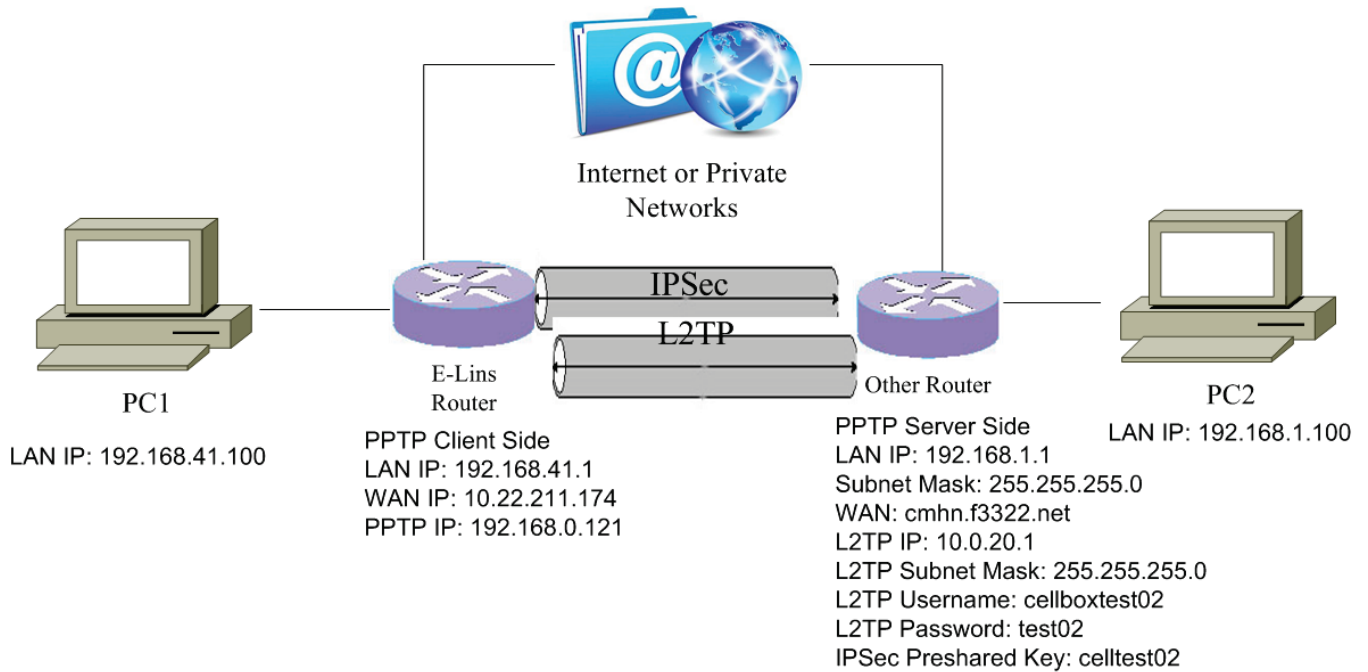





VPN Setting Example – IPSec over L2TP



L2TP Client Side (E-Lins Router)

