



HWL-2511-SS

取扱説明書



HYTEC INTER Co., Ltd.

第 4.0 版

ご注意

- 本書の中に含まれる情報は、弊社（ハイテクインター株式会社）の所有するものであり、弊社の同意なしに、全体または一部を複製または転載することは禁止されています。
- 本書の内容については、将来予告なしに変更することがあります。
- 本書の内容については万全を期して作成いたしましたが、万一、ご不審な点や誤り、記載漏れなどのお気づきの点がありましたらご連絡ください。

改版履歴

第 1 版	2019 年 10 月 29 日	新規作成
第 1.1 版	2019 年 11 月 15 日	梱包物一覧に AC アダプタを追加
第 1.2 版	2019 年 12 月 05 日	梱包物一覧にウォールマウントキットを追加
第 2 版	2019 年 12 月 25 日	アンテナ取り付け方法を追記
第 2.1 版	2020 年 02 月 12 日	仕様に WiFi クライアント数を追記
第 3 版	2020 年 03 月 26 日	Setting Wizard に関する説明を追記
第 3.1 版	2020 年 07 月 06 日	初期化時の注意点を追記
第 3.2 版	2020 年 12 月 02 日	Wi-Fi の初期パスワードを追記
第 4.0 版	2021 年 05 月 19 日	ファームアップデート(V1.05)追加機能を追記

ご使用上の注意事項

- 本製品及び付属品をご使用の際は、取扱説明書に従って正しい取り扱いをしてください。
- 本製品及び付属品を分解したり改造したりすることは絶対に行わないでください。
- 本製品及び付属品を直射日光の当たる場所や、温度の高い場所で使用しないでください。本体内部の温度が上がり、故障や火災の原因になることがあります。
- 本製品及び付属品を暖房器具などのそばに置かないでください。ケーブルの被覆が溶けて感電や故障、火災の原因になることがあります。
- 本製品及び付属品をほこりや湿気の多い場所、油煙や湯気のあたる場所で使用しないでください。故障や火災の原因になることがあります。
- 本製品及び付属品を重ねて使用しないでください。故障や火災の原因になることがあります。
- 通気口をふさがないでください。本体内部に熱がこもり、火災の原因になることがあります。
- 通気口の隙間などから液体、金属などの異物を入れないでください。感電や故障の原因になることがあります。
- 付属のACアダプタは本製品専用となります。他の機器には接続しないでください。また、付属品以外のACアダプタを本製品に接続しないでください。
- 本製品及び付属品の故障、誤動作、不具合、あるいは天災、停電等の外部要因によって、通信などの機会を逸したために生じた損害等の純粋経済損害につきましては、弊社は一切その責任を負いかねますので、あらかじめご了承ください。
- 本製品及び付属品は、改良のため予告なしに仕様が変更される可能性があります。あらかじめご了承ください。

目次

1. 製品概要	7
2. 梱包物一覧.....	7
3. 製品外観	8
3.1. LED	8
3.2. 前面	9
3.3. WPS/リセットボタン	10
3.4. 接地について	11
3.5. SIM カードの取り付け/取り外し方法	11
3.6. Digital INPUT・OUTPUT について	12
3.7. アンテナの取り付け	13
4. WEB GUI での設定について	14
4.1. WEB GUI へのアクセス.....	14
4.2. Setting Wizard.....	15
4.3. WEB GUI の概要説明.....	19
4.4. IP アドレスの設定	20
4.5. ログインパスワードの変更	21
4.6. APN 設定	22
4.7. セキュリティを高めるための設定	23
5. Status	25
6. System	26
6.1. Time and Date.....	27
6.2. COM Ports	29
6.3. Logging.....	31
6.4. Alarm	32
6.5. Ethernet.....	34
6.6. Client List	35
7. WAN.....	36
7.1. WAN > Priority	36
7.2. WAN > Ethernet.....	38

7. 3.	WAN > IPv6 DNS.....	40
7. 4.	WAN > Health Check.....	41
8.	LTE.....	42
8. 1.	LTE > LTE Config.....	42
8. 2.	LTE > APN Config (V1.05).....	44
8. 3.	LTE > APN1 Display	48
8. 4.	LTE > Serving Cell	49
8. 5.	LTE > Lock Bands.....	49
8. 6.	LTE > DNS	50
9.	WiFi.....	51
9. 1.	WiFi > WiFi Config.....	52
9. 2.	WiFi > Client List.....	53
10.	LAN.....	54
10. 1.	LAN > IPv4 (V1.05)	54
10. 2.	LAN > VLAN	56
10. 3.	LAN > Subnet.....	57
11.	IP Routing.....	58
11. 1.	IP Routing > Static Route	58
11. 2.	IP Routing > RIP.....	60
11. 3.	IP Routing > OSPF	62
11. 4.	IP Routing > BGP.....	65
12.	VPN.....	68
12. 1.	VPN > Open VPN	68
12. 2.	VPN > IPSec.....	75
12. 3.	VPN > GRE.....	80
12. 4.	VPN > PPTP Server.....	80
12. 5.	VPN > L2TP.....	82
13.	Firewall.....	89
13. 1.	Firewall > Basic Rules.....	89
13. 2.	Firewall > Port Forwarding.....	90
13. 3.	Firewall > DMZ.....	92
13. 4.	Firewall > Management IP (V1.05).....	92

13. 5.	Firewall > IP Filter	93
13. 6.	Firewall > MAC Filter (V1.05)	95
13. 7.	Firewall > URL Filter (V1.05)	96
13. 8.	Firewall > NAT	97
14.	Service	98
14. 1.	Service > SNMP	98
14. 2.	Service > Dynamic DNS	103
14. 3.	Service > VRRP	104
14. 4.	Service > UPnP	105
14. 5.	Service > SMTP	106
14. 6.	Service > IP Alias	107
15.	Management	108
15. 1.	Management > Identification	108
15. 2.	Management > Administration	109
15. 3.	Management > SSH	110
15. 4.	Management > WEB	110
15. 5.	Management > Firmware	111
15. 6.	Management > Configuration	111
15. 7.	Management > Load Factory	112
15. 8.	Management > Restart	112
15. 9.	Management > Schedule Reboot	113
16.	Diagnosis	114
16. 1.	Diagnosis > Ping	114
16. 2.	Diagnosis > Traceroute	115
17.	製品仕様	116
18.	付属 AC アダプタ仕様	117
19.	製品保証	118

1. 製品概要

HWL-2511-SS は、-20～+60℃の広い動作温度に対応した産業用の LTE ルータです。

カテゴリ 4 のモジュールが使用されており、DL: 150Mbps max, UL: 50Mbps max となっています。

また、IEEE802.11b/g/n に準拠した Wi-Fi インタフェースを搭載しており、2.4GHz 帯の無線 LAN アクセスポイントとしても使用できます。

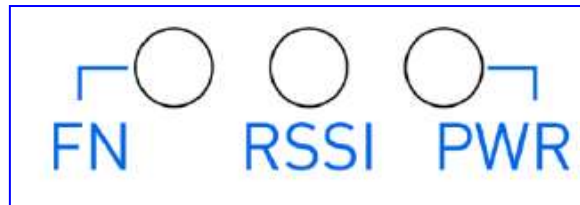
2. 梱包物一覧

ご使用いただく前に本体と付属品を確認してください。万一、不足の品がありましたら、お手数ですがお買い上げの販売店までご連絡ください。

名 称	数 量
本体	1 台
LTE アンテナ	2 個
Wi-Fi アンテナ	2 個
GPS アンテナ(ケーブル長 2m)	1 個
DIN レールマウントキット	1 式
ウォールマウントキット	1 式
AC アダプタ	1 個

3. 製品外観

3.1. LED



各 LED

表示		説明
<u>FN</u>	点灯	VPN が接続されています。
	遅い点滅	WAN が接続されています。
	早い点滅	システム起動中及び初期化中です。
	消灯	電源が入っていません。
<u>RSSI</u>	点灯	LTE の信号強度が＜強＞の状態です。
	遅い点滅	LTE の信号強度が＜中＞の状態です。
	早い点滅	LTE の信号強度が＜弱＞の状態です。
	消灯	LTE でエラーが発生しています。
<u>PWR</u>	点灯	電源が入っています。
	消灯	電源が入っていません。

3.2. 前面



表示	説明
LAN1	LAN1 ポートです。
WAN/LAN2	WAN/LAN2 ポートです。 初期設定では WAN ポートとなっていますが、System > Ethernet の設定を変更することで、LAN2 ポートとして動作させることも出来ます。
V+	DC10～32V を入力します。
V-	
DI	Digital Input ポートです。
DI_GND	詳細は P.11 の”Digital INPUT について”を参照願います。
DO	Digital Output ポートです。
DO_GND	詳細は P.11 の”Digital INPUT について”を参照願います。
TXD	RS-232 ポートです。 詳細は P.20 の”COM Ports”を参照願います。
RXD	
GND	

(注)ブロック端子の挿入・取り外しは電源を OFF (AC アダプタをコンセントから抜いた状態)で行ってください。

3.3. WPS/リセットボタン

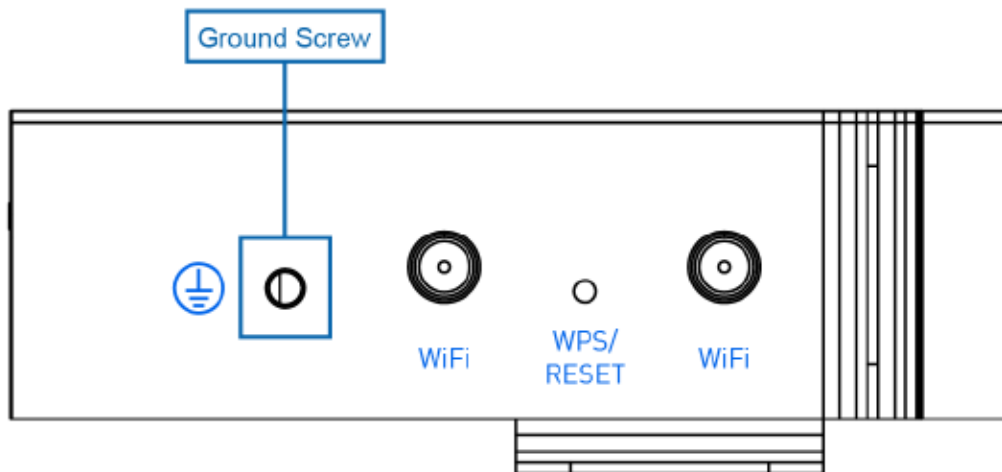


機能	操作
WPS 機能	5 秒以内で押下します。
再起動	5-10 秒の間押下します。
初期化と再起動	10 秒以上押下します。

3.4. 接地について

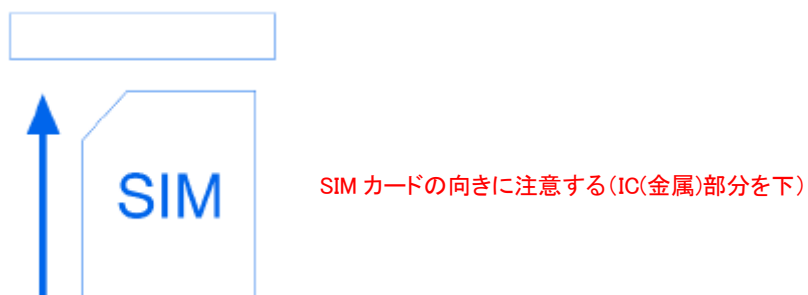
本体上面のネジを使用して、接地することが出来ます。

本体の電源を ON にする前に接地に使うリード線をネジで接続してください。



3.5. SIM カードの取り付け/取り外し方法

SIM カードの取り付け/取り外し方法について説明します。



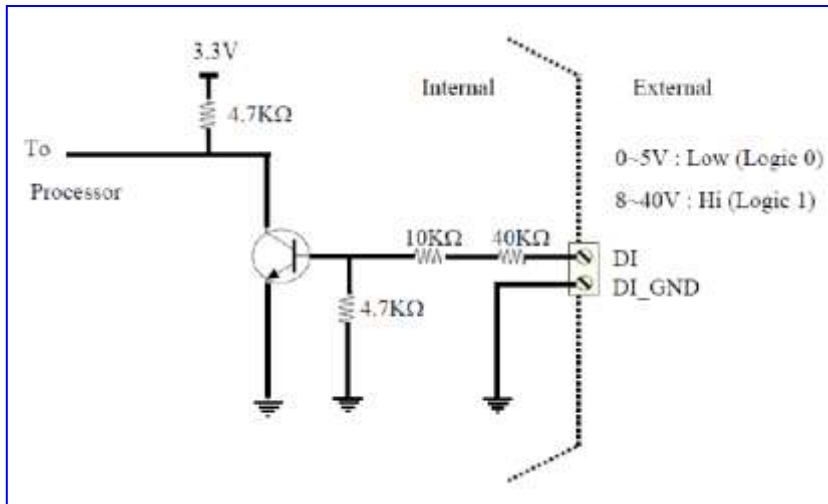
- 1) ルータの電源をオフにしてください。
- 2) SIM カードスロットに Micro SIM をカチッと音が鳴るまで挿入します。
- 3) 取り外しの際は、Micro SIM をカチッと音が鳴るまで押し込んだあとに引き出します。

注意事項

SIM カードの取り付け/取り外しを行う際は、必ずルータの電源をオフにしてください。

3. 6. Digital INPUT・OUTPUT について

- Digital INPUT について

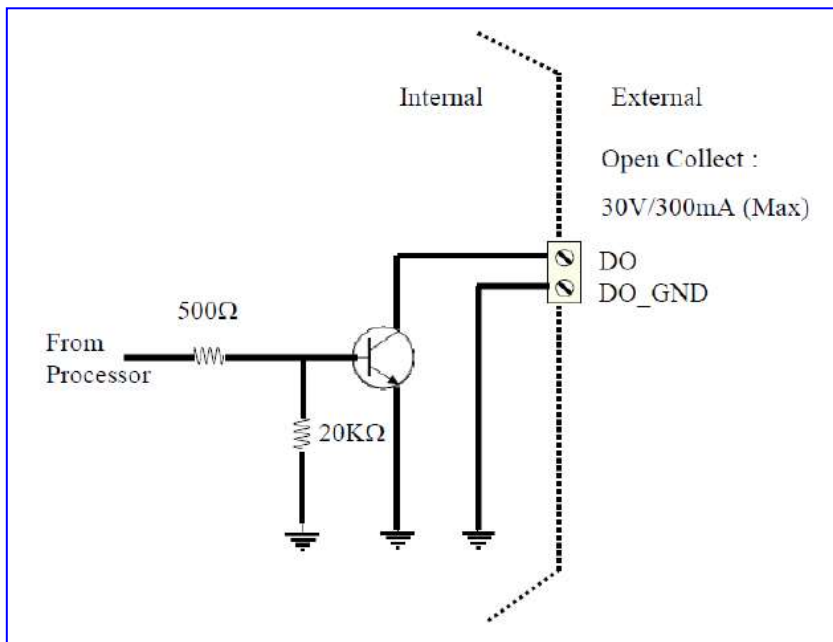


- Digital OUTPUT (アラーム出力) について

リモートから DO の制御が可能です。DO ポートは通常はフロー状態です。

・IP アドレス/DO_ON : DO が "Low" になります。

・IP アドレス/DO_OFF : DO が Float になります。

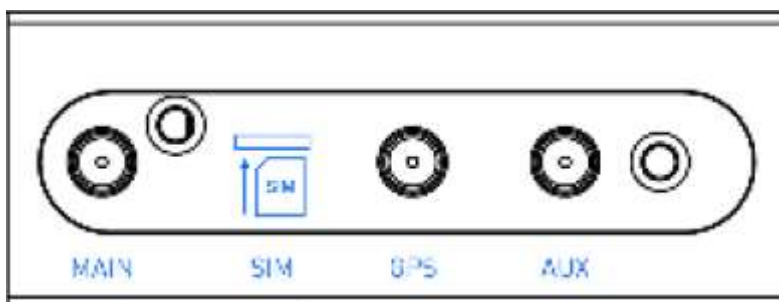


3.7. アンテナの取り付け

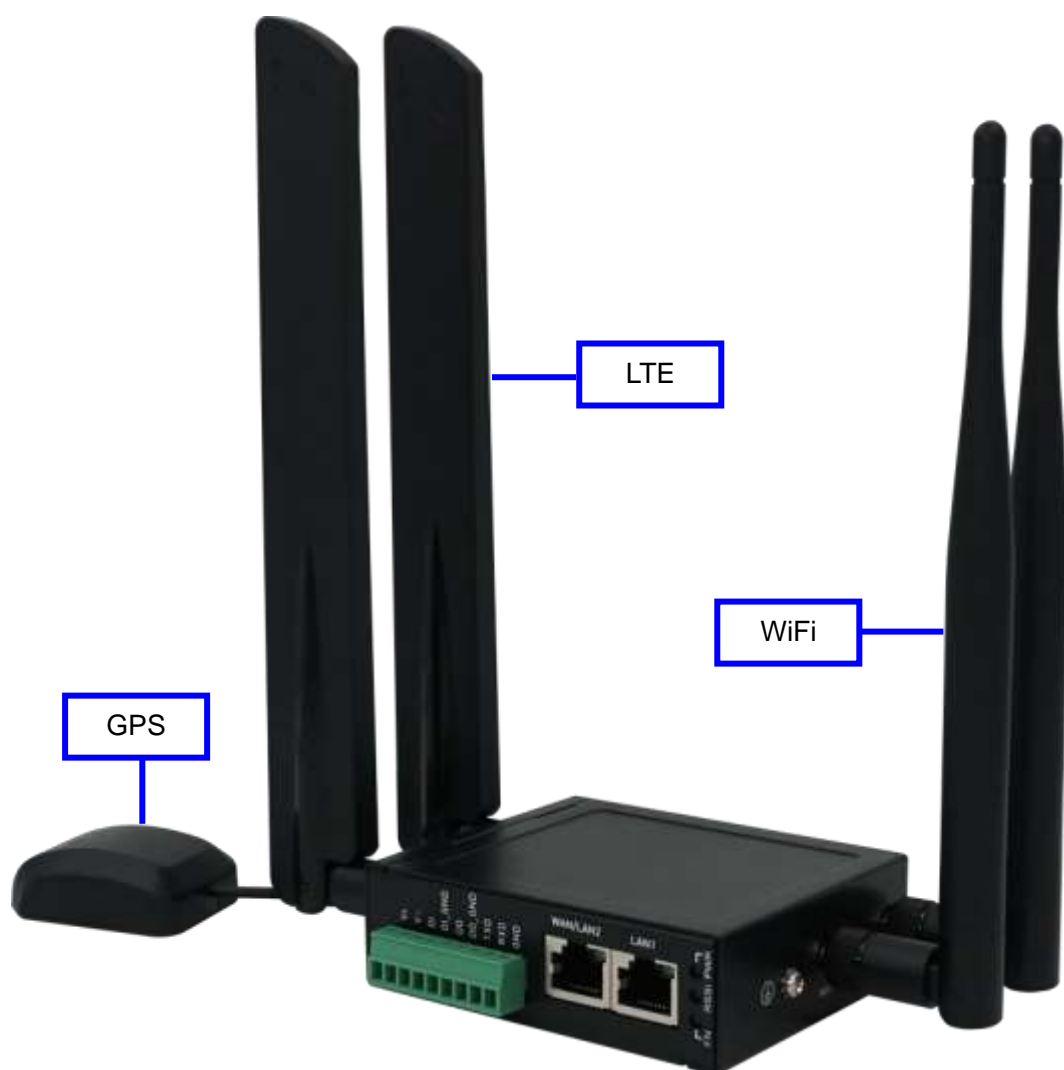
LTE アンテナ x2 本は、MAIN と AUX のコネクタにそれぞれ取り付けます。

