

有線 5 ポート VPN ルータ

hEX シリーズ

取扱説明書



HYTEC INTER Co., Ltd.

第 1 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 2021 年 02 月 12 日 新規作成

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	6
2. 梱包物一覧.....	6
3. 製品外観	7
3.1. hEX lite	7
3.2. hEX.....	8
4. WebFig へのログイン	9
4.1. Quick Set 画面について	10
4.2. インターネットに接続する前に	12
5. CLI(Telnet/SSH)へのログイン	13
5.1. CLI の基本機能について	14
5.2. CLI の一般的なコマンドについて.....	15
6. 基本設定	18
6.1. イーサネットインタフェースの状態確認.....	18
6.2. IP アドレスの変更	20
6.3. ログインパスワードの変更	21
6.4. 時刻同期の設定	22
6.5. Firewall の設定方法.....	24
6.6. タグベース VLAN の設定方法	27
6.7. DHCP サーバの設定方法	35
6.8. 本体の再起動	37
6.9. 本体の初期化方法.....	37
6.10. 設定のバックアップ	38
6.11. 設定のリストア	39
6.12. RouterOS のアップグレード	40
7. DDNS 機能の設定方法	42
7.1. DDNS 機能の有効(Web の場合).....	42
7.2. DDNS 機能の有効(CLI の場合).....	44

8. ポートフォワーディングの設定方法	45
8.1. ポートフォワーディングの設定(Web の場合)	45
8.2. ポートフォワーディングの設定(CLI の場合)	46
9. L2TP/IPSec を使用したリモートアクセス VPN の設定方法	47
9.1. L2TP/IPSec VPN サーバの設定	47
9.2. L2TP/IPSec VPN クライアントの設定	53
10. EoIP/IPSec を使用した拠点間同一セグメント VPN の設定方法	57
10.1. RouterA の設定(Web の場合)	57
10.2. RouterB の設定(Web の場合)	60
10.3. ステータスの確認(Web の場合)	60
10.4. RouterA の設定(CLI の場合)	63
10.5. RouterB の設定(CLI の場合)	64
10.6. ステータスの確認(CLI の場合)	65
11. 動的 IP のモバイルルータを使用した EoIP/IPSec の設定方法	66
11.1. RouterA の設定	67
11.2. RouterB の設定	69
11.3. ステータスの確認	70
12. L2TP/IPSec を使用した拠点間 VPN の設定方法	71
12.1. RouterA の設定(Web の場合)	72
12.2. RouterB の設定(Web の場合)	75
12.3. RouterA の設定(CLI の場合)	77
12.4. RouterB の設定(CLI の場合)	78
13. より詳細な操作説明について	79
14. 各ルータの処理能力について	80
14.1. Ethernet スループット	80
14.2. IPsec スループット	81
15. 製品仕様	82
16. 製品保証	84