1. Make sure the L2TP Client Router is online.

Status Overview Network Firewall Routes System Log Kernel Log Reboot Log Realtime Graphs VPN System Services Network Logout	Mobile WAN LAN		
	<h2>Mobile Status</h2>		
	<h3>Mobile 1</h3>		
	<table border="1"> <tr> <td>Cellular Status</td> <td>Up</td> </tr> </table>	Cellular Status	Up
	Cellular Status	Up	
	<table border="1"> <tr> <td>Cell Modem</td> <td>HUAWEI-ME906s-909s (12D1_15C1)</td> </tr> </table>	Cell Modem	HUAWEI-ME906s-909s (12D1_15C1)
	Cell Modem	HUAWEI-ME906s-909s (12D1_15C1)	
	<table border="1"> <tr> <td>IMEI/ESN</td> <td>867377020419028</td> </tr> </table>	IMEI/ESN	867377020419028
	IMEI/ESN	867377020419028	
	<table border="1"> <tr> <td>Sim Status</td> <td>SIM Ready</td> </tr> </table>	Sim Status	SIM Ready
	Sim Status	SIM Ready	
	<table border="1"> <tr> <td>Strength</td> <td> 30 / 31, dBm : -53</td> </tr> </table>	Strength	 30 / 31, dBm : -53
	Strength	 30 / 31, dBm : -53	
	<table border="1"> <tr> <td>Selected Network</td> <td>Automatic</td> </tr> </table>	Selected Network	Automatic
	Selected Network	Automatic	
<table border="1"> <tr> <td>Registered Network</td> <td>Registered on Home network: "CHN-UNICOM", 7,</td> </tr> </table>	Registered Network	Registered on Home network: "CHN-UNICOM", 7,	
Registered Network	Registered on Home network: "CHN-UNICOM", 7,		
<table border="1"> <tr> <td>Sub Network Type</td> <td>LTE</td> </tr> </table>	Sub Network Type	LTE	
Sub Network Type	LTE		
<table border="1"> <tr> <td>Location Area Code</td> <td>718A</td> </tr> </table>	Location Area Code	718A	
Location Area Code	718A		
<table border="1"> <tr> <td>Cell ID</td> <td>01F06C1B</td> </tr> </table>	Cell ID	01F06C1B	
Cell ID	01F06C1B		

- Check if L2TP Client Router can visit L2TP Server Router without L2TP. If cannot visit, the L2TP will not be connected. "Router Web --- Network --- Diagnostics",

Diagnostics

Network Utilities

cmhn.f3322.net	www.google.com	www.google.com
IPv4 <input type="button" value="Ping"/>	<input type="button" value="Traceroute"/>	<input type="button" value="Nslookup"/>

```
PING cmhn.f3322.net (112.66.72.166): 56 data bytes
64 bytes from 112.66.72.166: seq=0 ttl=52 time=111.742 ms
64 bytes from 112.66.72.166: seq=1 ttl=52 time=113.443 ms
64 bytes from 112.66.72.166: seq=2 ttl=52 time=114.503 ms
64 bytes from 112.66.72.166: seq=3 ttl=52 time=112.443 ms
64 bytes from 112.66.72.166: seq=4 ttl=52 time=112.183 ms
```

```
--- cmhn.f3322.net ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 111.742/112.862/114.503 ms
```

3. Open web management page, click "Services" -> "VPN" at the left navigation bar, then click "L2TP" to open L2TP Configuration page.

IPSec

PPTP



L2TP

OpenVPN

GRE Tunnel

Layer 2 Tunneling Protocol

L2TP Configuration


Name	Type	Enable	
QiuHome	Client	Yes	 Edit  Delete

New instance name:

Role:

Client



 Add New

L2TP NAT enable

Save & Apply

Save


Reset

Input new instance name, the example we input "QiuHome", and then select "Client" as role, finally Click Button "Add New".

Click button "Edit" in the row of "QiuHome" instance.

L2TP Client Instance: QiuHome

Main Settings

Enable	<input checked="" type="checkbox"/>
Server	<input type="text" value="cmhn.f3322.net"/>
Username	<input type="text" value="cellboxtest02"/>
Password	<input type="text" value="test02"/> 
Remote LAN subnet	<input type="text" value="10.0.20.0"/>
Remote LAN netmask	<input type="text" value="255.255.255.0"/>
MTU	<input type="text" value="1460"/>
Keep Alive	<input type="text" value="5"/>
Debug	<input checked="" type="checkbox"/>

[Save & Apply](#) [Save](#) [Reset](#)

Checked "Enable", fill in value of "Server" as L2TP Server WAN IP address. Here our L2TP Server Router has WAN *cmhn.f3322.net* and LAN IP address *192.168.1.1*

Set username/password we configured on L2TP server.

Set the PPTP Remote LAN subnet and PPTP Remote LAN netmask of L2TP server. Here is 10.0.20.0 and 255.255.255.0.

