

VPN

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

PPTP

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

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

PPTP VPN Configuration

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

PPTP VPN

☐ Disable ☒ Enable

PPTP Server

Auth. Type

PAP

Peer Address

start from:

Local Address

Apply

Encryption Mode

NONE

Server Account

Name

Username

Connection Type

☒ Remote Access ☐ LAN to LAN

Peer Network IP

Add

Edit

Tunnel Password

Peer Netmask

☐ Disable ☒ Enable

PPTP Server Table

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

PPTP Client

Name

Username

Auth. Type

PAP

Connection Type

☒ Remote Access ☐ LAN to LAN

Peer Network IP

Default Gateway

☐

Add

Edit

Server Address

Password

Encryption Mode

NONE

Peer Netmask

PPTP Client Table

Edit	Interface	Server	Connection Type	Peer Network IP	Peer Netmask	Action	Select
Delete Selected							

PPTP VPN: Enable/Disable PPTP function.

PPTP Server

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

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

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

Local IP Address: Enter the IP address for PPTP tunnel virtual interface.

Server Account

Name: Enter the name for this account profile.

Tunnel: Enable/Disable this tunnel.

Username: Enter the username for login authentication.

Password: Enter the password for login authentication.

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

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

PPTP Client

Name: Enter the name for this client rule.

Server Address: Specify the remote PPTP server IP address or domain name.

Username: Enter the username for PPTP login authentication.

Password: Enter the password for PPTP login authentication.

Auth.Type: Setup the authentication type for connecting to PPTP server. This setting must follow server side.

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

Default Gateway: Make this PPTP tunnel as default gateway for all local traffic when it is checked.

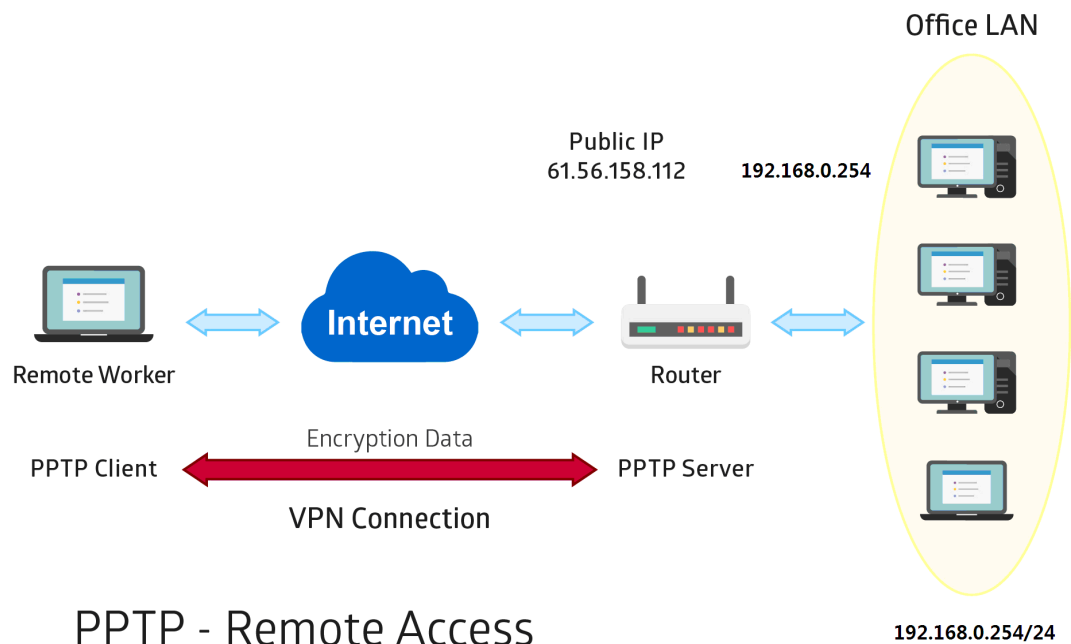
Peer IP: Enter the peer side LAN IP address for LAN to LAN type.

