bGwuzmKxGDAwBgNVBAsTD3d3dy50ZWxld2VsbC5maTEyBMBGGA1UEAxM5d3d3LnRl
bGv3ZlXw5LmZpIENBR09GwYjYkoZlIhvcNAQKBG9G5YU0B0ZWxld2VsbC5maTBNZ
BgqhkiG9w0BAQEFAA0BjQAwIGYjQGAkYEAuKHU5YpduQhD+SL33d9NS12MvX8ezOf1
EiPt8qhvhvCSUsv+MwPKI1Xcqolzf+kQw36iDRcgIyZDzQPtNjFvFuniBQpXW03W
yHua+dxj1lScqseg+y3oMBth034H8VRClp1fauTUowxAWC0dkJaMnQu46CpUnz
0IamZCWSWLkCAwEAaAOB/zCB/DadBgNVHQ4EFgQUFIQaeNB1Uc986ZLSy38JjN1P
q34wgCwGAIUCDAwIBSwSDCBwYAUFIQaeNB1Uc986ZLSy38JjN1Pq36hg22KgZowgZc
CzAJBgNVBAYTAkZJMQswCQYDVQEEwJGSTELMAKGAIUEBxMCTkExGDAwBgNVBAsT
D3d3dy50ZWxld2VsbC5maTEyBMBGGA1UECmFpd3d3LnRlbGv3ZlXw5LmZpMRswGQYD
VQOGEwJG3d3cudGv5ZXd1bGwuzmKxG00eXHTAbBgqhkiG9w0BCEwDmNhOHRlbGv3
ZlXw5LmZpggkAx0wMF4EKrQ0wDAYDVDR0BAUwAwEw/zANBgqhkiG9w0BAQUFAAOB
GQA7njkt+g0DM9cs5Yhgm2eUd8y+UV6vWruvN5if3cQvvaWe9X073jpdqQNI0d
5Cc54Amwrm/DX+YvZw7n7s5+vgfNFqZatVRrao+SBcvPAj5WfMHS/xTnG+IKXsImQ
```

Apply

Note: The CA contents must between wording “-----BEGIN CERTIFICATE-----”and “-----END CERTIFICATE-----”, they cannot be deleted.

8. Once the CA import successfully, you will see the page as below.

Trusted CA (Certificate Authority) Certificates

Add, View or Remove certificates from this page. CA certificates are used by you to verify peers' certificates.
Maximum entries: 4

| Name | Subject | Type | Action |
|---------|--|------|---|
| Test_CA | C=FI/ST=FI/L=NA/O=www.telewell.fi/OU=www.telewell.fi/CN=www.telewell.fi CA/emailAddress=ca@telewell.fi | ca | <button>View</button> <button>Remove</button> |

Import Certificate

9. Go to **Advanced Setup -> VPN -> OpenVPN -> OpenVPN Client**, click **Add** button to add a new OpenVPN connection.

OpenVPN Client

| | |
|--|---|
| Name: | <input type="text" value="OpenVPN-Test"/> |
| <input checked="" type="checkbox"/> Enable | |
| Local Gateway Interface: | <input type="text" value="ipoe_eth4/eth4.1"/> |
| Remote Gateway: | <input type="text" value="10.0.0.254"/> |
| Username: | <input type="text" value="test"/> |
| Password: | <input type="password" value="...."/> |
| Protocol: | <input type="text" value="TCP"/> |
| Port Number: | <input type="text" value="443"/> |
| Cipher Encryption: | <input type="text" value="BF-CBC"/> |
| HMAC Authentication: | <input type="text" value="SHA1"/> |
| <input checked="" type="checkbox"/> Enabled LZO data compression | |
| CA Profile: | <input type="text" value="Test_CA"/> |

Apply/Save

Click **Apply/Save** button to save account settings.

Note: The OpenVPN client side will get peer network information from server side, so no need to setup peer network.

OpenVPN Client

Maximum entries: 4

| Name | Local Gateway Interface | Remote Gateway | Username | Protocol | Port Number | Cipher Encryption | HMAC Authentication | LZO | CA Profile | Enable | Remove | Edit |
|--------------|-------------------------|----------------|----------|----------|-------------|-------------------|---------------------|--------|------------|-------------------------------------|--------------------------|-----------------------|
| OpenVPN-Test | eth4.1 | 10.0.0.254 | test | TCP | 443 | BF-CBC | SHA1 | Enable | Test_CA | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <button>Edit</button> |

Add Enable Remove

10. Go to **Device Info -> VPN -> Client Info** to check connection status. You can also click **Disconnect** button to disconnect the OpenVPN connection.

Device Info -- Client Info

| Name | Type | Enable | Status | Connection Type | Remote Gateway | Peer IP | Client IP | Action |
|--------------|---------|---------|-----------|-----------------|----------------|----------|-----------|-----------------------------|
| OpenVPN-Test | OpenVPN | Enabled | Connected | | 10.0.0.254 | 10.8.0.1 | 10.8.0.6 | <button>Disconnect</button> |

When **Status** shows **Connected**, you can now access to remote network.

Below is Server Info for reference.

Device Info -- Server Info

| Name | Type | Enable | Status | Connection Type | Peer IP | Connected By | Action |
|------|---------|---------|-----------|-----------------|--------------|--------------|--------|
| test | OpenVPN | Enabled | Connected | LAN TO LAN | 192.168.20.0 | 10.8.0.6 | |

GRE

Note: Please make sure that both LAN side networks are in different subnet.

Click the **Add** button and you will see the page as below:

GRE Setting

Name:

☐ Enable

Local Gateway Interface:

Select interface ▼

Remote Gateway:

Tunnel Source IP:

Tunnel Mask:

Tunnel Peer IP:

Remote Network Type:

Single Address ▼

IP Address:

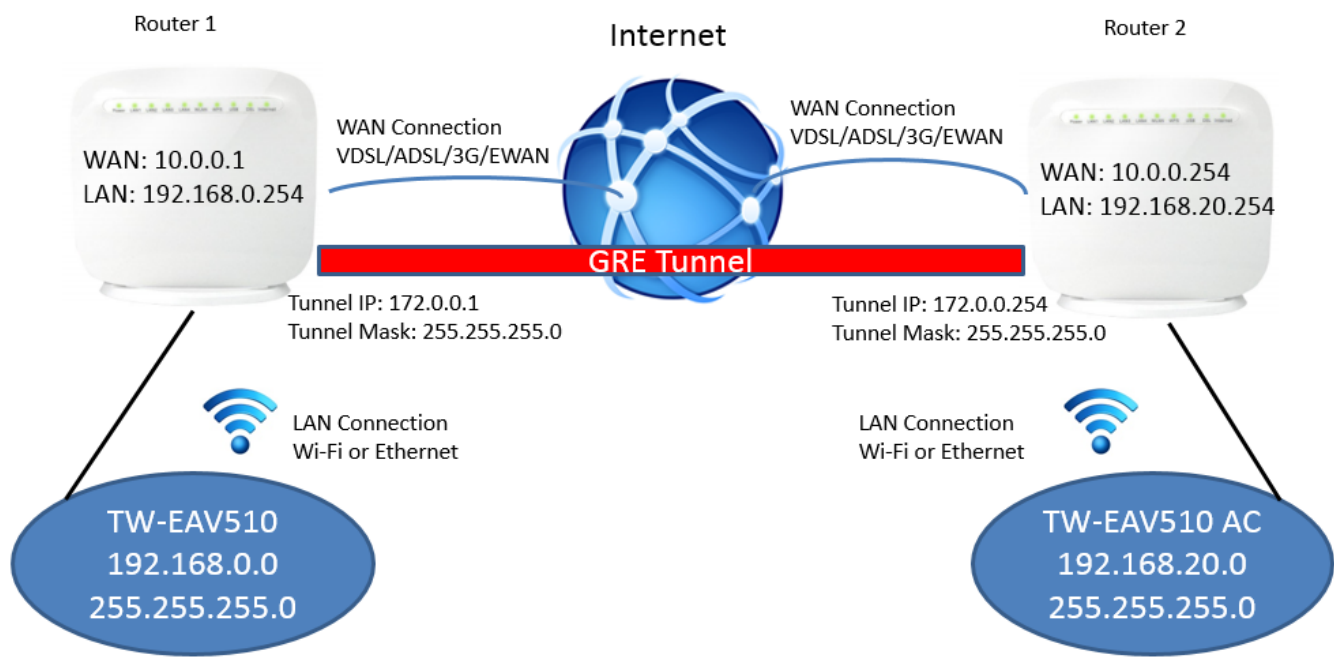
☐ Enable Keep Alive

Apply/Save

- Name:** Enter the name for this GRE Tunnel connection.