Set Keep Alive.

Click button "Save & Apply" if everything is done.

4. Open web management page, click "Services" → "VPN" at the left navigation bar, then click "IPSec" to open IPSec Configuration page.

Input new instance name, the example we input "ipsec_base", and then select "Client" as role, finally Click Button "Add New".

Click button "Edit" in the row of "ipsec_base" instance.

IPSec Instance: Ipsec_base

IPSec Configuration

Enable

Exchange mode

Operation Level


Authentication method

Remote VPN endpoint

Local endpoint

Local IKE identifier

Remote IKE identifier

Preshared Keys 

Perfect Forward Secrecy	<input type="text" value="Enable"/>	<input type="button" value="v"/>
DPD action	<input type="text" value="Restart"/>	<input type="button" value="v"/>
DPD delay	<input type="text" value="30"/>	seconds
DPD timeout	<input type="text" value="150"/>	seconds
NAT Traversal	<input type="text" value="Enable"/>	<input type="button" value="v"/>
Local LAN bypass	<input type="checkbox"/>	
Local subnet	<input type="text" value="192.168.41.0/24"/>	<input type="button" value="+"/>
Remote subnet	<input type="text" value="10.200.0.0/16"/>	<input type="button" value="+"/>

Phase 1 Proposal

Encryption algorithm	<input type="text" value="3DES"/>	▼
Hash algorithm	<input type="text" value="HMAC_MD5"/>	▼
DH group	<input type="text" value="MODP1024/2"/>	▼
Life time	<input type="text" value="1800"/>	seconds

Phase 2 Proposal

Encryption algorithm	<input type="text" value="3DES"/>	▼
PFS group	<input type="text" value="MODP1024/2"/>	▼
Authentication	<input type="text" value="HMAC_MD5"/>	▼
Life time	<input type="text" value="1800"/>	seconds

[Save & Apply](#) [Save](#) [Reset](#)



Configure all the parameters with right value from the VPN Server and click “Save & Apply”.

5. Wait some seconds until the Client Router connects to Server Router via L2TP, then on IPSec. Check the link status of L2TP Client Router.

Status
System
Services
Network
Operation Mode
Mobile
LAN
Wired WAN
WAN IPv6
Interfaces
Wi-Fi

Interfaces

Interface Overview

Network	Status	Actions
QIUHOME  l2tp-QiuHome	Uptime: 8h 58m 23s RX: 181.84 KB (1511 Pkts.) TX: 173.15 KB (1426 Pkts.) IPv4: 10.0.20.42/32	<input type="button" value="Connect"/> <input type="button" value="Stop"/> <input type="button" value="Edit"/>
TEST1  pptp-Test1	Uptime: 11h 48m 25s RX: 72.00 B (6 Pkts.) TX: 92.00 B (7 Pkts.) IPv4: 192.168.0.121/32	<input type="button" value="Connect"/> <input type="button" value="Stop"/> <input type="button" value="Edit"/>

Once the L2TP connection is up, the L2TP Client Router will display L2TP IP address at "Interface".