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

How to for PPTP Server/Client

Example: PPTP Remote Access connection

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



Configuring PPTP server in the office

1. Set the PPTP Server

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

PPTP VPN

☐ Disable

☒ Enable

PPTP Server

Auth. Type

MS-CHAPV2

Peer Address

start from: 192.168.100.2

Local Address

192.168.100.254

Apply

Encryption Mode

MPPE

Server Account

Name

test

Username

test

Connection Type

☒ Remote Access

☐ LAN to LAN

Peer Network IP

Add

Edit

Tunnel

☐ Disable

☒ Enable

Password

test

Peer Netmask

PPTP Server Table

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

Delete Selected

Save

Client Side: Windows series

Windows 10 (PPTP Client)

1. Make sure PC can access internet.
2. Go to **Control Panel -> Network and Internet -> Network and Sharing Center** click **Setup a new connection or network** to add a new PPTP connection.

Change your networking settings



Set up a new connection or network

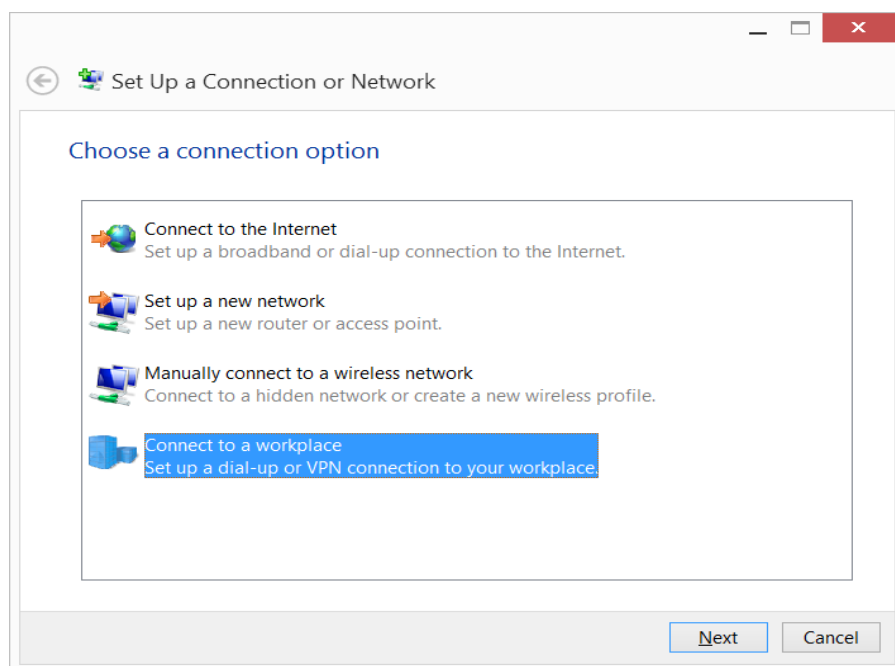
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.



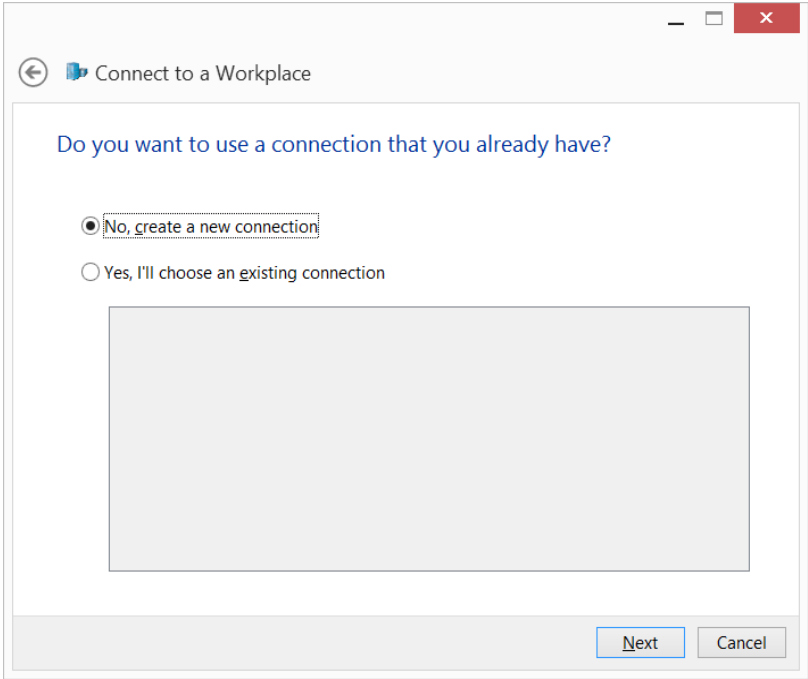
Troubleshoot problems

Diagnose and repair network problems, or get troubleshooting information.