- Enable:** Enable the tunnel connection immediately after clicking **Apply/Save** button.
- Local Gateway Interface:** Select the correct WAN interface that will be used for establishing a GRE Tunnel.
- Remote Gateway:** Enter the remote WAN IP/Domain that will be used for establishing a GRE Tunnel.
- Tunnel Source IP:** Enter the IP address for local tunnel interface.
- Tunnel Mask:** Enter the net mask for local tunnel interface.
- Tunnel Peer IP:** Enter the IP address of remote tunnel interface.
- Remote Network Type:** Select the remote side is a client or subnet.
- IP Address:** Enter the IP address of remote client.
- Mask:** Enter the net mask of remote subnet when **Remote Network Type** sets to **Subnet**.
- Enable Keep Alive:** Enable Keep Alive function for GRE Tunnel and can define the **Retry Times** and **Interval** once checked. This is follow Cisco’s GRE Tunnel Keep Alive mechanism.

GRE Example

Setup a GRE Tunnel between TW-EAV510 and TW-EAV510 AC.



TW-EAV510 (Router 1)

Go to **Advanced Setup** -> **VPN** -> **GRE**, click Add button and do the settings as below. Click **Apply/Save** button to save changes.

GRE Setting

Name: Router1_GRE

☒ Enable

Local Gateway Interface: ipoe_eth0/eth0.1

Remote Gateway: 10.0.0.254

Tunnel Source IP: 172.0.0.1

Tunnel Mask: 255.255.255.0

Tunnel Peer IP: 172.0.0.254

Remote Network Type: Subnet

IP Address: 192.168.20.0

Mask: 255.255.255.0

☒ Enable Keep Alive

Retry Times: 12

Interval: 5

Apply/Save

TW-EAV510 AC (Router 2)

Go to **Advanced Setup** -> **VPN** -> **GRE**, click Add button and do the settings as below. Click **Apply/Save** button to save changes.

GRE Setting

Name:

Router2_GRE

☒ Enable

Local Gateway Interface:

ipoe_eth4/eth4.1 ▼

Remote Gateway:

10.0.0.1

Tunnel Source IP:

172.0.0.254

Tunnel Mask:

255.255.255.0

Tunnel Peer IP:

172.0.0.1

Remote Network Type:

Subnet ▼

IP Address:

192.168.0.0

Mask:

255.255.255.0

☒ Enable Keep Alive

Retry Times:

12

Interval:

5

Apply/Save

The status of GRE Tunnel connection can be found at Device Info -> VPN -> GRE Info and shows as below when GRE Tunnel established.

Device Info -- GRE Info

| Name | Enable | Status | Remote Gateway |
|-------------|---------|-----------|----------------|
| Router1_GRE | Enabled | Connected | 10.0.0.254 |

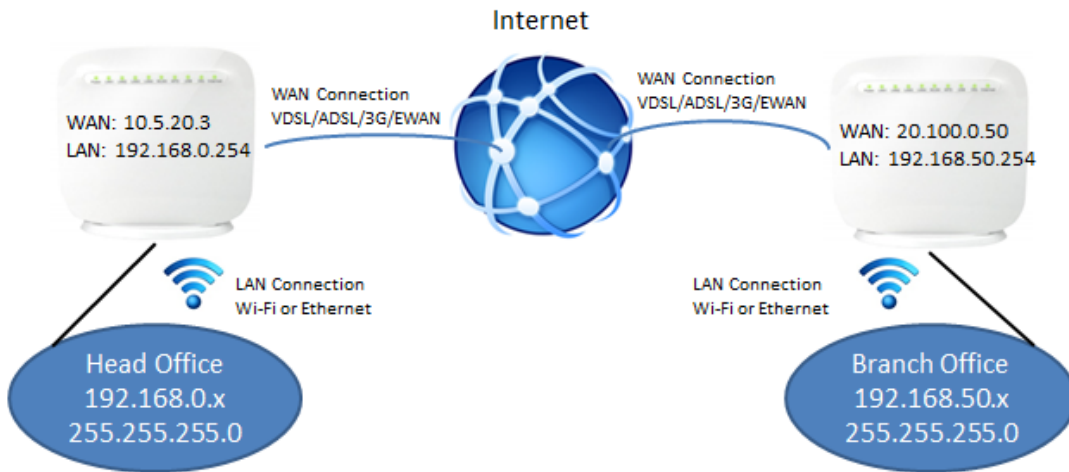
Device Info -- GRE Info

| Name | Enable | Status | Remote Gateway |
|-------------|---------|-----------|----------------|
| Router2_GRE | Enabled | Connected | 10.0.0.1 |

IPSec

Note 1: Please make sure that both LAN side networks are in different subnet.

We will take the following network topology as an example for reference.



The WAN IP address can be found at **Device Info** -> **WAN**. Also it depends on what interface you use, it could be VDSL/ADSL, 3G or EWAN.

