

# HWL-2501-DS

## 取扱説明書



**HYTEC INTER Co., Ltd.**

## 第 1.3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写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 09 月 05 日	新規作成
第 1.1 版	2020 年 03 月 30 日	対応キャリアの仕様を追記
第 1.2 版	2020 年 09 月 23 日	梱包物一覧の修正、一部仕様を変更
第 1.3 版	2020 年 12 月 01 日	誤記修正

## 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. 前面 .....	8
3.2. 上面 .....	10
3.3. Digital INPUT・OUTPUT について .....	13
3.4. SIM カードの取り付け方法 .....	14
4. WEB GUI での設定について .....	15
4.1. WEB GUI へのアクセス.....	15
4.2. WEB GUI の概要説明.....	16
4.3. IP アドレスの設定 .....	17
4.4. ログインパスワードの変更 .....	17
4.5. APN 設定 .....	18
5. Status .....	19
6. System .....	20
6.1. Time and Date.....	21
6.2. COM Ports .....	23
6.3. Logging.....	25
6.3.1. Logging > Logging .....	25
6.3.2. Logging > Log .....	25
6.4. Alarm .....	26
6.5. Ethernet.....	28
6.6. Client List .....	29
7. WAN.....	30
7.1. WAN > Priority .....	30
7.2. WAN > Ethernet.....	31
7.2.1. WAN Ethernet Configuration .....	31
7.2.2. Ethernet Ping Health.....	33

<b>8. LTE</b>	<b>34</b>
8.1. LTE > LTE Config	34
8.1.1. LTE Configuration	35
8.1.2. LTE Ping Health	35
8.2. LTE > GPS	36
8.2.1. GPS Status	36
8.3. LTE > Dual SIM	37
8.3.1. Connect Policy	37
8.3.2. SIM Configuration	38
8.3.3. Data Limitation	39
8.4. LTE > Usage Display	40
8.5. LTE > Serving Cell	41
8.6. LTE > DNS	42
<b>9. LAN</b>	<b>43</b>
9.1. LAN > IPv4	43
9.2. LAN > VLAN	44
9.2.1. Tag Base VLAN	44
9.2.2. Port Base VLAN	46
9.3. LAN > Subnet	47
<b>10. IP Routing</b>	<b>48</b>
10.1. IP Routing > Static Route	48
10.2. IP Routing > RIP	50
10.3. IP Routing > OSPF	52
10.4. IP Routing > BGP	55
<b>11. VPN</b>	<b>58</b>
11.1. VPN > Open VPN	58
11.1.1. Open VPN 設定例	59
11.2. VPN > IPSec	65
11.2.1. IPSec 設定例	65
11.3. VPN > GRE	70
11.4. VPN > PPTP Server	70
11.5. VPN > L2TP	73

<b>12. Firewall</b>	<b>75</b>
12.1. Firewall > Port Forwarding	75
12.2. Firewall > DMZ	77
12.3. Firewall > IP Filter	77
12.4. Firewall > MAC Filter	79
12.5. Firewall > URL Filter	81
12.6. Firewall > NAT	83
<b>13. Service</b>	<b>84</b>
13.1. Service > SNMP	84
13.1.1. SNMP Community	85
13.1.2. SNMP v3 User Configuration	86
13.1.3. SNMP Trap	88
13.2. Service > Dynamic DNS	89
13.3. Service > VRRP	90
13.4. Service > UPnP	91
13.5. Service > SMTP	92
13.6. Service > IP Alias	93
<b>14. Management</b>	<b>94</b>
14.1. Management > Identification	94
14.2. Management > Administration	95
14.3. Management > SSH	96
14.4. Management > Web	97
14.5. Management > Firmware	97
14.6. Management > Configuration	98
14.7. Management > Load Factory	98
14.8. Management > Restart	98
14.9. Management > Schedule Reboot	99
<b>15. Diagnosis</b>	<b>100</b>
15.1. Diagnosis > Ping	100
15.2. Diagnosis > Traceroute	101
<b>16. 製品仕様</b>	<b>102</b>
<b>17. 製品保証</b>	<b>103</b>

## 1. 製品概要

HWL-2501-DS 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。

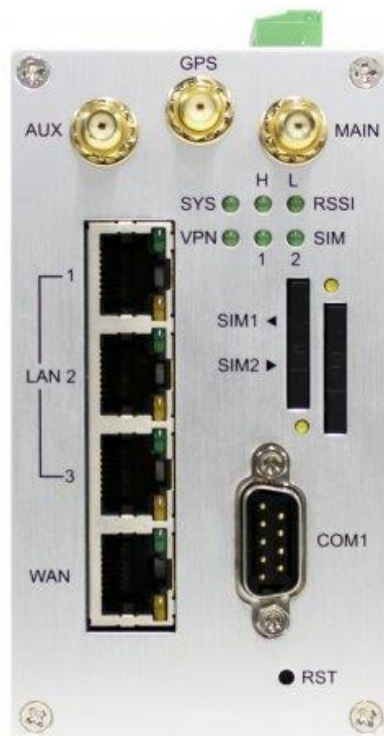
## 2. 梱包物一覧

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
GPS アンテナ	1 個
DIN レールマウント	1 個
電源ターミナルブロック 3 ピン	1 個
ターミナルブロック 11 ピン	1 個

### 3. 製品外観

#### 3.1. 前面



#### 各ポート

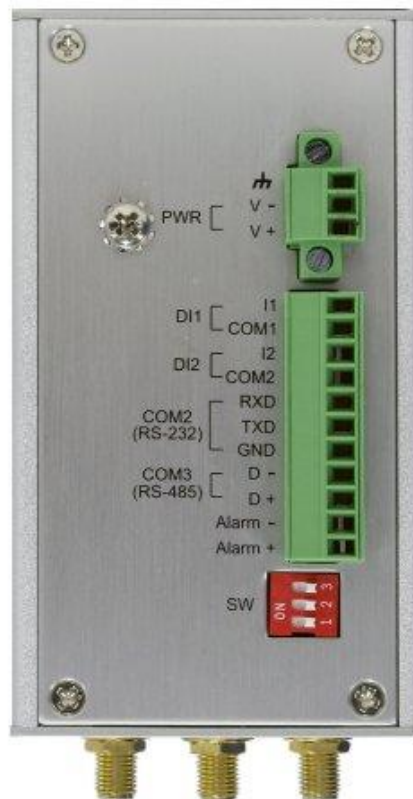
表示	説明
<u>MAIN/AUX</u>	付属の LTE アンテナを接続します。
<u>GPS</u>	付属の GPS アンテナを接続します。
<u>LAN</u>	LAN ポートです。
<u>WAN</u>	WAN ポートです。
<u>SIM1</u>	SIM1 の SIM カードスロットです。
<u>SIM2</u>	SIM2 の SIM カードスロットです。
<u>COM1</u>	コンソールポートです。 詳細は P.23 の”COM Ports”を参照願います。
<u>RST</u>	リセットボタンです。 5 秒以上押下すると、設定の初期化を行います。



各 LED

表示		説明
<u>SYS</u>	点灯	電源が入っています。
	遅い点滅	起動中です。
	消灯	電源が入っていません。
<u>VPN</u>	点灯	VPN 接続が確立されています。
	点滅	WAN のリンクが確立されています。
	消灯	WAN のリンクが確立されていません。
<u>RSSI</u> <u>High</u>	点灯	LTE の信号強度が＜強＞の状態です。
<u>RSSI</u> <u>Low</u>	点灯	LTE の信号強度が＜弱＞の状態です。
<u>SIM</u> <u>1/2</u>	点灯	アクセスポイントと接続されています。
	遅い点滅	アクセスポイントとの接続を試みています。
	早い点滅	エラーが発生しています。
	消灯	SIM カードが挿入されていません。

### 3.2. 上面



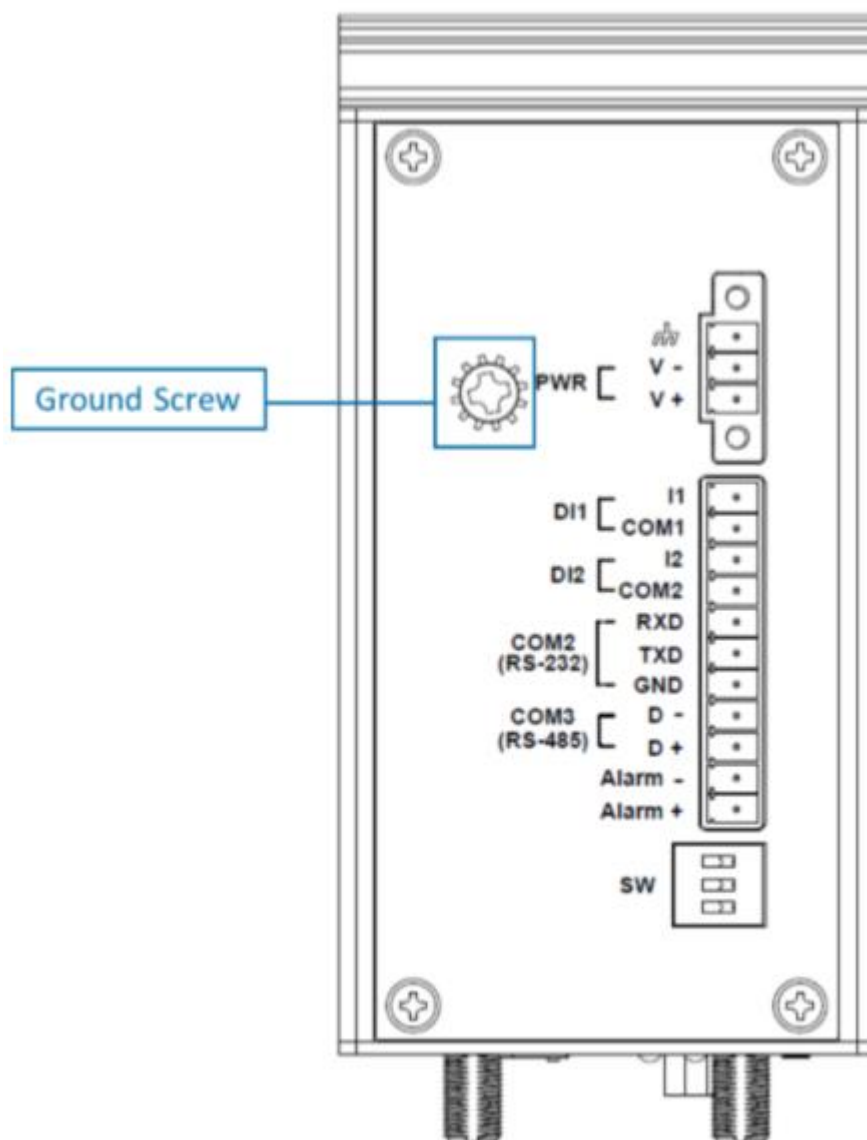
表示		説明
<b>PWR</b>		フレームグラウンドです。
	<b>V-</b>	DC10～32V の電源を接続します。
	<b>V+</b>	
<b>DI1/DI2</b>		Digital Input ポートです。
<b>COM2</b>		RS232 ポート(COM2)です。
<b>COM3</b>		RS485 ポート(COM3)です。
<b>Alarm</b>		Digital Output ポートです。
<b>SW</b>		DIP スイッチです。 詳細は P.12 の”DIP Switch について”を参照願います。