1. 製品概要

hEX シリーズは、小型筐体でありながら Mikrotik 独自の汎用 OS である RouterOS を搭載し、様々な機能を備えたルータです。

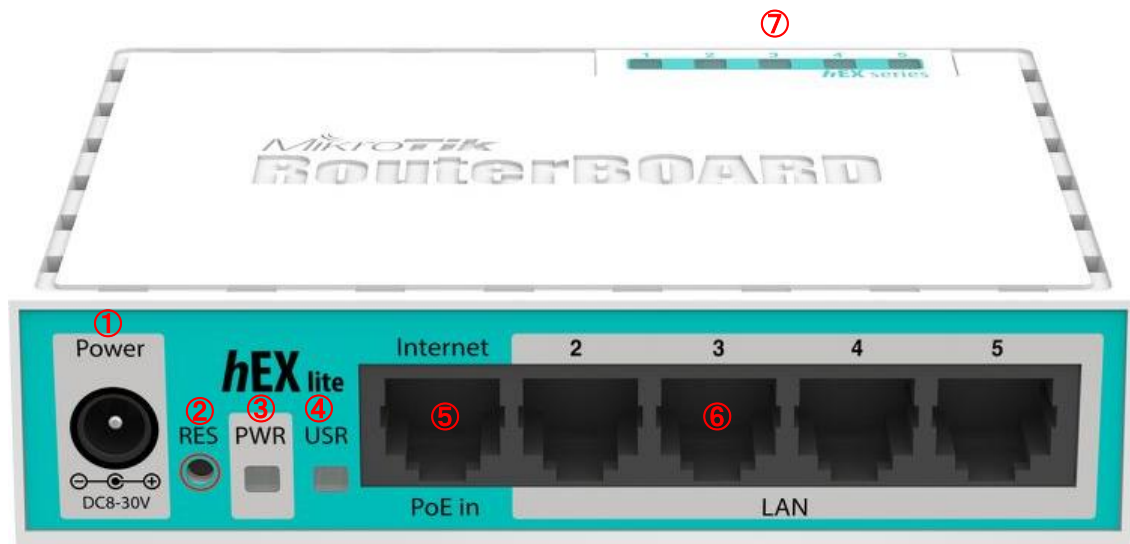
2. 梱包物一覧

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
AC アダプタ	1 個

3. 製品外観

3.1. hEX lite

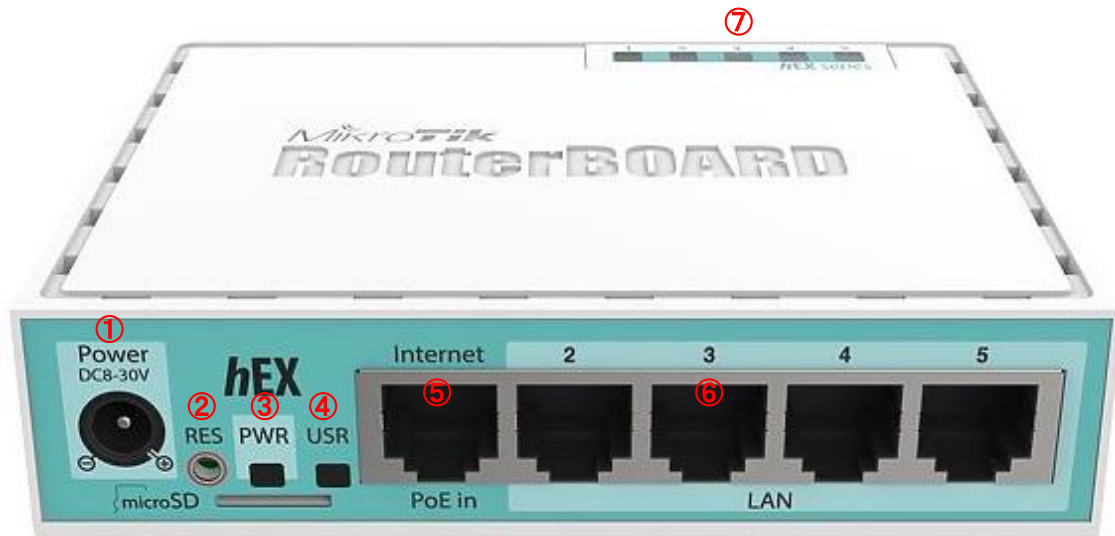


#	表示	説明
①	<u>Power</u>	付属の AC アダプタを接続します。
②	<u>RES</u>	リセットボタンです。
③	<u>PWR</u>	電源 LED です。 電源が ON の時に青点灯します。
④	<u>USR</u>	ユーザに割り当てられた LED です。 /system routerboard leds にて任意のイベントを割り当てることが出来ます。
⑤	<u>Internet</u> (<u>PoE In</u>)	Ether1 ポートです。 WAN ポートとして動作します。 Passive PoE 入力に対応しており、DC8-30V の電源入力でルータを動作させることが出来ます。
⑥	<u>2~5</u>	Ether2~5 ポートです。 LAN ポートとして動作します。
⑦	<u>1~5</u>	Ether1~5 のリンクランプです。 リンクアップすると点灯、通信時には点滅します。

設定初期化手順

- ① RES ボタンを押しながら電源を投入します。
- ② USR の緑色の LED が点滅したら、RES ボタンを離します。
- ③ 初期化と再起動が行われます。

3.2. hEX



#	表示	説明
①	<u>Power</u>	付属の AC アダプタを接続します。
②	<u>RES</u>	リセットボタンです。
③	<u>PWR</u>	電源 LED です。 電源が ON の時に青点灯します。
④	<u>USR</u>	ユーザに割り当てられた LED です。 /system routerboard leds にて任意のイベントを割り当てることが出来ます。
⑤	<u>Internet</u> (<u>PoE In</u>)	Ether1 ポートです。 WAN ポートとして動作します。 Passive PoE 入力に対応しており、DC8-30V の電源入力でルータを動作させることが出来ます。
⑥	<u>2~5</u>	Ether2~5 ポートです。 LAN ポートとして動作します。
⑦	<u>1~5</u>	Ether1~5 のリンクランプです。 リンクアップすると点灯、通信時には点滅します。

設定初期化手順

- ① RES ボタンを押しながら電源を投入します。
- ② USR の緑色の LED が点滅したら、RES ボタンを離します。
- ③ ビープ音が1回鳴り、初期化と再起動が始まります。
- ④ しばらくしてビープ音が2回鳴ったら、初期化完了です。

4. WebFig へのログイン

WEB ブラウザを使用して、RouterOS にログインすることで、RouterOS の管理機能の一つである WebFig にログインすることが出来ます。

- ログイン初期設定

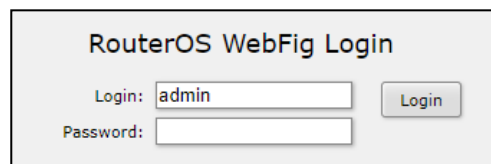
IP アドレス : 192.168.88.1

ユーザ名 : admin

パスワード : 無し

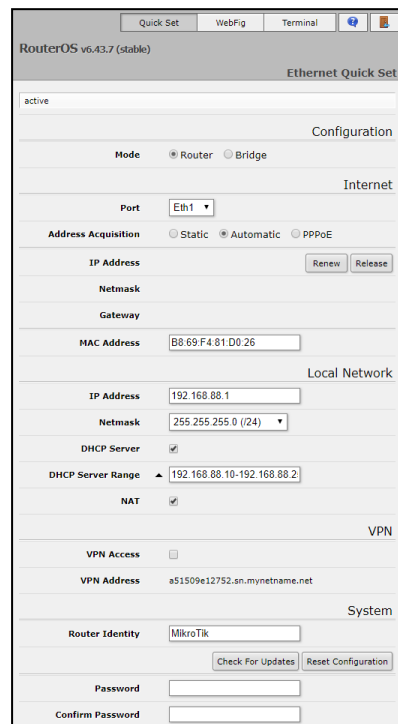
- ログイン手順

- ① ブラウザのアドレスバーに”http://192.168.88.1”と入力して接続します。
- ② ユーザ名を入力して **Log in** をクリックします。



The image shows the RouterOS WebFig Login interface. It has a title "RouterOS WebFig Login". Below the title, there are two input fields: "Login:" with the text "admin" entered, and "Password:" which is empty. To the right of the "Login:" field is a button labeled "Login".