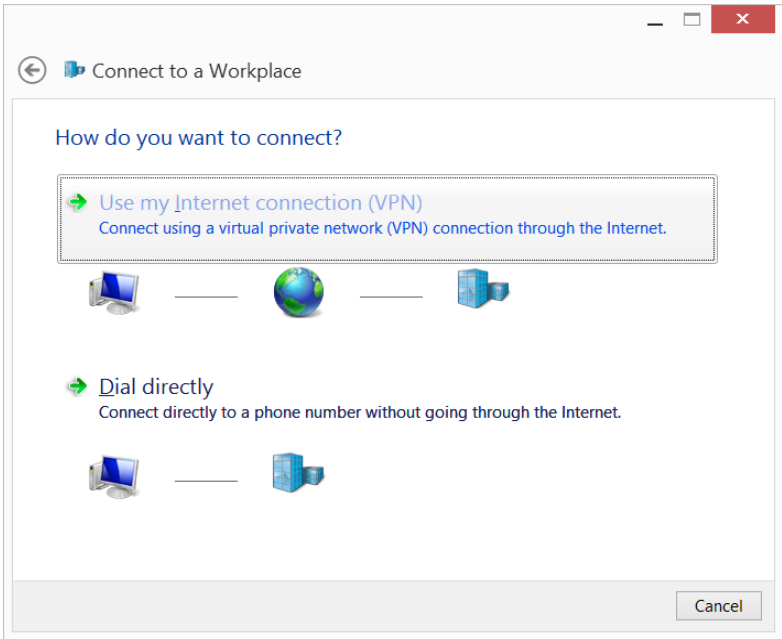
3. Select **Connect to a workplace**.



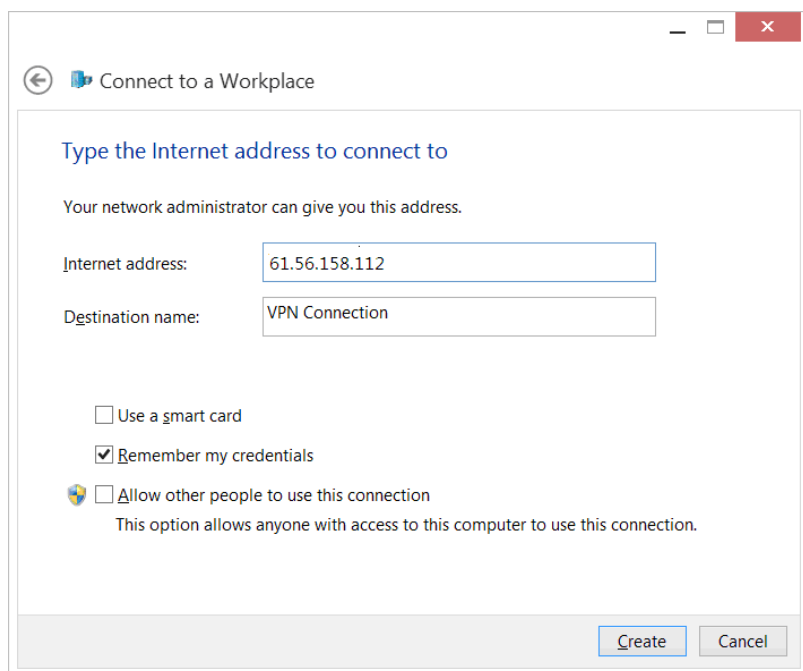
4. Select **No, create a new connection** and click **Next** button for next step.