適合電線範囲 = AWG 14～28

- 接地について

本体上面のネジを使用して、接地することができます。

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。



- DIP Switch について

RS-485 の通信を改善するために、DIP Switch によって Pull High/Pull Low または 120  $\Omega$  の終端抵抗を有効にすることが出来ます。



**DIP SWITCH**

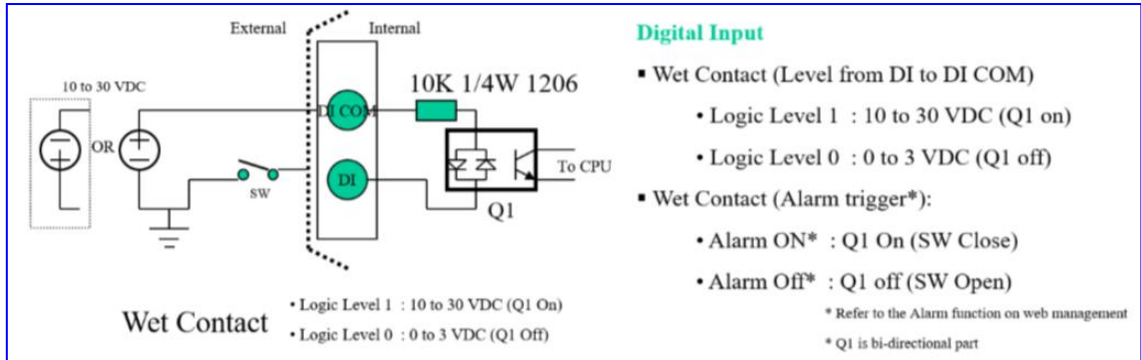
SW1 と 2 は、Pull High/Pull Low、  
SW3 は 120  $\Omega$  の終端抵抗の有効/無効を切り替えます。

Pull High (510 $\Omega$ )/ Pull Low(510 $\Omega$ ) Bias Resistor	SW 1(Pull Low)	SW 2 (Pull High)
有効	ON	ON
無効 (Default)	OFF	OFF

Terminal Resistor (120 $\Omega$ )	SW 3
有効	ON
無効 (Default)	OFF

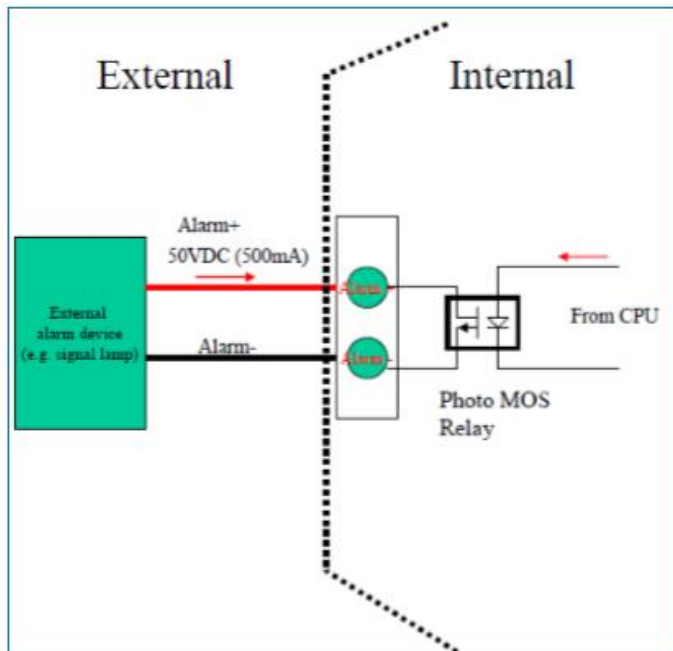
### 3.3. Digital INPUT・OUTPUT について

#### ● Digital INPUT について



Pin	説明
<u>DI I1</u>	Digital INPUT1の入力ポートです。
<u>DI_COM1</u>	
<u>DI I2</u>	Digital INPUT2の入力ポートです。
<u>DI_COM2</u>	

#### ● Digital OUTPUT (アラーム出力) について



### 3.4. SIM カードの取り付け方法

SIM カードの取り付け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 カードスロット付近のイジェクトボタンを押して、SIM トレイを引き出します。



- 3) SIM トレイに SIM カードを乗せます。
- 4) SIM トレイを SIM カードスロットに挿入します。



#### **注意事項**

- 1) 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。
- 2) SIM トレイを挿入する前に必ずトレイの方向を確認してください。誤った方向で挿入した場合、トレイが引き抜けなくなる可能性があります。

## 4. WEB GUI での設定について

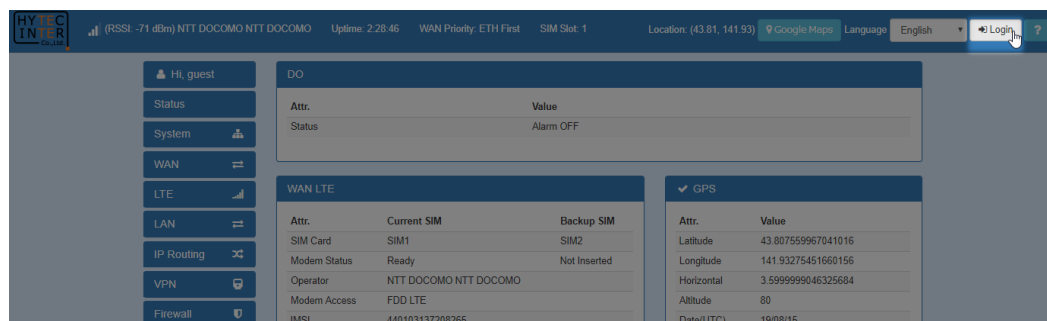
### 4.1. WEB GUI へのアクセス

#### ● ログイン初期設定

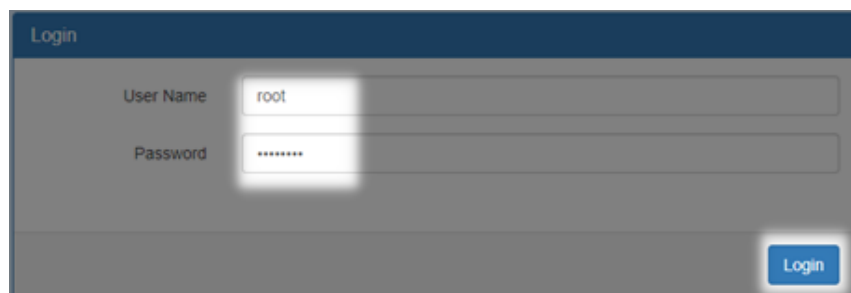
項目	初期値
IP アドレス	192.168.1.1
ユーザ名	Admin
パスワード	2wsx#EDC

#### ● 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。



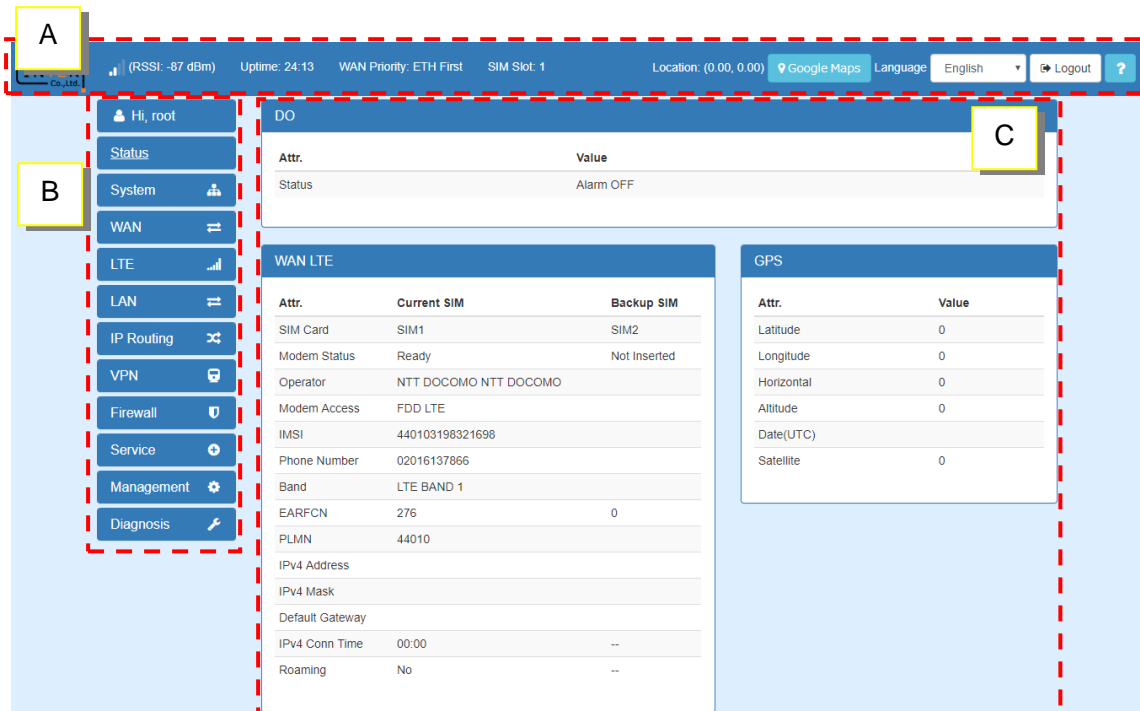
- 5) ユーザ名とパスワードを入力して、Login ボタンをクリックします。



## 4. 2. 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。
SIM Slot	現在アクティブになっている SIM カードスロットの番号を表示します。
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出来ます。

### 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。



### 4.3. 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: 192.168.1.1

IP Mask: 255.255.255.0

DHCP Server Configuration

DHCP Server: On

IP Address Pool: From 192.168.1.2 To 192.168.1.254

Static IP Addresses

+ Add Static IP Address

Apply

### 4.4. 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。

Administration

System Setup

Model Name: HWL-2511-SS

Session TTL: 5 (minutes, 0 means no timeout)

Admin Password

New Password

Retype to confirm

Apply

- 3) **Apply** ボタンをクリックします。

#### 4.5. APN 設定

- 1) ナビゲーションパネルから、**LTE** ⇒ **Dual SIM** の順にクリックします。
- 2) SIM1 Configuration または SIM2 Configuration を選択し、APN, Username, Password, Auth を入力します。

The screenshot displays the 'SIM2 Configurations' tab in a web interface. At the top, the status is 'Ready'. Below this are input fields for 'SIM PIN', 'Confirmed SIM PIN', 'SIM PUK', and 'Confirmed SIM PUK'. A central white box highlights the APN configuration fields: 'APN' (containing 'mopera.net'), 'Username', 'Password', 'Confirm Password', and 'Auth' (set to 'NONE'). Below these is a 'Change SIM PIN' button with a 'Change' link. The 'Data Limitation' section shows 'Already Used Data (MB)' as 0, 'Mode' as 'Disable', and 'Max Data Limitation (MB)' as 0. It also includes a 'Monthly Reset' section with date and time pickers. An 'Apply' button is located in the bottom right corner.