GPS アンテナは、GPS のコネクタに取り付けます。

また、本体反対側の WiFi のコネクタには WiFi アンテナを取り付けます。



すべてのアンテナの取り付けが完了すると、下図の状態になります。



4. WEB GUI での設定について

4.1. WEB GUI へのアクセス

- ログイン初期設定

項目	初期値
IP アドレス	192.168.1.1
ユーザ名	root
パスワード	2wsx#EDC

- ログイン手順

- 1) 接続する PC の IP アドレスを 192.168.1.0/24 のネットワークの 192.168.1.1 以外のホストアドレスに設定します。
- 2) PC をルータの LAN ポートに接続します。
- 3) ブラウザのアドレスバーに http://192.168.1.1 と入力して接続します。
※ WAN 側からアクセスする場合は、https でアクセスする必要があります。
- 4) ルータの WEB GUI のトップ画面が表示されたら、画面右上の Login ボタンをクリックします。



- 5) ユーザ名とパスワードを入力して、Login ボタンをクリックします。



4. 2. Setting Wizard

初回ログイン時は Setting Wizard が表示されます。

Setting Wizard による設定方法を以下に示します。

- 1) **Step.1 Super User Password** をクリックします。



- 2) 新しいパスワードを設定して、**Step 2. WAN Setting** をクリックします。

- 3) WAN Priority を設定して、**Step 2.1 WAN Setting – Ethernet** もしくは **Step 2.2 WAN Setting – LTE** をクリックします。この例では”LTE Only”を選択しています。

- 4) APN の設定を行い、**Step 3. LAN Setting** をクリックします。

Setting Wizard

Step 2.2. WAN Setting - LTE

SIM Configuration APN1

APN:

Username:

Password:

Confirm Password:

Auth:

Cancel Reset ← Step 2. WAN Setting Step 3. LAN Setting →

- 5) IP アドレス、DHCP サーバの設定を行い、**Step 4. Time Zone Setting** をクリックします。

Setting Wizard

Step 3. LAN Setting

IP Address:

IP Mask:

DHCP Server Configuration

☒ DHCP Server Configuration

IP Address Pool: From To

Cancel Reset ← Step 2. WAN Setting Step 4. Time Zone Setting →

- 6) Time Zone にて”Osaka, Sapporo, Tokyo”を選択し、
[Step 5. WiFi Config](#)をクリックします。

Setting Wizard

Step 4. Time Zone Setting

Time Zone: (GMT+09:00) Osaka, Sapporo, Tokyo ▼

Daylight Savings: ☒ Off ☐ On

Ahead of standard time: 60 mins

Start Date: 3 / 2 / 0 (Month / Week / Day)

Start Time: 2 : 0 (Hour : Minute)

End Date: 11 / 2 / 0 (Month / Week / Day)

End Time: 2 : 0 (Hour : Minute)

[Cancel](#)
[Reset](#)
[← Step 3. LAN Setting](#)
[Step 5. WIFI Config →](#)

- 7) Setting Wizard での WIFI 設定はサポートしていませんので、
 そのまま [Review Setting](#) をクリックします。

Setting Wizard

Step 5. WIFI Config

WiFi Network

AP Enable: ☐ Disable ☒ Enable

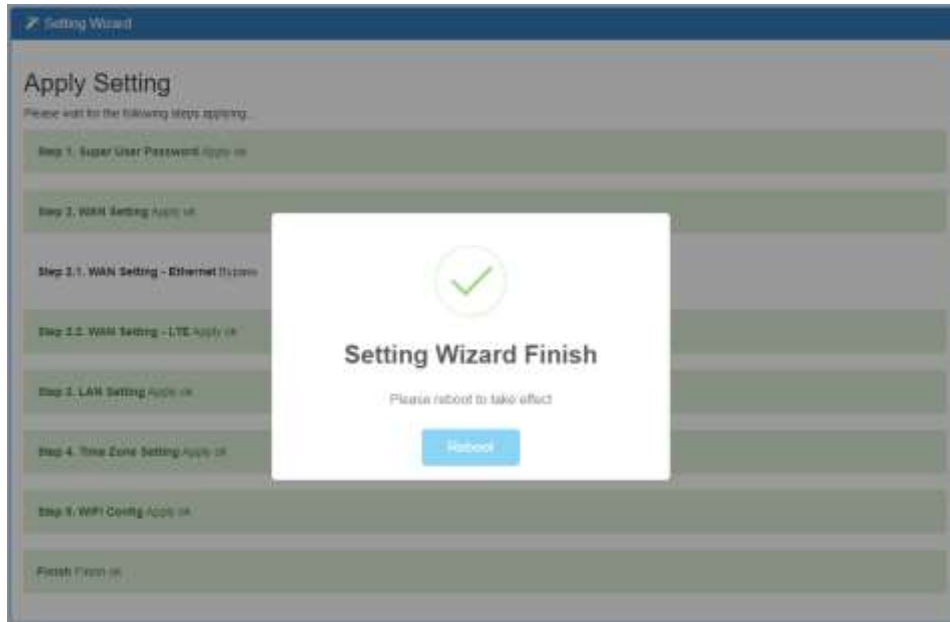
WPS Button: ☒ None ☐ SSID-1 ☐ SSID-2

Tx Power: 100 (t=100)%

- 8) 設定の確認が終わったら、**Apply Setting**をクリックします。



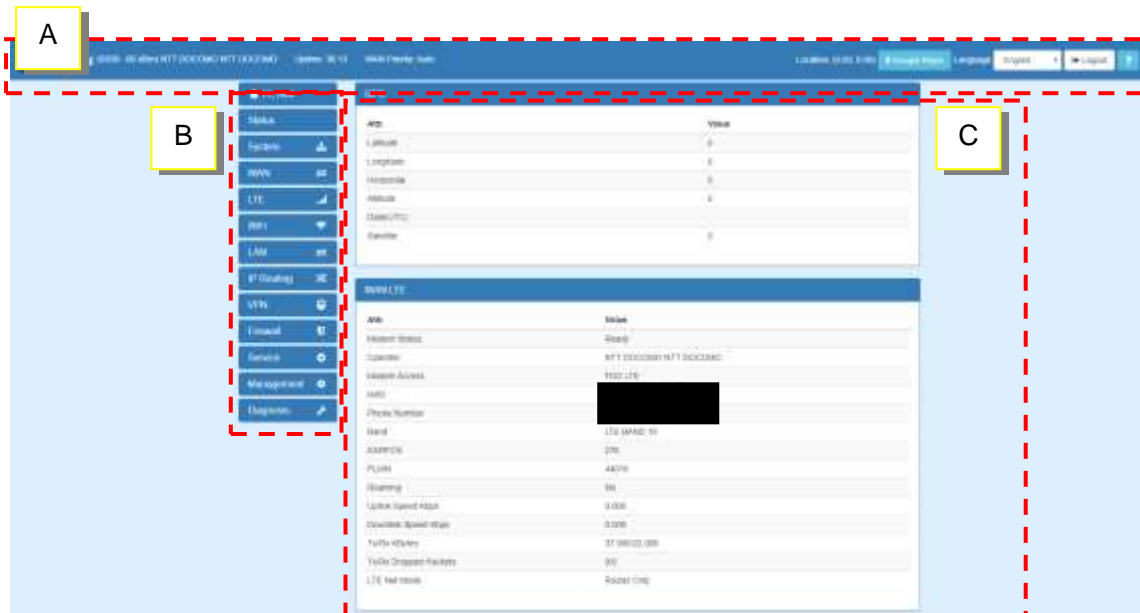
- 9) **Reboot**ボタンが表示されたら、クリックします。



4.3. WEB GUI の概要説明

WEB GUI のメインスクリーンは3つのパートに分割されています。

A-タイトルバー、B-ナビゲーションパネル、C-メインウィンドウ



1) A: タイトルバー

タイトルバーには、ルータの状態が確認出来る情報が記載されています。

項目	説明
RSSI	LTE の信号強度と、契約している携帯電話キャリアの名前を表示します。
Uptime	ルータの電源を入れてからの経過時間を表示します。
WAN Priority	現在の WAN Priority の設定状況を表示します。
Location	GPS で測位した現在位置を DEG 形式で緯度経度の順に表示します。 Google Map のボタンをクリックすると、Google Map 上にプロット出来ます。
Login/Logout	WEB GUI のログイン/ログアウトを行います。

2) **B**:ナビゲーションパネル

各項目を選択することで、それぞれの機能のステータス画面や設定画面を呼び出すことができます。

3) **C**:メインウィンドウ

ナビゲーションパネルで選択した機能についてのステータス画面や設定画面を表示します。

4.4. IP アドレスの設定

- 1) ナビゲーションパネルから、**LAN** ⇒ **IPv4** の順にクリックします。
- 2) IP Address と IP Mask を設定します。
- 3) 必要に応じて DHCP Server も設定を行います。
- 4) **Apply** ボタンをクリックします。

⇐ LAN IPv4

IP Address

IP Mask

DHCP Server Configuration

DHCP Server ☒ On

IP Address Pool From To

Gateway

Lease Time Minutes

Manual DNS [+](#)

Anti-Spoofing ☐ Off

Strict Bind ☐ Off

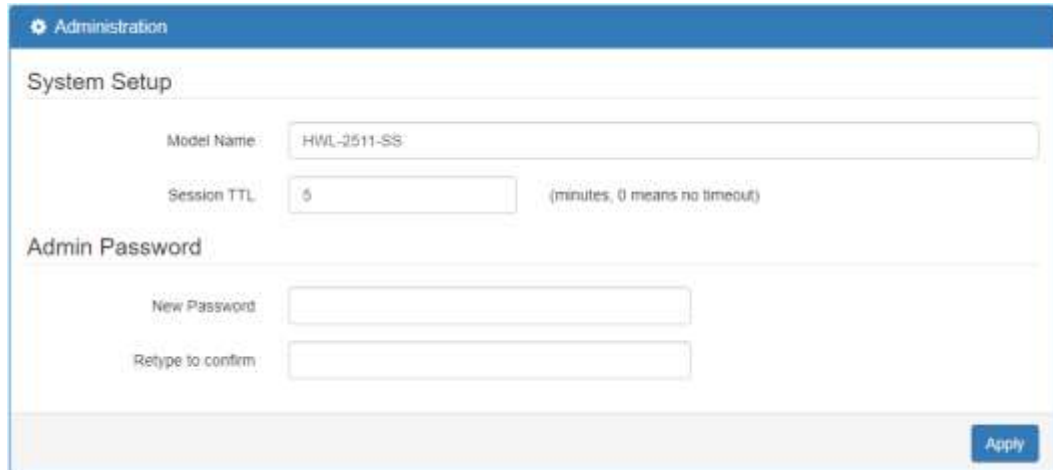
Static IP Addresses

[+ Add Static IP Address](#)

Apply

4.5. ログインパスワードの変更

- 1) ナビゲーションパネルから、**Management** ⇒ **Administration** の順にクリックします。
- 2) Admin Password にて、New Password と Retype to confirm に新しいパスワードを入力します。



The screenshot shows the 'Administration' section of a web interface. Under the 'System Setup' heading, there are two main sections: 'Model Name' and 'Session TTL'. The 'Model Name' field contains 'HWL-2511-SS'. The 'Session TTL' field contains '5', with a note '(minutes, 0 means no timeout)'. Below these is the 'Admin Password' section, which contains two empty text input fields labeled 'New Password' and 'Retype to confirm'. At the bottom right of the form is a blue 'Apply' button.

- 3) **Apply** ボタンをクリックします。

4. 6. APN 設定

- 1) ナビゲーションパネルから、LTE ⇒ APN Config ⇒ APN1 の順にクリックします。
- 2) Recovery APN1 を Yes にチェックし Reboot を選択します。
- 3) APN, Username, Password, Auth を入力します。

The screenshot shows the 'APN Config' web interface. At the top, there's a blue header with 'APN Config' and a signal icon. Below the header, the 'Connect Policy' section includes a 'Connect Action' button labeled 'Connect' and a 'Disable Roaming' section with radio buttons for 'No' and 'Yes' (selected). The 'Recover APN1' section has a 'Recover APN1' section with radio buttons for 'No' and 'Yes' (selected). Below this, there's a field 'When APN1 continuous link down for' with a value of '5' and the text 'times (3 ~ 15)'. There are three radio buttons for recovery actions: 'Reboot' (selected), 'Recover to default APN', and 'Recover to previous working APN'. Below the 'Recover APN1' section, there's a 'SIM Configuration' section with a tab labeled 'APN1'. Under this tab, there are input fields for 'APN', 'Username', 'Password', and 'Confirm Password'. There's also a dropdown menu for 'Auth' currently set to 'NONE'. At the bottom, there's a checkbox for 'Enable IPv6' which is unchecked.

- 4) Apply ボタンをクリックします。

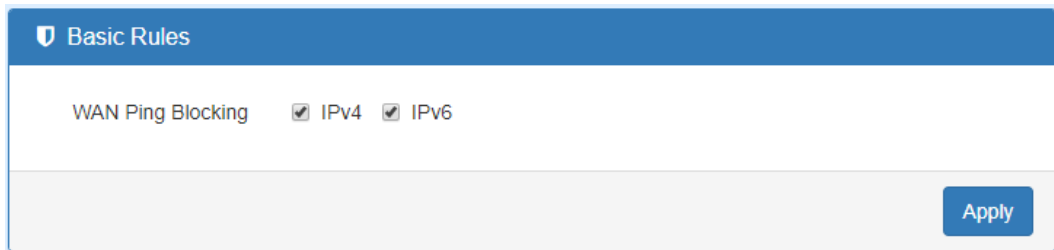
4.7. セキュリティを高めるための設定

インターネットから本機に対する不正アクセスを防止するための設定を示します。

4.7.1. インターネットからの Ping をブロックする

WAN 側からの Ping に対して、ルータが応答しなくなります。

- 1) ナビゲーションパネルから、**Firewall** ⇒ **Basic Rules** の順にクリックします。
- 2) WAN Ping Blocking を有効にして **Apply** ボタンをクリックします。



Basic Rules

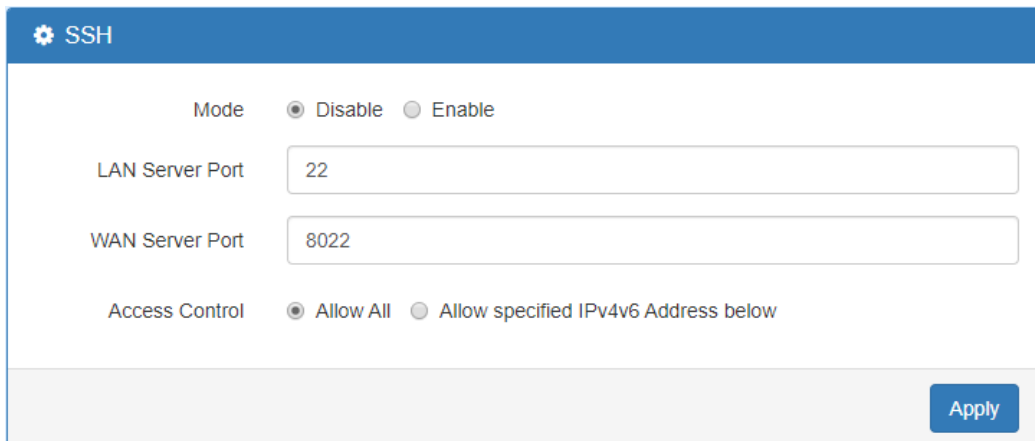
WAN Ping Blocking ☒ IPv4 ☒ IPv6

Apply

4.7.2. SSH 接続を無効にする

通常時は使用しない SSH を無効にすることで、不正アクセスを防止します。

- 1) ナビゲーションパネルから、**Management** ⇒ **SSH** の順にクリックします。
- 2) Disable にチェックを入れて、**Apply** をクリックします。



SSH

Mode ☒ Disable ☐ Enable

LAN Server Port 22

WAN Server Port 8022

Access Control ☒ Allow All ☐ Allow specified IPv4v6 Address below

Apply

4.7.3. インターネットからの WEB アクセスをブロックする

インターネットからの WEBGUI へのアクセスをブロックします。

- 1) ナビゲーションパネルから、**Firewall** ⇒ **IP Filter** の順にクリックします。
- 2) Enable と Black にチェックを入れて、Edit ボタンをクリックします。

Warning: All existing connections will be dropped after apply

Mode ☐ Disable ☒ Enable

List ☒ Black ☐ White (Warning: White List will block device services, enable them in 'Service Port'.)