- ③ ログインに成功すると、Quick Set 画面が表示されます。



The image shows the RouterOS v6.43.7 (stable) Ethernet Quick Set configuration screen. The screen is divided into several sections: "Configuration", "Internet", "Local Network", "VPN", and "System". The "Configuration" section shows "Mode" set to "Router". The "Internet" section shows "Port" set to "Eth1", "Address Acquisition" set to "Automatic", and "IP Address" set to "192.168.88.1". The "Local Network" section shows "IP Address" set to "192.168.88.1", "Netmask" set to "255.255.255.0 (/24)", "DHCP Server" checked, "DHCP Server Range" set to "192.168.88.10-192.168.88.2", and "NAT" checked. The "VPN" section shows "VPN Access" unchecked and "VPN Address" set to "a51509e12752.an.myname.net". The "System" section shows "Router Identity" set to "MikroTik", "Check For Updates" button, "Reset Configuration" button, "Password" field, and "Confirm Password" field.

- ④ 画面右上の **WebFig** をクリックすることで、WebFig の画面を開くことが出来ます。

4.1. Quick Set 画面について

Quick Set 画面では、基本的なルータの設定を行うことができます。

- ① Mode を Router、Bridge から選択します。

The screenshot shows a web interface titled "Configuration". Below the title, there is a "Mode" section with two radio buttons: "Router" (which is selected) and "Bridge".

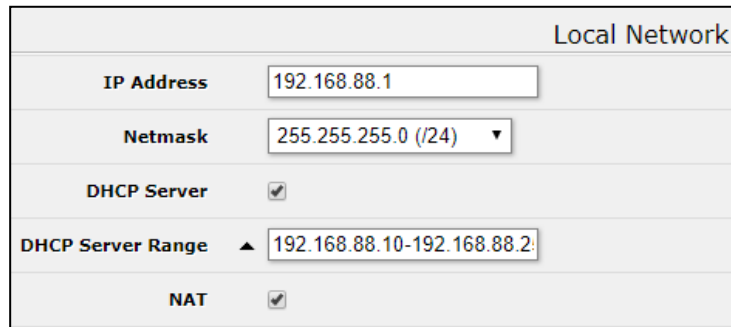
- ② Internet に関する設定を行います。

The screenshot shows a web interface titled "Internet". It contains several configuration fields:

- Port:** A dropdown menu showing "Eth1".
- Address Acquisition:** Three radio buttons: "Static", "Automatic" (selected), and "PPPoE".
- IP Address:** A text input field, followed by "Renew" and "Release" buttons.
- Netmask:** A text input field.
- Gateway:** A text input field.
- MAC Address:** A text input field containing the value "B8:69:F4:81:D0:26".

項目	説明
Port	WAN ポートとして使用するポートを選択します。
Address Acquisition	アドレスの取得方法を選択します。 Static: 静的 IP アドレスを設定します。 Automatic: DHCP サーバから IP アドレスを取得します。 PPPoE: PPPoE ユーザ名とパスワードを入力して ISP から IP アドレスを取得します。

③ LANに関する設定を行います。



Local Network

IP Address 192.168.88.1

Netmask 255.255.255.0 (/24) ▼

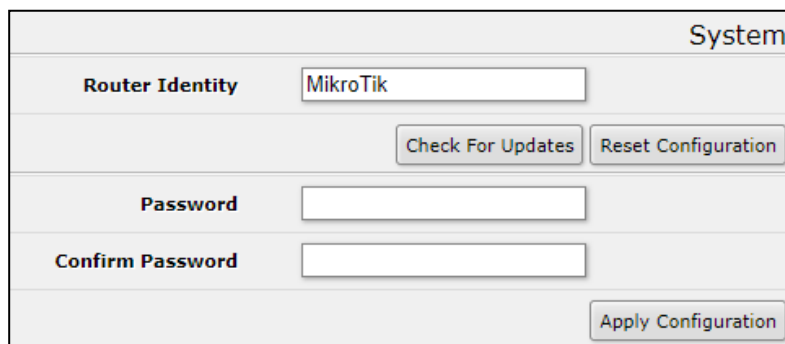
DHCP Server ☒

DHCP Server Range ▲ 192.168.88.10-192.168.88.2

NAT ☒

項目	説明
IP Address	LAN の IP アドレスを設定します。
Netmask	LAN の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/無効を設定します。
DHCP Server Range	DHCP サーバ機能を有効にした際に払い出す IP アドレスの範囲を設定します。
NAT	NAT の有効/無効を設定します。

④ システムに関する設定を行います。



System

Router Identity MikroTik

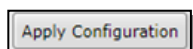
Check For Updates Reset Configuration

Password

Confirm Password

Apply Configuration

項目	説明
Router Identity	ルータのシステム名を設定します。
Password	ログインパスワードを設定します。 ※ セキュリティ強化のため、必ず設定してください。
Confirm Password	確認のため、ログインパスワードをもう一度入力します。