- 3) **Apply** ボタンをクリックします。

## 5. Status

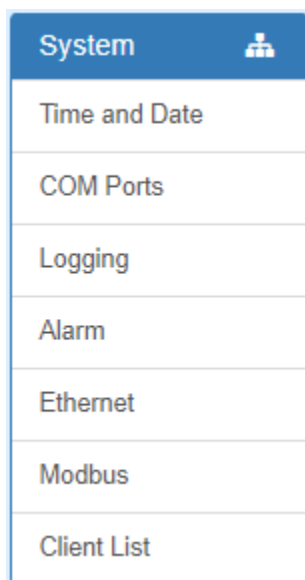
ナビゲーションパネルにて **Status** をクリックすると、ルータのステータスを確認することが出来ます。

The screenshot displays the router's web interface with the 'Status' page selected. The left sidebar contains navigation links: Hi, root, Status, System, WAN, LTE, LAN, IP Routing, VPN, Firewall, Service, Management, and Diagnosis. The main content area is divided into several sections:

- DO**: A table showing the DO Status as 'Alarm OFF'.
- WAN LTE**: A table showing LTE status for Current SIM (SIM1) and Backup SIM (SIM2). It includes fields for SIM Card, Modem Status (Ready), Operator (NTT DOCOMO), Modem Access (FDD LTE), Band (LTE BAND 19), EARFCN (6100), PLMN (44010), IPv4 Address, IPv4 Mask, Default Gateway, IPv4 Conn Time (00:00), and Roaming (No).
- GPS**: A table showing GPS status with fields for Latitude, Longitude, Horizontal, Altitude, Date(UTC), and Satellite, all currently at 0.
- WAN Ethernet**: A table showing Ethernet status with fields for IPv4 Address, IPv4 Mask, Default Gateway, and IPv4 Conn Time (00:00).
- WAN DNS**: A table showing DNS status with fields for IPv4 DNS Server #1, #2, #3, and IPv6 DNS Server #1, #2, #3.

## 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 Setup' configuration page. Under the 'Mode' section, 'Get from Time Server' is selected with a radio button. The 'GPS Time' section has 'On' selected. Below, there are six input 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' configuration page. Under the 'Mode' section, 'Manual' is selected with a radio button. Below the 'YYYY-MM-DD HH:MM:SS' label, there are input fields for date and time: Year (2019), Month (3), Day (27), Hour (13), Minute (8), and Second (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' configuration page. There is a single dropdown menu labeled 'Time Zone' with the selected value being '(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


## 6.2. COM Ports

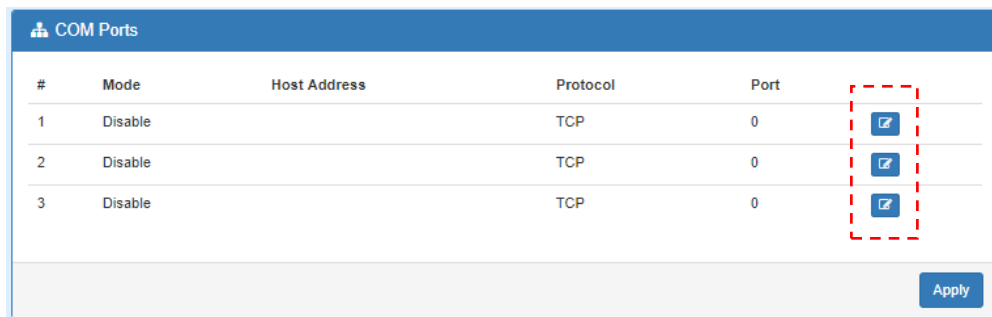
COM ポート及び Virtual COM ポートの設定を行います。

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。

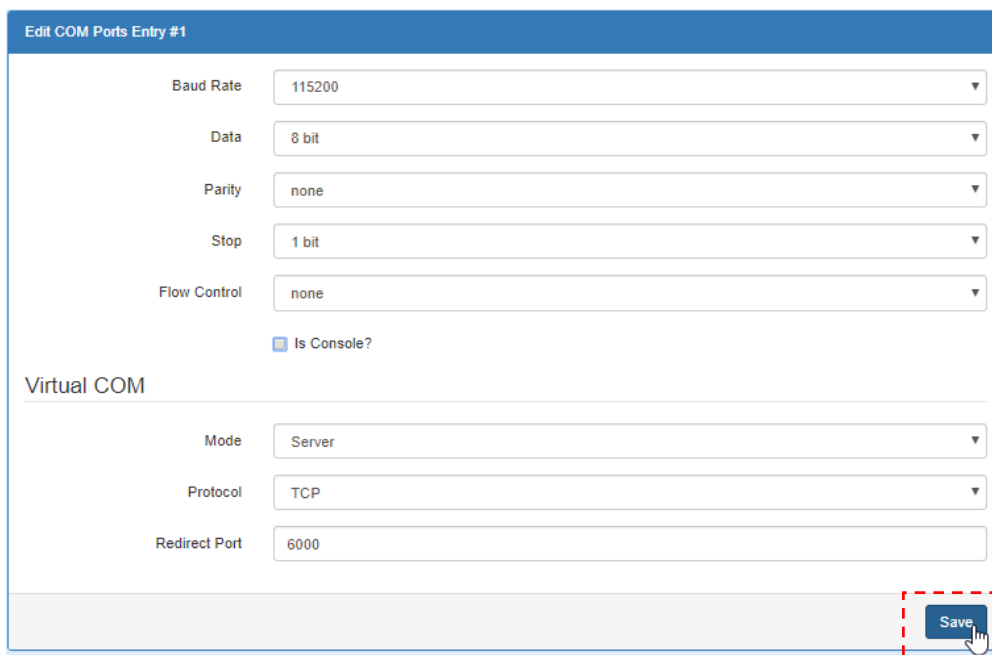
各ポートの  ボタンをクリックすると設定を開くことができます。



#	Mode	Host Address	Protocol	Port	
1	Disable		TCP	0	
2	Disable		TCP	0	
3	Disable		TCP	0	

Apply

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

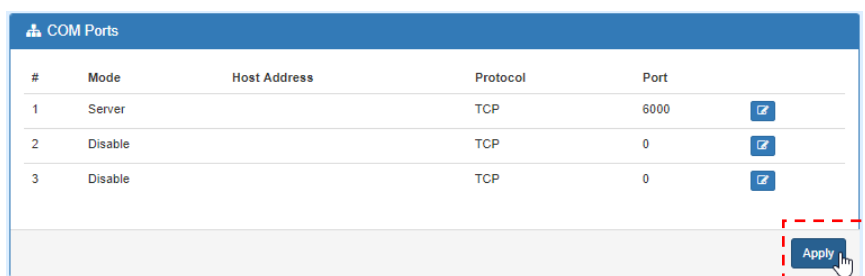
Mode: Server

Protocol: TCP

Redirect Port: 6000

Save

3) **Apply**をクリックします。



#	Mode	Host Address	Protocol	Port	
1	Server		TCP	6000	
2	Disable		TCP	0	
3	Disable		TCP	0	

Apply

System > COM Ports	
項目	説明
Baud Rate	ボーレートを設定します。
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?	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-232 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。

Alarm

Mode

☒ Disable
 ☐ Enable

Alarm input

☒ SMS
 ☒ DI 1
 ☒ DI 2
 ☒ VPN disconnect
 ☒ WAN disconnect
 ☒ LAN disconnect
 ☒ Reboot

Alarm output

☒ SMS
 ☒ DO
 ☒ SNMP trap
 ☒ E-mail
 ☒ TR069

DI 1 Trigger

☒ High
 ☐ Low

DI 2 Trigger

☒ High
 ☐ Low

DO behavior

☒ Always
 ☐ Pulse

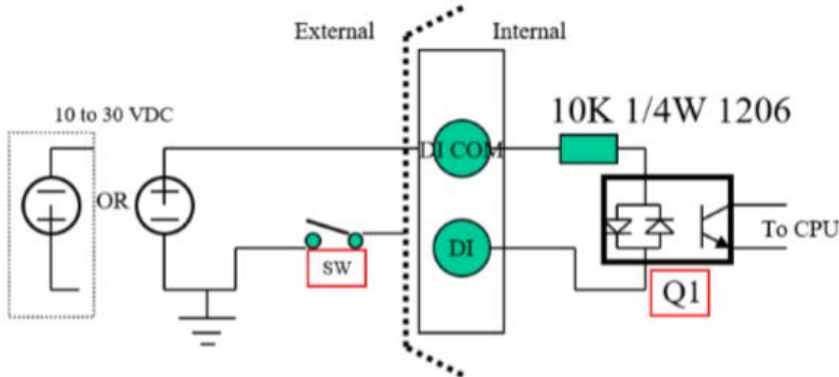
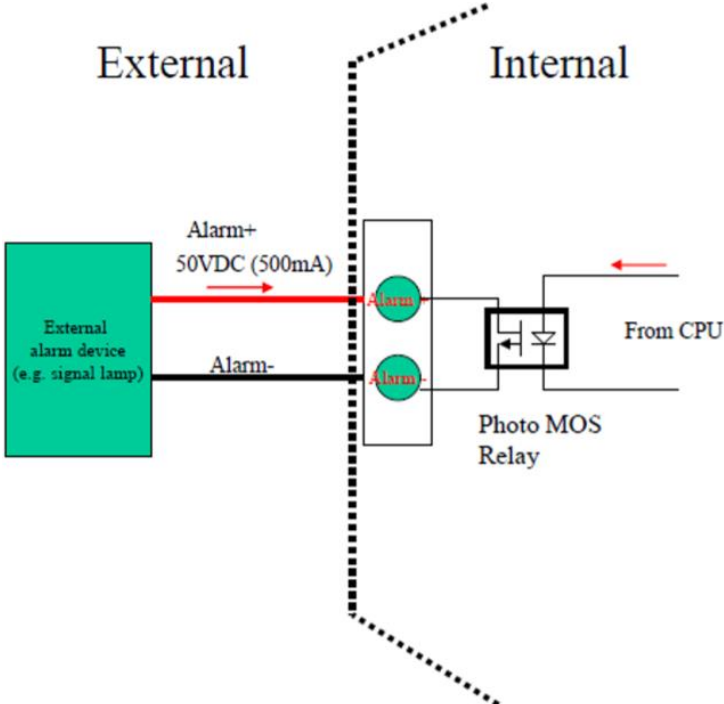
SMS/E-mail