#	Mode	Protocol	Source / Port	Destination / Port	Edit
1	Disable	All	0.0.0.0 / --	0.0.0.0 / --	

- 3) 以下の様に設定します。

Black List Setting

Mode ☐ Disable ☒ Enable

Protocol ☐ All ☐ ICMP ☒ TCP ☐ UDP

Source IP
 Example:

- 192.168.0.123
- 192.168.1.0/24
- 192.168.1.0/255.255.255.0
- 192.168.1.1-192.168.1.123
- 2607:f0d0:1002:51::4
- 2607:f0d0:1002:51::0/64
- 2607:f0d0:1002:51::4-2607:f0d0:1002:51::aaaa

Source Port
 Example:

- 1234
- 1234:5678:

Destination IP

Destination Port

TCP:443宛てに来たパケットをブロックすることで、インターネット側から本機の WEBGUI にはログイン出来なくなります。

5. Status

ナビゲーションパネルにて **Status** をクリックすると、ルータのステータスを確認することが出来ます。

Hi root

Status

System

WAN

LTE

WiFi

LAN

IP Routing

VPN

Firewall

Service

Management

Diagnosis

GPS

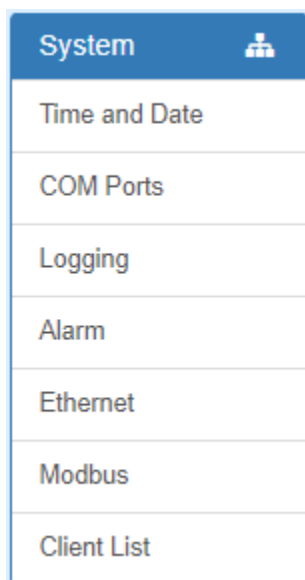
Attr.	Value
Latitude	0
Longitude	0
Horizontal	0
Altitude	0
Date(UTC)	
Satellite	0

WAN LTE

Attr.	Value
Modem Status	Ready
Operator	NTT DOCOMO NTT DOCOMO
Modem Access	FDD LTE
IMSI	
Phone Number	
Band	LTE BAND 19
EARFCN	276
PLMN	44010
Roaming	No
Uplink Speed Kbps	0.000
Downlink Speed Kbps	0.000
Tx/Rx KBytes	38.000/23.000
Tx/Rx Dropped Packets	0/0
LTE Net Mode	Router Only

6. System

ナビゲーションパネルにて **System** をクリックすると、システム関連の設定を開くことが出来ます。



6.1. Time and Date

ルータ内部の時刻設定および、GPS Time Server 機能の有効/無効の設定を行います。

GPS Time Server 機能を有効にすることでルータは NTP サーバとして動作し、LAN に接続した NTP Client からのリクエストに応答することができます。

- NTP サーバと時刻同期する場合
 - 1) Mode で Get from Time server を選択します。
 - 2) IPv4 Server #1～#5 に同期する NTP サーバのアドレスを入力します。

The screenshot shows the 'Time And Date' configuration page. At the top, it displays the 'Current Time' as 'Oct 6, 2020 5:58:10 AM'. Below this is the 'Time and Date Setup' section. The 'Mode' is set to 'Get from Time Server' (indicated by a selected radio button). The 'YYYY-MM-DD HH:MM:SS' field shows '2020 - 10 - 6 5 - 57 - 25'. The 'GPS Time' is set to 'On'. Below these are fields for NTP servers: 'IPv4 Server #1' (0.openwrt.pool.ntp.org), 'IPv4 Server #2' (pool.ntp.org), 'IPv4 Server #3' (clock.sjc.he.net), 'IPv6 Server #1' (time-d.nist.gov), 'IPv6 Server #2' (2.pool.ntp.org), and 'IPv6 Server #3' (clock.nyc.he.net).

- 手動で時刻設定する場合
 - 1) Mode で Manual を選択します。
 - 2) 手動で日付と時刻を入力します。

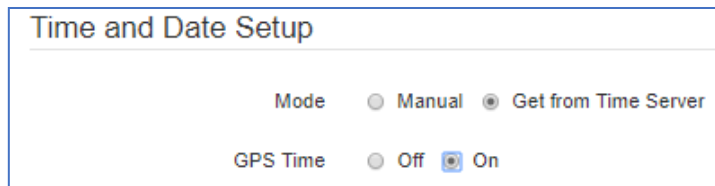
The screenshot shows the 'Time and Date Setup' page with 'Mode' set to 'Manual' (selected radio button). The 'YYYY-MM-DD HH:MM:SS' field shows '2019 - 3 - 27 13 : 8 : 5'.

- タイムゾーンの設定
 - 1) Time Zone で”(GMT+09:00)Osaka, Sapporo, Tokyo”を選択します。

The screenshot shows the 'Time Zone Setup' page. The 'Time Zone' dropdown menu is set to '(GMT+09:00) Osaka, Sapporo, Tokyo'.

- GPS Time Server 機能の設定

1) GPS Time で On を選択します。

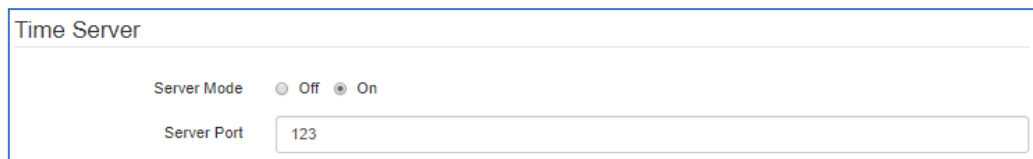


Time and Date Setup

Mode ☐ Manual ☒ Get from Time Server

GPS Time ☐ Off ☒ On

2) Time Server の Server Mode で On を選択し、ポート番号を設定します。



Time Server

Server Mode ☐ Off ☒ On

Server Port

(注)NTP サーバーまたは GPS による時刻同期が完了した後、Time Server 機能が有効になります。


6.2. COM Ports

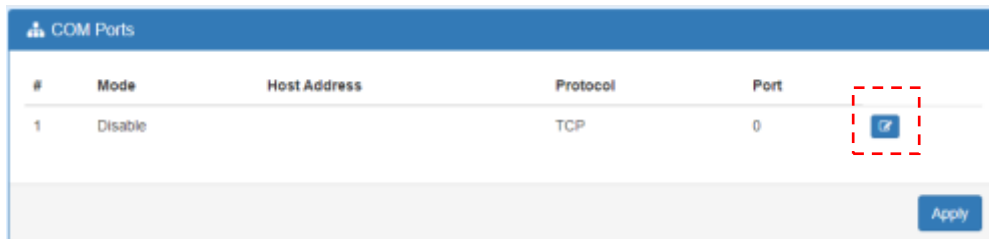
COM ポート及び Virtual COM ポートの設定を行います。

ルータの Virtual COM ポートを通して、シリアルインタフェースで接続した装置を遠隔から管理することができます。

● COM ポートの設定

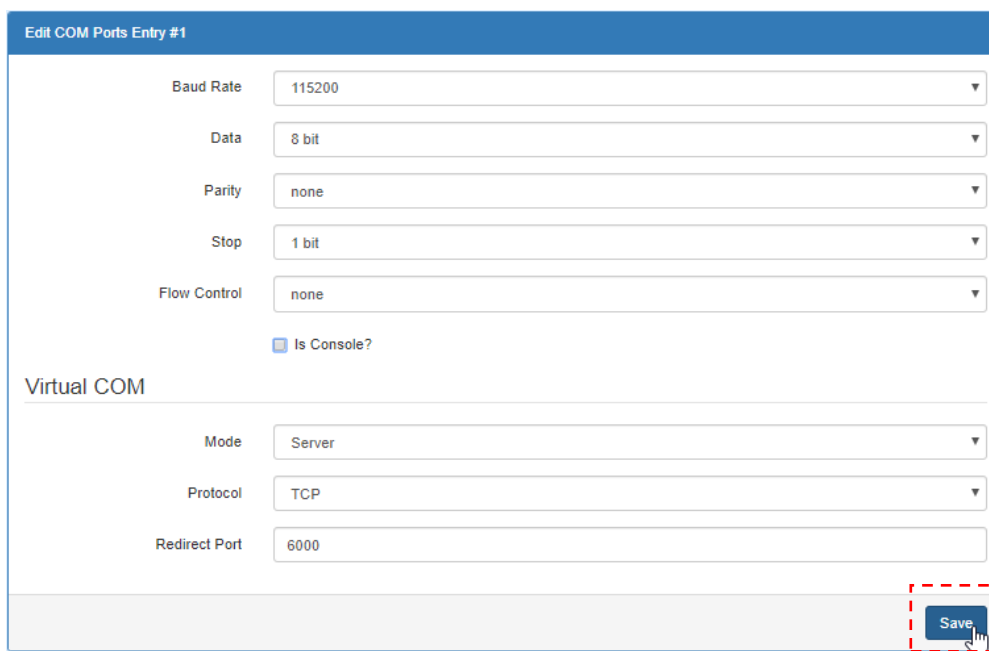
- 1) デフォルトではすべての COM ポートが無効になっています。

各ポートの  ボタンをクリックすると設定を開くことができます。



#	Mode	Host Address	Protocol	Port
1	Disable		TCP	0

- 2) COM ポートの設定を行い、**Save**をクリックします。



Edit COM Ports Entry #1

Baud Rate: 115200
 Data: 8 bit
 Parity: none
 Stop: 1 bit
 Flow Control: none
☐ Is Console?

Virtual COM

Mode: Server
 Protocol: TCP
 Redirect Port: 6000

- 3) **Apply**をクリックします。



#	Mode	Host Address	Protocol	Port
1	Disable		TCP	0

System > COM Ports	
項目	説明
Baud Rate	ボーレートを設定します。 ※ “110”はサポートしておりません。
Data	7bit もしくは 8bit から選択します。
Parity	パリティビットを設定します。
Stop	ストップビットを 1bit もしくは 2bit から選択します。
Flow Control	フローコントロールの有効/無効を選択します。
Is Console?	この項目にチェックが入っている場合、COM ポートをルータの CLI 用のマ ネジメントポートとして利用します。 PC と RS-232C で接続し、Teraterm などを開くことでルータの CLI にログイ ン出来ます。 別の装置を接続する場合はチェックを外す必要があります。
Mode	動作モードを選択します。
Protocol	TCP もしくは UDP を選択します。
Host Address	Client モードを選択した場合に、接続する Virtual COM サーバアドレスを入 力します。
Redirect Port	Virtual COM で使用するポート番号を設定します。

6.3. Logging

ルータのログの設定を行います。

6.3.1. Logging > Logging

System > Logging > Logging	
項目	説明
Mode	System Logging の有効/無効を選択します。
Remote Log	Syslog サーバへのログの転送を行います。
Log Server Address	Syslog サーバの IP アドレスを入力します。

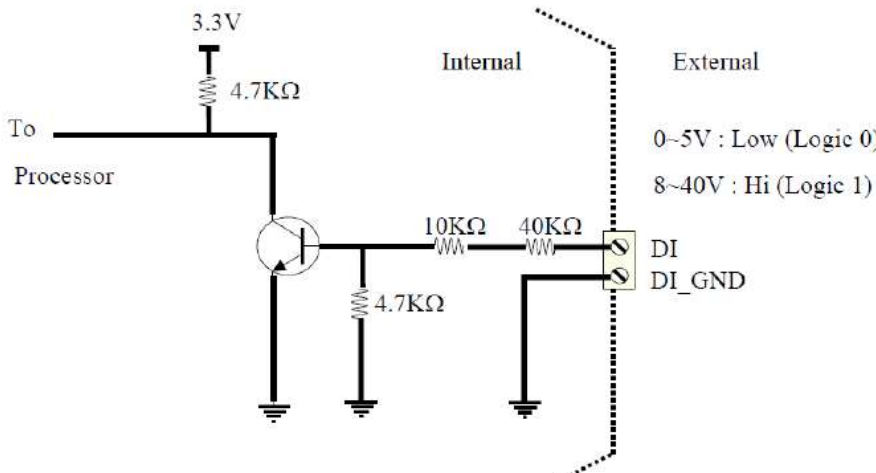
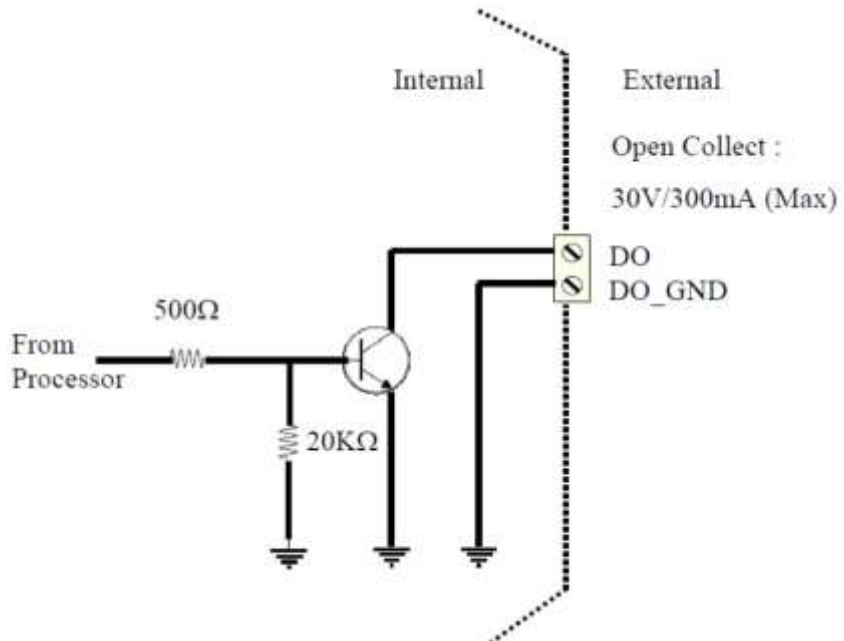
6.3.2. Logging > Log

System > Logging > Log	
項目	初期値
Filter	キーワードを入力して関連するログを表示します。
Clear	ログをすべて削除します。
Refresh	ログを更新します。
Download Logs	ログをテキスト形式でダウンロードします。

6.4. Alarm

ルータのアラームの設定を行います。

System > Alarm	
項目	説明
Mode	アラームの有効/無効を選択します。
Alarm Input	アラームのトリガを選択します。 <ul style="list-style-type: none"> • DI : Digital Input の入力電圧に応じて • VPN disconnect: すべての VPN 接続が切断された時 • WAN disconnect: WAN 接続が切断された時 • LAN disconnect: LAN ポートがリンクダウンした時 • Reboot: 再起動したとき
Alarm output	アラームの出力先を選択します。 SNMP Trap は WAN 接続が無い場合には送信しません。
DI Trigger	Digital Input 端子のトリガを選択します。 High: DI Input の入力電圧が 8～40V の時にアラームを発報します。 Low: DI Input の入力電圧が 0～5V 時にアラームを発報します。

	 <p>3.3V 4.7KΩ To Processor Internal External 0~5V : Low (Logic 0) 8~40V : Hi (Logic 1) DI DI_GND 10KΩ 4.7KΩ 40KΩ</p>
DO behavior	<p>Digital Output 端子の動作について設定します。</p> <ul style="list-style-type: none"> • Always: アラーム発報時に常時出力状態にします。 • Pulse: アラーム発報時に出力と停止を繰り返します。  <p>Internal External Open Collect : 30V/300mA (Max) DO DO_GND From Processor 500Ω 20KΩ</p>

6.5. Ethernet

Ethernet インタフェースに関する設定を行います。

Ethernet

Ethernet Ports Status

LAN 100M Full

WAN Off

Ethernet Ports Configurations

LAN ☒ Auto ☐ 100M Full ☐ 100M Half ☐ 10M Full ☐ 10M Half ☐ Disable

WAN ☒ Auto ☐ 100M Full ☐ 100M Half ☐ 10M Full ☐ 10M Half ☐ Disable

WAN Ethernet

WAN MTU min: 700; max: 1500

Flow Control

LAN ☐ Off ☒ On

Refresh

Apply

System > Ethernet	
項目	説明
Status	現在のインタフェースの状態を表示します。
Configurations	インタフェースの速度を選択します。
WAN Ethernet	この機能は現在サポートしていません。
Flow Control	フローコントロールの有効/無効を選択します。

6. 6. Client List

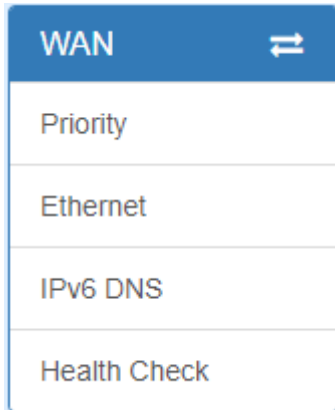
ルーターに接続されているクライアントのリストを表示します。

Client List		
List Type	<input type="checkbox"/> DHCP Client <input type="checkbox"/> Online	
#	IP Address	MAC Address
1	192.168.1.2	00:E0:B3:21:0B:AE
2	192.168.1.29	8C:16:45 [REDACTED]

System > Client List	
項目	説明
List Type	<ul style="list-style-type: none"> • DHCP Client: DHCP クライアントのリストを表示します。 • Online: オンラインのクライアントのリストを表示します。

7. WAN

ナビゲーションパネルにて **WAN** をクリックすると、WAN 関連の設定を開くことができます。



7.1. WAN > Priority

WAN 接続に使うインタフェースの優先度の設定を行います。

WAN > Priority	
項目	説明
WAN Priority	<ul style="list-style-type: none"> • Auto: WAN Ethernet を優先で使用し、次に LTE を使用します。 • LTE Only: LTE のみ使用します。 • ETH Only: WAN Ethernet のみ使用します。
Connect Order	WAN Priority が Auto の場合に、WAN ポートの優先順位を設定します。 <ul style="list-style-type: none"> • 1st: 最初に接続するWANポートを ETH/LTE から選択します。 • 2nd: 1st で設定した WAN ポート以外を選択します。
WAN/LAN2 Port Function	WAN/LAN2 の機能を選択します。本設定は WAN Priority が LTE Only の場合のみ有効です。

WAN > Priority	
LTE Net Mode	<ul style="list-style-type: none">• Bridge Only: LTE モードを Bridge にします。本モードを選択すると LAN ポートには 1 台の端末しか接続できません。• Router Only: LTE モードを Router に設定します。本モードを選択すると NAT 機能や Routing 機能を使用することができます。

7.2. WAN > Ethernet

WAN Ethernet の動作モードなどの設定を行います。

7.2.1. WAN Ethernet Configuration

DHCP Client, PPPoE Client, Static IPv4 の中から動作モードを選択します。

デフォルトは DHCP Client となります。

WAN > Ethernet	
項目	説明
WAN Ethernet	<ul style="list-style-type: none"> • DHCP Client: DHCP サーバから払い出された IP アドレスを使用します。 • PPPoE Client: ISP から提供されたユーザ名とパスワードを入力して接続します。 • Static IPv4: 任意の静的 IP アドレスを設定します。

- DHCP Client

DHCP Client を選択した場合、DNS サーバの設定を行うことができます。

The screenshot shows the 'WAN Ethernet' configuration interface. At the top, 'Work As' is set to 'DHCP Client'. Below this, the 'DNS Server Configuration' section contains three rows for 'IPv4 DNS Server #1', '#2', and '#3'. Each row has a dropdown menu currently set to 'From ISP' and an adjacent empty text input field. An 'Apply' button is located at the bottom right of the configuration area.

WAN > Ethernet > DHCP Client	
項目	説明
IPv4 DNS Server	<ul style="list-style-type: none"> • From ISP: DHCP サーバから払い出された DNS サーバの情報を使用します。 • User Defined: 任意の DNS サーバを設定します。

- PPPoE Client

PPPoE Client を選択した場合、ユーザ名とパスワードを入力します。

The screenshot shows a web interface for configuring WAN Ethernet. At the top, there's a blue header with a hamburger menu icon and the text "WAN Ethernet". Below the header, there's a section titled "Work As:" with three radio button options: "DHCP Client", "PPPoE Client" (which is selected), and "Static IPv4". Underneath, the "PPPoE Client Configuration" section contains two input fields: "User Name" with the value "test" and "Password" with masked characters "*****". An "Apply" button is located at the bottom right of the configuration area.