⑤ 最後に Apply Configuration をクリックします。

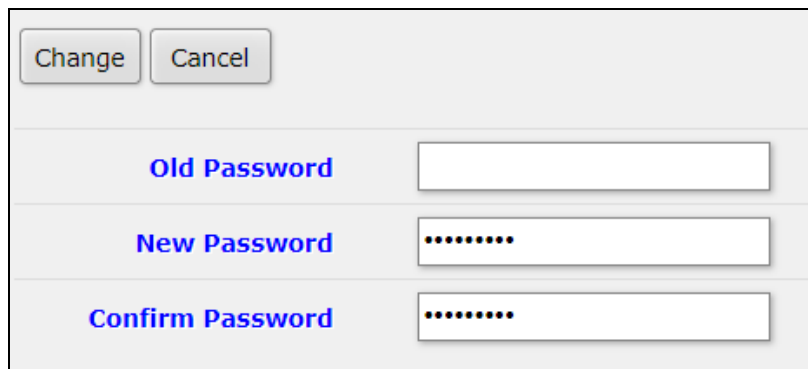
4.2. インターネットに接続する前に

ルータをインターネットに接続する前に、セキュリティ強化のために以下の設定を必ず行ってください。

① ログインパスワードの変更

System⇒Passwordを選択し、New Password 及び Confirm Password にパスワードを入力します。

※ デフォルト状態ではパスワードが無いので、Old Password は空欄になります。



② 不要なサービスの停止

IP⇒Servicesを選択し、不要なサービスは **D**(Disable)をクリックして停止させます。

8 items

		▲ Name	Port	Available From	Certificate	TLS Version
E	X	● api	8728			any
E	X	● api-ssl	8729		none	any
E	X	● ftp	21			any
D		● ssh	22			any
E	X	● telnet	23			any
E	X	● winbox	8291			any
D		● www	80			any
E	X	● www-ssl	443		none	any



8 items

		▲ Name	Port	Available From	Certificate	TLS Version
D		● api	8728			any
D		● api-ssl	8729		none	any
D		● ftp	21			any
D		● ssh	22			any
D		● telnet	23			any
D		● winbox	8291			any
D		● www	80			any
E	X	● www-ssl	443		none	any

5. CLI(Telnet/SSH)へのログイン

CLI を使用して、RouterOS にログインすることで設定を行います。

- ログイン初期設定

IP アドレス : 192.168.88.1
ユーザ名 : admin
パスワード : 無し

- ログイン手順

- ① コマンドプロンプトにて以下のコマンドを実行します。

```
telnet 192.168.88.1
```

- ② Login に”admin”、パスワードは何も入力せず[Enter]キーを押してログインします。

```
Login: admin  
Password:
```

5.1. CLI の基本機能について

- ヘルプの呼び出し

“?”を入力することで、使用可能なコマンドの一覧を表示させることができます。

```
[admin@MikroTik] >?
```

- 階層

Mikrotik の CLI は階層に分かれています。

例えば”/ip address”と入力すると、IP アドレスのメニュー階層に移動することができます。

```
[admin@MikroTik] >/ip address
```

```
[admin@MikroTik] /ip address>?
```

一番上の階層に戻るには”/”を入力し、ひとつ前の階層に戻るには”..”を入力します。

- Item Numbers

それぞれの設定値(アイテム)にはそれぞれ Item Numbers が振られています。

set コマンドなどで設定を変更する際、変更したい設定値(アイテム)の Item Numbers を指定する必要があります。

Item Numbers を確認するにはそれぞれの階層で”print”コマンドを使用します。

- [Tab]キーによるコマンド補完

[Tab]キーを使用することで、コマンドの補完を行うことができます。

例えば”>inte”の状態ですべての[Tab]キーを押すと、”>interface”と補完されます。

5.2. CLI の一般的なコマンドについて

- Print コマンド

print コマンドを使用することで、各設定値の情報と Item Numbers を確認することが出来ます。

Item Numbers は設定変更を行う際に使用します。

以下の例では、ether1 の 10.10.10.1/24 という IP アドレスには Item Numbers=1 番が割り当てられていることが分かります。

```
[admin@MikroTik] /ip address> print
Flags: X - disabled, I - invalid, D - dynamic
# ADDRESS NETWORK INTERFACE
0 ::: defconf
1 192.168.88.1/24 192.168.88.0 bridge
2 10.10.10.1/24 10.10.10.0 ether1
```

Item Numbers

- add コマンド

アイテムリストの最後に設定値を追加することが出来ます。

以下の例では、ether1 の 10.10.10.1/24 という IP アドレスを ip address のアイテムリストに追加しています。

```
[admin@MikroTik] /ip address> print
Flags: X - disabled, I - invalid, D - dynamic
# ADDRESS NETWORK INTERFACE
0 ::: defconf
1 192.168.88.1/24 192.168.88.0 bridge
[admin@MikroTik] /ip address> add address=10.10.10.1/24 interface=ether1 network=10.10.10.0
[admin@MikroTik] /ip address> print
Flags: X - disabled, I - invalid, D - dynamic
# ADDRESS NETWORK INTERFACE
0 ::: defconf
1 192.168.88.1/24 192.168.88.0 bridge
2 10.10.10.1/24 10.10.10.0 ether1
```

- set コマンド

指定した Item Numbers の設定を変更することが出来ます。

以下の例では、ip address の Item Numbers=1(ether1)の設定を address=10.10.10.1/24 から address10.10.10.2/24 に変更しています。

① /ip address print

と入力して、現在の IP アドレスのリストを表示します。

以下の例では、bridge の Item Numbers が”0”、ether1 の Item Numbers が”1”であることがわかります。

```
[admin@MikroTik] /ip address> print
Flags: X - disabled, I - invalid, D - dynamic
# ADDRESS NETWORK INTERFACE
0 ::: defconf
  192.168.88.1/24 192.168.88.0 bridge
1 10.10.10.1/24 10.10.10.0 ether1
```

② set numbers=1 address=10.10.10.2/24

Item Numbers=”1”である、ether1 の IP アドレスを変更します。

```
[admin@MikroTik] /ip address> set numbers=1 address=10.10.10.2/24
```

③ 再び”print”と入力すると、ether1 の IP アドレスが変更されたのが確認出来ます。

```
[admin@MikroTik] /ip address> print
Flags: X - disabled, I - invalid, D - dynamic
# ADDRESS NETWORK INTERFACE
0 ::: defconf
  192.168.88.1/24 192.168.88.0 bridge
1 10.10.10.2/24 10.10.10.0 ether1
```