Limit 150 english characters

Hint: for SMS/E-mail only accept trusted and on duty members

Apply

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"> <li>• DI 1/2: Digital Input の入力電圧に応じて</li> <li>• VPN disconnect: すべての VPN 接続が切断された時</li> <li>• WAN disconnect: WAN 接続が切断された時</li> <li>• LAN disconnect: LAN ポートがリンクダウンした時</li> <li>• Reboot: 再起動したとき</li> </ul>
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。
DI1/2 Trigger	Digital Input 端子のトリガを選択します。 High: 下図の例で、SW が CLOSE の時にアラームを発報します。 Low: 下図の例で、SW が OPEN の時にアラームを発報します。

	
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"> <li>• Always: 下図の例で、アラーム発報時にリレーを CLOSE 状態にします。</li> <li>• Pulse: 下図の例で、アラーム発報時にリレーの CLOSE と OPEN を繰り返します。</li> </ul> 

## 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 1	100M Full
LAN 2	100M Full
LAN 3	Off
WAN	Off

### Ethernet Ports Configurations

LAN 1	<input checked="" type="radio"/> Auto <input type="radio"/> 100M Full <input type="radio"/> 100M Half <input type="radio"/> 10M Full <input type="radio"/> 10M Half <input type="radio"/> Disable
LAN 2	<input checked="" type="radio"/> Auto <input type="radio"/> 100M Full <input type="radio"/> 100M Half <input type="radio"/> 10M Full <input type="radio"/> 10M Half <input type="radio"/> Disable
LAN 3	<input checked="" type="radio"/> Auto <input type="radio"/> 100M Full <input type="radio"/> 100M Half <input type="radio"/> 10M Full <input type="radio"/> 10M Half <input type="radio"/> Disable
WAN	<input checked="" type="radio"/> Auto <input type="radio"/> 100M Full <input type="radio"/> 100M Half <input type="radio"/> 10M Full <input type="radio"/> 10M Half <input type="radio"/> Disable

### WAN Ethernet

WAN MTU
min: 500; max: 1500

### Flow Control

LAN 1	<input type="radio"/> Off <input checked="" type="radio"/> On
LAN 2	<input type="radio"/> Off <input checked="" type="radio"/> On
LAN 3	<input type="radio"/> Off <input checked="" type="radio"/> On
WAN	<input type="radio"/> Off <input checked="" type="radio"/> 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	WAN Ethernet インタフェースの MTU サイズを設定します。

## 6. 6. Client List

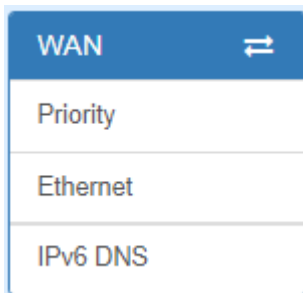
ルーターに接続されているクライアントのリストを表示します。

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"> <li>• DHCP Client: DHCP クライアントのリストを表示します。</li> <li>• Online: オンラインのクライアントのリストを表示します。</li> </ul>

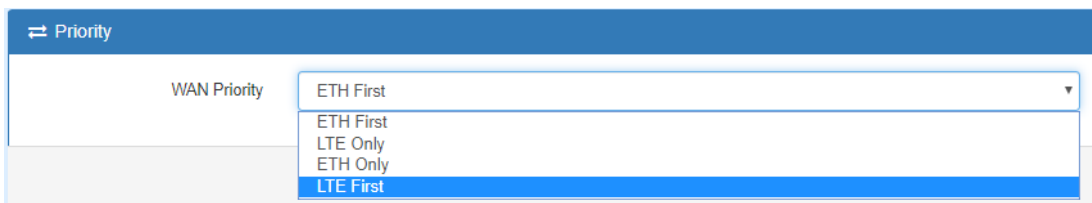
## 7. WAN

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"> <li>•ETH First:WAN Ethernet を優先で使します。</li> <li>•LTE Only:LTE のみ使します。</li> <li>•ETH Only:WAN Ethernet のみ使します。</li> <li>•LTE First:LTE を優先で使します。</li> </ul>

## 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"> <li>• 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。</li> <li>• 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。</li> <li>• Static IPv4: 任意の静的 IP アドレスを設定します。</li> </ul>

#### ● 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 page. At the top, there's a header 'WAN Ethernet'. Below it, a 'Work As' section has three radio buttons: 'DHCP Client' (selected), 'PPPoE Client', and 'Static IPv4'. There are two tabs: 'Configuration' (active) and 'Ethernet Ping Health'. The 'DNS Server Configuration' section contains three rows for 'IPv4 DNS Server #1', '#2', and '#3'. Each row has a dropdown menu set to 'From ISP' and an adjacent 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"> <li>• 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。</li> <li>• User Defined: 任意の DNS サーバを設定します。</li> </ul>

- 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 the 'WAN Ethernet' configuration page. At the top, there are radio buttons for 'Work As': 'DHCP Client', 'PPPoE Client' (which is selected), and 'Static IPv4'. Below this, there are two tabs: 'Configuration' and 'Ethernet Ping Health'. The 'Configuration' tab is active, showing the 'PPPoE Client Configuration' section. It 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。



### 7.2.2. Ethernet Ping Health

WAN Priority を ETH First または LTE First 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

Work As ☐ DHCP Client ☒ PPPoE Client ☐ Static IPv4

Configuration Ethernet Ping Health

Ethernet Ping Health ☐ Disable ☒ Enable

Interval  (1 ~ 60 Seconds)

IPv4 Host 1

IPv4 Host 2

IPv6 Host 1

IPv6 Host 2

Hint Wan Priority: Auto  
Ethernet ping health: Enable

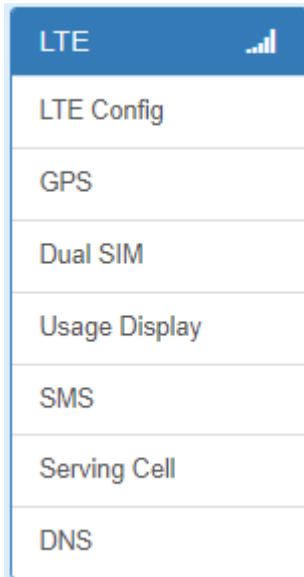
- The ethernet connection will switch to existed LTE connection whenever ping specified url fail.
- The ethernet connection will switch back whenever ping specified url pass.

Apply

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。
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。
IPv6 Host	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 設定と LTE Ping ヘルスチェックの設定を行います。

**LTE Config**

LTE Config: Auto Change this field require rebooting

MTU: 1500 min: 500; max: 1500

**LTE Ping Health**

LTE Ping Health: ☐ Disable ☒ Enable

Interval: 60 Seconds

IPv4 Host 1: 8.8.8.8

IPv4 Host 2: 8.8.4.4

IPv6 Host 1: 2001:4860:4860::8888

IPv6 Host 2: 2001:4860:4860::8844

**Hint** LTE ping health: Enable

- Then system ping specified IP address to avoid the base station kick out the idle device.
- In 'Dual SIM' mode and both SIM are ready, all URL ping fail would jump into another SIM slot for connection.

**Apply**

## 8. 1. 1. LTE Configuration

LTE 設定と LTE の MTU の設定を行います。

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"> <li>• Auto: 自動的に接続するネットワークを選択します。</li> <li>• 4G Only: 4G のネットワークにのみ接続します。</li> <li>• 3G Only: 3G のネットワークにのみ接続します。</li> </ul>
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. 1. 2. LTE Ping Health

LTE Ping ヘルスチェックの設定を行います。

Dual SIM モードで操作している場合、現在使用中の SIM でヘルスチェックに失敗すると待機中の SIM に切り替えます。

LTE Ping Health

LTE Ping Health ☐ Disable ☒ Enable

Interval 60 Seconds

IPv4 Host 1 8.8.8.8

IPv4 Host 2 8.8.4.4

IPv6 Host 1 2001:4860:4860::8888

IPv6 Host 2 2001:4860:4860::8844

LTE > LTE Ping Health	
項目	説明
LTE Ping Health	本機能の有効/無効を選択します。
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。
IPv6 Host	

## 8.2. LTE > GPS

GPS のステータス確認を行います。

### 8.2.1. GPS Status

GPS の情報を表示します。

緯度、経度は DEG 形式での表示となります。

GPS	
Status	NMEA
Attr.	Value
Latitude	43.8073616027832
Longitude	141.93296813964844
Horizontal	1.600000023841858
Altitude	82
Date(UTC)	19/08/13
Satellite	4
Refresh	

### 8.3. LTE > Dual SIM

SIM の設定を行います。

#### 8.3.1. Connect Policy

Dual SIM の動作についての設定を行います。

The screenshot shows the 'Dual SIM' settings screen. At the top, it says 'Dual SIM'. Below that, the title 'Connect Policy' is displayed. The settings are as follows:

- Current SIM Card:** SIM1. There is a 'Disconnect' button next to it.
- Disable Roaming:** Radio buttons for 'No' and 'Yes'. 'Yes' is selected.
- Used SIM:** Radio buttons for 'Dual SIM', 'SIM1', and 'SIM2'. 'Dual SIM' is selected.
- SIM Priority:** Radio buttons for 'Auto', 'SIM1', and 'SIM2'. 'Auto' is selected.
- Roaming Switch:** A checkbox labeled 'Switch to another SIM when roaming is detected' is checked.
- Connect Retry Number:** A text input field containing the number '3'. To the right of the field, it says '(1 ~ 100) \* 60 seconds'.

LTE > Dual SIM > Connect Policy	
項目	説明
Current SIM Card	現在使用中の SIM カードを表示します。
Disable Roaming	データローミング機能を無効にします。
Used SIM	使用する SIM のモードを選択します。 <ul style="list-style-type: none"> <li>● Dual SIM: 状況に応じて SIM1 と SIM2 を切り替えて通信します。</li> <li>● SIM1: SIM1 のみを使用します。</li> <li>● SIM2: SIM2 のみを使用します。</li> </ul>
SIM Priority	Dual SIM モードを使用している際に優先して使用する SIM カードを選択します。
Roaming Switch	ローミングを検出した際に、READY 状態の SIM に接続を切り替えます。
Connect Retry Number	基地局と接続できない状態になった場合に、再接続するまでの時間を設定します。

## 8. 3. 2. SIM Configuration

APN 設定等を行います。

✓ SIM1 Configurations

SIM2 Configurations

Status

Ready

SIM PIN

Confirmed SIM PIN

SIM PUK

Confirmed SIM PUK

APN

mmtcom.jp

Username

mmt@mmtsgb

Password

...

Confirm Password

...