WAN > Ethernet > PPPoE Client	
項目	説明
User Name	ISP から提供されたユーザ名を入力します。
Password	ISP から提供されたパスワードを入力します。

7.3. WAN > IPv6 DNS

IPv6 DNS Server の設定を行います。

⇌ IPv6 DNS

APN1 DNS Server Configuration

IPv6 DNS Server #1

From ISP ▼

IPv6 DNS Server #2

From ISP ▼

IPv6 DNS Server #3

From ISP ▼

Apply

WAN > IPv6 DNS	
項目	説明
IPv6 DNS Server #1 IPv6 DNS Server #2 IPv6 DNS Server #3	<ul style="list-style-type: none"> • 3 つの IPv6 DNS Server を登録することができます。 • それぞれのサーバに対して、From ISP、User Defined または None から選択できます。 • From ISP を選択すると、IPv6 DNS アドレスは ISP から取得します。 • User Defined を選択した場合は、IPv6 DNS Server アドレスを手動で設定します。

7.4. WAN > Health Check

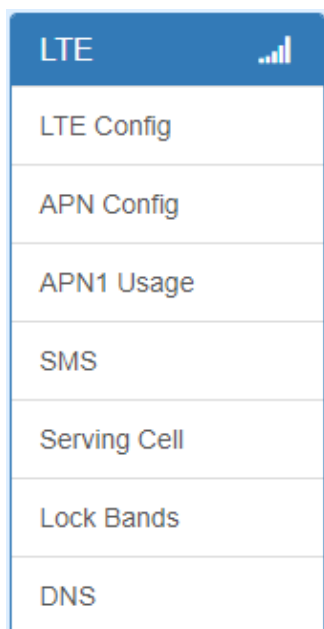
WAN Priority を Auto に設定している場合、この機能を使用することで現在の WAN 接続からインターネットへのアクセスが可能かどうかを判別することが出来ます。

もし、インターネットへのアクセスが不可能と判断した場合は、別の WAN 接続に切り替えます。

WAN > Ethernet > Ethernet Ping Health	
項目	説明
Ethernet Ping Health	本機能の有効/無効を選択します。
Method	ヘルスチェックの方法を選択します。
Use the first two DNS from ISP	ISP から提供されている DNS サーバの情報をヘルスチェックで使用します。
Interval	ヘルスチェックのインターバルを設定します。
IPv4 Host	ヘルスチェックに使用するアドレスを設定します。 このアドレスからの応答が無くなった場合に、ルータはインターネットへのアクセスが不可能と判断して、別の WAN 接続に切り替えます。

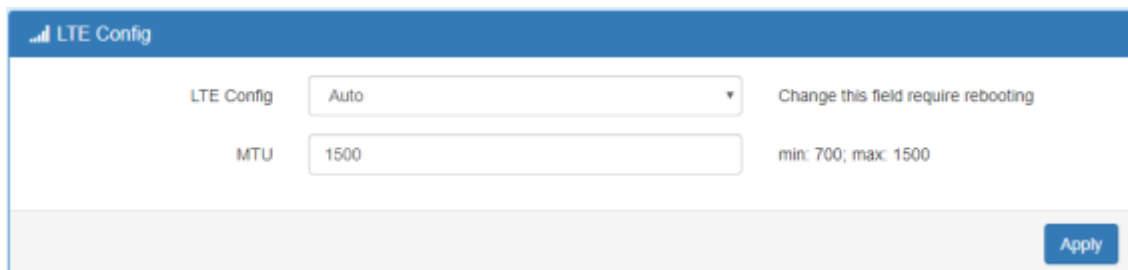
8. LTE

ナビゲーションパネルにて **LTE** をクリックすると、LTE 関連の設定を開くことができます。



8.1. LTE > LTE Config

LTE 設定を行います。



8. 1. 1. LTE Configuration

LTE 設定と LTE の MTU の設定を行います。

LTE Config

LTE Config

Auto

▼

Change this field require rebooting

MTU

1500

min: 500; max: 1500

LTE > LTE Config	
項目	説明
LTE Config	<ul style="list-style-type: none"> • Auto: 自動的に接続するネットワークを選択します。 • 4G Only: 4G のネットワークにのみ接続します。 • 3G Only: 3G のネットワークにのみ接続します。 • 2G Only: 2G のネットワークにのみ接続します。
MTU	<p>MTU を設定します。</p> <p>※ 本機では MTU サイズが 1320byte より高い場合でも MSS は 1280byte に固定されます。</p> <p>MTU サイズが 1320byte より低い場合は、MSS=MTU-40byte となります。</p>

8. 2. LTE > APN Config (V1.05)

SIM の設定を行います。

8. 2. 1. Recovery APN1 (V1.05)

回線切断後再接続失敗に対する処理を設定します。

Recover APN1

☐ No
☒ Yes

When APN1 continuous link down for times (3 ~ 15)

☒ Reboot
☐ Recover to default APN
☐ Recover to previous working APN

LTE > APN Config > Recover APN1	
項目	説明
Recover APN1	<ul style="list-style-type: none"> ・APN1 が連続して Link Down してもリカバーを行いません。 ・下記で指定した場合に APN1 をリカバーします。
When APN1 continuous link down for xx times.	<p>設定した回数だけ Link Down が連続した場合に、選択した方法でリカバー処理が動作します。</p> <ul style="list-style-type: none"> ・Reboot: システムをリブートします。 ・Recover to default APN: 本機では対応していません。 ・Recover to previous working APN: APN1 でリカバー処理を行います。

8. 2. 2. SIM Configuration

SIM PIN 及び PUK の設定を行います。

LTE > APN Config > SIM Configuration	
項目	説明
Status	SIM の現在のステータスを表示します。
SIM PIN	SIM の不正利用を防ぐためにあらかじめ SIM に設定してある PIN 番号を入力します。
Confirmed SIM PIN	
	PIN 番号を設定していない場合は、空欄にしてください。
SIM PUK	PIN ロックがかかっている SIM カードの PIN ロックを解除するためのコードを入力します。
Confirmed SIM PUK	
	PUK コードは契約した SIM の事業者にお問い合わせください。
Change SIM PIN	SIM の PIN 番号を変更します。

8.2.3. APN1 (V1.05)

APN 設定等を行います。

The screenshot shows the 'SIM Configuration' menu with 'APN1' selected. The configuration fields are as follows:

- APN**: Text input field
- Username**: Text input field
- Password**: Text input field
- Confirm Password**: Text input field
- Auth**: Dropdown menu currently set to 'NONE'
- Enable IPv6**: Checkbox (unchecked)

LTE > APN Config > APN1	
項目	説明
APN	APN、ユーザ名、パスワードを入力します。 契約した SIM の事業者から提供された情報を入力します。
Username	
Password	
Auth	認証方式を選択します。
Enable IPv6 (V1.05)	LTE の IPv6 接続を有効にします。(動作は回線契約に依存します。)

8. 2. 4. Data Limitation (V1.05)

使用できるデータ量を契約に合わせて制限する機能を設定できます。

Data Limitation

Already Used Data (MB) 0

Mode ☐ Disable ☒ Enable

Max Data Limitation (MB)

Monthly Reset Date: Hours: Minutes: Seconds:

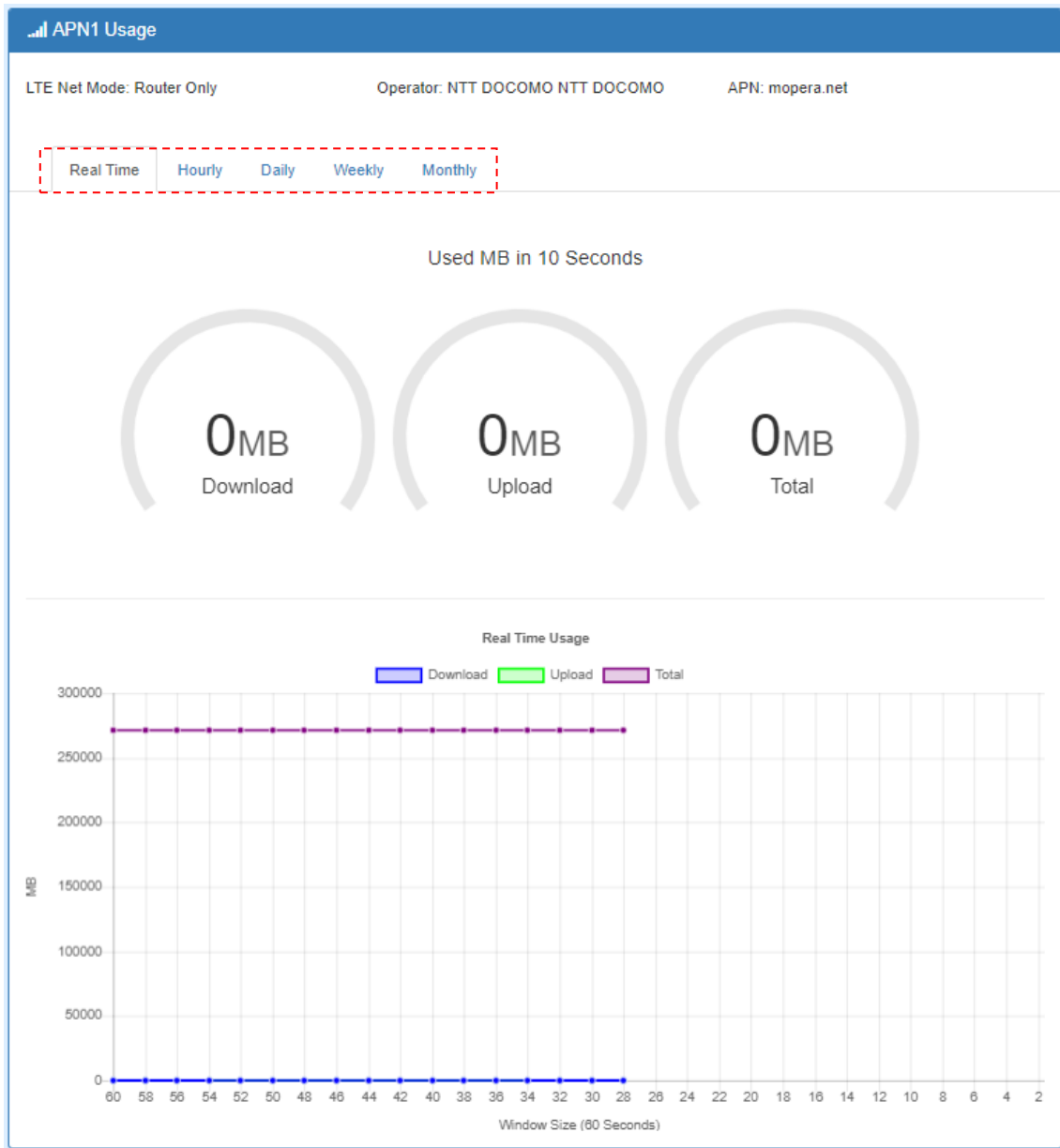
Now Time Date: 6 Hours: 10 Minutes: 39 Seconds: 56

LTE > APN Config > Data Limitation	
項目	説明
Mode	APN1 のデータ量制限の Enable/Disable を設定します。
Already Used Data(MB)	既に使用したデータ量を表示します。
Max Data Limitation(MB)	最大データ通信量を入力します。
Monthly Reset	月毎で使用済データ量をリセットする日時を設定します。
Now Time	システムの現在時刻を表示します。

8.3. LTE > APN1 Display

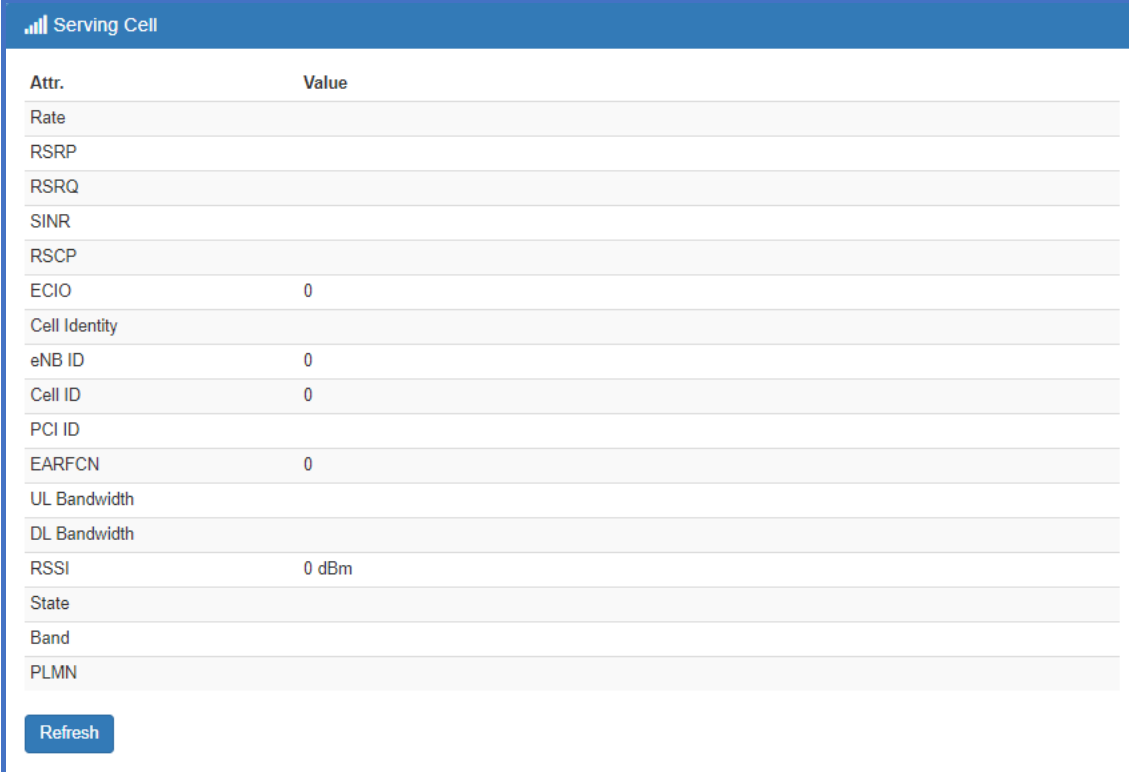
リアルタイム、毎時、毎日、毎週、毎月の単位でデータ使用量のステータスを確認することができます。

画面上部のタブから、Real Time/Hourly/Daily/Weekly/Monthly をクリックし、それぞれのステータスを表示します。



8. 4. LTE > Serving Cell

RSRP、RSRQ、SINR などの LTE 接続に関連するステータスを表示します。




Attr.	Value
Rate	
RSRP	
RSRQ	
SINR	
RSCP	
ECIO	0
Cell Identity	
eNB ID	0
Cell ID	0
PCI ID	
EARFCN	0
UL Bandwidth	
DL Bandwidth	
RSSI	0 dBm
State	
Band	
PLMN	

Refresh

(注)RSSI,State,Band,PLMN は V1.05 のみ

8. 5. LTE > Lock Bands

接続する LTE Band を選択することが出来ます。



LTE Bands: ☐ B01 ☐ B02 ☐ B03 ☐ B04 ☐ B05 ☐ B06 ☐ B07 ☐ B08 ☐ B09 ☐ B10

☐ B11 ☐ B12 ☐ B13 ☐ B14 ☐ B15 ☐ B16 ☐ B17 ☐ B18 ☐ B19 ☐ B20

☐ B21 ☐ B22 ☐ B23 ☐ B24 ☐ B25 ☐ B26 ☐ B27 ☐ B28 ☐ B29 ☐ B30

☐ B31 ☐ B32 ☐ B33 ☐ B34 ☐ B35 ☐ B36 ☐ B37 ☐ B38 ☐ B39 ☐ B40

☐ B41 ☐ B42 ☐ B43

Hint [EC25J] TDD:B41, FDD:B1/B3/B6/B18/B19/B26

Restore Default Band Apply

8.6. LTE > DNS

LTE 接続で使用する DNS サーバを設定します。

DNS

DNS Server Configuration

IPv4 DNS Server #1 From ISP ▼

IPv4 DNS Server #2 From ISP ▼

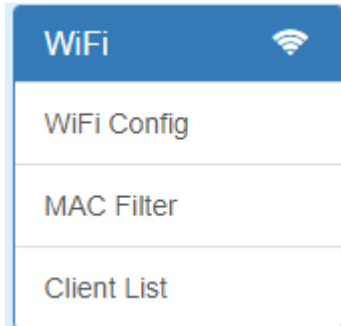
IPv4 DNS Server #3 From ISP ▼

[Apply](#)

LTE > DNS > DNS Server Configuration	
項目	説明
IPv4 DNS Server	<ul style="list-style-type: none"> From ISP: DHCP サーバから払い出された DNS サーバの情報を使用します。 User Defined: 任意の DNS サーバを設定します。

9. WiFi

ナビゲーションパネルにて **WiFi** をクリックすると、WiFi 関連の設定を開くことができます。



※ MAC Filter 機能はサポートしていません。

9.1. WiFi > WiFi Config

WiFi 関連の設定を行います。

The screenshot shows the 'WiFi Network' configuration page. At the top, there are radio buttons for 'AP Enable' (checked) and 'WPS Button' (checked). Below these are tabs for 'SSID-1' and 'SSID-2'. The 'SSID-1' tab is active, showing settings for 'Isolate' (checked), 'HT Mode' (20M), 'Country Code' (JP - Japan), 'Channel' (Auto), 'Name(SSID)' (HWL-2511-SS-000379063e2c), 'Hidden SSID' (checked), 'Encrypt' (Encryption(WPA2-PSK/A)), 'Passphrase' (masked), 'Key Update' (0), and 'VLAN Subnet' (NET1). An 'Apply' button is located at the bottom right.