- remove コマンド

指定した Item Numbers の設定を削除することが出来ます。

以下の例では、ip address の Item Numbers=1 の設定を削除しています。

```
[admin@MikroTik] /ip address> print
Flags: X - disabled, I - invalid, D - dynamic
# ADDRESS NETWORK INTERFACE
0 ::: defconf
  192.168.88.1/24 192.168.88.0 bridge
1 10.10.10.2/24 10.10.10.0 ether1
[admin@MikroTik] /ip address> remove numbers=1
[admin@MikroTik] /ip address> print
Flags: X - disabled, I - invalid, D - dynamic
# ADDRESS NETWORK INTERFACE
0 ::: defconf
  192.168.88.1/24 192.168.88.0 bridge
```

- move コマンド

指定した Item Numbers の設定を移動させることが出来ます。

以下の例では、ip firewall filter の Item Numbers=2 の設定値と Item Numbers=1 の設定値の順番を入れ替えています。

ファイアウォールは、Item Numbers が小さい順番に処理されるルールなので、アイテムリストの順番が特に重要です。

```
[admin@MikroTik] >/ip firewall filter
[admin@MikroTik] /ip firewall filter>move numbers=2 destination=1
```

- export コマンド

現在の階層で実行されているコマンドのリストを表示します。

```
[admin@MikroTik] /ip address> export
# jan/02/1970 00:49:27 by RouterOS 6.47
# software id = MQS7-08N8
#
# model = 960PGS
# serial number = A51509081D54
/ip address
add address=192.168.88.1/24 comment=defconf interface=bridge network=192.168.88.0
add address=10.10.10.1/24 interface=ether1 network=10.10.10.0
```

- quit コマンド

一番上の階層でこのコマンドを実行すると、CLI からログアウトすることが出来ます。

6. 基本設定

基本的な設定変更方法について説明します。

6.1. イーサネットインタフェースの状態確認

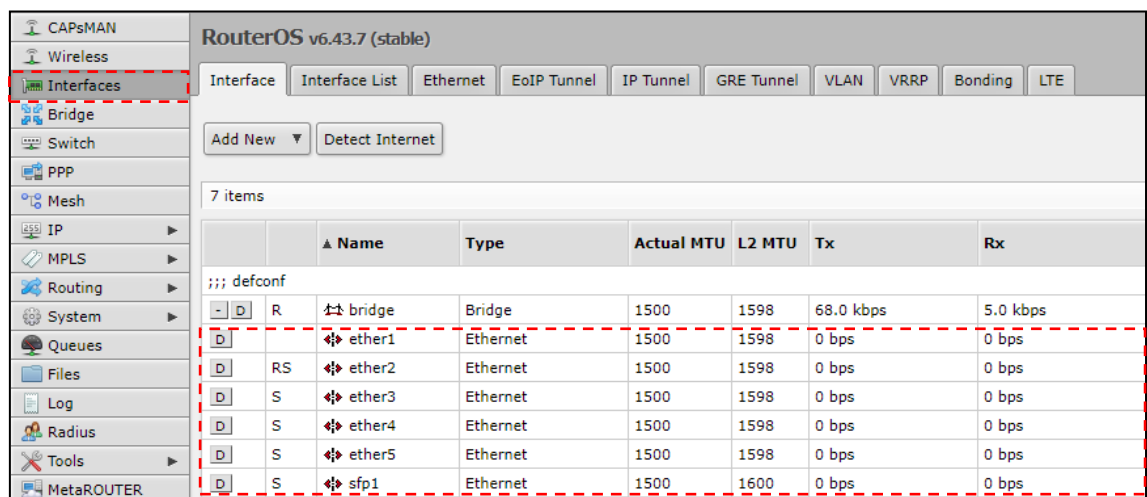
- Web による確認方法

Interface を選択すると、インタフェースの状態を確認することができます。

Name の左側のアルファベットはポートのステータスを表します。

R :ポートがリンクアップしていることを表します。

S :ポートがブリッジに所属していることを表します。



	Name	Type	Actual MTU	L2 MTU	Tx	Rx
;; defconf						
R	bridge	Bridge	1500	1598	68.0 kbps	5.0 kbps
D	ether1	Ethernet	1500	1598	0 bps	0 bps
RS	ether2	Ethernet	1500	1598	0 bps	0 bps
S	ether3	Ethernet	1500	1598	0 bps	0 bps
S	ether4	Ethernet	1500	1598	0 bps	0 bps
S	ether5	Ethernet	1500	1598	0 bps	0 bps
S	sfp1	Ethernet	1500	1600	0 bps	0 bps