WAN Info

| Interface | Description | Type | VlanMuxId | IPv6 | Igmp | MLD | NAT | Firewall | Status | IPv4 Address | IPv6 Address |
|-----------|--------------|--------|-----------|----------|----------|----------|----------|----------|-----------|--------------|--------------|
| atm0.1 | ipoe_0_0_33 | IPoE | Disabled | Enabled | Enabled | Enabled | Enabled | Enabled | Unconnect | | |
| atm0.2 | br_0_0_33 | Bridge | Disabled | Disabled | Disabled | Disabled | Disabled | Disabled | Unconnect | | |
| atm1.1 | ipoe_0_0_100 | IPoE | Disabled | Enabled | Enabled | Enabled | Enabled | Enabled | Unconnect | | |
| atm1.2 | br_0_0_100 | Bridge | Disabled | Disabled | Disabled | Disabled | Disabled | Disabled | Unconnect | | |
| ptm0.1 | ipoe_4_1_1 | IPoE | Disabled | Enabled | Enabled | Enabled | Enabled | Enabled | Unconnect | | |
| ptm0.2 | br_4_1_1 | Bridge | Disabled | Disabled | Disabled | Disabled | Disabled | Disabled | Unconnect | | |
| eth2 | ipoe_eth2 | IPoE | Disabled | Disabled | Disabled | Disabled | Enabled | Enabled | Connected | 10.5.20.3 | |
| ppp7 | 3G dongle | PPPoE | Disabled | Disabled | Disabled | Disabled | Enabled | Disabled | Unconnect | | |

Note 3: The IPSec supports IPv4 Address only.

Step for setting the IPSec (The setting is for TW-EAV510 in head office, only IP address will different for Branch Office's setting):

Step 1: Go to **Advanced Setup** -> **IPSec**, then click button "**Add New Connection**".

IPSec Tunnel Mode Connections

Add, remove or enable/disable IPSec tunnel connections from this page.

| Connection Name | Remote Gateway | Local Addresses | Remote Addresses | Remove |
|--|----------------|-----------------|------------------|--------|
| <div> <div>Add New Connection</div> <div>Remove</div> </div> | | | | |

Step 2: Edit details in IPSec setting

IPSec Settings

| | | |
|---|---|---|
| IPSec Connection Name | <input type="text" value="ToBranch1"/> | |
| Tunnel Mode | <input type="text" value="ESP"/> | |
| Remote IPSec Gateway Address (IPv4 address in dotted decimal) | <input type="text" value="20.100.0.50"/> | ← This is the WAN IP address on Branch Office's TW-EAV510. |
| Tunnel access from local IP addresses | <input type="text" value="Subnet"/> | |
| IP Address for VPN | <input type="text" value="192.168.0.0"/> | ← This is the Local subnet on Head Office's TW-EAV510. |
| IP Subnetmask | <input type="text" value="255.255.255.0"/> | |
| Tunnel access from remote IP addresses | <input type="text" value="Subnet"/> | |
| IP Address for VPN | <input type="text" value="192.168.50.0"/> | ← This is the Local subnet on Branch Office's TW-EAV510. |
| IP Subnetmask | <input type="text" value="255.255.255.0"/> | |
| Key Exchange Method | <input type="text" value="Auto(IKE)"/> | |
| Authentication Method | <input type="text" value="Pre-Shared Key"/> | |
| Pre-Shared Key | <input type="text" value="12345678"/> | ← It is the Pre-Shared Key that will be used for IPSec tunnel. Must make sure both sides are use the same key |
| Perfect Forward Secrecy | <input type="text" value="Disable"/> | |
| Advanced IKE Settings | <input type="text" value="Show Advanced Settings"/> | |
| <input type="button" value="Apply/Save"/> | | |

Four parts with red mark are the major items which need to be check and edit according to your network topology. All other settings are related to security level how deep you want; just make sure both sides use the same security level settings.

When all settings are done, click button “Apply/Save” to activate your IPSec setting.

IPSec Tunnel Mode Connections

Add, remove or enable/disable IPSec tunnel connections from this page.

| Connection Name | Remote Gateway | Local Addresses | Remote Addresses | Remove |
|-----------------|----------------|-----------------|------------------|--------------------------|
| ToBranch1 | 20.100.0.50 | 192.168.0.0 | 192.168.50.0 | <input type="checkbox"/> |

Note 4: Check in advanced setup -> LAN IP settings that DSL Router IP Address is the same LAN subnet like in this config sample 192.168.50.254 (LAN pool 192.168.50.100-200)

Note 5: Disable IPv6 (Advanced Setup -> LAN -> IPv6 autoconfig)

IPv6 LAN Auto Configuration

Note: Stateful DHCPv6 is supported based on the assumption of prefix length less than 64. Interface ID does NOT support ZERO COMPF

Static LAN IPv6 Address Configuration

Interface Address (prefix length is required):

IPv6 LAN Applications

☐ Enable DHCPv6 Server

☒ Enable RADVD

☐ Enable MLD Snooping

Step 3: Repeat the Step 1 and 2 on Branch Office’s TW-EAV510

Step 4: Once both sites finish the above settings, the IPSec tunnel should be established immediately. And both parties just work like in the same network, easy to share everything securely.

Note 6: If the IPSec tunnel doesn’t work, please go to Management -> System Log, click the button “View System Log” to check anything wrong with IPSec’s setting. When the IPSec tunnel works ok, in system log is the info as below.

| | | | |
|----------------|--------|------|--|
| | | | SRC=222.186.3.15 DST=80.220.117.190 LEN=40 TOS=0x00 PREC=0x00 TTL=98 ID=256 PROTO=T |
| Nov 8 12:01:20 | daemon | info | racoon: INFO: IPsec-SA established: ESP/Tunnel 188.67.198.152[0]->80.220.117.190[0] spi=156242718(0x950131e) |
| Nov 8 12:01:20 | daemon | info | racoon: INFO: IPsec-SA established: ESP/Tunnel 80.220.117.190[0]->188.67.198.152[0] spi=129852710(0x7bd6526) |

Refresh

Close

Power Management

Power management is a feature of some electrical appliances, especially computers that turn off the power or switch to a low-power state when inactive.

Five main parameters are listed for users to check to manage the performance of the router.

Power Management

This page allows control of Hardware modules to evaluate power consumption. Use the control buttons to select the desired option, click Apply and check the status response.

MIPS CPU Clock divider when Idle

☒ Enable Status: Enabled

Wait instruction when Idle

☒ Enable Status: Enabled

DRAM Self Refresh

☒ Enable Status: Enabled

Energy Efficient Ethernet

☐ Enable Status: Disabled

Ethernet Auto Power Down and Sleep

☐ Enable Status: Disabled

Apply/Save Refresh

Multicast

Multicast is one of the three network transmission modes, Unicast, Multicast, Broadcast. It is a transmission mode that supports point-to-multipoint connections between the sender and the recipient. IGMP protocol is used to establish and maintain the relationship between IP host and the host directly connected multicast router.

IGMP stands for Internet Group Management Protocol, it is a communications protocols used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and the adjacent multicast routers to establish multicast group members. There are three versions for IGMP, that is IGMPv1, IGMPv2 and IGMPv3.

MLD, short for Multicast Listener Discovery protocol, is a component if the Internet Protocol version 6(IPv6) suite. MLD is used by IPv6 to discover multicast listeners on a directly attached link, much as IGMP used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol. MLDv1 is similar to IGMPv2 and MLDv2 is similar to IGMPv3.

Multicast Precedence: Disable ▾ lower value, higher priority

IGMP Configuration

Enter IGMP protocol configuration fields if you want modify default values shown below.