WiFi > WiFi Config	
項目	説明
Isolate	On を選択した場合、クライアント同士の通信を遮断します。
HT Mode	帯域幅を選択します。
Country Code	必ず”JP - Japan”を選択してください。
Channel	チャンネルを選択します。
Name(SSID)	SSID を設定します。
Hidden SSID	SSID ステルス機能の有効/無効を選択します。
Encrypt	暗号化方式を選択します。
Passphrase	パスフレーズを設定します。初期値は「12345678」となります。
Key Update	暗号化キーの更新間隔を設定します。
VLAN Subnet	VLAN サブネットを選択します。SSID-1 では NET1 以外を選択出来ません。
SSID-2	SSID-2 の設定を行います。

※ TX Power の変更はサポートしていません。

9. 2. WiFi > Client List

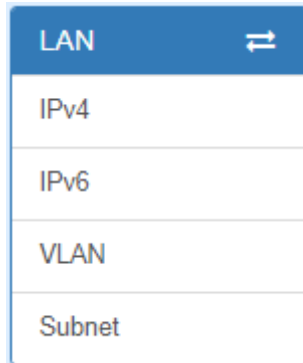
WiFi クライアントの一覧を表示します。



MAC Address	IP Address	Connected Time
BC:FE:D9: [redacted]	10.0.0.3	2
00:21:6B: [redacted]	10.0.0.2	263

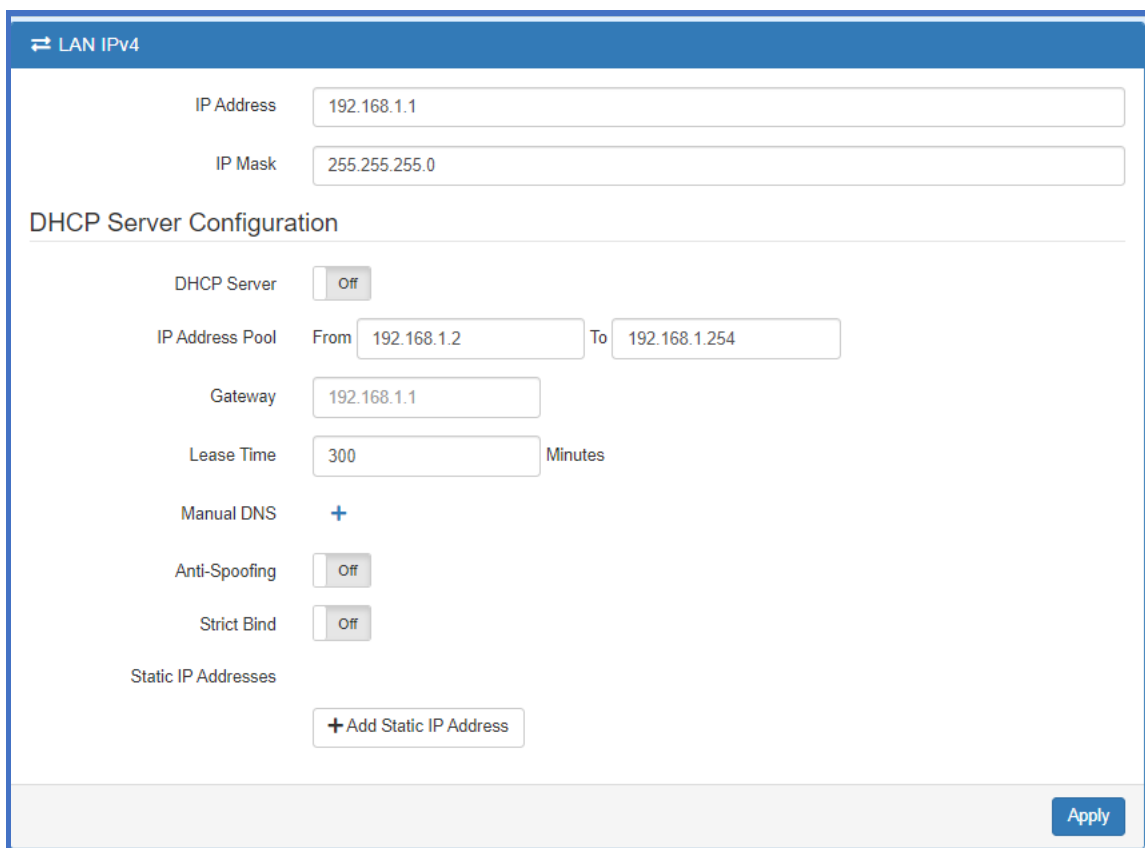
10. LAN

ナビゲーションパネルにて **LAN** をクリックすると、LAN 関連の設定を開くことができます。



10.1. LAN > IPv4 (V1.05)

LAN 側の IP アドレス関連の設定を行います。

The screenshot shows the 'LAN IPv4' configuration page. At the top is a blue header bar with a double-headed arrow icon and the text 'LAN IPv4'. Below this, there are two input fields: 'IP Address' with the value '192.168.1.1' and 'IP Mask' with the value '255.255.255.0'. A section titled 'DHCP Server Configuration' follows. It contains several settings: 'DHCP Server' is a toggle switch set to 'Off'; 'IP Address Pool' has 'From' and 'To' fields with values '192.168.1.2' and '192.168.1.254' respectively; 'Gateway' is an input field with '192.168.1.1'; 'Lease Time' is an input field with '300' followed by the text 'Minutes'; 'Manual DNS' is a button with a plus sign; 'Anti-Spoofing' and 'Strict Bind' are toggle switches both set to 'Off'. At the bottom of the configuration area is a button labeled '+ Add Static IP Address'. A blue 'Apply' button is located in the bottom right corner of the page.

LAN > IPv4	
項目	説明
IP Address	ルータの LAN 側 IP アドレスを設定します。
IP Mask	サブネットマスクを設定します。
DHCP Server	DHCP サーバ機能の有効/無効を選択します。
IP Address Pool	DHCP サーバ機能が有効の場合に、割り当てる IP アドレスのプールを設定します。
Gateway (V1.05)	通知する Gateway IP アドレスを設定します。 初期値は本機の IP アドレスです。
Lease Time (V1.05)	DHCP で付与する IP Address のリースタイムを設定します。 範囲: 5~43,200 分(30 日) 初期設定値 300 分 Static IP Address の場合は 720 分固定となります。
Manual DNS (V1.05)	DHCP で通知する DNS サーバアドレスを指定します。(最大 3 件)
Anti-Spoofing (V1.05)	DHCP Anti-Spoofing(なりすまし防止)機能の有効/無効を設定します。
Strict Bind (V1.05)	DHCP Strict Bind 機能の有効/無効を設定します。 本機能を有効にすると、Static IP Address リストに登録された MAC-IP アドレス機器以外は WAN との通信ができなくなります。
Static IP Addresses	指定した MAC アドレスの端末に固定で IP アドレスを割り当てます。

10.2. LAN > VLAN

VLAN の設定を行います。

The screenshot shows the 'VLAN' configuration page. At the top, there is a blue header with a double arrow icon and the text 'VLAN'. Below the header, there are two radio button options: 'Mode' with 'Off' selected and 'Tag Base' unselected, and 'VLAN Isolation' with 'Off' selected and 'On' unselected. At the bottom right, there is a blue 'Apply' button.

10.2.1. Tag Base VLAN

802.1p VLAN を使用した Tag ベースの VLAN を設定します。

The screenshot shows the 'VLAN' configuration page in 'Tag Base' mode. The 'Mode' radio button is now 'Tag Base' (selected) and 'Off' (unselected). The 'VLAN Isolation' remains 'Off'. Below the settings, there is a table with 4 columns: 'Enable', 'Subnet', 'VID', and 'Name'. The table contains 8 rows of VLAN configurations. At the bottom right, there is a blue 'Apply' button.

Enable	Subnet	VID	Name
<input checked="" type="checkbox"/>	NET1	1	lan(Full Feature LAN)
<input checked="" type="checkbox"/>	NET2	2	lan.2(LAN)
<input type="checkbox"/>	NET3	3	lan.3(LAN)
<input type="checkbox"/>	NET4	4	lan.4(LAN)
<input type="checkbox"/>	NET5	5	lan.5(LAN)
<input type="checkbox"/>	NET6	6	lan.6(LAN)
<input type="checkbox"/>	NET7	7	lan.7(LAN)
<input type="checkbox"/>	NET8	8	lan.8(LAN)

LAN > VLAN > Tag Base	
項目	説明
VLAN Isolation	VLAN 間ルーティングの有効/無効を設定します。
Enable	VLAN の有効/無効を設定します。
Subnet	サブネットを選択します。 サブネットの設定は LAN > Subnet で行います。
VID	VLAN ID を 1-4094 の間で入力します。








10.3. LAN > Subnet

サブネットの設定を行います。

Edit ボタンをクリックすることで、LAN>IPv4 と同様の IP 設定を各サブネットに対して行うことが出来ます。

LAN > VLAN にて Tag Base モードで VLAN を使用している場合、このメニューで設定したサブネットの設定が各 VLAN のネットワーク設定になります。

Subnet

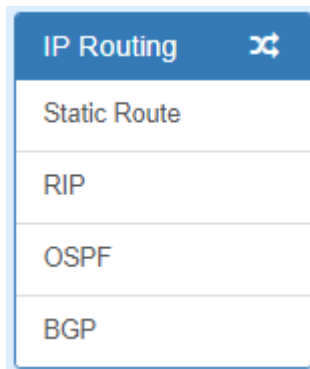
Name	IP Address	IP Mask	Edit
NET2	192.168.2.1	255.255.255.0	
NET3	192.168.3.1	255.255.255.0	
NET4	192.168.4.1	255.255.255.0	
NET5	192.168.5.1	255.255.255.0	
NET6	192.168.6.1	255.255.255.0	
NET7	192.168.7.1	255.255.255.0	
NET8	192.168.8.1	255.255.255.0	

Note: Subnet NET1 is the default IPv4 LAN, go [IPv4](#) for configuration.

Apply

11. IP Routing

ナビゲーションパネルにて **IP Routing** をクリックすると、ルーティング関連の設定を開くことができます。



11.1. IP Routing > Static Route

スタティックルーティングの設定を行います。

スタティックルーティングの設定を行うことで、特定のホストやネットワークに対しての経路を静的に設定することができます。

 A screenshot of the "Static Route" configuration page. The page has a blue header with a gear icon and the text "Static Route". Below the header, there are two tabs: "Settings" (selected) and "Status". Under the "Settings" tab, there is a "Mode" section with radio buttons for "Off" and "On". Below this, there are input fields for "Name", "Destination", "Gateway", and "Interface" (which has a dropdown menu showing "<empty>"). There is an "Add" button below the input fields. At the bottom right of the page, there is an "Apply" button.

IP Routing > Static Route	
項目	説明
Mode	スタティックルーティング機能の有効/無効を選択します。
Settings	
Mode	このスタティックルートの有効/無効を選択します。
Name	任意の名前を設定します。
Destination	宛先ホストまたはネットワークを入力します。
Gateway	ネクストホップのルータの IP アドレスを入力します。
Interface	宛先ホストまたはネットワークへとつながるインタフェースを選択します。

注意事項

- 1) Destination は必ず入力する必要があります。
- 2) Destination や Gateway に IP アドレス以外の値が入力された場合、エラーが発生します。
- 3) Gateway と Interface はどちらかを入力、もしくは両方入力することが出来ます。

ステータスタブをクリックすると、ルーティングテーブルを確認することができます。

Static Routing で設定したルートは Protocol に"Static"と表示され、それ以外は"Kernel"と表示されます。

Settings Status			
Destination	Gateway	Interface	Protocol
default	146.99.138.89	LTE	
146.99.138.80/28		LTE	kernel
192.168.0.0/24		WAN Ethernet	static
192.168.1.0/24		lan	kernel
fe80::/64		eth0	kernel
fe80::/64		lan	kernel
fe80::/64		LTE	kernel

11.2. IP Routing > RIP

RIP の設定を行います。

IP Routing > RIP > General	
項目	説明
Mode	RIP の有効/無効を選択します。
Redistribute local routes	それぞれのプロトコルで学習したルートの再配布を行うかどうか設定します。
Redistribute connected routes	
Redistribute OSPF routes	
Redistribute BGP routes	

RIP

General
 Interfaces

#	Mode	Interface	Authentication	Key	Key ID	Passive	Edit	Delete
Add RIP Interface								
Mode <input type="radio"/> Off <input checked="" type="radio"/> On								
Interface <input type="text" value="eth1(WAN Ethernet)"/>								
Authentication <input type="text" value="md5"/>								
Key <input type="text"/> The key used for authentication (maxlength=16)								
Key ID <input type="text" value="1"/> The ID of the key used for authentication (1-255)								
Passive <input checked="" type="radio"/> Off <input type="radio"/> On Do not send out RIP packets on this interface								
<input type="button" value="Add"/>								
<input type="button" value="Apply"/>								

IP Routing > RIP > Interfaces	
項目	説明
Mode	インタフェースでの RIP の有効/無効を選択します。
Interface	RIP を有効にするインタフェースを設定します。
Authentication	認証の有効/無効を選択します。 <ul style="list-style-type: none"> ● md5: HMAC-MD5 のハッシュアルゴリズムによる認証を行います。 ● none: 認証を行いません。
Key	認証キーを設定します。
Key ID	認証キー識別子を 1-255 の範囲で設定します。
Passive	Passive を On に設定したインタフェースからは RIP のルーティングアップデートを送信しなくなります。

11.3. IP Routing > OSPF

OSPF の設定を行います。

IP Routing > OSPF > General	
項目	説明
Mode	OSPF の有効/無効を選択します。
Redistribute local routes	それぞれのプロトコルで学習したルートの再配布を行うかどうか設定します。
Redistribute connected routes	
Redistribute RIP routes	
Redistribute BGP routes	

OSPF

General

Interfaces

Networks

#	Mode	Interface	Authentication	Key	Key ID	Cost	Passive	Edit	Delete
Add OSPF Interface									
<div> <div>Mode</div> <div> <input type="radio"/> Off <input checked="" type="radio"/> On </div> </div> <div> <div>Interface</div> <div>eth1(WAN Ethernet) ▼</div> </div> <div> <div>Authentication</div> <div>md5 ▼</div> </div> <div> <div>Key</div> <div></div> <div>The key used for authentication (maxlength=16)</div> </div> <div> <div>Key ID</div> <div>1</div> <div>The ID of the key used for authentication (1-255)</div> </div> <div> <div>Cost</div> <div>0</div> <div>The cost for sending packets via this interface (0: OSPF defaults)</div> </div> <div> <div>Passive</div> <div> <input checked="" type="radio"/> Off <input type="radio"/> On </div> <div>Do not send out OSPF packets on this interface</div> </div> <div>Add</div>									

Apply

IP Routing > OSPF > Interfaces	
項目	説明
Mode	インタフェースでの OSPF の有効/無効を選択します。
Interface	OSPF を有効にするインタフェースを設定します。
Authentication	認証の有効/無効を選択します。 <ul style="list-style-type: none"> ● md5: HMAC-MD5 のハッシュアルゴリズムによる認証を行います。 ● none: 認証を行いません。
Key	認証キーを設定します。
Key ID	認証キー識別子を 1-255 の範囲で設定します。
Cost	インタフェースのコストを設定します。
Passive	Passive を On に設定したインタフェースからは OSPF のルーティングアップデートを送信なくなります。

OSPF

General

Interfaces

Networks

#	Mode	Prefix	Prefix Length	Area	Edit	Delete
1	on	192.168.1.0	24	0		
2	on	10.10.10.0	24	0		

Add OSPF Network

Mode

☐ Off
 ☒ On

Prefix

xxx.xxx.xxx.xxx

Prefix of the network

Prefix Length

24

Length of the prefix

Area

0

Routing area to which this interface belongs (0-65535, 0 means backbone)

Add

Apply

IP Routing > OSPF > Networks	
項目	説明
Mode	ネットワークでの OSPF の有効/無効を選択します。
Prefix	OSPF を有効にするネットワークを設定します。
Prefix Length	ネットワークのプレフィックス長を設定します。
Area	ルーティングエリアの設定を行います。

11.4. IP Routing > BGP

BGP の設定を行います。

BGP

General

Neighbors

Networks

Mode

☒ Off

☐ On

AS Number

1

The number of the autonomous system (1 ~ 4294967295)

Redistribute local routes

☒ Off

☐ On

from the device's own routing table

Redistribute connected routes

☒ Off

☐ On

to networks which are directly connected to the device

Apply

IP Routing > BGP > General	
項目	説明
Mode	BGP の有効/無効を選択します。
AS Number	AS 番号を設定します。
Redistribute local routes	それぞれのプロトコルで学習したルートの再配布を行うかどうか設定します。
Redistribute connected routes	

✖ BGP

General
Neighbors
Networks

#	Mode	IP Address	AS Number	Multihop	Update Source Address	Edit	Delete
Add BGP Neighbor							
<div style="display: flex; justify-content: space-between;"> <div> <p>Mode <input type="radio"/> Off <input checked="" type="radio"/> On</p> <p>IP Address <input style="width: 150px;" type="text"/></p> <p>AS Number <input style="width: 150px; text-align: center;" type="text" value="1"/></p> <p>Multihop <input type="radio"/> Off <input checked="" type="radio"/> On</p> <p>Update Source Mode <input checked="" type="radio"/> Off <input type="radio"/> On</p> <p>Update Source Address <input style="width: 150px;" type="text"/></p> </div> <div> <p>IP address of the peer router</p> <p>Autonomous system number of the peer router</p> <p>Allow multiple hops between this router and the peer router</p> <p>Whether to specify the source address to this neighbor</p> <p>The source address to this neighbor</p> </div> </div> <div style="text-align: center; margin-top: 10px;"> Add </div>							

Apply

IP Routing > BGP > Neighbors	
項目	説明
Mode	BGP の有効/無効を選択します。
IP Address	相手先ルータの IP アドレスを入力します。
AS Number	相手先ルータの AS 番号を入力します。
Multihop	このルータと相手先ルータとの間でマルチホップを有効にするかどうか選択します。有効にすると TTL が 255 に設定されます。
Update Source Mode	この機能は未サポートです。
Update Source Address	

BGP

General Neighbors **Networks**

#	Mode	Prefix	Prefix Length	Edit	Delete
1	on	10.10.10.0	24		

Add BGP Network

Mode ☐ Off ☒ On

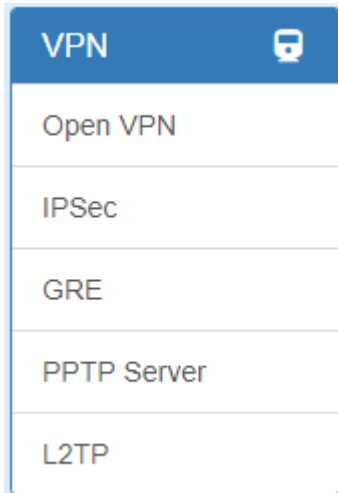
Prefix Prefix of the network

Prefix Length Length of the prefix

IP Routing > BGP > Networks	
項目	説明
Mode	BGP の有効/無効を選択します。
Prefix	BGP を有効にするネットワークを設定します。
Prefix Length	ネットワークのプレフィックス長を設定します。