Ethernet インタフェースをクリックすると、さらに詳細な情報が確認できます。

- CLI による確認方法

`/interface print` と入力すると、インタフェースの状態を確認することができます。

Name の左側のアルファベットはポートのステータスを表します。

R :ポートがリンクアップしていることを表します。

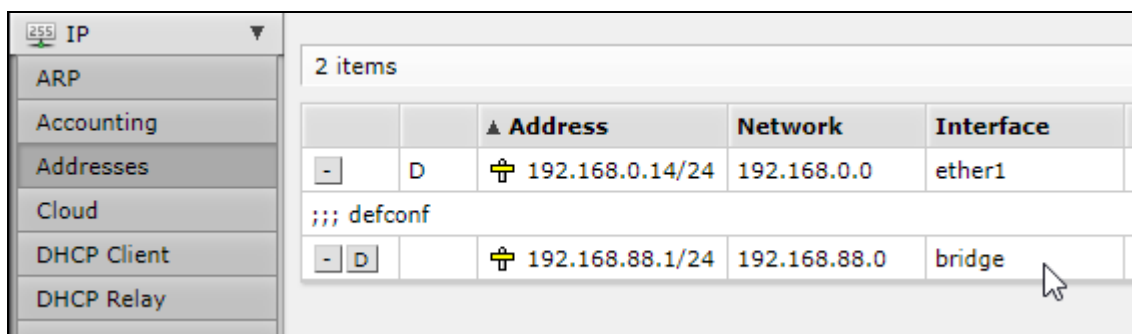
S :ポートがブリッジに所属していることを表します。

```
[admin@MikroTik] > /interface print
Flags: D - dynamic, X - disabled, R - running, S - slave
#  NAME          TYPE      ACTUAL-MTU  L2MTU  MAX-L2MTU  MAC-ADDRESS
0  R ether1        ether      1500      1598      4074 B8:69:F4:81:D5:C6
1  RS ether2        ether      1500      1598      4074 B8:69:F4:81:D5:C7
2  S ether3        ether      1500      1598      4074 B8:69:F4:81:D5:C8
3  S ether4        ether      1500      1598      4074 B8:69:F4:81:D5:C9
4  S ether5        ether      1500      1598      4074 B8:69:F4:81:D5:CA
5  S sfp1          ether      1500      1600      4076 B8:69:F4:81:D5:CB
6  R ::: defconf   bridge     1458      1598      B8:69:F4:81:D5:C7
7  S eoip-tunnel1 eoip       1458      65535     FE:09:D5:94:56:13
```

6.2. IP アドレスの変更

- Web による設定方法

- ① IP⇒Addresses を選択します。
- ② bridge インタフェースをクリックします。



- ③ IP アドレスを変更して、OK をクリックします。

not invalid

Enabled ☒

Address

Network

Interface

- CLI による設定方法

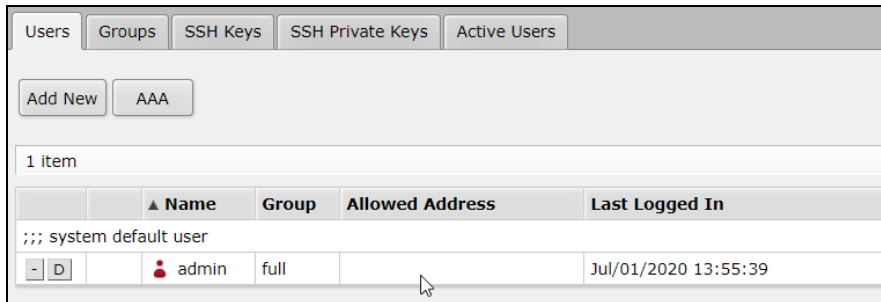
以下のコマンドを入力します。

```
/ip address
set numbers=0 address=192.168.10.1/24 network=192.168.10.0
```

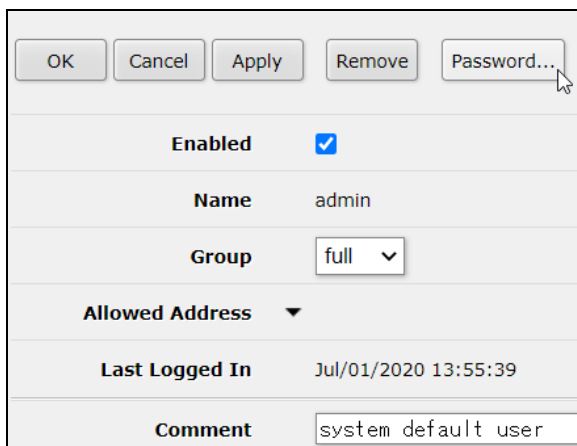
6.3. ログインパスワードの変更

- Web による設定方法

- ① System⇒Users を選択します。
- ② パスワードを変更するユーザをクリックします。



- ③ Password..をクリックして、新しいパスワードを設定します。



- CLI による設定方法

以下のコマンドを入力します。

```
/user
set numbers=0 password=admin
```

6.4. 時刻同期の設定

● Web による設定方法

- ① System⇒SNTP Client を選択します。
- ② SNTP Client メニューで **Enable** にチェックを入れて、NTP サーバの IP アドレスを入力します。
(ドメインでの入力是不可)
- ③ 時刻同期が成功すると、各ステータスが表示されます。

- ④ 続いてタイムゾーンの設定を行います。

System⇒Clock を選択して、Time Zone Name を Asia/Tokyo に変更します。

- **CLI による設定方法**

以下のコマンドを入力します。

```
/system ntp client  
set enabled=yes primary-ntp=133.243.238.243  
  
/system clock  
set time-zone-name=Asia/Tokyo
```

6.5. Firewall の設定方法

IP⇒Firewall を選択すると、Firewall の設定画面が開きます。

Firewall ルールは上に表示されているものが高い優先度になり、優先順位のルールから順に処理していきます。

パケットが上のルールで処理された場合、その下のルールが適用されることはありません。

優先順位を変更する場合は、優先順位を変更したいルールをドラッグアンドドロップして移動させます。

The screenshot shows the Firewall configuration window with the following tabs: Filter Rules, NAT, Mangle, Raw, Service Ports, Connections, Address Lists, Layer7 Protocols, and Firewall. The Firewall tab is active, showing a list of 14 items. The list includes various rules such as 'special dummy rule to show fasttrack counters', 'defconf: accept established,related,untracked', 'defconf: drop invalid', 'defconf: accept ICMP', 'defconf: accept in ipsec policy', 'defconf: accept out ipsec policy', 'defconf: fasttrack', and 'defconf: drop invalid'. Each rule has a checkbox, a number, an action, a chain, and statistics for bytes and packets. A large red arrow on the right points upwards, indicating that rules at the top have higher priority (高い) and rules at the bottom have lower priority (低い). The arrow is labeled '優先順位' (Priority).