| | |
|--|-------------------------------------|
| Default Version: | <input type="text" value="2"/> |
| Query Interval: | <input type="text" value="60"/> |
| Query Response Interval: | <input type="text" value="4"/> |
| Last Member Query Interval: | <input type="text" value="4"/> |
| Robustness Value: | <input type="text" value="45"/> |
| Maximum Multicast Groups: | <input type="text" value="25"/> |
| Maximum Multicast Data Sources (for IGMPv3): | <input type="text" value="10"/> |
| Maximum Multicast Group Members: | <input type="text" value="25"/> |
| Fast Leave Enable: | <input checked="" type="checkbox"/> |

MLD Configuration

Enter MLD protocol (IPv6 Multicast) configuration fields if you want modify default values shown below.

| | |
|---|----------------------------------|
| Default Version: | <input type="text" value="2"/> |
| Query Interval: | <input type="text" value="125"/> |
| Query Response Interval: | <input type="text" value="10"/> |
| Last Member Query Interval: | <input type="text" value="10"/> |
| Robustness Value: | <input type="text" value="2"/> |
| Maximum Multicast Groups: | <input type="text" value="10"/> |
| Maximum Multicast Data Sources (for mldv2): | <input type="text" value="10"/> |
| Maximum Multicast Group Members: | <input type="text" value="10"/> |
| Fast Leave Enable: | <input type="checkbox"/> |

Apply/Save

Multicast Precedence: It is for multicast QoS. With lower multicast precedence, IGMP packets will be put into higher-priority queue. Default is set to disable.

IGMP

Default Version: Enter the supported IGMP version, 1-3, default is IGMP v3.

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

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

Last Member Query Interval: Enter the interval time (sec) the multicast router query the specified group after it has received leave message.

Robustness Value: Enter the router robustness parameter, 2-7, the greater the robustness value, the more robust the Querier is.

Maximum Multicast Groups: Enter the Maximum Multicast Groups.

Maximum Multicast Data Sources (for IGMP v3): Enter the Maximum Multicast Data Sources, 1- 24.

Maximum Multicast Group Members: Enter the Maximum Multicast Group Members.

Fast leave: Check to determine whether to support fast leave. If this value is enabled, IGMP proxy removes the membership of a group member immediately without sending an IGMP membership query on downstream. This is very helpful if user wants fast channel (group change) changing in cases like IPTV environment.

MLD

Default Version: Enter the supported MLD version, 1-2, default is MLDv2.

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

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

Last Member Query Interval: Enter the interval time (sec) the multicast router query the specified group after it has received leave message.

Robustness Value: Enter the router robustness parameter, default is 2, the greater the robustness value, the more robust the Querier is.

Maximum Multicast Groups: Enter the Maximum Multicast Groups.

Maximum Multicast Data Sources(for MLDv2): Enter the Maximum Multicast Data Sources, 1-24.

Maximum Multicast Group Members: Enter the Maximum Multicast Group Members.

Fast leave: Check to determine whether to support fast leave. If this value is enabled, MLD proxy removes the membership of a group member immediately without sending an MLD membership query on downstream. This is very helpful if user wants fast channel (group change) changing in cases like IPTV environment.

Wireless

Wireless 2.4GHz

This section provides you ways to configure wireless access.
The TW-EAV510 supports wireless on the 2.4 GHz.

This part has sub-items as Basic, Security, MAC Filter, Wireless Bridge, Advanced and Station Info here. Please select which one wireless you want to configure.

Basic

It let you determine whether to enable Wireless function and set the basic parameters of an AP and the Virtual APs.

Wireless -- Basic

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements. Click "Apply/Save" to configure the basic wireless options.

☒ Enable Wireless

☐ Enable Wireless Hotspot2.0

☐ Hide Access Point

☐ Clients Isolation

☐ Disable WMM Advertise

☒ Enable Wireless Multicast Forwarding (WMF)

SSID:

BSSID:

Country:

Country RegRev

Max Clients:

Wireless - Guest/Virtual Access Points:

| Enabled | SSID | Hidden | Isolate Clients | Disable WMM Advertise | Enable WMF | Max Clients | BSSID |
|--------------------------|---|--------------------------|--------------------------|--------------------------|--------------------------|---------------------------------|-------|
| <input type="checkbox"/> | <input type="text" value="wl0_Guest1"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="text" value="16"/> | N/A |
| <input type="checkbox"/> | <input type="text" value="wl0_Guest2"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="text" value="16"/> | N/A |
| <input type="checkbox"/> | <input type="text" value="wl0_Guest3"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="text" value="16"/> | N/A |

Wireless: Default setting is set to Enable. If you do not have any wireless devices, check the checkbox again to unselect.

Hide Access Point: It is function in which transmits its SSID to the air so that when wireless client searches for a network, router can then be discovered and recognized. Check the checkbox to determine whether you want to hide SSID.

Clients Isolation: if you enabled this function, then each of your wireless clients will not be able to communicate with each other.

Disable WMM Advertise: Stop the router from 'advertising' its Wireless Multimedia (WMM) functionality, which provides basic quality of service for time-sensitive applications (e.g. VoIP, Video). Check to disable or enable this function.

Enable wireless multicast Forwarding (WMF): check to enable or disable wireless multicast forwarding.

SSID: The SSID is the unique name of a wireless access point (AP) to be distinguished from another. For security purpose, change the default SSID to a unique ID name to the AP already built-in to the router's wireless interface. It is case sensitive and must not exceed 32 characters. Make sure your wireless clients have exactly the SSID as the device, in order to get connected to your network.

Note: SSID is case sensitive and must not exceed 32 characters.

BSSID: Basic Set Service Identifier, it is a local managed IEEE MAC address, and is 48 bits value.

Country: Different countries have different wireless band resources, so you can select the appropriate Country according to your location.

Max Clients: enter the number of max clients the wireless network can supports, 1-16.

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

Here you can enable some Virtual APs according to the request. And the other parameters of virtual APs are the same to the above.

Click Apply to apply your settings.

Security

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

Wireless -- Security

This page allows you to configure security features of the wireless LAN interface.
You may setup configuration manually

OR

through WiFi Protected Setup(WPS)

Note: When both STA PIN and Authorized MAC are empty, PBC is used. If Hide Access Point enabled or Mac filter list is empty with "allow" chosen, WPS2 will be disabled

WPS Setup

Enable WPS

Disabled ▼

Manual Setup AP

Select SSID:

TW-EAV510-2.4GHz-EFB2 ▼

Network Authentication:

Mixed WPA2/WPA -PSK ▼

WPA/WAPI passphrase:

[Click here to display](#)

WPA Group Rekey Interval:

3600

WPA/WAPI Encryption:

AES ▼

WEP Encryption:

Disabled ▼

Apply/Save

Note:

The WPS feature will also be unavailable when the security setting is not WPA2 or OPEN. So, if you manually set the wireless security setting, you should give notice to it, but you can find prompt indicating configuration.

Manual Setup AP

Select SSID: Select the SSID you want these settings apply to.

Network Authentication

i Open

WEP Encryption: Select to enable or disable WEP Encryption. Here select Enable.

Encryption Strength: Select the strength, 128-bit or 64-bit.

Current Network Key: Select the one to be the current network key. Please refer to key 1- 4 below.

Network Key (1- 4): Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys. Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys.