12. VPN

ナビゲーションパネルにて **VPN** をクリックすると、VPN 関連の設定を開くことができます。

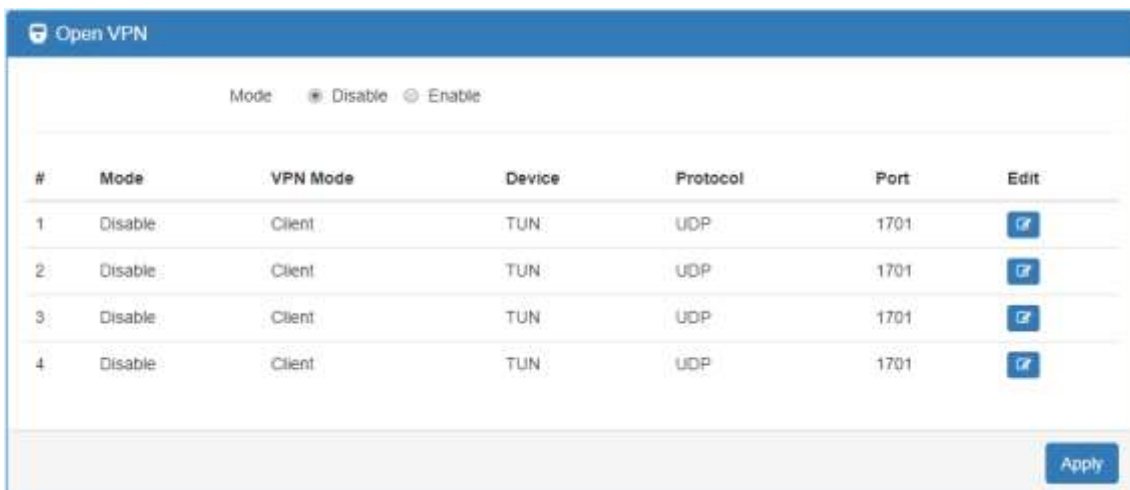


※ 本機は、VPN のメッシュ構成に対応していません。

12.1. VPN > Open VPN

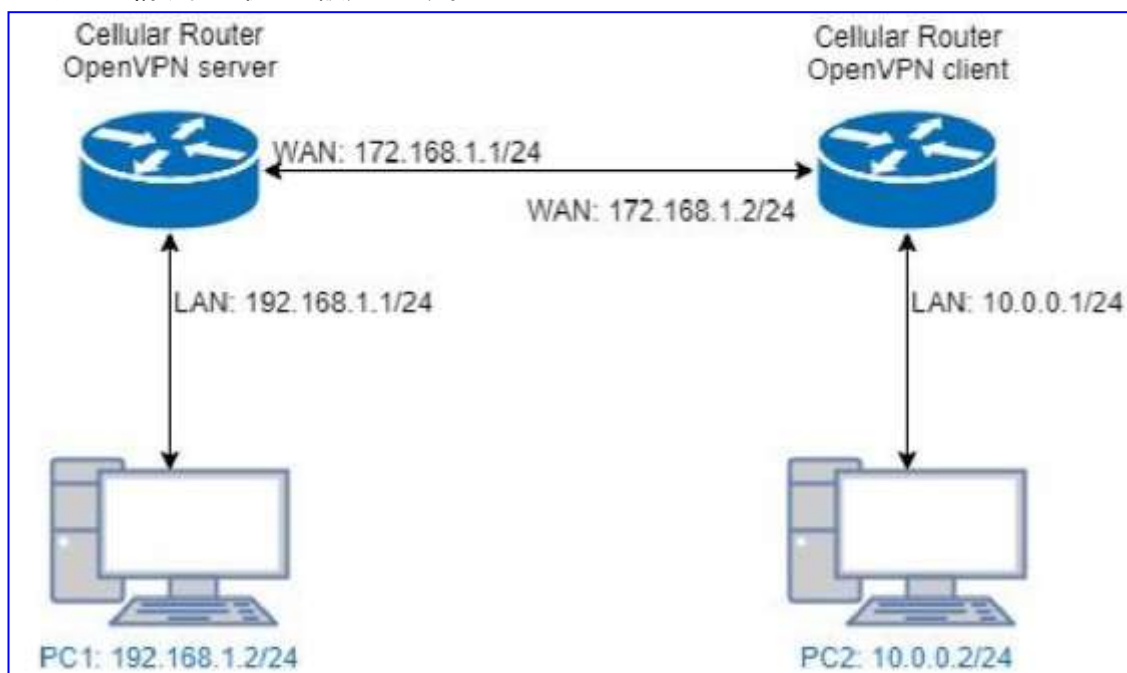
Open VPN の設定を行います。

Edit ボタンをクリックすることで、Open VPN 接続の設定を行うことができます。



12. 1. 1. Open VPN 設定例

以下の構成例に従って設定します。



※ 本機は、VPN のメッシュ構成に対応していません。

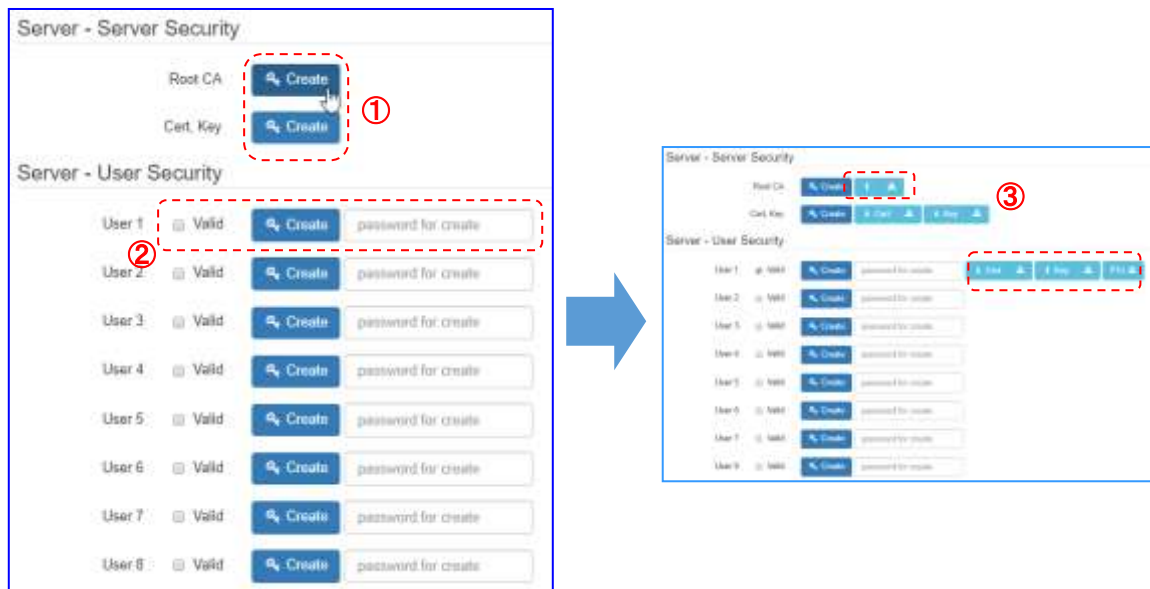
● Open VPN Server の設定

1. サーバの基本設定

Mode	<input type="radio"/> Disable <input checked="" type="radio"/> Enable ①						
VPN Mode	<input checked="" type="radio"/> Server <input type="radio"/> Client <input type="radio"/> Custom ②						
VPN Type	<input checked="" type="radio"/> Roadwarrior <input type="radio"/> Bridging ③						
Status	<div>Running</div> <table border="1"> <thead> <tr> <th>CN</th> <th>IP</th> <th>Connected since</th> </tr> </thead> <tbody> <tr> <td>user-00-00@openvpn</td> <td>192.168.30.6</td> <td>2019-08-16 14:31:50</td> </tr> </tbody> </table>	CN	IP	Connected since	user-00-00@openvpn	192.168.30.6	2019-08-16 14:31:50
CN	IP	Connected since					
user-00-00@openvpn	192.168.30.6	2019-08-16 14:31:50					
TLS Mode	<input checked="" type="radio"/> Disable <input type="radio"/> Enable						
Cipher	AES-256-CBC ④						
IPv6 Mode	<input checked="" type="radio"/> Disable <input type="radio"/> Enable						
Device	<input checked="" type="radio"/> TUN <input type="radio"/> TAP ⑤						
Protocol	<input checked="" type="radio"/> UDP <input type="radio"/> TCP						
Port	1701						
VPN Compression	<input type="radio"/> Disable <input checked="" type="radio"/> Enable						
Authentication	Certificate						
Server							
VPN Network	192.168.30.0 ⑥						
VPN Netmask	255.255.255.0						
Roadwarrior							
Route Client Networks	<input type="radio"/> Off <input checked="" type="radio"/> On ⑦						
Connections - Net / Mask							
#1	10.0.0.0 / 255.255.255.0						

手順	内容
①	Mode を Enable(有効)に設定します。
②	VPN Mode を Server に設定します。
③	VPN Type を Roadwarrior に設定します。
④	Cipher を”AES-256-CBC”に設定します。 この設定はクライアント側と同じにする必要があります。
⑤	Device を TUN に設定します。
⑥	VPN Network と VPN Netmask に Open VPN 用の仮想ネットワークを設定します。
⑦	Route Client Networks を on にし、Open VPN Client(相手側ルータ)の LAN 側ネットワークを入力します。 この設定を入れることで、VPN が確立した時に自動でルーティングしてくれます。

2. Root CA 証明書などの発行



手順	内容
①	Root CA と Cert Key の Create ボタンをクリックする。 Cert Key の Create には 10 分ほどかかります。そのままの画面でお待ちください。
②	Valid にチェックを入れて、Password を入力したあとに Create ボタンをクリックし、ユーザの証明書、キーを発行します。 ここで入力したパスワードはクライアントの設定時にも使用します。
③	発行されたファイルのうち、以下のファイルをダウンロードします。 <u>Server – Server security</u> <ul style="list-style-type: none"> ● Root CA <u>Server – User security</u> <ul style="list-style-type: none"> ● Cert ● Key ● P12

● Open VPN Client の設定

1. クライアントの基本設定

Mode ☐ Disable ☒ Enable ①

VPN Mode ☐ Server ☒ Client ☐ Custom ②

VPN Type ☒ Roadwarrior ☐ Bridging ③

Status Connected

IP	Connected since
192.168.30.6	2019-08-16 14:31:54

TLS Mode ☒ Disable ☐ Enable

Cipher AES-256-CBC ④

IPv6 Mode ☒ Disable ☐ Enable

Device ☒ TUN ☐ TAP ⑤

Protocol ☒ UDP ☐ TCP ⑥

Port 1701

VPN Compression ☐ Disable ☒ Enable

Authentication pkcs #12 Certificate ⑦

Client

Server Address 172.168.1.1 ⑧

PKCS12 Password hoge hoge

Route Client Networks ☐ Off ☒ On ⑨

手順	内容
①	Mode を Enable(有効)に設定します。
②	VPN Mode を Client に設定します。
③	VPN Type を Roadwarrior に設定します。
④	Cipher を”AES-256-CBC”に設定します。 この設定はサーバ側と同じにする必要があります。
⑤	Device を TUN に設定します。
⑥	Authentication で”pkcs #12 Certificate”を選択します。
⑦	サーバの WAN 側 IP アドレスを入力します。
⑧	サーバの設定でユーザの証明書などを発行した際のパスワードを入力します。
⑨	Route Client Networks を on にします。

2. ローカルネットワークの指定

Local Network

Network

10.0.0.0 ①

Netmask

255.255.255.0

手順	内容
①	クライアントの LAN 側のネットワークを入力します。

3. 証明書のインポート

Client - Security

Root CA ①

Import

i

↓

Cert

Import

i

↓

Key

Import

i

↓

P12

Import

↓

手順	内容
①	サーバ側で発行してダウンロードした以下のファイルをインポートします。 <u>Server - Server security</u> <ul style="list-style-type: none"> Root CA
②	サーバ側で発行してダウンロードした以下のファイルをインポートします。 <u>Server - User security</u> <ul style="list-style-type: none"> Cert Key P12

4. VPN 確立の確認

VPN が確立されると、Status に以下のように表示されます。

Status	Running		
	CN	IP	Connected since
	user-00-00@openvpn	192.168.30.6	2019-08-16 14:31:50

12. 2. VPN > IPsec

IPsec の設定を行います。

IPsec

Mode ☐ Disable ☒ Enable

Type ☒ Policy-based ☐ Route-based

Connections Authentication IDs X.509 Certificates CA Certificates

- IPsec SA active and link up
- Only IPsec SA active
- Connecting
- IPsec SA inactive
- Disabled

- Phase 1 : Edit IPsec Phase 1 setting
- Phase 2 : Edit IPsec Phase 2 setting
- ... : Edit IPsec Advance setting

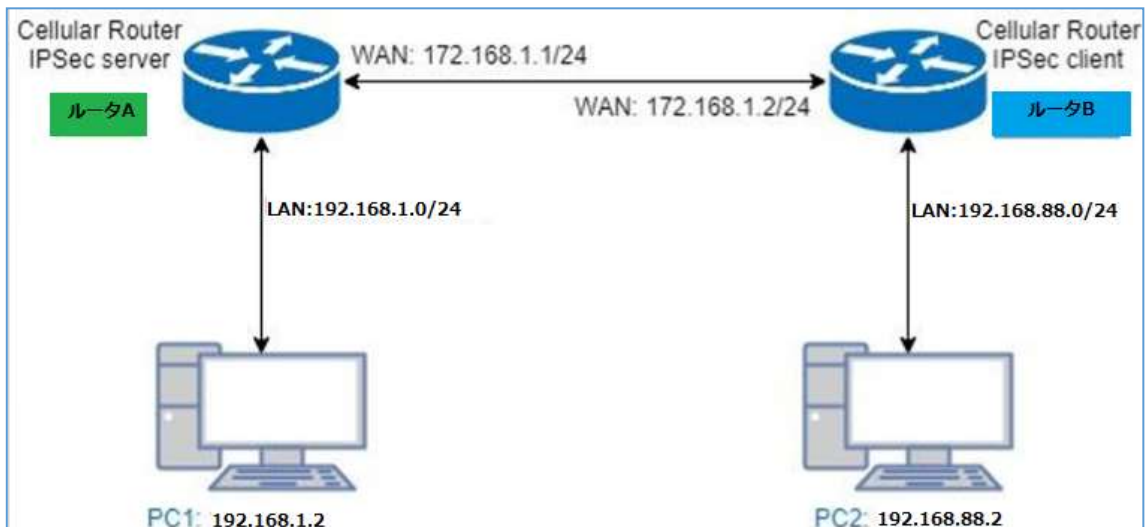
#	Name	State	IKE information	Tunnel information
1	IPSEC_TEST	✓	IKEv2 : 172.168.1.1 [test] ... 172.168.1.2 [172.168.1.2]	Phase 1 192.168.1.0/24 ... 192.168.88.0/24 Phase 2 ...

+ Add Connection

Apply

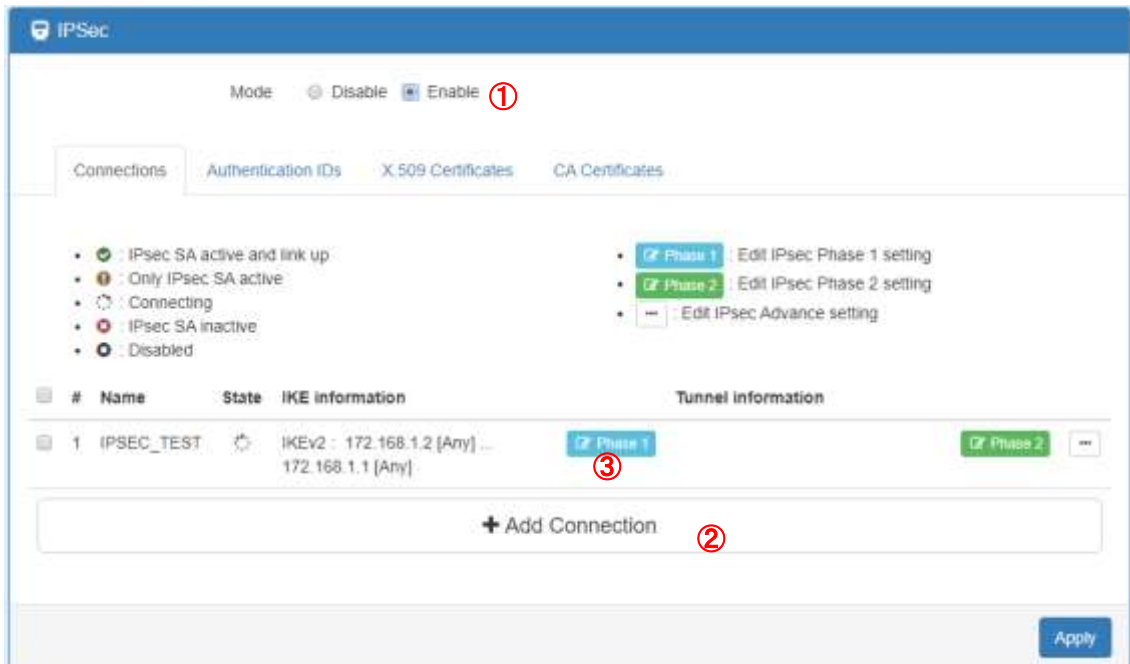
12. 2. 1. IPsec 設定例

以下の構成例に従って設定します。



※ 本機は、VPN のメッシュ構成に対応しておりません。

1. ルータ A とルータ B で共通の設定



手順	内容
①	Mode を Enable(有効)に設定します。
②	Add Connection をクリックします。
③	Phase 1 をクリックします。

2. Phase 1 の設定

Connection #1 Phase 1

Mode ☐ Disable ☒ Enable

Name testtunnel

Protocol IKEv2

Auth Type PSK

Encryption AES256

Hash SHA256

DH Group 5 (1536 bit)

Lifetime 3 hours

Local Host

Local ID <empty> (allow any)

Remote Host 172.16.1.2

Remote ID <empty> (allow any)

Back Save

手順	内容
①	プロトコル、認証方式、暗号化方式などを各ルータで同じ設定にします。
②	<p>Remote Host に相手先ルータの WAN 側 IP アドレスを入力します。</p> <p>ルータ A に入力する場合は、172.168.1.2(ルータ B の WAN 側 IP)</p> <p>ルータ B に入力する場合は、172.168.1.1(ルータ A の WAN 側 IP)と入力します。</p> <p>※ この設定は、どちらか一方のルータで入力されていれば問題ありません。</p> <p>例えば、ルータAが固定グローバルIPアドレスを所持している場合は、ルータB側でルータAの固定グローバル IP を指定すれば、ルータA側では入力する必要がありません。</p>

3. Phase2 の設定

Connection #1 Phase 2

①	Protocol	ESP
	Encryption	AES256
	Hash	SHA256
	DH Group	5 (1536 bit)
	Lifetime	
②	Local Subnet	192.168.1.0/24
③	Remote Subnet	192.168.88.0/24
	Service	Any

Back Save

手順	内容
①	プロトコル、暗号化方式、ハッシュアルゴリズムを各ルータで同じ設定にします。
②	Local Subnet に自ルータの LAN 側ネットワークアドレスを入力します。 ルータ A の場合は、192.168.1.0/24 ルータ B の場合は、192.168.88.0/24 と入力します。
③	Remote Subnet に相手先ルータの LAN 側ネットワークアドレスを入力します。 ルータ A の場合は、192.168.88.0/24 ルータ B の場合は、192.168.1.0/24 と入力します。

4. PSK の設定

手順	内容
①	Authentication IDs をクリックします。
②	Add Authentication ID をクリックします。
③	ID は空白のまま、Preshared Key のみ入力します。 この時、ルータ A とルータ B で同じ設定にします。

5. VPN 確立の確認

VPN が確立されると、Connections の画面で State が マークになります。

12.3. VPN > GRE

GRE の設定を行います。

※ 本機は、VPN のメッシュ構成に対応しておりません。

VPN > GRE	
項目	説明
Mode	GRE の有効/無効を選択します。
Local Address	自ルータの GRE に使用するインタフェースのアドレスを入力します。
Remote Address	相手先ルータの GRE に使用するインタフェースのアドレスを入力します。
Tunnel Device Address	トンネルインタフェース用の任意の IP アドレスとプレフィックスを入力します。
Tunnel Device Prefix	