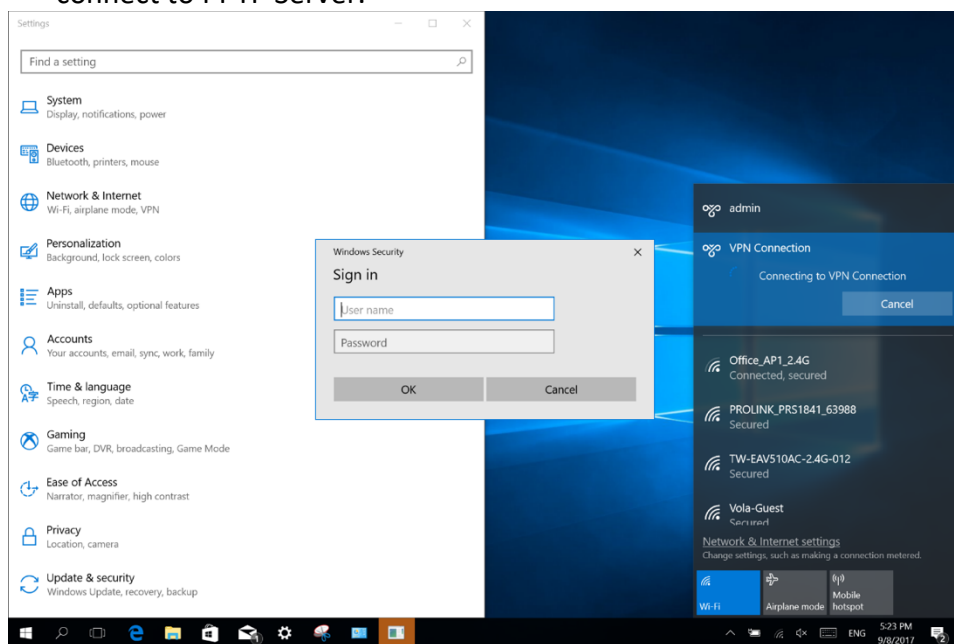
5. Select **Use my Internet connection (VPN)**.



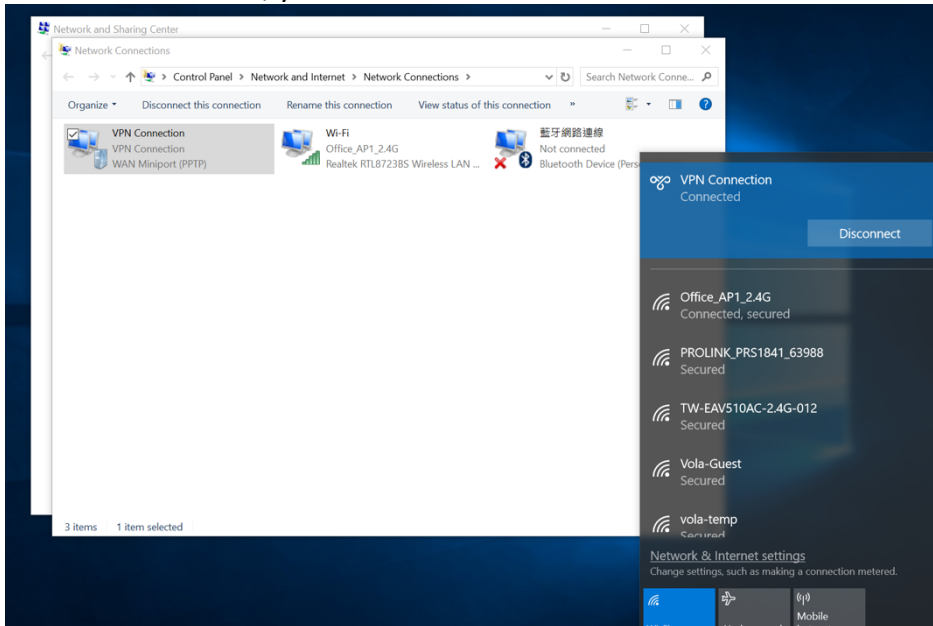
6. Enter the PPTP Server address/domain to field named **Internet address**. Please make sure your domain name address is work correctly if you are use domain name instead of IP address. Click **Create** button finish the PPTP client settings on Windows.