Auth

CHAP

Change SIM PIN

Change

LTE > Dual SIM > 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	
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	
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。
Change SIM PIN	SIM の PIN 番号を変更します。

## 8.3.3. Data Limitation

LTE のデータ使用量制限についての設定を行います。

**Data Limitation**

Already Used Data (MB) 77

Mode ☒ Disable ☐ Enable

Max Data Limitation (MB)

Monthly Reset Date:  Hours:  Minutes:  Seconds:

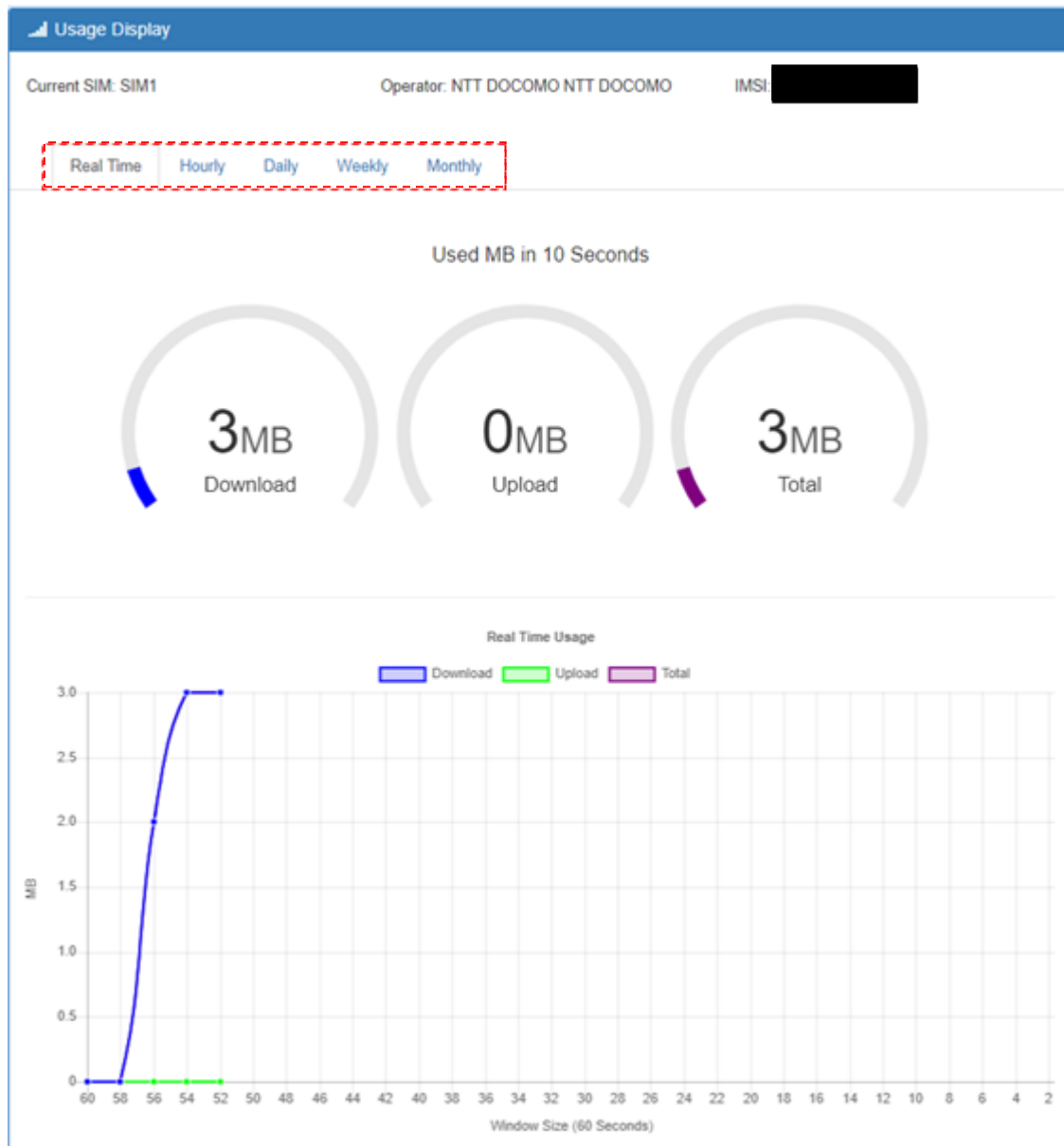
Now Time Date: 0 Hours: 0 Minutes: 0 Seconds: 0

LTE > Dual SIM > Data Limitation	
項目	説明
Already Used Data	これまでのデータ使用量を表示します。
Mode	データ使用量制限機能の有効/無効を設定します。
Max Data Limitation(MB)	許可するデータ使用量を設定します。 ここで設定したデータ使用量を超過した場合、“Monthly Reset”で設定した時間まで該当 SIM 経由のデータ通信をブロックします ルータを再起動した場合も制限は解除されます。
Monthly Reset	制限をリセットするまでの時間を設定します。
Now Time	経過時間を表示します。

#### 8. 4. LTE > Usage 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。





## 8.5. 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。

Serving Cell	
Attr.	Value
Rate	LTE
RSRP	-92
RSRQ	-6
SINR	16
RSCP	
ECIO	0
Cell Identity	751911-17
eNB ID	751911
Cell ID	17
PCI ID	277
EARFCN	6100
UL Bandwidth	10MHz
DL Bandwidth	10MHz
Refresh	

## 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

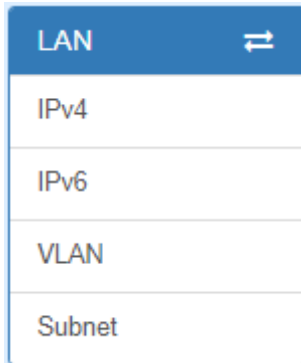
From ISP ▼

Apply

LTE > DNS > DNS Server Configuration	
項目	説明
IPv4 DNS Server	<ul style="list-style-type: none"><li>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。</li><li>User Defined: 任意の DNS サーバを設定します。</li></ul>

## 9. 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。



### 9.1. LAN > IPv4

LAN 側の IP アドレス関連の設定を行います。

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。
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。

## 9.2. LAN > VLAN

VLAN の設定を行います。

VLAN

Mode

☒ Off
 ☐ Tag Base
 ☐ Port Base

Apply

### 9.2.1. Tag Base VLAN

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

VLAN

Mode

☐ Off
 ☒ Tag Base
 ☐ Port Base

VLAN Isolation

☒ Off
 ☐ On

Enable	Subnet	VID	Port			
			LAN1	LAN2	LAN3	Router
<input checked="" type="checkbox"/>	NET1	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	NET2	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	NET3	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	NET4	4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	NET5	5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	NET6	6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	NET7	7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	NET8	8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
PVID			1	1	1	--
Tag Mode			Trunk	Trunk	Trunk	--

Apply

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。
Port	VLAN にアサインするポートを選択します。
PVID	Untagged フレームを受信した際に割り当てる VLAN ID を 1-4094 の間で入力します。
Tag Mode	<ul style="list-style-type: none"> <li>● Trunk: 802.1p VLAN に対応している他のデバイスとの接続時に使用します。</li> <li>● Access: Untagged デバイスとの接続時に使用します。</li> </ul>

## 9.2.2. Port Base VLAN

ポートベースの VLAN を設定します。

同じ VLAN に所属するポート同士は通信可能で、違う VLAN に所属するポートとは通信出来ません。

VLAN

Mode

☐ Off
 ☐ Tag Base
 ☒ Port Base

Enable	Port			
	LAN1	LAN2	LAN3	Router
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Apply

LAN > VLAN > Port Base	
項目	説明
Enable	VLAN の有効/無効を設定します。
Port	VLAN にアサインするポートを選択します。








### 9.3. 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

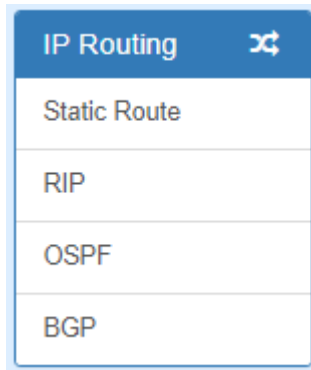
Name	IP Address	IP Mask	Edit
NET2	192.168.2.1	255.255.255.0	
NET3	192.168.3.1	255.255.255.0	
NET4	192.168.4.1	255.255.255.0	
NET5	192.168.5.1	255.255.255.0	
NET6	192.168.6.1	255.255.255.0	
NET7	192.168.7.1	255.255.255.0	
NET8	192.168.8.1	255.255.255.0	

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

Apply

## 10.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。



### 10.1. 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. At the top, there's a header "Static Route" with a gear icon. Below it, a "Mode" section has radio buttons for "Off" (selected) and "On". There are two tabs: "Settings" (active) and "Status". The "Settings" tab contains a form with fields for "Name", "Destination", "Gateway", and "Interface" (a dropdown menu showing "<empty>"). There is an "Add" button below the form. At the bottom right, there is an "Apply" button. A table with headers "Mode", "Name", "Destination", "Gateway", "Interface", and "Delete" is visible but empty.



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

## 10.2. IP Routing > RIP

RIP の設定を行います。

**RIP**

General Interfaces

Mode ☒ Off ☐ On

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

Redistribute OSPF routes ☒ Off ☐ On learned via the OSPF routing protocol

Redistribute BGP routes ☒ Off ☐ On learned via the BGP routing protocol

Apply

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								
<div style="display: flex; justify-content: space-between; align-items: flex-start;"> <div style="width: 60%;"> <p>Mode <input type="radio"/> Off <input checked="" type="radio"/> On</p> <p>Interface <span style="border: 1px solid #ccc; padding: 2px 10px;">eth1(WAN Ethernet) ▼</span></p> <p>Authentication <span style="border: 1px solid #ccc; padding: 2px 10px;">md5 ▼</span></p> <p>Key <span style="border: 1px solid #ccc; padding: 2px 20px;"></span></p> <p>Key ID <span style="border: 1px solid #ccc; padding: 2px 10px;">1</span></p> <p>Passive <input checked="" type="radio"/> Off <input type="radio"/> On</p> </div> <div style="width: 35%;"> <p>The key used for authentication (maxlength=16)</p> <p>The ID of the key used for authentication (1-255)</p> <p>Do not send out RIP packets on this interface</p> </div> </div> <div style="text-align: center; margin-top: 10px;"> <span style="background-color: #0056b3; color: white; padding: 5px 15px; border: 1px solid #0056b3;">Add</span> </div>								

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"> <li>● md5: HMAC-MD5 のハッシュアルゴリズムによる認証を行います。</li> <li>● none: 認証を行いません。</li> </ul>
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なくなります。

### 10.3. 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

Mode

☐ Off
☒ On

Interface

eth1(WAN Ethernet)

Authentication

md5

Key

The key used for authentication (maxlength=16)

Key ID

1

The ID of the key used for authentication (1-255)

Cost

0

The cost for sending packets via this interface (0: OSPF defaults)

Passive

☒ Off
☐ On

Do not send out OSPF packets on this interface

Add

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"> <li>● md5: HMAC-MD5 のハッシュアルゴリズムによる認証を行います。</li> <li>● none: 認証を行いません。</li> </ul>
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

Prefix of the network

Prefix Length

Length of the prefix

Area

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。

10.4. IP Routing > BGP

BGP の設定を行います。

BGP

General

Neighbors

Networks

Mode

☒ Off ☐ On

AS Number

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

Redistribute RIP routes

☒ Off ☐ On

learned via the RIP routing protocol

Redistribute OSPF routes

☒ Off ☐ On

learned via the OSPF routing protocol

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	
Redistribute RIP routes	
Redistribute OSPF 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; align-items: flex-start;"> <div style="width: 45%;"> <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 style="width: 50%;"> <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;"> <span style="background-color: #005596; color: white; padding: 5px 15px; border: 1px solid #005596;">Add</span> </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