12.4. VPN > PPTP Server

PPTP Server の設定を行います。

VPN > PPTP Server > General	
項目	説明
Mode	PPTP サーバの有効/無効を選択します。
Server	PPTP サーバ用の仮想 IP アドレスを設定します。
Client Address Range	PPTP クライアントに割り当てる IP アドレスの範囲を設定します。

PPTP Server

General
Clients

#	Mode	Username	Edit	Delete
Add PPTPD Client				
Mode <input type="radio"/> Off <input checked="" type="radio"/> On				
Username <input type="text"/>				
Password <input type="password"/>				
Add				
Apply				

VPN > PPTP Server > Clients	
項目	説明
Mode	クライアントの有効/無効を選択します。
Username	クライアントのユーザ名/パスワードを入力します。
Password	

● クライアント側の PPTP 設定の例

接続名

PPTP

サーバー名またはアドレス

146.99.37.150

VPNの種類

Point to Point トンネリング プロトコル (PPTP)

サインイン情報の種類

ユーザー名とパスワード

ユーザー名 (オプション)

test

パスワード (オプション)

●●●●●●●●●●

12.5. VPN > L2TP

L2TP の設定を行います。(本製品は L2TP version 2 に対応しています。)

L2TP

Mode

☐ Off
 ☒ Server
 ☐ Client

Auth

☐ PAP
 ☐ CHAP
 ☐ MS-CHAP
 ☒ MS-CHAPv2

Local IP

192.168.10.1

Remote begin IP

192.168.10.2

Remote end IP

192.168.10.10

User List

#	Username	Edit	Delete
1	test		

Add L2TP User for Server Mode


Username

Password

Add

Apply

VPN > L2TP > Server	
項目	説明
Mode	L2TP の動作モードを選択します。
Auth	認証方式を設定します。
Local IP	L2TP サーバ用の仮想 IP アドレスを設定します。
Remote begin IP	L2TP クライアントに割り当てる IP アドレスの範囲を設定します。
Remote end IP	
User List	作成済みのユーザのリストを表示します。
Add L2TP User for Server Mode	
Username	クライアントのユーザ名とパスワードを設定します。 Add ボタンをクリックすることでユーザを追加できます。
Password	

 L2TP

Mode ☐ Off ☐ Server ☒ Client

Connection List

Empty Connections

Add L2TP Connection for Client Mode

Mode ☐ Off ☒ On

Server

Auth ☐ PAP ☐ CHAP ☐ MS-CHAP ☒ MS-CHAPv2

Username

Password

NAT ☐ Off ☒ On

Default Route ☐ Off ☒ On

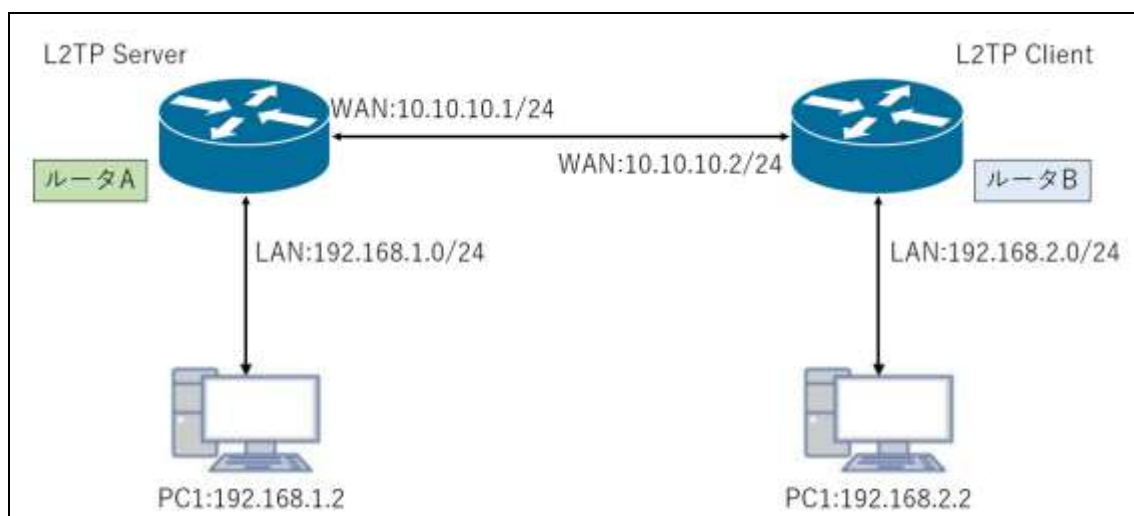
Add

Apply

VPN > L2TP > Client	
項目	説明
Mode	L2TP の動作モードを選択します。
Server	L2TP サーバの IP アドレスを入力します。
Auth	認証方式を選択します。
Username	ユーザ名とパスワードを入力します。
Password	
NAT	LAN 側 IP アドレスを L2TP 仮想 IP アドレスに NAT するかどうか選択します。 基本的には ON に設定します。
Default Route	L2TP サーバをデフォルトゲートウェイに設定するかどうかを選択します。 全ての通信を L2TP サーバ宛てに送信することになります。 ※ 本機は L2TP トンネル経由でのインターネット接続が出来ません。

12.5.1. L2TP 設定例(Site-to-Site)

以下の構成例に従って設定します。



※ L2TP のバージョンは L2TPv2 となります。

1. L2TP サーバ(ルータ A)の設定

VPN > L2TP の画面を開きます。

L2TP

Mode

☐ Off ☒ Server ☐ Client

Auth

☐ PAP ☐ CHAP ☐ MS-CHAP ☒ MS-CHAPv2

Local IP

192.168.10.1

Remote begin IP

192.168.10.10

Remote end IP

192.168.10.20

User List

#	Username	Edit	Delete
1	test		

Add L2TP User for Server Mode

Username

Password

Add

Apply

手順	内容
①	Mode で Server を選択し、Auth で認証方式を選択します。
②	任意の Local IP を入力します。
③	クライアントに割り当てる IP アドレスの範囲を入力します。
④	ユーザ名、パスワードを入力して、“Add”をクリックします。
⑤	Add をクリックします。
⑥	Apply をクリックします。

2. L2TP クライアント(ルータ B)の設定

VPN > L2TP の画面を開きます。

L2TP

① Mode: ☐ Off ☐ Server ☒ Client

Connection List

#	Mode	Server	Auth	Username	NAT	Default Route	Edit	Delete
1	On	10.10.10.1	mschapv2	test	On	Off		

Edit L2TP Connection #1 for Client Mode

② Mode: ☐ Off ☒ On

③ Server:

④ Auth: ☐ PAP ☐ CHAP ☐ MS-CHAP ☒ MS-CHAPv2

Username:

⑤ Password:

NAT: ☐ Off ☒ On

⑥ Default Route: ☒ Off ☐ On

⑦

⑧

手順	内容
①	Mode で Client を選択します。
②	Mode で On を選択します。
③	Server の WAN 側 IP アドレスを入力します。
④	Server で選択した認証方式と同じものを選択します。
⑤	ユーザ名、パスワードを入力します。
⑥	NAT を On、Default Route を Off に設定します。
⑦	Add をクリックします。
⑧	Apply をクリックします。

3. ルータ B のルーティングの設定

IP Routing > Static Route の画面を開きます。

手順	内容
①	Mode で On を選択します。
②	Mode で On を選択します。
③	任意の名前を設定します。
④	Destination にルータ A の LAN 側ネットワークを入力します。
⑤	Interface に L2TP client#1 を選択します。(Gateway は空欄で構いません)
⑥	Add をクリックします。
⑦	Apply をクリックします。

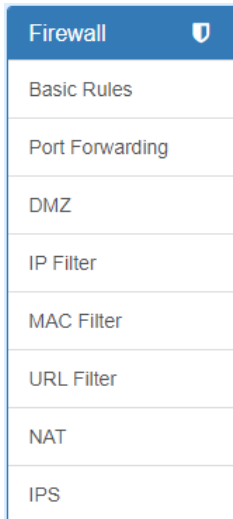
4. ステータスの確認

Statu 画面下部の”Connected VPN Connections”にて L2TP の数値が 0⇒1 になっていれば
接続は完了です。

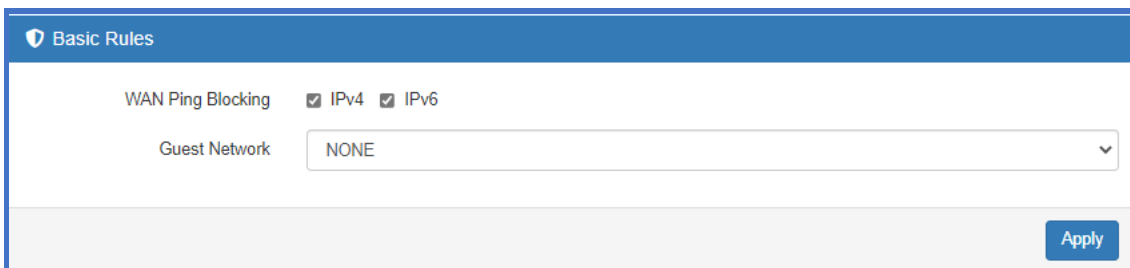
Connected VPN Connections	
Attr.	Value
OpenVPN	0
IPSec	0
GRE	0
PPTP Server	0
L2TP	1

13. Firewall

ナビゲーションパネルにて **Firewall** をクリックすると、ファイアウォール関連の設定を開くことができます。



13.1. Firewall > Basic Rules



Firewall > Port Forwarding	
項目	説明
WAN Ping Blocking	WAN インタフェースの Ping 応答をブロックするか選択します。 チェックを入れた場合、WAN インタフェースは Ping に応答しません。
Guest Network (V1.05)	Guest Network を指定します。VLAN/Subnet で設定した NET1～NET8 を Guest Network として使用できます。

13.2. Firewall > Port Forwarding

ポートフォワーディングの設定を行います。

本機では最大で 16 個までのルールを作成することが出来ます。

#	Mode	Description	Protocol	Edit
1	Enable	ssh	TCP	[Edit]
2	Disable		TCP	[Edit]
3	Disable		TCP	[Edit]
4	Disable		TCP	[Edit]
5	Disable		TCP	[Edit]
6	Disable		TCP	[Edit]
7	Disable		TCP	[Edit]
8	Disable		TCP	[Edit]
9	Disable		TCP	[Edit]
10	Disable		TCP	[Edit]
11	Disable		TCP	[Edit]
12	Disable		TCP	[Edit]
13	Disable		TCP	[Edit]
14	Disable		TCP	[Edit]

Apply

Firewall > Port Forwarding	
項目	説明
Mode	本機でのポートフォワーディング機能の有効/無効を設定します。
Edit	このボタンをクリックすることで、ポートフォワーディングの設定を行うことができます。

● Edit Port Forwarding Entry

Edit Port Forwarding Entry #1

Mode ☐ Disable ☒ Enable

Description

Protocol ☒ TCP ☐ UDP

Source Port Begin

Source Port End

Destination IP

Destination Port Begin

Destination Port End

Save

Firewall > Port Forwarding > Edit Port Forwarding Entry	
項目	説明
Mode	このルールの有効/無効を設定します。
Description	このルールの説明文を設定します。
Protocol	TCP、UDP から選択します。
Source Port Begin	ルータの WAN 側待ち受けポート番号を設定します。
Source Port End	
Destination IP	このパケットを転送する LAN 側の端末の IP アドレスを入力します。
Destination Port Begin	LAN 側の端末に転送する際に使用するポート番号を設定します。
Destination Port End	

13.3. Firewall > DMZ

DMZ の設定を行います。

Firewall > DMZ	
項目	説明
Mode	DMZ の有効/無効を設定します。
Host IP Address	DMZ ホストに指定する LAN 側端末の IP アドレスを入力します。 指定された端末には WAN 側からのすべての通信が転送されます。 ただし、初期設定では https(tcp:443)、ssh(tcp:8022)についてはルータが応答します。 “Management > Web”、“Management > SSH”メニューでそれぞれルータの待ち受けポート番号を変更することが出来ます。

13.4. Firewall > Management IP (V1.05)

IP フィルタ/MAC フィルタ/URL フィルタで White List を選択した場合、List 以外のパケットは破棄されます。管理者の IP を設定することで、管理者が White List 条件に当たらない場合でも通信することができます。

Firewall > Management IP	
項目	説明
Management IP Address	管理者用の IP アドレスを指定します。 0.0.0.0 は Management IP Address 機能が無効になります。

13.5. Firewall > IP Filter

IP フィルタの設定を行います。

IP Filter

Mode

☒ Disable
 ☐ Enable

List

☒ Black
 ☐ White

(Warnig: White List will block device services, enable them in 'Service Port'.)

#	Mode	Protocol	Source / Port	Destination / Port	Edit
1	Disable	All	0.0.0.0 / --	0.0.0.0 / --	

Firewall > IP Filter	
項目	説明
Mode	IP フィルタの有効/無効を設定します。
List	リストのデフォルトルールを設定します。 ・Black: リストに追加した条件のパケットを破棄します。 ・White: リストに追加した条件以外のパケットを破棄します。
Edit	Edit ボタンをクリックすることで各ルールの編集を行います。

Edit IP Filter Black List Entry #1

Black List Setting

Mode

☐ Disable
 ☒ Enable

Protocol

☒ All
 ☐ ICMP
 ☐ TCP
 ☐ UDP

Source IP

0.0.0.0

Example:

- 192.168.0.123
- 192.168.1.0/24
- 192.168.1.0/255.255.255.0
- 192.168.1.1-192.168.1.123
- 2607:f0d0:1002:51::4
- 2607:f0d0:1002:51::0/64
- 2607:f0d0:1002:51::4-2607:f0d0:1002:51::aaaa

Source Port

0

Example:

- 1234
- 1234:5678:

Destination IP

0.0.0.0

Destination Port

0

Save

93

Firewall > IP Filter > List Entry	
項目	説明
Mode	このルールの有効/無効を設定します。
Protocol	プロトコルを選択します。
Source IP	送信元 IP アドレスを入力します。 IP アドレスは、以下のような形式で入力できます。 <ul style="list-style-type: none"> ● 単体指定 = 192.168.1.123 ● ネットワーク指定 = 192.168.1.0/24 ● 範囲指定 = 192.168.1.1-192.168.1.2
Source Port	プロトコルで TCP、UDP を選択している場合に、ポート番号を入力します。 ポート番号は、以下のような形式で入力できます。 <ul style="list-style-type: none"> ● 単体指定(1234 のみ) = 1234 ● 範囲指定(1234-5678) = 1234:5678
Destination IP	宛先 IP アドレスを入力します。
Destination Port	プロトコルで TCP、UDP を選択している場合に、ポート番号を入力します。

13. 6. Firewall > MAC Filter (V1.05)

MAC フィルタの設定を行います。

MAC Filter

Warning: All existing connections will be dropped after apply

Mode ☒ Disable ☐ Enable
List ☒ Black ☐ White

#	Mode	MAC Address	Edit
1	Disable		
2	Disable		

Firewall > MAC Filter	
項目	説明
Mode	MAC フィルタの有効/無効を設定します。
List (V1.05)	リストのデフォルトルールを設定します。 ・Black: リストに追加した条件のパケットを破棄します。 ・White: リストに追加した条件以外のパケットを破棄します。
Edit	Edit ボタンをクリックすることで各ルールの編集を行います。

Edit MAC Filter Black List Entry #1

Mode ☒ Disable ☐ Enable
MAC Address

Save

Firewall > MAC Filter > List Entry	
項目	説明
Mode	MAC フィルタの有効/無効を設定します。
MAC Address	通信を許可または拒否する端末の MAC アドレスを入力します。

13.7. Firewall > URL Filter (V1.05)

URL フィルタの設定を行います。

URL Filter

Warning: All existing connections will be dropped after apply

Mode ☒ Disable ☐ Enable
List ☒ Black ☐ White

#	Mode	Filter	Key/Full	Edit
1	Disable	Key		
2	Disable	Key		

Firewall > URL Filter	
項目	説明
Mode	URL フィルタの有効/無効を設定します。
List (V1.05)	リストのデフォルトルールを設定します。 ・Black: リストに追加した条件のパケットを破棄します。 ・White: リストに追加した条件以外のパケットを破棄します。
Edit	Edit ボタンをクリックすることで各ルールの編集を行います。

Edit URL Filter Black List Entry #1

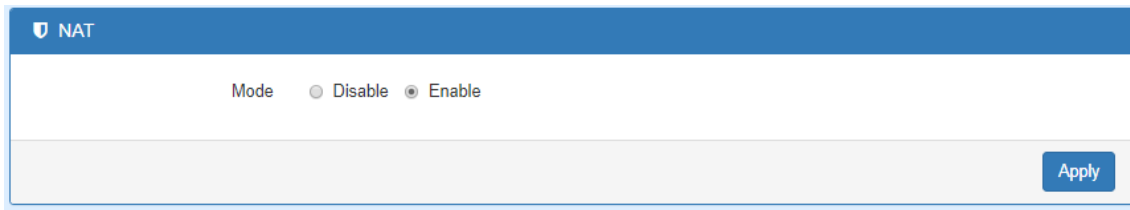
Mode ☒ Disable ☐ Enable
Filter ☒ Key ☐ Full
Key/Full

Save

Firewall > URL Filter > List Entry	
項目	説明
Mode	URL フィルタの有効/無効を設定します。
Filter	URL フィルタのモードを選択します。 ・Key: 入力した URL の一部が含まれる URL へのアクセスを許可または拒否します。 ・Full: 入力した URL と完全一致する URL へのアクセスを許可または拒否します。
Key / Full	URL または URL の一部を入力します。

13. 8. Firewall > NAT

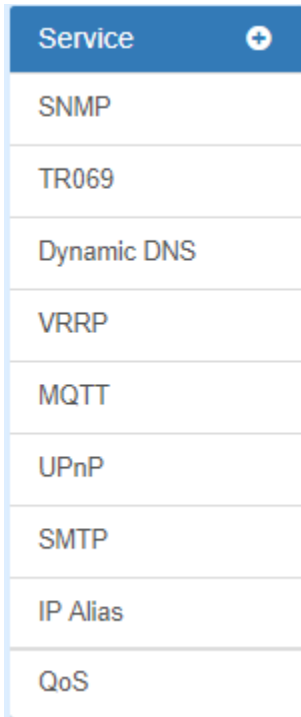
NAT の有効/無効を設定します。



The screenshot shows a web interface for NAT configuration. At the top, there is a blue header bar with a shield icon and the text "NAT". Below the header, the word "Mode" is displayed in red. To its right are two radio buttons: "Disable" and "Enable". The "Enable" radio button is selected, indicated by a filled circle. At the bottom right of the configuration area, there is a blue button labeled "Apply".