6. Check the link status of IPSec Client at "Router Web --- Status --- VPN".

<table border="1"> <tr><td>Status</td></tr> <tr><td> Overview</td></tr> <tr><td> Network</td></tr> <tr><td> Firewall</td></tr> <tr><td> Routes</td></tr> <tr><td> System Log</td></tr> <tr><td> Kernel Log</td></tr> <tr><td> Reboot Log</td></tr> <tr><td> Realtime Graphs</td></tr> <tr><td>VPN</td></tr> <tr><td>System</td></tr> <tr><td>Services</td></tr> <tr><td>Network</td></tr> <tr><td>Logout</td></tr> </table>	Status	Overview	Network	Firewall	Routes	System Log	Kernel Log	Reboot Log	Realtime Graphs	VPN	System	Services	Network	Logout	<p>IPSec IPSec Log OpenVPN</p> <h3>IPSec Status</h3> <p><input type="button" value="Refresh"/></p> <pre> worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 15 loaded plugins: charon aes des sha1 sha2 md5 gmp random nonce hmac stroke kernel-netlink socket-default updown Listening IP addresses: 192.168.41.1 fdcc:26ec:bf11::1 10.239.86.45 10.0.20.42 192.168.0.121 Connections: ipsec_base: 10.0.20.42...10.0.20.1 IKEv1, dpddelay=30s ipsec_base: local: [10.0.20.42] uses pre-shared key authentication ipsec_base: remote: [10.0.20.1] uses pre-shared key authentication ipsec_base: child: 192.168.41.0/24 === 10.200.0.0/16 TUNNEL, dpdaction=restart Security Associations (1 up, 0 connecting): ipsec_base[13]: ESTABLISHED 7 minutes ago, 10.0.20.42[10.0.20.42]...10.0.20.1[10.0.20.1] ipsec_base[13]: IKEv1 SPIs: 7aac5ac9b923beb8_i* 603ec83dc904af16_r, pre-shared key reauthentication in 12 minutes ipsec_base[13]: IKE proposal: 3DES_CBC/HMAC_MD5_96/PRF_HMAC_MD5/MODP_1024 ipsec_base[7]: INSTALLED, TUNNEL, reqid 1, ESP SPIs: ce685dfe_i 09bd8d63_o ipsec_base[7]: 3DES_CBC/HMAC_MD5_96, 0 bytes_i, 0 bytes_o, rekeying in 5 minutes ipsec_base[7]: 192.168.41.0/24 === 10.200.0.0/16 ipsec_base[8]: INSTALLED, TUNNEL, reqid 1, ESP SPIs: c1210822_i 070b0eaa_o ipsec_base[8]: 3DES_CBC/HMAC_MD5_96_0 bytes_i, 0 bytes_o, rekeying in 11 minutes ipsec_base[8]: 192.168.41.0/24 === 10.200.0.0/16 </pre>
	Status														
	Overview														
	Network														
	Firewall														
	Routes														
	System Log														
	Kernel Log														
	Reboot Log														
	Realtime Graphs														
VPN															
System															
Services															
Network															
Logout															

7. Ping from Client Router to Server Router (with L2TP IP 10.0.20.1)

Diagnostics

Network Utilities

10.0.20.1	www.google.com	www.google.com	
IPv4 <input type="button" value="v"/>	<input type="button" value="▶ Ping"/>	<input type="button" value="▶ Traceroute"/>	<input type="button" value="▶ Nslookup"/>

```
PING 10.0.20.1 (10.0.20.1): 56 data bytes
64 bytes from 10.0.20.1: seq=0 ttl=64 time=115.043 ms
64 bytes from 10.0.20.1: seq=1 ttl=64 time=111.443 ms
64 bytes from 10.0.20.1: seq=2 ttl=64 time=104.543 ms
64 bytes from 10.0.20.1: seq=3 ttl=64 time=102.083 ms
64 bytes from 10.0.20.1: seq=4 ttl=64 time=109.363 ms

--- 10.0.20.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 102.083/108.495/115.043 ms
```

Status
System
Services
Network
Operation Mode
Mobile
LAN
Wired WAN
WAN IPv6
Interfaces
Wi-Fi
Firewall
Static Routes
Switch
DHCP and DNS
Diagnostics
Loopback Interface

Diagnostics

Network Utilities

IPv4

```
PING 192.168.0.1 (192.168.0.1): 56 data bytes
64 bytes from 192.168.0.1: seq=0 ttl=64 time=55.644 ms
64 bytes from 192.168.0.1: seq=1 ttl=64 time=56.024 ms
64 bytes from 192.168.0.1: seq=2 ttl=64 time=55.804 ms
64 bytes from 192.168.0.1: seq=3 ttl=64 time=54.384 ms
64 bytes from 192.168.0.1: seq=4 ttl=64 time=54.144 ms
```

```
--- 192.168.0.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 54.144/55.200/56.024 ms
```