i Shared

This is similar to network authentication "Open". But here the WEP Encryption must be enabled.

i 802.1x

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 Key: Enter the password of RADIUS authentication server.

WEP Encryption: Select to enable or disable WEP Encryption. Here select Enable.

Current Network Key: Select the one to be the current network key. Please refer to key 2- 3 below.

Network Key (1- 4): Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys. Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys.

i WPA

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

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 Key: Enter the password of RADIUS authentication server.

WPA/WAPI Encryption: There are two Algorithms, AES (Advanced Encryption Standard) and TKIP(Temporal Key Integrity Protocol) which help to protect the wireless communication.

i WPA-PSK / WPA2-PSK

WPA/WAPI passphrase: Enter the WPA.WAPI passphrase; you can click here to display to view it.

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

WPA/ WAPI Encryption: There are two Algorithms, AES (Advanced Encryption Standard) and TKIP (Temporal Key Integrity Protocol) which help to protect the wireless communication.

i WPA2

WPA2 Preauthentication: When a wireless client wants to handoff to another AP, with preauthentication, it can perform 802.1X authentication to the new AP, and when handoff happens, this mode will help reduce the association time.

Network Re-auth Interval: the interval for network Re-authentication. This is in seconds.

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

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

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

RADIUS Key: Enter the password of RADIUS authentication server.

WPA/WAPI Encryption: There are two Algorithms, AES (Advanced Encryption Standard) and TKIP (Temporal Key Integrity Protocol) which help to protect the wireless communication.

i Mixed WPA2/WPA

WPA2 Preauthentication: When a wireless client wants to handoff to another AP, with preauthentication, it can perform 802.1X authentications to the new AP, and when handoff happens, this mode will help reduce the association time used.

Network Re-auth Interval: the interval for network Re-authentication. The unit is second.

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

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 Key: Enter the password of RADIUS authentication server.

WPA/WAPI Encryption: There are two Algorithms, AES (Advanced Encryption Standard) and TKIP (Temporal Key Integrity Protocol) which help to protect the wireless communication.

i Mixed WPA2/WPA-PSK

WPA/WAPI passphrase: enter the WPA.WAPI passphrase, you can click here to display to view it.

WPA Group ReKey Internal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). The unit is second.

WPA/WAPI Encryption: here are two Algorithms, AES (Advanced Encryption Standard) and TKIP (Temporal Key Integrity Protocol) which help to protect the wireless communication.

WPS Setup

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.

WPS: Select enable to enable WPS function. Please note that WPS can only be available when WPA2-PSK or OPEN mode is configured.

Wireless -- Security

This page allows you to configure security features of the wireless LAN interface.
You may setup configuration manually
OR
through WiFi Protected Setup(WPS)
Note: When both STA PIN and Authorized MAC are empty, PBC is used. If Hide Access Point enabled or Mac filter list is empty with "allow" chosen, WPS2 will be disabled

WPS Setup

Enable WPS

Enabled ▼

Add Client (This feature is available only when WPA-PSK(WPS1), WPA2 PSK or OPEN mode is configured)

☐ Use STA PIN

☐ Use AP PIN

Add Enrollee

Set WPS AP Mode

Configured ▼

Device PIN

12715657

MAC Filter

Wireless -- MAC Filter

Select SSID: TW-EAV510-2.4GHz-EFB2 ▼

MAC Restrict Mode: ☒ Disabled ☐ Allow ☐ Deny Note: If 'allow' is choosed and mac filter is empty, WPS will be disabled

| | |
|-------------|--------|
| MAC Address | Remove |
|-------------|--------|

| | |
|-----|--------|
| Add | Remove |
|-----|--------|

Select SSID: select the SSID you want this filter applies to.

MAC Restrict Mode:

- i Disable: disable the MAC Filter function.
- i Allow: allow the hosts with the following listed MACs to access the wireless network.
- i Deny: deny the hosts with the following listed MACs to access the wireless network.

Click Add to add the MACs.

MAC Address: enter the MAC address(es). The format of MAC address could be: xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx.

Click Apply to apply your settings and the item will be listed below.

If you don't need a rule, check the remove checkbox and press Remove to delete it.

Wireless Bridge

WDS (wireless distributed system) is a wireless access point mode that enables wireless link and communication with other access points. It's easy to install, simply define the peer's MAC address of the connected AP. WDS takes advantage of cost saving and flexibility with no extra wireless client device required to bridge between two access points and extending an existing wired or wireless infrastructure network to create a larger network.

Bridge Restrict: Enabled ▾

Remote Bridges MAC Address: Enabled

Enabled(Scan)

Disabled

Bridge Restrict: Enabled, Enabled (scan), disabled

Remote Bridge MAC Address:

Enabled: Enter the remote bridge MAC addresses. Here up to 4 bridge MAC addresses are supported.

Enabled(Scan): Only those scanned by the gateway can communicate.

Disabled: Does not restrict the gateway communicating with bridges that have their MAC address listed, but it is still open to communicate with all bridges that are in the same network.

Click Apply to apply your settings.

Advanced

Here users can set some advanced parameters about wireless.

| | | |
|----------------------------------|----------------------------|---------------------------------------|
| Band: | <div>2.4GHz ▾</div> | |
| Channel: | <div>9 ▾</div> | Current: 9 (interference: acceptable) |
| Auto Channel Timer(min) | <div>0</div> | |
| 802.11n/EWC: | <div>Auto ▾</div> | |
| Bandwidth: | <div>20MHz / 40MHz ▾</div> | Current: 20MHz |
| Control Sideband | <div>Lower ▾</div> | Current: N/A |
| 802.11n Rate: | <div>Auto ▾</div> | |
| 802.11n Protection: | <div>Auto ▾</div> | |
| Support 802.11n Client Only: | <div>Off ▾</div> | |
| RIFS Advertisement: | <div>Auto ▾</div> | |
| OBSS Coexistence: | <div>Enable ▾</div> | |
| RX Chain Power Save: | <div>Disable ▾</div> | Power Save status: Full Power |
| ARX Chain Power Save Quiet Time: | <div>10</div> | |
| RX Chain Power Save PPS: | <div>10</div> | |
| 54g™ Rate: | <div>1 Mbps ▾</div> | |
| Multicast Rate: | <div>Auto ▾</div> | |
| Basic Rate: | <div>Default ▾</div> | |
| Fragmentation Threshold: | <div>2346</div> | |
| RTS Threshold: | <div>2347</div> | |
| DTIM Interval: | <div>1</div> | |
| Beacon Interval: | <div>100</div> | |
| Global Max Clients: | <div>64</div> | |
| XPress™ Technology: | <div>Disabled ▾</div> | |
| Transmit Power: | <div>100% ▾</div> | |
| WMM(Wi-Fi Multimedia): | <div>Enabled ▾</div> | |
| WMM No Acknowledgement: | <div>Disabled ▾</div> | |
| WMM APSD: | <div>Enabled ▾</div> | |
| Beamforming Transmission (BFR): | <div>Disabled ▾</div> | |
| Beamforming Reception (BFE): | <div>Disabled ▾</div> | |

- Band:** Select frequency band. Here 2.4GHz.