14. Service

ナビゲーションパネルにて **Service** をクリックすると、サービス関連の設定を開くことが出来ます。



14.1. Service > SNMP

SNMP の設定を行います。

The screenshot shows the 'SNMP' configuration page. At the top, there's a 'Mode' section with radio buttons for 'Disable' and 'Enable' (selected). Below this are three tabs: 'Community' (selected), 'SNMP v3 User Configuration', and 'SNMP trap configuration'. The main area contains a table with three columns: '#', 'Mode', 'Name', and 'Access'.

#	Mode	Name	Access
1	Enable	public	Read-Only
2	Enable	private	Read-Write
3	Disable		Read-Only

An 'Apply' button is located at the bottom right of the configuration area.

14.1.1. SNMP Community

SNMP v1/v2c コミュニティの設定を行います。

SNMP

Mode

☐ Disable
 ☒ Enable

Community

SNMP v3 User Configuration

SNMP trap configuration

#	Mode	Name	Access
1	Enable	public	Read-Only
2	Enable	private	Read-Write
3	Disable		Read-Only

Apply

Service > SNMP > Community	
項目	説明
Mode	SNMP の有効/無効を設定します。
Community	
Mode	このコミュニティの有効/無効を設定します。
Name	コミュニティ名を設定します。
Access	アクセス権限を選択します。 <ul style="list-style-type: none"> Read-Only: 読み込み専用のコミュニティになります。 Read-Write: 読み書き可能のコミュニティになります。

14. 1. 2. SNMP v3 User Configuration

SNMP v3 ユーザの設定を行います。

SNMP

Mode

☐ Disable
 ☒ Enable

Community

SNMP v3 User Configuration

SNMP trap configuration

#	Mode	Name	Access
1	Disable ▼		Read-Only ▼
2	Disable ▼		Read-Only ▼
3	Disable ▼		Read-Only ▼

Authentication

#	Mode	Auth Password	Auth Protocol	Privacy Password	Privacy Protocol
1	Auth ▼		MD5 ▼		DES ▼
2	Auth ▼		MD5 ▼		DES ▼
3	Auth ▼		MD5 ▼		DES ▼

Apply

Service > SNMP > SNMP v3User Configuration	
項目	説明
SNMP v3 User Configuration	
Mode	このユーザの有効/無効を設定します。
Name	ユーザ名を設定します。
Access	アクセス権限を選択します。 ・Read-Only: 読み込み専用のユーザになります。 ・Read-Write: 読み書き可能なユーザになります。

Authentication	
Mode	<p>認証モードを選択します。</p> <ul style="list-style-type: none"> ● Auth: 認証のみ行い、暗号化は行いません。 ● Privacy: 認証と暗号化を行います。 <p>この設定は User Configuration で作成したユーザの番号と関連しています。 #1 のユーザには #1 の認証モード、パスワードが適用されます。</p>
Auth Password	認証パスワードを設定します。
Auth Protocol	<p>認証プロトコルを選択します。</p> <p>※ MD5 のみサポートしております。</p>
Privacy Password	暗号化パスワードを設定します。
Privacy Protocol	<p>暗号化方式を選択します。</p> <p>※ DES のみサポートしております。</p>

14.1.3. SNMP Trap

SNMP Trap の設定を行います。

SNMP

Mode

☐ Disable
 ☒ Enable

Community

SNMP v3 User Configuration

SNMP trap configuration

#	Mode	Community Name	Destination
1	Disable ▼	public	
2	Disable ▼	private	

Apply

Service > SNMP > SNMP trap configuration	
項目	説明
Mode	SNMP Trap の有効/無効を設定します。
Community Name	Trap コミュニティ名を設定します。
Destination	SNMP Trap の宛先 IP アドレスを入力します。

14.2. Service > Dynamic DNS

DDNS の設定を行います。(下図は noip.com を選択した例です。)

Dynamic DNS

Mode

☒ Disable
 ☐ Enable

Service Provider

www.noip.com ▼

Host Name

Username

Password

Update Period Time (Sec)

2592000

IP Address Selection

☒ Internet IP
 ☐ WAN IP

Apply

Service > Dynamic DNS	
項目	説明
Mode	DDNS の有効/無効を設定します。
Service Provider	DDNS サービスのプロバイダを選択します。 本機は以下のプロバイダに対応しています。 <ul style="list-style-type: none"> ● dynv6.com ● www.nsupdate.info ● www.duckdns.org ● No-ip.com ● Freedns.afraid.org ● dyndns.org
Hostname	DDNS プロバイダにてあらかじめ登録しているホスト名を入力します。
Username	DDNS プロバイダへのログインパスワードとユーザ名を入力します。
Password	
Update Period Time	情報更新の間隔を入力します。

14.3. Service > VRRP

VRRP の設定を行います。

+

VRRP

Mode

☒ Disable ☐ Enable

Group ID

Priority

Virtual IP

Apply

Service > VRRP	
項目	説明
Mode	VRRP の有効/無効を設定します。
Group ID	VRRP グループ ID を 1-255 の範囲で設定します。
Priority	プライオリティを 1-254 の範囲で設定します。 より高い値のプライオリティを持つルータがアクティブルータになります。
Virtual IP	マスタールータが保持する仮想 IP アドレスを設定します。 Virtual IP は物理インタフェースの IP アドレスと同じネットワークのアドレスにする必要があります。

14.4. Service > UPnP

UPnP の設定を行います。

UPnP

Mode ☐ Disable ☒ Enable

Apply

Service > UPnP	
項目	説明
Mode	UPnP の有効/無効を設定します。 有効にすることで UPnP によるデバイス検知や LAN 側端末への WAN 側 IP 通知、LAN 側端末からのポートマッピング要求が出来るようになります。

14.5. Service > SMTP

SMTP の設定を行います。

SMTP

Mode

☒ Disable ☐ Enable

Server

Port

587

Username

Password

Apply

Service > SMTP	
項目	説明
Mode	SMTP の有効/無効を設定します。
Server	e-mail サーバのアドレスを入力します。
Port	SMTP で使用するポート番号を入力します。 ポート番号は使用するメールサービスによって異なります。
Username	メールサーバにログインするためのユーザ名とパスワードを入力します。
Password	

14. 6. Service > IP Alias

IP エイリアスの設定を行います。

この機能を使用することで、1つの物理インタフェースに複数の IP アドレスを設定することが可能です。

IP Alias

Mode ☐ Off ☒ On

Entries

Empty Entries

Add IP Alias Entry

Mode ☐ Off ☒ On

Interface

eth1(WAN Ethernet)

Addr

xxx.xxx.xxx.xxx

Mask

255.255.255.0


Add

Apply

Service > IP Alias	
項目	説明
Mode	IP エイリアスの有効/無効を設定します。
Add IP Alias Entry	
Mode	この IP エイリアスの有効/無効を設定します。
Interface	IP エイリアスを使って仮想的な IP アドレスを追加するインタフェースを選択します。
Addr	IP エイリアスで使用する IP アドレスのネットマスクを入力します。
Mask	


15. Management

ナビゲーションパネルにて **Management** をクリックすると、マネージメント関連の設定を開くことができます。

Management 
Identification
Administration
Contacts / On Duty
SSH
Web
Firmware
Configuration
Load Factory
Restart
Schedule Reboot

15.1. Management > Identification

ルータの各情報の確認を行います。(下図は V1.05 の画面)

 Identification	
Attr.	Value
Active Image Partition	a
Model Name	HWL-2511-SS
Host Name	HWL-2511-SS
LAN Ethernet MAC Address	00:03:79:06:84:14
WAN Ethernet MAC Address	00:03:79:06:84:15
WiFi 2.4G MAC Address	00:03:79:06:84:16
Bootloader Version	1.03
Software Version	3.3.8
Firmware Version	1.05
Hardware Version	1.0
Software MCSV	014B00531053112E
Hardware MCSV	014B00531053112E
Dual Image A MCSV	014B00531053112E
Dual Image B MCSV	014B00531053112E
Serial Number	BL7VB3WR0030
Modem Firmware Version	EC25JFAR06A05M4G
IMEI	<div></div>
Uptime	37:09

15.2. Management > Administration

管理アカウントの設定を行います。

Management ＞ Administration	
項目	説明
System Setup	
Model Name	ルータの名前を設定します。
Session TTL	自動ログアウトまでの時間を設定します。 0 と入力すると、自動ログアウトしません。
Super User	
New Password	スーパーユーザのパスワードを変更します。
Retype to confirm	Retype to confirm には確認のためにもう一度入力します。
User #1～#3	
Name	ユーザ名を設定します。
User Level	ユーザの権限を設定します。
New Password	ユーザのパスワードを変更します。
Retype to confirm	Retype to confirm には確認のためにもう一度入力します。

15.3. Management > SSH

SSH の設定を行います。

Management > SSH	
項目	説明
Mode	SSH の有効/無効を設定します。
LAN Server Port	SSH の LAN 側待ち受けポート番号を設定します。
WAN Server Port	SSH の WAN 側待ち受けポート番号を設定します。
Access Control	アクセス制限の設定を行います。 ・Allow All: すべての端末からの SSH アクセスを許可します。 ・Allow specified IPv4v6 Address below: リストに登録した IP アドレスからの SSH アクセスのみ許可します。

15.4. Management > WEB

WEB のポート番号の設定を行います。

Management > WEB	
項目	説明
HTTP Port	HTTP の待ち受けポート番号を設定します。
HTTPS Port	HTTPS の待ち受けポート番号を設定します。

15.5. Management > Firmware

ファームウェアのアップグレードを行います。

Management > Firmware	
項目	説明
Select the firmware to upgrade	アップグレードするファームウェアファイルを選択します。
Upgrade	アップグレードを開始します。 ファームウェアの更新には 5 分程度かかり、更新後にはルータの再起動が必要です。


15.6. Management > Configuration

設定情報のバックアップ/リストアを行います。

Management > Configuration	
項目	説明
Backup for running configuration	現在の設定をバックアップします。
Select the configuration file to restore	設定のバックアップファイルをリストアして設定を復元します。

15.7. Management > Load Factory

設定の初期化を行います。

 Load Factory

Load the factory default configuration and restart the device immediately


Load Factory and Restart

Management > Load Factory	
項目	説明
Load Factory and Restart	設定の初期化を行い、ルータを再起動します。

※ 設定の初期化が上手くいかない場合は、ブラウザのキャッシュクリアを実行してください。

15.8. Management > Restart

ルータの再起動を行います。

 Restart

Restart the device immediately

Restart

Management > Restart	
項目	説明
Restart	ルータを再起動します。

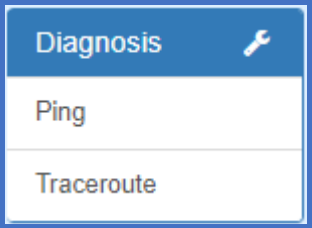
15.9. Management > Schedule Reboot

ルータのスケジュール再起動の設定を行います。

Management > Schedule Reboot	
項目	説明
Mode	スケジュール再起動の有効/無効を設定します。
Type	再起動間隔のタイプを選択します。 ・Interval : 設定した時間が経過するたびに再起動します。 ・Per Day : 1 日毎に設定した時刻に再起動します。 ・Per Week : 1 週間毎に設定した時刻に再起動します。 ・Per Month : 1 か月ごとに設定した時刻に再起動します。
Interval Plan	Interval を選択した場合は再起動までの間隔、 それ以外の場合は再起動を行う時刻を設定します。

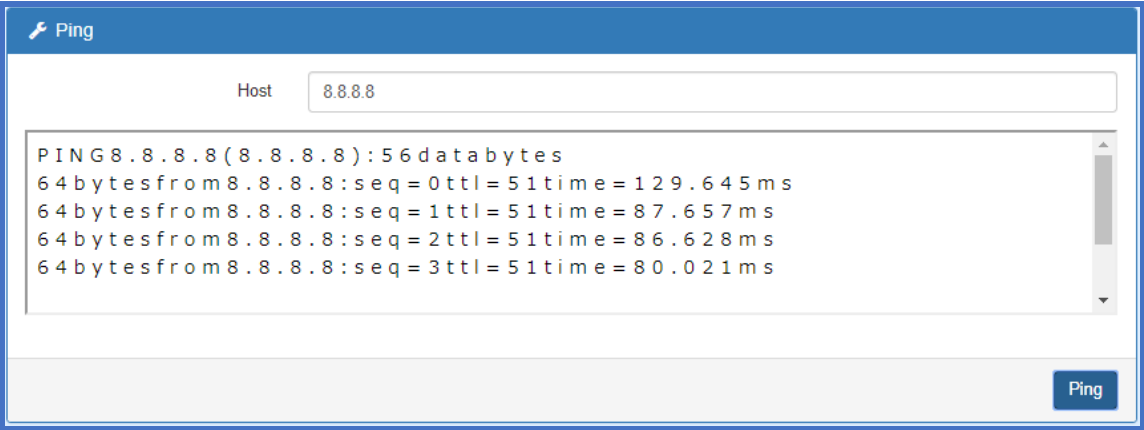
16. Diagnosis

ナビゲーションパネルにて **Diagnosis** をクリックすると、診断ツールを開くことができます。



16.1. Diagnosis > Ping

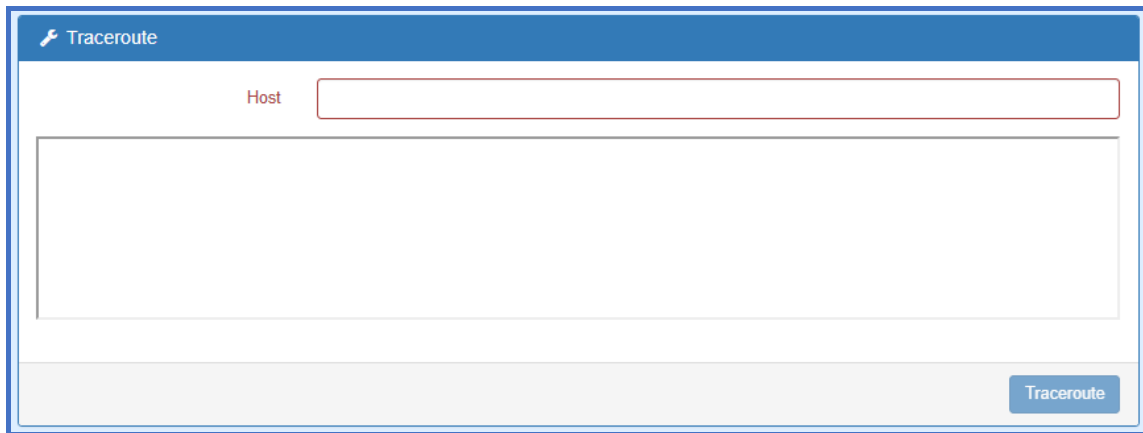
Ping を行います。



Diagnosis > Ping	
項目	説明
Host	Ping の宛先アドレスを入力します。 IP アドレスまたはホスト名で入力できます。
Ping	Ping ボタンをクリックすることで、Ping を実行します。 実効結果は画面中央に表示されます。

16.2. Diagnosis > Traceroute

トレースルートをを行います。



Diagnosis > Ping	
項目	説明
Host	トレースルートの宛先アドレスを入力します。 IP アドレスまたはホスト名で入力できます。
Traceroute	Traceroute ボタンをクリックすることで、トレースルートを実行します。 実効結果は画面中央に表示されます。

17. 製品仕様

製品型番		HWL-2511-SS
対応バンド		FDD LTE: B1/B3/B8/B18/B19/B26
		TDD LTE: B41
		WCDMA: B1/B6/B8/B19
対応キャリア		NTT Docomo 系のみ対応
カテゴリ		LTE Cat4
Wi-Fi (2.4GHz)		802.11b,g,n
インターフェース		1xSIM Card Slot
		1xLAN 10/100 Mbps Ethernet port
		1xWAN 10/100 Mbps Ethernet port
		2xRPSMA コネクタ (Wi-Fi 2.4GHz)
		2xSMA コネクタ (LTE アンテナ)
		1xGPS アンテナ
		1xRS232C (TXD/RXD)
		1xDI, 1xDO
		PWR V+/ V-
VPN トンネル数	IPsec	4
	L2TP*1	2
	OPENVPN	4
WiFi クライアント数		50
対応 SIM カード		マイクロ SIM
アンテナ部		外付け LTE: Main/AUX, Wi-Fi: MIMO, GPS
LED 表示		Power, FN, RSSI (H/L): 全て緑
防水		なし
電源		AC100V(AC アダプタ使用時) DC10～32V
消費電力		7W(最大)
動作温度		-20 ～ +60℃
保存温度		-30 ～ +80℃
相対湿度		0 ～ 95% (結露なきこと)
寸法		(W)91mm x (D)74mm x (H)28mm
重量		250g 以下
認定		工事設計認証番号: 211-161102 TELEC 認定番号: 210-134066 技術基準適合認定番号: ADF18-0088018 VCCI Class A

*1)本製品は L2TP version 2 に対応しています。

18. 付属 AC アダプタ仕様

製品名	TRG1512-A-62E13 AC アダプタ	
商品コード	154-CN-019	
電源	入力	AC 100～240V
	出力	DC 12V
動作温度	-20～+60℃	
保存温度	-20～+85℃	
認定	RoHS、PSE ほか	

19. 製品保証

- ◆ 故障かなと思われた場合には、弊社カスタマサポートまでご連絡ください。

- 1) 修理を依頼される前に今一度、この取扱説明書をご確認ください。
- 2) 本製品の保証期間内の自然故障につきましては無償修理させていただきます。
- 3) 故障の内容により、修理ではなく同等品との交換にさせて頂く事があります。
- 4) 弊社への送料はお客様の負担とさせていただきますのでご了承ください。

初期不良保証期間：

ご購入日より **3ヶ月間**（弊社での状態確認作業後、交換機器発送による対応）

製品保証期間：

《本体》ご購入日より **1年間**（お預かりによる修理、または交換対応）

- ◆ 保証期間内であっても、以下の場合は有償修理とさせていただきます。
（修理できない場合もあります）
 - 1) 使用上の誤り、お客様による修理や改造による故障、損傷
 - 2) 自然災害、公害、異常電圧その他外部に起因する故障、損傷
 - 3) 本製品に水漏れ・結露などによる腐食が発見された場合
- ◆ 保証期間を過ぎますと有償修理となりますのでご注意ください。
- ◆ 一部の機器は、設定を本体内に記録する機能を有しております。これらの機器は修理時に設定を初期化しますので、お客様が行った設定内容は失われます。恐れ入りますが、修理をご依頼頂く前に、設定内容をお客様にてお控えください。
- ◆ 本製品に起因する損害や機会の損失については補償致しません。
- ◆ 修理期間中における代替品の貸し出しは、基本的に行っておりません。別途、有償サポート契約にて対応させて頂いております。有償サポートにつきましてはお買い上げの販売店にご相談ください。
- ◆ 本製品の保証は日本国内での使用においてのみ有効です。

製品に関するご質問・お問い合わせ先

ハイテクインター株式会社

カスタマサポート

TEL 0570-060030

E-mail support@hytec.co.jp

受付時間 平日 9:00～17:00

Copyright © 2019–2021

HYTEC INTER Co., Ltd.