#	Action	Chain	Src. Address	Dst. Address	Prot...	Src. Port	Dst. Port	Any. Port	In. Interf...	Out. Interf...	Bytes	Packets
0	passthroi forward										12.2 KiB	11
1	accept	input									889.7 KiB	2 908
2	drop	input									1720 B	43
3	accept	input			1 (icmp)						0 B	0
4	accept	forward									0 B	0
5	accept	forward									0 B	0
6	fasttrack	forward									1665 B	18
7	accept	forward									1665 B	18
8	drop	forward									0 B	0

例えば、ルータに対する Telnet(TCP:23)を遮断したい場合は以下の様に設定します。

General

Chain: input

Src. Address: [dropdown]

Dst. Address: [dropdown]

Protocol: tcp

Src. Port: [dropdown]

Dst. Port: 23

Any. Port: [dropdown]

In. Interface: [dropdown]

Out. Interface: [dropdown]

Action

Action: drop

Log: [checkbox]

Log Prefix: [dropdown]

Input を選択します。
ルータに対するパケットに対して Firewall を適用します。

TCP:23 を選択します。
TCP:23 宛てのパケットに対して Firewall を適用します。

Drop を選択します。
ルールに該当したパケットを拒否します。

項目	説明
Chain	Firewall を適用するパケットの流れを選びます Input: ルータに対するパケット Output: ルータから出てゆくパケット Forward: ルータが転送するパケット
Src/Dst Address	Firewall を適用するパケットの送信元、宛先を指定します。
Protocol	Firewall を適用するプロトコルを指定します。
Src/Dst Port	Firewall を適用するポート番号を指定します。
In/Out Interface	Firewall を適用するインタフェースを指定します。
Action	ルールに該当するパケットに対する処理を選びます。 Accept: パケットを許可 Drop: パケットを拒否 REJECT: パケットを拒否して制御メッセージを送信 LOG: パケットのログを記録

- **CLIによる設定方法**

以下のコマンドを入力します。

```
/ip firewall filter
```

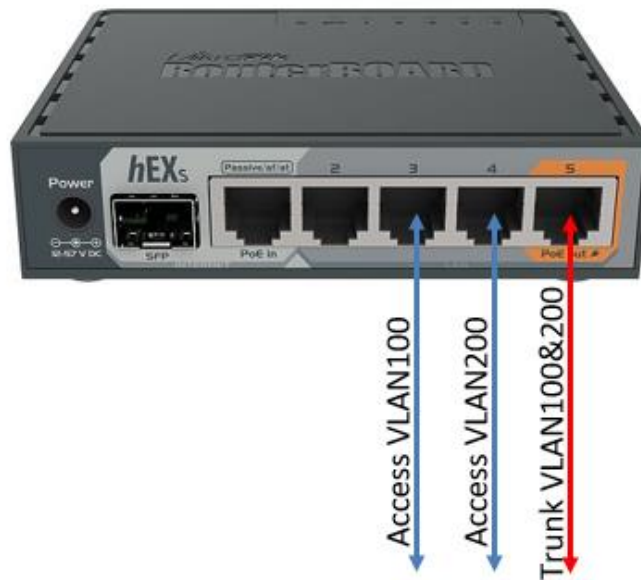
```
add action=drop chain=input protocol=tcp dst-port=23 place-before=1
```

※ place-before=1 と入力することで、1 番に登録されたルールよりも優先度を高く、このルールを追加することが出来ます。

6. 6. タグベース VLAN の設定方法

以下の例のように VLAN 設定を行う方法を説明します。

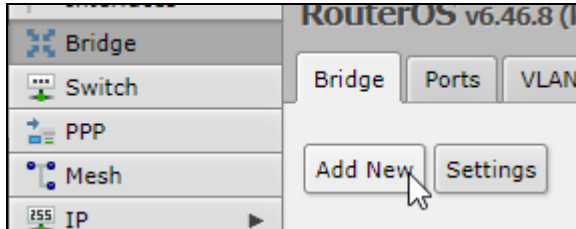
- Ether3 : VLAN100 の Access ポート
- Ether4 : VLAN200 の Access ポート
- Ether5 : Trunk ポート



- Web による設定方法

- ① Trunk ポート用のブリッジを作成します。

Bridge⇒Bridge を選択し、Add New をクリックします。



Name に bridge-trunk と入力し、OK をクリックします。

OK		Cancel	Apply	Torch
not running		not slave		
Enabled		☒		
Name	bridge-trunk			
Type	Bridge			

- ② Trunk ポート用のブリッジに Ether5 ポートを追加します。

Bridge⇒Ports を選択し、ether5 をクリックします。

	#	Interface	Bridge	Horiz...	Trust...	Priority (hex)	Path Cost
;;; defconf	0	ether2	bridge		no	80	10
;;; defconf	1	ether3	bridge		no	80	10
;;; defconf	2	ether4	bridge		no	80	10
;;; defconf	3	ether5	bridge		no	80	10

所属させるブリッジを bridge-trunk に変更し、OK をクリックします。

Bridge configuration window showing the following settings:

- Buttons: OK, Cancel, Apply, Remove
- Status: inactive
- Enabled: ☒
- Interface: ether5
- Bridge: bridge-trunk

- ③ Trunk ポート用のブリッジに VLAN インタフェースを作成します。

Interface⇒VLAN を選択し、Add New をクリックします。

RouterOS v6.46.8 (long-term) Interfaces menu showing the 'VLAN' tab selected and the 'Add New' button highlighted.