- Channel:** Allows channel selection of a specific channel (1-7) or Auto mode.
- Auto Channel Timer (min):** The auto channel times length it takes to scan in minutes. Only available for auto channel mode.
- 802.11n/EWC:** select to auto enable or disable 802.11n.
- Bandwidth:** Select bandwidth. The higher the bandwidth the better the performance will be.
- Control Sideband:** only available for 40MHz. It allows you to select upper sideband or lower sideband. Sideband refers to the frequency band either above (upper sideband) or below ower sideband) the carrier frequency, within which fall the spectral components produced by modulation of a carrier wave.

802.11n Rate: This allows you to select the fixed transmission rate or auto.

802.11n Protection: turn off for maximize throughput. Auto for greater security.

Support 802.11n Client Only: turn on the option to only provide wireless access to the clients operating at 802.11n speeds.

RIFS Advertisement: Reduced Inter-frame Spacing (RIFS) is a 802.11n feature that also improves performance by reducing the amount of dead time required between OFDM transmissions. Select Off to disable this function or auto to enable this function.

OBSS Co-Existence: coexistence (or not) between 20 MHZ and 40 MHZ overlapping basic service sets (OBSS) in wireless local area networks.

RX Chain Power Save: Enabling this feature turns off one of the Receive chains, going from 2x2 to 2x1 to save power.

RX Chain Power Save Quiet Time: The number of seconds the traffic must be below the PPS value before the Rx Chain Power Save feature activates itself.

RX Chain Power Save PPS: The maximum number of packets per seconds that can be processed by the WLAN interface for a duration of Quiet Time, described above, before the Rx Chain Power Save feature activates itself.

54g™ Rate:

Multicast Rate: Setting for multicast packets transmission rate.

Basic Rate: Setting for basic transmission rate. It is not a specific kind of rate, it is a series of rates supported. When set to Default, the router can transmit with all kinds of standardized rates.

Fragmentation 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.

DTIM Interval: Delivery Traffic Indication Message (DTIM). The entry range is a value between 1 and 255. A DTIM is countdown variable that informs clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM interval value. AP clients hear the beacons and awaken to receive the broadcast and multicast messages. The default is 1.

Beacon Interval: The amount of time between beacon transmissions in is milliseconds. The default is 100ms and the acceptable is 1- 65535. The beacon transmissions identify the presence of an access point.

Global Max Clients: Here you have the option of setting the limit of the number of clients who can connect to your wireless network.

XPress™ Technology: It has been designed to improve the wireless network efficiency. Default is disabled.

Transmit Power: select the transmitting power of your wireless signal.

WMM (Wi-Fi Multimedia): you can choose to enable or disable this function which allows for priority of certain data over wireless network.

WMM No Acknowledgement: Refers to the acknowledge policy at the MAC level. Enabling WMM No Acknowledgement can result in more efficient throughput but higher error rates in noisy Radio Frequency (RF) environment.

WMM APSD: Automatic Power Save Delivery. Enable this to save power.

Station Info

Here you can view information about the wireless clients.

st SSID -- Authenticated Stations

This page shows authenticated wireless stations and their status.

| MAC | Associated | Authorized | SSID | Interface |
|-----|------------|------------|------|-----------|
|-----|------------|------------|------|-----------|

Refresh

- MAC Address:** The MAC address of the wireless clients.
- Associated:** List all the stations that are associated with the Access Point. If a station is idle for too long, it is removed from this list
- Authorized:** List those devices with authorized access. SSID: Show the current SSID of the client.
- SSID:** To show wireless SSID
- Interface:** To show which interface the wireless client is connected to.
- Refresh:** To get the latest information.

Time Schedule

Time Schedule is aimed to offer methods to flexibly control when the wireless network (SSID) is allowed for access.

The Wireless schedule only functions whilst Wireless is enabled.
The Guest/Virtual AP schedule control only operates whilst the associated AP is enabled.

Time Schedule

Name:

Select SSID:

TW-EAV510-2.4GHz-EFB2 ▼

| Days of the week | Sun | Mon | Tue | Wed | Thu | Fri | Sat |
|------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| Click to select | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Note: Start Time same as End Time means the whole day.

Start Time (hh:mm):

End Time (hh:mm):

Apply/Save

Click to select: Set when the SSID works. If user wants the SSID do not work all the time, please set the exact time your want the SSID works. Select wanted day(s) and set start time and end time.

Diagnostics

Tools

TeleWell TW-EAV510 offers diagnostics tools including “Ping” and “Trace route test” tools to check for problems associated with network connections.

Ping Test: to verify the connectivity between source and destination.

Trace route Test: to trace the route to see how many hops (also see the exact hops) the packet of data has to take to get to the destination.

Ping and Trace Route

Please input the IP address or Domain name and click "Ping" , "Trace Route" or "Nslookup".

IP Address/Domain Name:

Source IP Address/Interface Name:

Ping

Trace Route

Nslookup

IP Address/Domain Host: Enter the destination host (IP, domain name) to be checked for connectivity.

Source Address: Set the source address to test the connectivity from the source to the destination.

Ping Test: Press this button to proceed ping test.

Diagnostics

Check the connections, including Ethernet connection, Internet Connection and wireless connection.
Click Help link that can lead you to the interpretation of the results and the possible, simply troubleshooting.

ipoe_0_0_33 Diagnostics

Your modem is capable of testing your DSL connection. The individual tests are listed below.

Test the connection to your local network

| | |
|--------------------------------|----------|
| Test your Connection (LAN1): | FAIL |
| Test your Connection (LAN2): | PASS |
| Test your Connection (LAN3): | FAIL |
| Test your Connection (LAN4): | FAIL |
| Test your Wireless Connection: | PASSPASS |

Test the connection to your DSL service provider

| | |
|----------------------------------|----------|
| Test xDSL Synchronization: | FAIL |
| Test ATM OAM F5 segment ping: | DISABLED |
| Test ATM OAM F5 end-to-end ping: | DISABLED |

Test the connection to your Internet service provider

| | |
|----------------------------------|------|
| Ping default gateway: | FAIL |
| Ping primary Domain Name Server: | PASS |

Next Connection

TestTest With OAM F4

Management

Settings

Backup / Update

These functions allow you to save and backup your router’s current settings to a file on your PC, or to restore from a previously saved backup. This is useful if you wish to experiment with different settings, knowing that you have a backup handy in the case of any mistakes. It is advisable to backup your router’s settings before making any significant changes to your router’s configuration.

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

Settings - Backup

Backup Broadband Router configurations. You may save your router configurations to a file on your PC.

Backup Settings

Click Browse and browse to the location where your backup file is saved, then click Open. Then in the above page, click Update Settings. Let it update to 100%, it will automatically turn to the Device Info page.

Tools -- Update Settings

Update Broadband Router settings. You may update your router settings using your saved files.

Settings File Name: Ei valittua tiedostoa

Update Settings

Restore Default

If you wish to restart the router using the factory default settings (for example, after a firmware upgrade or if you have saved an incorrect configuration), select restore default to reset to factory default settings.