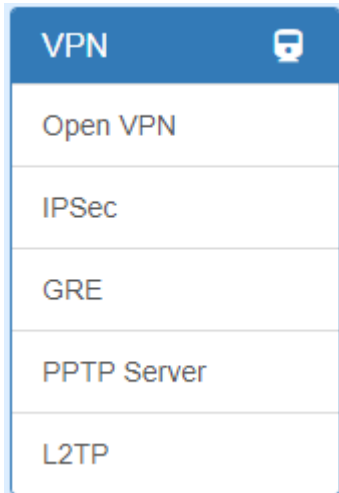
Add

Apply

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。

## 11.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。



### 11.1. 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。

Open VPN

Mode

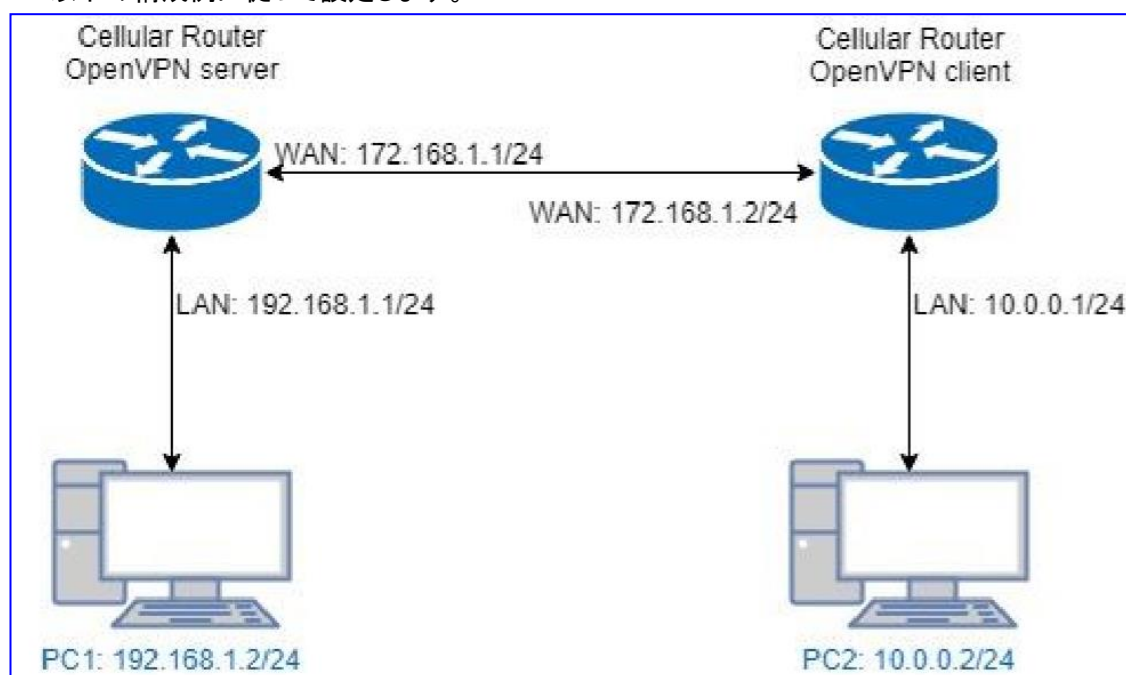
☒ Disable
 ☐ Enable

#	Mode	VPN Mode	Device	Protocol	Port	Edit
1	Disable	Client	TUN	UDP	1701	
2	Disable	Client	TUN	UDP	1701	
3	Disable	Client	TUN	UDP	1701	
4	Disable	Client	TUN	UDP	1701	
5	Disable	Client	TUN	UDP	1701	
6	Disable	Client	TUN	UDP	1701	
7	Disable	Client	TUN	UDP	1701	
8	Disable	Client	TUN	UDP	1701	
9	Disable	Client	TUN	UDP	1701	
10	Disable	Client	TUN	UDP	1701	

Apply

## 11.1.1. Open VPN 設定例

以下の構成例に従って設定します。



※ VPN のメッシュ構成には対応しておりません。

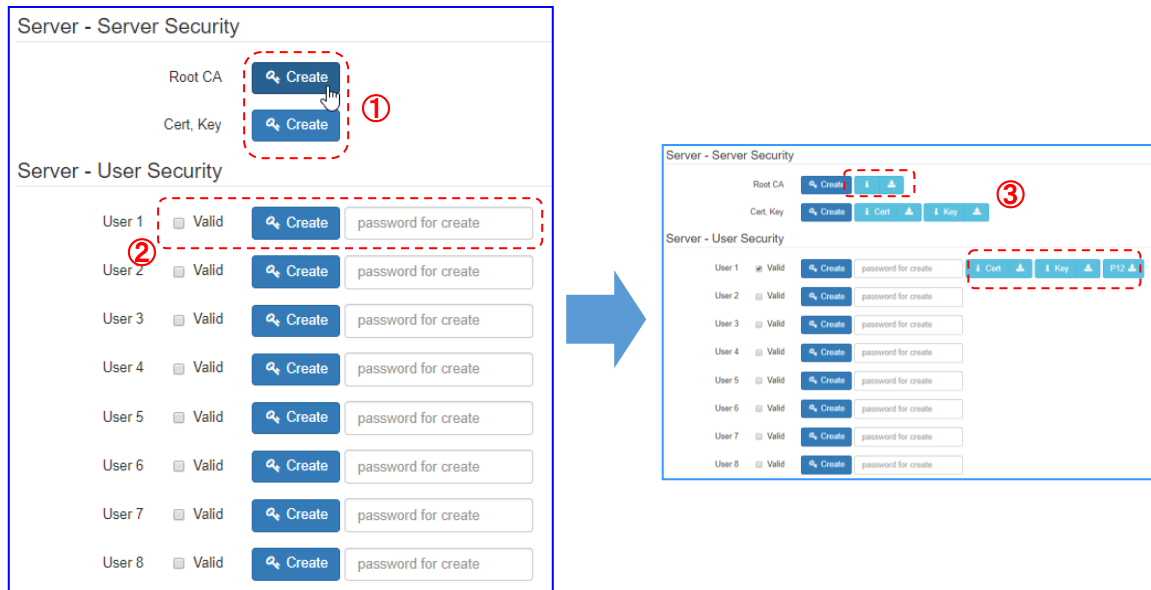
● Open VPN Server の設定

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	<p>Running</p> <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						
<b>Server</b>							
VPN Network	192.168.30.0 ⑥						
VPN Netmask	255.255.255.0						
<b>Roadwarrior</b>							
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"> <li>● Root CA</li> </ul> <u>Server – User security</u> <ul style="list-style-type: none"> <li>● Cert</li> <li>● Key</li> <li>● P12</li> </ul>

## ● Open VPN Client の設定

### 1. クライアントの基本設定

Mode	<input type="radio"/> Disable <input checked="" type="radio"/> Enable ①				
VPN Mode	<input type="radio"/> Server <input checked="" type="radio"/> Client <input type="radio"/> Custom ②				
VPN Type	<input checked="" type="radio"/> Roadwarrior <input type="radio"/> Bridging ③				
Status	Connected				
	<table border="1"> <thead> <tr> <th>IP</th> <th>Connected since</th> </tr> </thead> <tbody> <tr> <td>192.168.30.6</td> <td>2019-08-16 14:31:54</td> </tr> </tbody> </table>	IP	Connected since	192.168.30.6	2019-08-16 14:31:54
IP	Connected since				
192.168.30.6	2019-08-16 14:31:54				
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 ⑥				
Port	1701				
VPN Compression	<input type="radio"/> Disable <input checked="" type="radio"/> Enable				
Authentication	pkcs #12 Certificate ⑦				
Client					
Server Address	172.168.1.1 ⑧				
PKCS12 Password	hoge hoge				
Route Client Networks	<input type="radio"/> Off <input checked="" type="radio"/> 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 ⓘ ⬇
Cert	Import ⓘ ⬇
Key ②	Import ⓘ ⬇
P12	Import ⬇

手順	内容
①	<p>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。</p> <p><u>Server - Server security</u></p> <ul style="list-style-type: none"> <li>● Root CA</li> </ul>
②	<p>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。</p> <p><u>Server - User security</u></p> <ul style="list-style-type: none"> <li>● Cert</li> <li>● Key</li> <li>● P12</li> </ul>