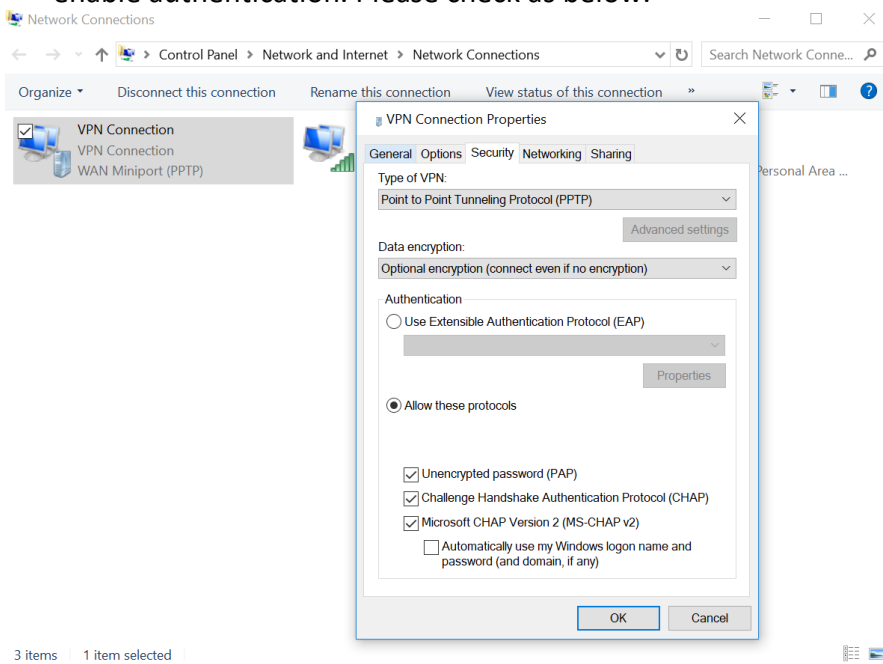
7. Enter the **username** and **password** that set on TW-EAV510 AC's PPTP Server and click **OK** button to connect to PPTP Server.



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



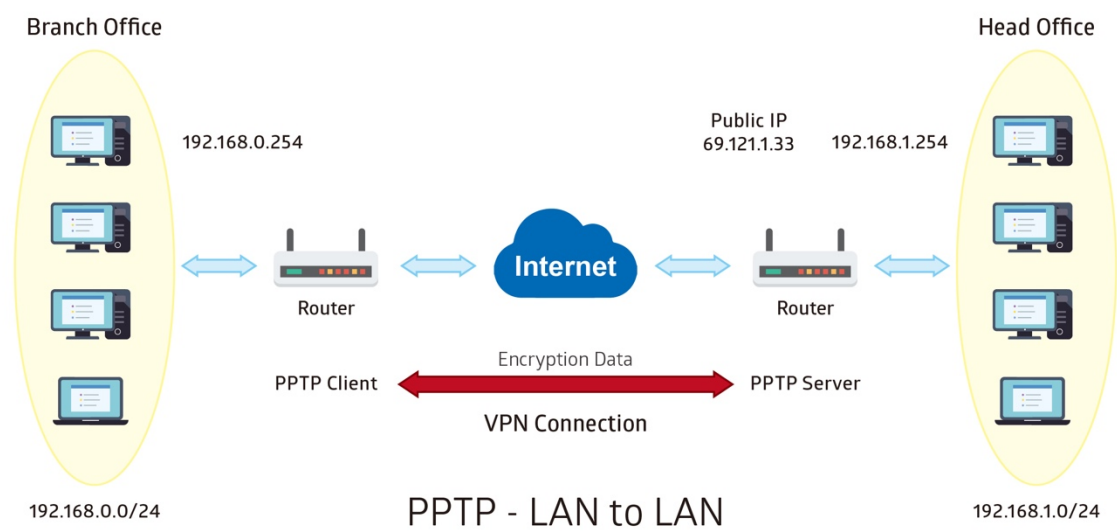
9. If you have problem connect with PPTP VPN via PC, please check **Control Panel -> Network and Internet -> Network and Sharing Center**, click **Change adapter settings** on left side, would show VPN Connection then right click to select **Properties -> Security**. Choose **Type of VPN** to **Point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