Tools -- Restore Default Settings

Restore Broadband Router settings to the factory defaults.

Restore Default Settings

System Log

System Log -- Configuration

If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.

Configuration

Log: ☐ Disable ☒ Enable

Log Level:

Display Level:

Mode:

Log: Enable or disable this function.

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:

- i Emergency = system is unusable
- i Alert = action must be taken immediately
- i Critical = critical conditions
- i Error = error conditions
- i Warning = warning conditions
- i Notice = normal but significant conditions
- i Informational = information events
- i 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.

- i Local: Select this mode to store the logs in the router's local memory.
- i 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.
- i Both: Logs stored adopting above two ways.

Click Apply to save your settings.

SNMP Agent

SNMP, Simple Network Management Protocol, is the most popular one in network. It consists of SNMP Manager, SNMP Agent and MIB. Every network device supporting SNMP will have a SNMP Agent which is a management software running in the device.

SNMP Manager, the management software running on the server, it uses SNMP protocol to send GetRequest 、 GetNextRequest, SetRequest message to Agent to view and change the information of the device.

SNMP Agents, the management software running in the device, accepts the message from the manager, Reads or Writes the management variable in MIB accordingly and then generates Response message to send it to the manager. Also, agent will send Trap message to the manager when agent finds some exceptions. Trap message, is the message automatically sent by the managed device without request to the manager about the emergency events.

SNMP - Configuration

Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device.

Select the desired values and click "Apply" to configure the SNMP options.

SNMP Agent ☒ Disable ☐ Enable

Read Community:

Set Community:

System Name:

System Location:

System Contact:

Trap Manager IP:

public

private

TW-EAVS10AC

unknown

unknown

0.0.0.0

Save/Apply

- SNMP Agent:** enable or disable SNMP Agent.
- Read Community:** Type the Get Community, which is the authentication for the incoming Get-and GetNext requests from the management station.
- Set Community:** Type the Set Community, which is the authentication for incoming Set requests from the management station.
- System Name:** here it refers to your router.
- System Location:** user-defined location.
- System Contact:** user-defined contact message.
- Trap manager IP:** enter the IP address of the server receiving the trap sent by SNMP agent.

Alert

Mail Alert

Mail alert is designed to keep system administrator or other relevant personnel alerted of any unexpected events that might have occurred to the network computers or server for monitoring efficiency. With this alert system, appropriate solutions may be tackled to fix problems that may have arisen so that the server can be properly maintained.

Mail Alert

SMTP Server Configuration

WAN: DSL ▼ Apply the same setting to the other WAN: ☐ EWAN ☐ 3G/LTE

SMTP Server:

Username:

Password:

Sender's E-mail:

Sender's Display Name:

☐ Enabled SSL/TLS

SSL/TLS Port:

WAN IP Address Changed Alert

Recipient's E-mail:

WAN: Mail Alert feature can be applicable to every WAN mode: Ethernet, DSL and 3G/LTE. Select the port you want to use Mail Alert.

For example DSL, then when the WAN connection is in DSL mode and when there is any unexpected event, the alert message will be sent to your specified E-mail.

Apply all settings to: check whether you want to have a copy of the settings to apply to other WAN port, suppose the above Main port is DSL, then if you enable this function, then Ethernet port will have the same configuration.

SMTP Server: Enter the SMTP server that you would like to use for sending emails. **Username:** Enter the username of your email account to be used by the SMTP server. **Password:** Enter the password of your email account.

Username:

Password:

Sender's Email: Enter your email address.

SSL: check to whether to enable SSL encryption feature.

SSL/TLS Port: the port, default is 25.

Sender's account Test: Press this button to test the connectivity and feasibility to your sender's e-mail.

WAN IP Change Alert:

Recipient's Email Enter the email address that will receive the alert message once a WAN IP change has been detected.

SMS Alert

SMS, Short Message Service, is to inform clients the information clients subscribe. The TeleWell TW-EAV510 offers SMS alert sending clients alert messages when a WAN IP change is detected.

SMS Alert

WAN IP Changed Alert Number: (ex. +35840xxxxxxx)

Apply/Save

WAN IP Change Alert: Enter the Recipient's number that will receive the alert message once a WAN IP change has been detected.

The TW-EAV510 series can be controlled by SMS message through 3G/LTE dongles. Below is supported command for reference.

reboot → Restart the Router.

wanip → Get all connected WAN IP address information.

remote on → Enable remote WEB GUI management service.

remote off → Disable remote WEB GUI management service.

pptp-lan username password gateway mppe peer_ip peer_mask → Setup a temporary PPTP Client LAN to LAN connection.

pptp-remote username password gateway mppe → Setup a temporary PPTP Client Remote Access connection.

SMS Control

Note:

1. The SIM card must support SMS service and it also depends on dongle you use, some of dongles may not support SMS when data connection is up.
2. All command are case sensitivity.
3. You will get SMS response message once the command is executed successfully, please check the command and send it again if you don't get any response message after 30 seconds.

For security reason, you must enter the number that has access right to the TW-EAV510/AC. You can find this setting at **Management -> SMS Control**. The TW-EAV510/AC only responses to the command which sending from allowed phone number here.

Example:

SMS Control

Maximum entries: 8

| Allowed Phone Number | Remove | Edit |
|----------------------|--------------------------|------|
| 0412345678 | <input type="checkbox"/> | Edit |

The command “**reboot**”, “**wanip**”, “**remote on**” and “**remote off**” have no extract parameters. Below is more details for PPTP SMS command for reference.

Example for command “pptp-lan”:

The value for mppe is 1 or 0 (1: Enable, 0: Disable)

SMS Text: pptp-lan testuser testpw lantolan.pptp.server 1 192.168.50.0 255.255.255.0

With the above SMS text, you will get settings as below.

Client

Maximum entries: 4

| Name | Type | Local Gateway Interface | Remote Gateway | Username | MPPE | Connection Type | Peer IP | Peer Netmask | Enable | Remove | Edit |
|----------|------|-------------------------|----------------------|----------|--------|-----------------|--------------|---------------|--------------------------|--------|------|
| SMS_temp | pptp | pppo3g0 | lantolan.pptp.server | testuser | Enable | LAN TO LAN | 192.168.50.0 | 255.255.255.0 | <input type="checkbox"/> | | |

Example for command “pptp-remote”:

The value for mppe is 1 or 0 (1: Enable, 0: Disable)

SMS Text: pptp-remote testuser testpw lantolan.pptp.server 0

With the above SMS text, you will get settings as below.

Client

Maximum entries: 4

| Name | Type | Local Gateway Interface | Remote Gateway | Username | MPPE | Connection Type | Peer IP | Peer Netmask | Enable | Remove | Edit |
|----------|------|-------------------------|----------------------|----------|---------|-----------------|---------|--------------|--------------------------|--------|------|
| SMS_temp | pptp | pppo3g0 | lantolan.pptp.server | testuser | Disable | Remote Access | | | <input type="checkbox"/> | | |

Note:

1. The system will only create one SMS temporary PPTP client connection and overwrite the setting if you send SMS message again.