## 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



## 11.2. 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 ...

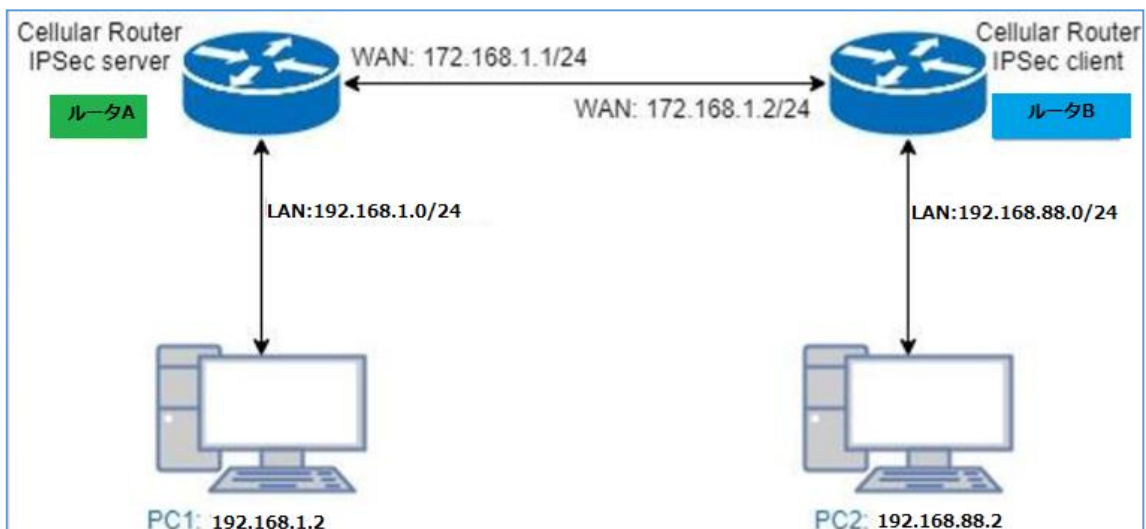
+ Add Connection

Apply

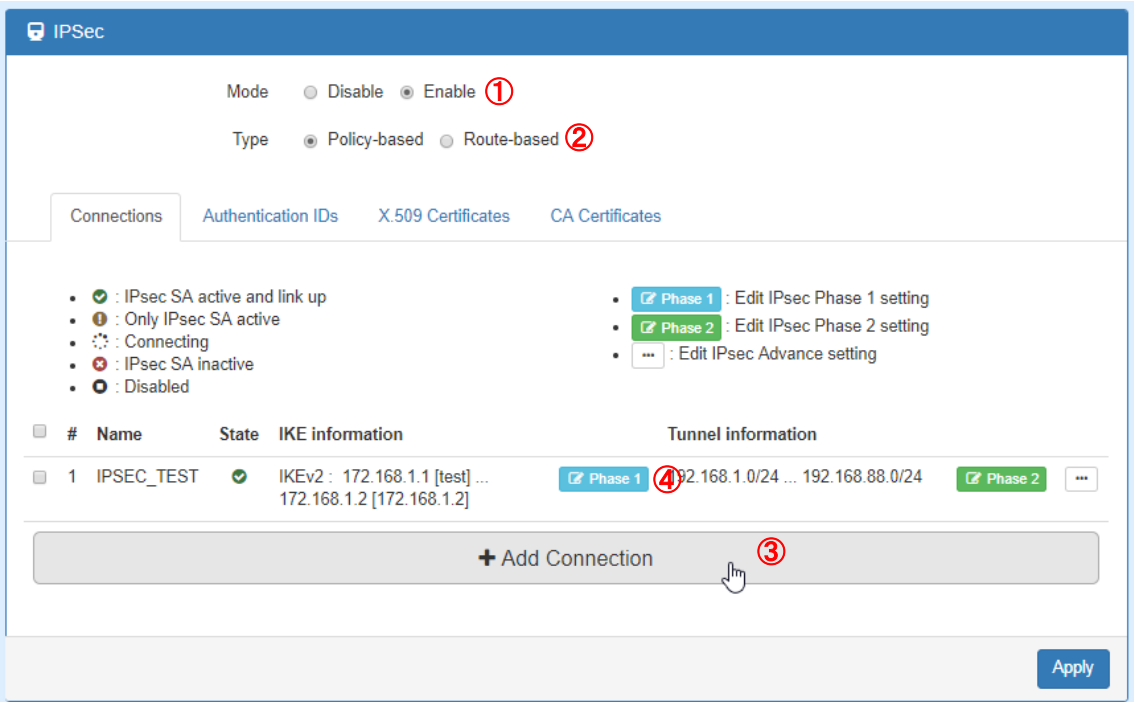
※ VPN のメッシュ構成には対応しておりません。

### 11.2.1. IPsec 設定例

以下の構成例に従って設定します。



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	Type を Policy-based に設定します。
③	Add Connection をクリックします。
④	Phase 1 をクリックします。

## 2. Phase 1 の設定

Connection #1 Phase 1

Mode ☐ Disable ☒ Enable

Name

Protocol

① Auth Type

Encryption

Hash

DH Group

Lifetime

Local Host

Local ID

② Remote Host

Remote ID

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

Mode ☒ Disable ☐ Enable

Type ☒ Policy-based ☐ Route-based

①

Connections Authentication IDs X.509 Certificates CA Certificates

#	ID	Type	Pre-shared Key / X.509 Certificate
1		PSK	..... ③

② + Add Authentication ID

Apply

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。

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

### 11.3. VPN > GRE

GRE の設定を行います。

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	

### 11.4. VPN > PPTP Server

PPTP Server の設定を行います。

暗号化は MPPE128 に対応しています。

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="text"/>				
<input type="button" value="Add"/>				
<input type="button" value="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)

●●●●●●●●●●

● クライアント側で”暗号化が必要”を選択した場合

VPNの種類(T):  
Point to Point トンネリング プロトコル (PPTP) ▼

データの暗号化(D):  
暗号化が必要 (サーバーが拒否する場合は切断します) ▼

認証

☐ 拡張認証プロトコル (EAP) を使う(E)

☒ 次のプロトコルを許可する(P)

☐ 暗号化されていないパスワード (PAP)(U)

☐ チャレンジ ハンドシェイク認証プロトコル (CHAP)(H)

☒ Microsoft CHAP Version 2 (MS-CHAP v2)

☐ Windows のログオン名とパスワード (およびドメインがある場合はドメイン) を自動的に使う(A)

プロパティ	値
デバイス名	WAN Miniport (PPTP)
デバイスの種類	vpn
認証	MS CHAP V2
暗号化	MPPE 128
圧縮	(なし)
PPP マルチリンク フレーム	オフ
クライアント IPv4 アドレス	192.168.10.2
サーバー IPv4 アドレス	192.168.10.1

● クライアント側で”暗号化は省略可能”を選択した場合

VPNの種類(T):  
Point to Point トンネリング プロトコル (PPTP) ▼

データの暗号化(D):  
暗号化は省略可能 (暗号化なしでも接続します) ▼

認証

☐ 拡張認証プロトコル (EAP) を使う(E)

☒ 次のプロトコルを許可する(P)

☐ 暗号化されていないパスワード (PAP)(U)

☐ チャレンジ ハンドシェイク認証プロトコル (CHAP)(H)

☒ Microsoft CHAP Version 2 (MS-CHAP v2)

☐ Windows のログオン名とパスワード (およびドメインがある場合はドメイン) を自動的に使う(A)

プロパティ	値
デバイス名	WAN Miniport (PPTP)
デバイスの種類	vpn
認証	MS CHAP V2
圧縮	(なし)
PPP マルチリンク フレーム	オフ
クライアント IPv4 アドレス	192.168.10.2
サーバー IPv4 アドレス	192.168.10.1



11.5. VPN > L2TP

L2TP の設定を行います。

L2TP

Mode

☐ Off ☒ Server ☐ Client

Auth

☐ PAP ☐ CHAP ☐ MS-CHAP ☒ MS-CHAPv2

Local IP

Remote begin IP

Remote end IP

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

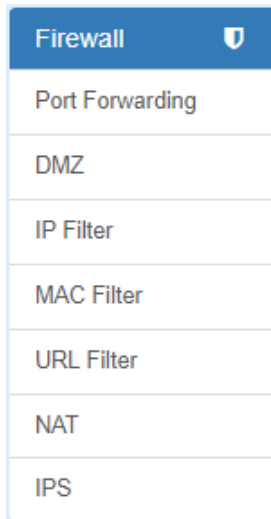
Add

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 するかどうかを選択します。
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。

## 12.Firewall

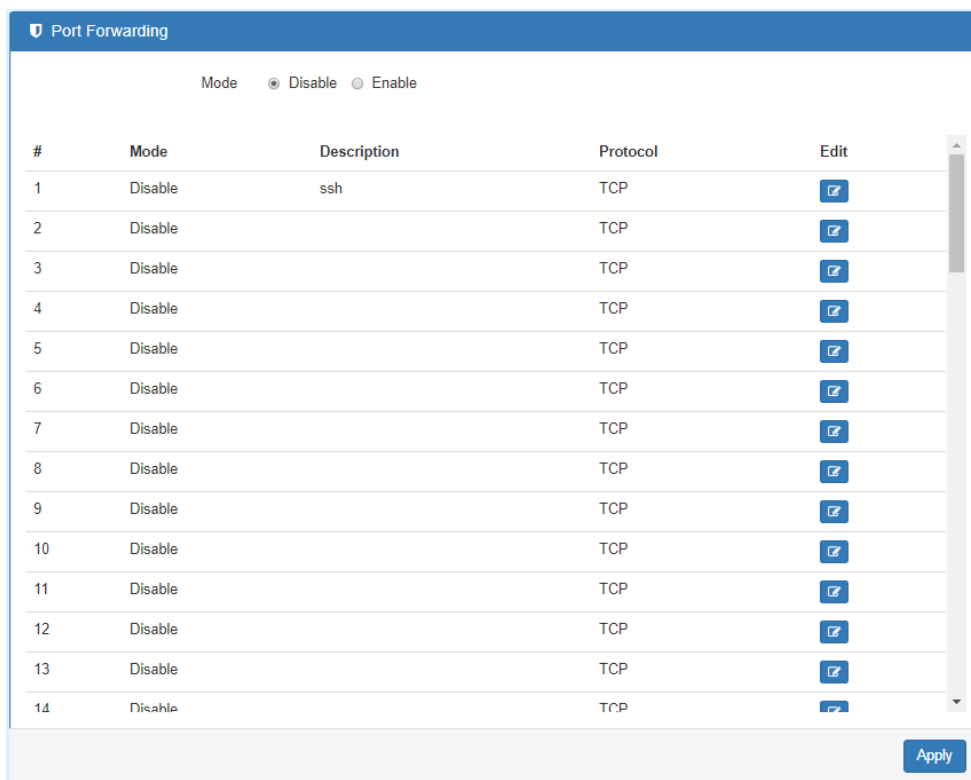
ナビゲーションパネルにて **Firewall** をクリックすると、ファイアウォール関連の設定を開くことができます。



### 12.1. 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 64 個までのルールを作成することができます。



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	

## 12.2. 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 http(tcp:80)、https(tcp:443)、ssh(tcp:22)についてはルータが応答します。

## 12.3. Firewall > IP Filter

IP フィルタの設定を行います。

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。 <ul style="list-style-type: none"> <li>● Black: リストに追加した条件のパケットを破棄します。</li> <li>● White: リストに追加した条件以外のパケットを破棄します。</li> </ul>
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

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

Save

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"> <li>● 単体指定 = 192.168.1.123</li> <li>● ネットワーク指定 = 192.168.1.0/24</li> <li>● 範囲指定 = 192.168.1.1-192.168.1.2</li> </ul>
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"> <li>● 単体指定(1234 のみ) = 1234</li> <li>● 範囲指定(1234-5678) = 1234:5678</li> </ul>
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。

## 12.4. Firewall > MAC Filter

MAC フィルタの設定を行います。

MAC Filter

Mode
☒ Disable
☐ Enable

#	Mode	MAC Address	Edit
1	Disable		
2	Disable		
3	Disable		
4	Disable		
5	Disable		
6	Disable		
7	Disable		
8	Disable		
9	Disable		
10	Disable		
11	Disable		
12	Disable		
13	Disable		
14	Disable		
15	Disable		
16	Disable		

Apply

Firewall > MAC Filter	
項目	説明
Mode	MAC フィルタの有効/無効を設定します。
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	通信を拒否する端末の MAC アドレスを入力します。



## 12.5. Firewall > URL Filter

URL フィルタの設定を行います。

URL Filter

Mode

☒ Disable
 ☐ Enable

#	Mode	Filter	Key/Full	Edit
1	Disable	Key		
2	Disable	Key		
3	Disable	Key		
4	Disable	Key		
5	Disable	Key		
6	Disable	Key		
7	Disable	Key		
8	Disable	Key		
9	Disable	Key		
10	Disable	Key		
11	Disable	Key		
12	Disable	Key		
13	Disable	Key		
14	Disable	Key		
15	Disable	Key		
16	Disable	Key		

Apply

Firewall > URL Filter	
項目	説明
Mode	URL フィルタの有効/無効を設定します。
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