Example: PPTP LAN-to-LAN connection

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

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



Configuring PPTP server in the office

Set the PPTP Server

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

PPTP VPN

☐ Disable ☒ Enable

PPTP Server

Auth. Type

MS-CHAPV2

Peer Address

start from: 192.168.100.2

Local Address

192.168.100.254

Apply

Encryption Mode

MPPE

Server Account

Name

test

Username

test

Connection Type

☐ Remote Access ☒ LAN to LAN

Peer Network IP

192.168.0.0

Add

Edit

Tunnel

☐ Disable ☒ Enable

Password

test

Peer Netmask

255.255.255.0

PPTP Server Table

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

Delete Selected

Save

Configuring PPTP client in the branch office

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

PPTP Client

Name

test

Username

test

Auth. Type

MS-CHAPV2

Connection Type

Remote Access

LAN to LAN

Peer Network IP

192.168.1.0

Default Gateway

Add

Edit

Server Address

69.121.1.33

Password

test


Encryption Mode

MPPE

Peer Netmask

255.255.255.0

PPTP Client Table

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

L2TP

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

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

L2TP VPN Configuration

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

L2TP VPN

☐ Disable ☒ Enable

L2TP Server

Auth. Type

PAP

Encryption Mode

NONE

Tunnel Authentication

☐

Secret

Peer Address

start from

Local Address

Apply

Server Account

Name

Username

Connection Type

☒ Remote Access ☐ LAN to LAN

Peer Network IP

Tunnel Password

Peer Netmask

Add

Edit

L2TP Server Table

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

L2TP Client

Name

Username

Tunnel Authentication

☐

Auth. Type

PAP

PPP Connection Type

Persistent

MTU

Connection Type

☒ Remote Access ☐ LAN to LAN

Peer Network IP

Server Address

Password

Secret

Encryption Mode

NONE

Idle Time (min)

Default Gateway

☐

Peer Netmask

Add

Edit

L2TP Client Table

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

L2TP VPN: Enable/Disable L2TP function.

L2TP Server

Auth. Type: Setup the authentication type for client.

Encryption Mode: Setup MPPE encryption for L2TP tunnel, MPPE can only be enabled when *Auth. Type* set to MS-CHAPV2.

Tunnel Authentication: Enable/Disable the tunnel authentication.

Secret Key: Enter the secret key for tunnel authentication.

Assigned to Peer IP Address start from: Enter the IP address that will be assigned to remote L2TP client. The IP address cannot in DHCP IP Pool range.

Local IP Address: Enter the IP address for L2TP tunnel virtual interface.

Server Account

Name: Enter the name for this account profile.

Account: Enable/Disable this account.

Username: Enter the username for login authentication.

Password: Enter the password for login authentication.

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

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

L2TP Client

Name: Enter the name for this client rule.

Server Address: Specify the remote L2TP server IP address or domain name.

Username: Enter the username for L2TP login authentication.

Password: Enter the password for L2TP login authentication.

Tunnel Authentication: Enable/Disable the tunnel authentication.

Secret Key: Enter the secret key for tunnel authentication.

Authentication Type: Setup the authentication type for connecting to L2TP server. This setting must follow server side.

Encryption Mode: Setup MPPE encryption for L2TP tunnel, MPPE can only be enabled when *Auth. Type* set to MS-CHAPV2. This setting must follow server side.

Default Gateway: Make this PPTP tunnel as default gateway for all local traffic when it is checked.

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

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

How to for L2TP Server/Client

Please Refer to PPTP.

IPSec

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

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

IPSec VPN Table									
Select	Connection Name	Active	Protocol	Local Port	Remote Port	Local Network	Remote Network	Remote Security Gateway	Edit
<div>Add New ConnectionDelete SelectedEnableDisable</div>									

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

IPsec VPN Configuration

IPsec Settings

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

Phase 1

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

Phase 2

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

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

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

IPsec Connection Setting

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Phase 1

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

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

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

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

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

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

Phase 2

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

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

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

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

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

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

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

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

Keep Alive:

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

Detection Interval: The period cycle for dead peer detection.