2. This entry is not included in maximum entries, totally you can have 4 x normal PPTP client entries + 1 x SMS PPTP client entry.
3. This SMS temporary PPTP client connection can only work one time and the state will change to disable if connection lost or disconnected. You must send SMS message to enable it again.

Internet Time

The router does not have a real time clock on board; instead, it uses the Network Time Protocol (NTP) to get the most current time from an NTP server.

NTP is a protocol for synchronization of computers. It can enable computers synchronize to the NTP server or clock source with a high accuracy.

Time settings

This page allows you to the modem's time configuration.

☒ Automatically synchronize with Internet time servers

| | | |
|-------------------------|---|-------------------|
| First NTP time server: | Other ▼ | ntp.inet.fi |
| Second NTP time server: | Other ▼ | ntp.elisa.fi |
| Third NTP time server: | Other ▼ | 1.fi.pool.ntp.org |
| Fourth NTP time server: | Other ▼ | ntp.tdc.fi |
| Fifth NTP time server: | ntp1.tummy.com ▼ | |
| Time zone offset: | (GMT+02:00) Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius ▼ | |

Apply/Save

Choose the NTP time server from the drop-down menu, if you prefer to specify an NTP server other than those in the drop-down list, simply enter its IP address in their appropriate blanks provided as shown above. Your ISP may also provide an SNTP server for you to use.

Choose your local time zone from the drop-down menu. After a successful connection to the Internet, the router will retrieve the correct local time from the NTP server you have specified. If you prefer to specify an NTP server other than those in the drop-down list, simply enter its IP address in their appropriate blanks provided as shown above. Your ISP may also provide an NTP server for you to use.

Click Apply to apply your settings.

Access Control

Passwords

Access Control is used to prevent unauthorized access to the router configuration page. Here you can change the login user password. Three user levels are provided here. Each user level there's a default provided user. You must access the router with the appropriate username and password. Here the corresponding passwords are allowed to change.

Access Control -- Passwords

Access to your broadband router is controlled through admin account.

The user name "admin" has unrestricted access to change and view configuration of your Broadband Router.

Use the fields below to enter up to 16 characters and click "Apply/Save" to change passwords.

Note: Password cannot contain a space.

| | |
|-------------------|--------------------------|
| User Name: | admin |
| Old Password: | <input type="password"/> |
| New Password: | <input type="password"/> |
| Confirm Password: | <input type="password"/> |

Apply/Save

Username: the default username is admin, it cannot be changed

Old Password: Enter the old password.

New Password: Enter the new password.

Confirm Password: Enter again the new password to confirm.

Click Apply to apply your new settings.

Services

It is to allow remote access to the router to view or configure.

Access Control -- Services

A Service Control List ('SCL') enables or disables services from remote access.

- ☐ Enable FTP service
- ☐ Enable HTTP service
- ☒ Enable ICMP service
- ☐ Enable SNMP service
- ☐ Enable SSH service
- ☐ Enable TELNET service
- ☐ Enable TFTP service

Save/Apply

Enable Service: Select to determine which service(s) is (are) allowed for remote access. By default ICMP service is allowed for remote access.

Click Apply button to submit your settings.

IP Addresses

The IP Address Access Control mode, if enabled, permits access to local management services from IP addresses contained in the Access Control List. If the Access Control mode is disabled, the system will not validate IP addresses for incoming packets. The services are the system applications listed in the Service Control List.

Click the **Add** button, access the following window displayed on the next page.

Access Control -- IP Addresses

The IP Address Access Control mode, if enabled, permits access to local management services from IP addresses contained in the Access Control List. If the Access Control mode is disabled, the system will not validate IP addresses for incoming packets.

Access Control Mode: ☒ Disable ☐ Enable

| | | |
|------------|-------------|--------|
| IP Address | Subnet Mask | Remove |
|------------|-------------|--------|

Add

Remove

Input the IP Address and Subnet Mask which you want to configure, and then click **Apply/Save** to enable this IP Address.

Add IP Addresses

Enter the IP address of the management station permitted to access the local management services, and click "Apply/Save".

IP Address:

Subnet Mask:

Apply/Save

Miscellaneous

In the page can define the name for the router

Auto Reboot

Auto reboot offers flexible rebooting service (reboot with the current configuration) of router for users in line with scheduled timetable settings.

Auto Reboot

Configure Schedule:

1. ☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat 00 ▼ : 00 ▼

2. ☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat 00 ▼ : 00 ▼

Enable to set the time schedule for rebooting.

Update Software

Software upgrading lets you experience new and integral functions of your router.

Tools -- Update Software

Step 1: Obtain an updated software image file from your ISP.

Step 2: Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.

Step 3: Click the "Update Software" button once to upload the new image file.

Software File Name: Ei valittua tiedostoa

Your router's "firmware" is the software that allows it to operate and provides all its functionality. Think of your router as a dedicated computer, and the firmware as the software it runs. Over time this software may be improved and revised, and your router allows you to upgrade the software it runs to take advantage of these changes.

Clicking on Browse will allow you to select the new firmware image file you have downloaded to your PC. Once the correct file is selected, click Upgrade to update the firmware in your router.

After the update, the device must restore to default settings (Management / Settings / Restore default)

Reboot

If you want to restart after the current setting, click reboot

Click the button below to reboot the router.

Declaration of Conformity

in accordance with the Radio and Telecommunications Terminal Equipment Act (FTEG)
and Directive 1999/5/EC (R&TTE Directive)

The Manufacturer: TeleWell Oy
Kinnarinkatu 1
04430 Järvenpää FINLAND

declares that the product: TW-EAV510 ADSL2+ / VDSL2

complies with the essential requirements of §3 and the other relevant provisions of the FTEG
(Article 3 of the R&TTE Directive), when used for its intended purpose.

Harmonised standards: Health and Safety requirements contained in §3 (1) 1. (Article 3 (1) a))
EN60950-1: 2001+A11: 2006, IEC60950-1-2001: 2005

Harmonised standards: Protection requirements with respect to EMC §3 (1) 2, (Article 3 (1) b))

EN 55022:2006/A1:2007 (Class B), EN 61000-3-2: 2006, EN 61000-3-3: 1995+ A1: 2001+ A2:
2005, EN 55024: 1998+A1: 2001+ A2: 2003 (IEC 61000-4-2: 1995+A1: 1998+A2: 2000,
IEC 61000-4-3: 2006, IEC 61000-4-4: 2004, IEC 61000-4-5: 2005, IEC 61000-4-6 : 2006, IEC
61000-4-8: 1993+A1: 2000, IEC 61000-4-11: 2004)

Harmonised standards: Measures for the efficient use of the radio frequency spectrum ETSI
EN 301 489-1 V1.8.1 (2008-04), EN 301 489-17 V1.3.2 (2008-04)
EN 300 328 V1.7.1 (2006-10)

Interface specification: Air interface of the radio systems pursuant to § 3(2) (Article 3(2))
2.412 — 2.472 GHz

This declaration is issued by:

Järvenpää

1.5.2015

(Place)

(Date)



04430 Järvenpää

Managing Director
TeleWell Oy Finland