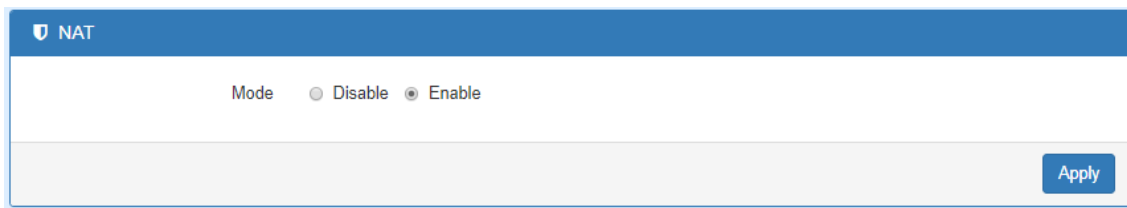
Key/Full

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。 <ul style="list-style-type: none"> <li>● Key: 入力した URL の一部が含まれる URL へのアクセスを拒否します。</li> <li>● Full: 入力した URL と完全一致する URL へのアクセスを拒否します。</li> </ul>
Key / Full	URL または URL の一部を入力します。

## 12. 6. Firewall > NAT

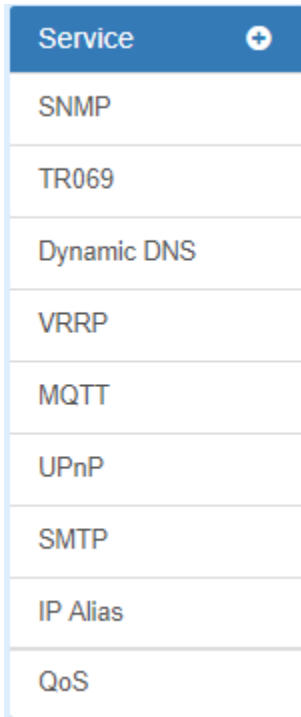
NAT の有効/無効を設定します。



The screenshot shows the NAT configuration interface. At the top, there is a blue header bar with a shield icon and the text "NAT". Below this, the word "Mode" is followed by two radio button options: "Disable" and "Enable". The "Enable" option is selected, indicated by a filled radio button. At the bottom right of the configuration area, there is a blue button labeled "Apply".

## 13. 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。



### 13.1. Service > SNMP

SNMP の設定を行います。

The SNMP configuration page shows a 'Mode' section with radio buttons for 'Disable' and 'Enable' (selected). Below are three tabs: 'Community' (selected), 'SNMP v3 User Configuration', and 'SNMP trap configuration'. A table lists three community configurations:

#	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.

## 13.1.1. 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"> <li>Read-Only: 読み込み専用のコミュニティになります。</li> <li>Read-Write: 読み書き可能のコミュニティになります。</li> </ul>

## 13.1.2. 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 v3 User 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。 <ul style="list-style-type: none"> <li>● Read-Only: 読み込み専用のユーザになります。</li> <li>● Read-Write: 読み書き可能なユーザになります。</li> </ul>

Authentication	
Mode	<p>認証モードを選択します。</p> <ul style="list-style-type: none"><li>● Auth: 認証のみ行い、暗号化は行いません。</li><li>● Privacy: 認証と暗号化を行います。</li></ul> <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	認証プロトコルを選択します。
Privacy Password	暗号化パスワードを設定します。
Privacy Protocol	暗号化方式を選択します。

## 13.1.3. 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。



## 13.2. 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"> <li>● dynv6.com</li> <li>● <a href="http://www.nsupdate.info">www.nsupdate.info</a></li> <li>● <a href="http://www.duckdns.org">www.duckdns.org</a></li> <li>● No-ip.com</li> <li>● Freedns.afraid.org</li> <li>● dyndns.org</li> </ul>
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。

13.3. 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。

### 13.4. 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。

### 13.5. 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	

13. 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

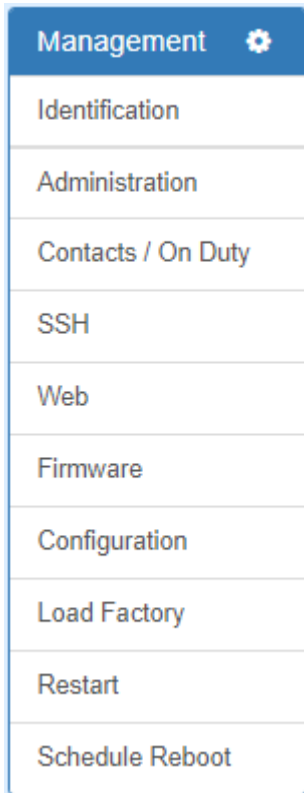
Add

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	

## 14.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出来ます。



### 14.1. Management > Identification

ルータの各情報の確認を行います。

Identification	
Attr.	Value
Active Image Partition	a
Model Name	HWL-2501-DS
LAN Ethernet MAC Address	00:03:79:05:9F:F6
WAN Ethernet MAC Address	00:03:79:05:9F:F7
Bootloader Version	1.0
Software Version	V1.77
Serial Number	BL9TW3SL0001
Software MCSV	013600531772E712
Hardware MCSV	013700531752E698
Modem Firmware Version	EC25JFAR06A05M4G
IMEI	865036040000711
Uptime	1 Day 36:43

## 14.2. 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。

### 14.3. 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。
Server Port	SSH の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。 <ul style="list-style-type: none"> <li>● Allow All: すべての端末からの SSH アクセスを許可します。</li> <li>● 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。</li> </ul>



#### 14. 4. Management > Web

Web GUI 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。 WAN 側からルータの WEBGUI にアクセスする際は HTTPS でアクセスする必要があります。

#### 14. 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。

#### 14. 6. Management > Configuration

設定情報のバックアップ/リストアを行います。

⚙️ Configuration

Backup the running configurations
Select the configuration file to restore

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。

#### 14. 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。

#### 14. 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。

## 14.9. Management > Schedule Reboot

ルータのスケジュール再起動の設定を行います。

Schedule Reboot

Mode

☒ Off
 ☐ On

Schedule

Type

☒ Interval
 ☐ Per Day
 ☐ Per Week
 ☐ Per Month

Interval Plan

per

60

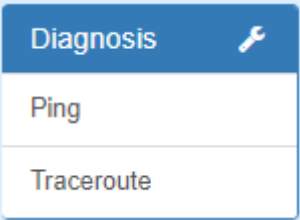
minutes (30 ~ 1440)

Apply

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。 <ul style="list-style-type: none"> <li>● Interval : 設定した時間が経過するたびに再起動します。</li> <li>● Per Day : 1 日毎に設定した時刻に再起動します。</li> <li>● Per Week : 1 週間毎に設定した時刻に再起動します。</li> <li>● Per Month : 1 か月ごとに設定した時刻に再起動します。</li> </ul>
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。

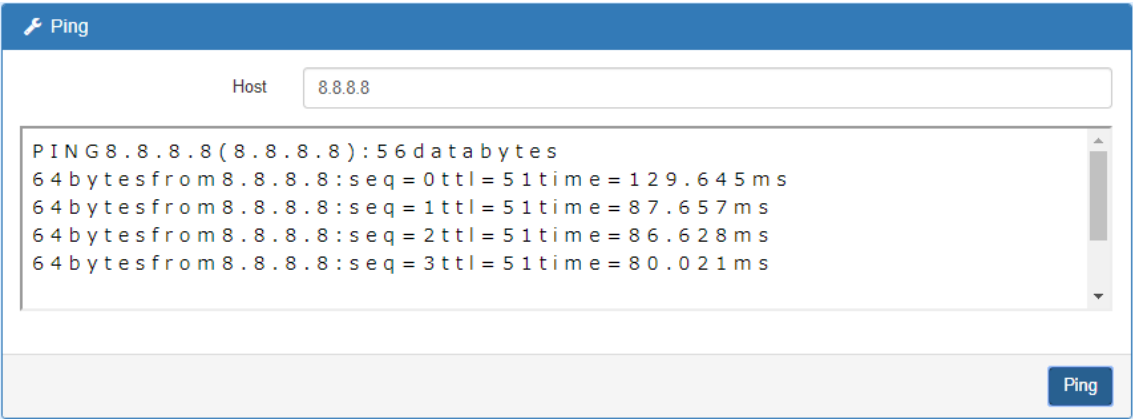
15.Diagnosis

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。



15.1. Diagnosis > Ping

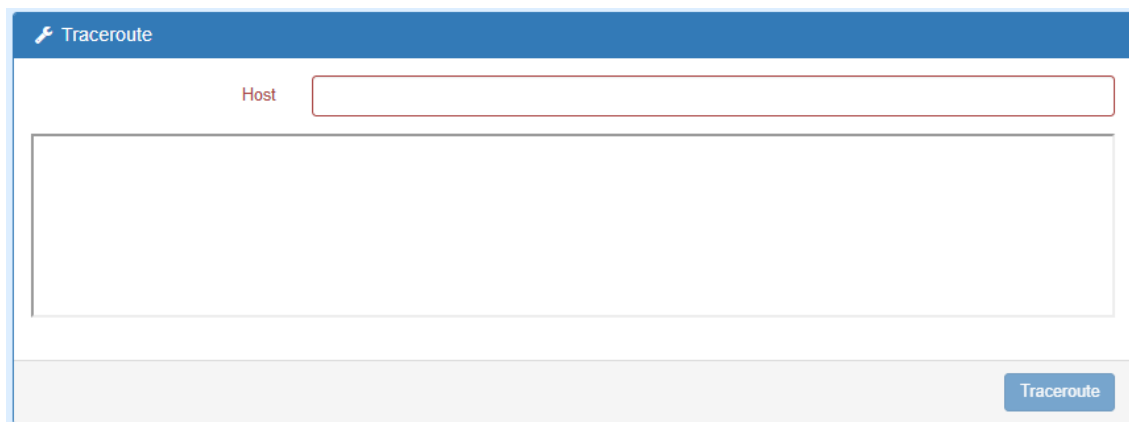
Ping を行います。



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。

## 15.2. 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。

## 16. 製品仕様

製品型番		HWL-2501-DS
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
インタフェース		2xSIM Card Slots
		3xLAN 10/100 Mbps Ethernet ports
		1xWAN 10/100 Mbps Ethernet port
		1xConsole RS232C (DB9)
		2xSMA コネクタ (LTE アンテナ)
		1xGPS アンテナ(オプション)
		1xRS485 (D+/D-)
		1xRS232C (TXD/RXD)
		2xDI, 1xDO (Alarm +/-)
		PWR V+ / V-
VPN トンネル数	IPsec	12
	L2TP	5
	OPENVPN	10
対応 SIM カード		標準 SIM
アンテナ部		外付け Main/AUX MIMO (受信のみ)、GPS
LED 表示		System, VPN, SIM (1/2), RSSI (H/L): 全て緑
防水		なし
電源		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)110mm x (D)60mm x (H)106mm
重量		400g 以下
製品保証期間		1 年間
認定		工事設計認証番号: 211-161102 技術適合認定番号: AD160016211 VCCI Class A、RoHS2 10 物質、CE、FCC

## 17. 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](mailto:support@hytec.co.jp)

受付時間 平日 9:00～17:00