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

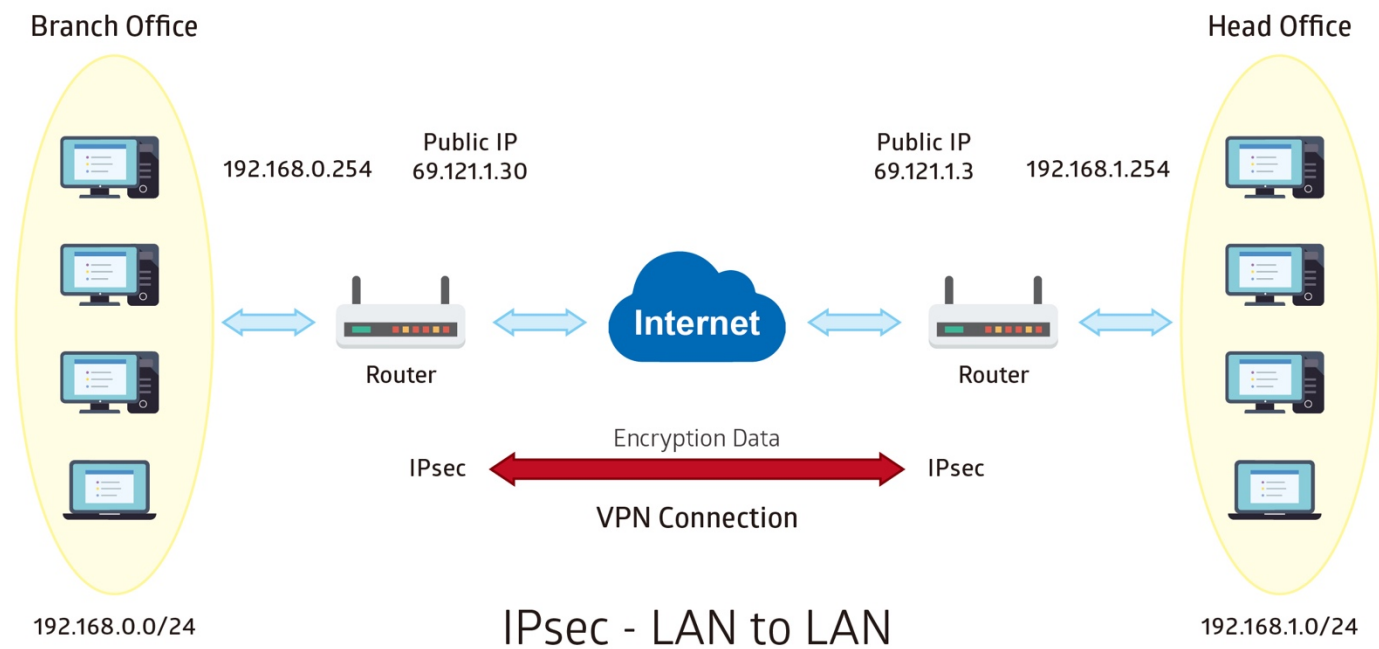
Click **SAVE** to submit the settings.

How to for IPsec

1. LAN-to-LAN connection

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

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



Head Office Side:

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

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

Phase 1

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

Phase 2

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

Branch Office Side:

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

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

Phase 1

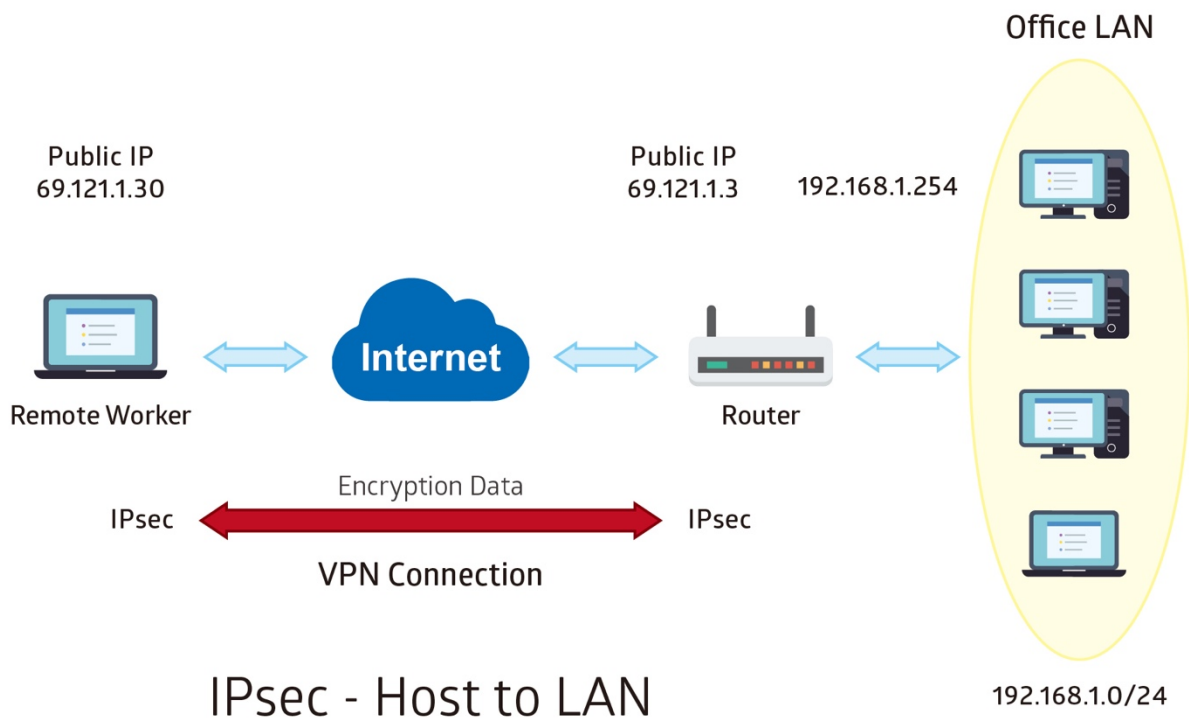
Encryption Algorithm	DES	Authentication Algorithm	MD5
Diffie-Hellman Group	MODP1024(DH2)	SA Lifetime	480 min(s)

Phase 2

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

2. Host to LAN

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



Head Office Side:

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

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

Phase 1

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

Phase 2

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

GRE Settings

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

GRE Configuration

This page is used to configure the parameters for GRE.

GRE

☐ Enabled ☒ Disabled

Apply Changes

Name

Admin Status

☐

CheckSum

☐

Sequencing

☐

Key

☐

DSCP

GRE Endpoint

GRE Backup Endpoint

802.1Q VLAN ID

(0-4092),empty means no VLAN tag

Upstream Bandwidth

kbps,empty mean no limitation

Downstream Bandwidth

kbps,empty mean no limitation

Add

Modify

Remove

GRE Table

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

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

Name: A given name for identification for GRE tunnel.

Admin Status: Choose to enable or disable this tunnel.

Sequencing: Enable to serialize all incoming and outgoing packets.

CheckSum: Enable to generate/require checksums for tunneled packets

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

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

GRE Endpoint: Set the remote gateway address.

GRE Backup Endpoint: a backup address for remote gateway.

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

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

How to for GRE:

1. Set a route WAN

Ethernet WAN

This page is used to configure the parameters for EthernetWAN

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

WAN IP Settings

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

2. Create a GRE Tunnel

GRE Configuration

This page is used to configure the parameters for GRE.

GRE

☒ Enabled ☐ Disabled

Apply Changes

Name

GRETunnel1

Admin Status

☒

CheckSum

☒

Sequencing

☒

Key

☒ 200

DSCP

AF12(001100) ▾

GRE Endpoint

172.16.1.102

GRE Backup Endpoint

172.16.1.103

802.1Q VLAN ID

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

Upstream Bandwidth

1024 kbps,empty mean no limitation

Downstream Bandwidth

2048 kbps,empty mean no limitation

Add

Modify

Remove

GRE Table

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

3. Map LAN interface(s) on the GRE tunnel with Bridge Grouping

Configuration

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

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

Grouped Interfaces

Available Interfaces

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

Select

Interfaces

Default

LAN1, LAN2, LAN3, LAN4, TW-EAV510AC_5G_6688, TW-EAV510AC_2.4G_6688, ptm0_0, vc3, gret0, gret0.100

☒

Configuration

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

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

Grouped Interfaces

Available Interfaces

gret0.100
LAN4
TW-EAV510AC_5G_6688

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

Select

Interfaces

Default

LAN1, LAN2, LAN3, LAN4, TW-EAV510AC_5G_6688, TW-EAV510AC_2.4G_6688, ptm0_0, vc3, gret0, gret0.100

☒

Select

Interfaces

Default

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

☐

LAN4, TW-EAV510AC_5G_6688, gret0.100

4. Disable DHCP assignment for the LAN interfaces.

Port-Based Filter

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

Filter DHCP Discover packet

☐ LAN1

☐ LAN2

☐ LAN3

☒ LAN4

☒ TW-EAV510AC_5G_6688

☐ TW-EAV510AC_2.4G_6688

Apply Changes

Close