Name に vlan100、VLAN ID に 100 と入力し、Interface は bridge-trunk を選択し、OK をクリックします。

VLAN configuration window showing the following settings:

- Buttons: OK, Cancel, Apply, Torch
- Status: not running, not slave
- Enabled: ☒
- Name: vlan100
- Type: VLAN
- MTU: 1500
- Actual MTU: (empty)
- L2 MTU: (empty)
- MAC Address: (empty)
- ARP: enabled
- ARP Timeout: (empty)
- VLAN ID: 100
- Interface: bridge-trunk

同様に vlan200 も作成します。

not running not slave

Enabled ☒

Name

Type VLAN

MTU

Actual MTU

L2 MTU

MAC Address

ARP

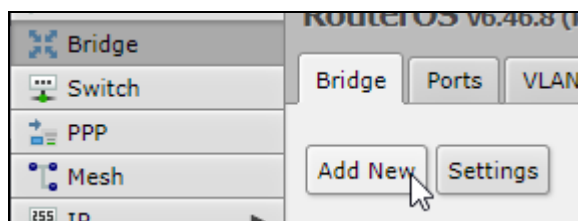
ARP Timeout ▼

VLAN ID

Interface

- ④ Access ポート用のブリッジを作成します。

Bridge⇒Bridge を選択し、Add New をクリックします。



bridge-vlan100 と bridge-vlan200 を作成します。

not running not slave

Enabled ☒

Name

Type Bridge

not running not slave

Enabled ☒

Name

Type Bridge

- ⑤ Access ポート用ブリッジに Access ポートと VLAN を追加します。

Bridge⇒Ports を選択し、ether3 と vlan100 を bridge-vlan100 に、ether4 と vlan200 を bridge-vlan200 に追加します。

Add New								
6 items								
	#	Interface	Bridge	Horiz...	Trust...	Priority (hex)	Path Cost	
;;; defconf								
- D	0	ether2	bridge		no	80	10	
;;; defconf								
- D	1	ether3	bridge-vlan100		no	80	10	
;;; defconf								
- D	2	ether4	bridge-vlan200		no	80	10	
;;; defconf								
- D	3	ether5	bridge-trunk		no	80	10	
- D	4	vlan100	bridge-vlan100		no	80	10	
- D	5	vlan200	bridge-vlan200		no	80	10	

- ⑥ 作成した VLAN を LAN のグループに追加します。

Interface

Interface List

Ethernet

EoIP Tunnel

IP Tunnel

GRE Tunnel

Add New

Lists

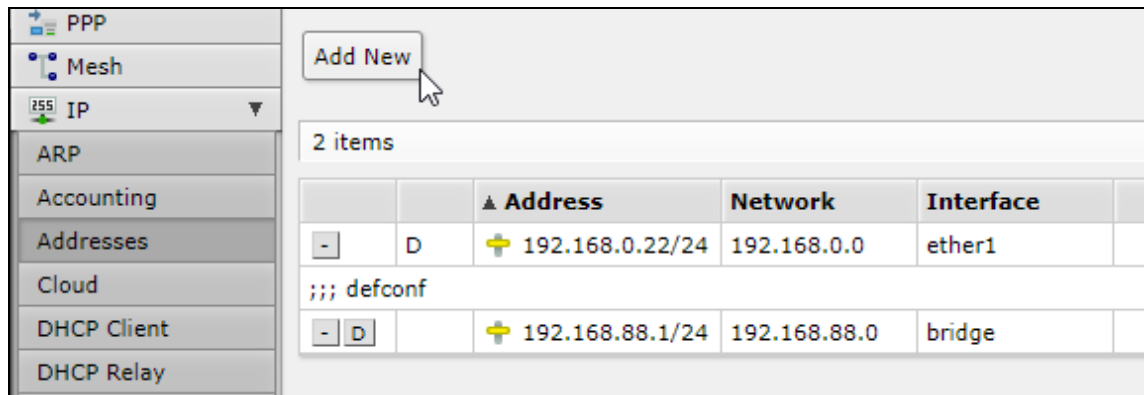
4 items

		▲ List	Interface
-	D	LAN	vlan200
-	D	LAN	vlan100
;;; defconf			
-	D	LAN	bridge
;;; defconf			
-	D	WAN	ether1

※ 追加しない場合は、この VLAN からマネージメントアクセス出来ません。

⑦ VLAN に IP アドレスを付与します。(必要な場合のみ)

IP⇒Address を選択し、Add New をクリックします。



Interface で vlan100 もしくは vlan200 を選択して、Address に IP アドレスを入力します。

The screenshot shows a dialog box for configuring an IP address. At the top are buttons for 'OK', 'Cancel', and 'Apply'. Below them is a text field containing 'not invalid'. The main configuration area has the following fields:

- Enabled**: A checkbox that is checked.
- Address**: A text field containing '192.168.100.1/24'.
- Network**: A dropdown menu with a downward arrow.
- Interface**: A dropdown menu with 'vlan100' selected.
- Comment**: An empty text field.

- CLI による設定方法

- ① Trunk ポート用のブリッジを作成します。

```
/interface bridge  
add name=bridge-trunk
```

- ② Trunk ポート用のブリッジに Ether5 ポートを追加します。

```
/interface bridge port  
set 3 bridge=bridge-trunk interface=ether5
```

- ③ Trunk ポート用のブリッジに VLAN インタフェースを作成します。

```
/interface vlan  
add interface=bridge-trunk name=vlan100 vlan-id=100  
add interface=bridge-trunk name=vlan200 vlan-id=200
```

- ④ Access ポート用のブリッジを作成します。

```
/interface bridge  
add name=bridge-vlan100  
add name=bridge-vlan200
```

- ⑤ Access ポート用ブリッジに Access ポートと VLAN を追加します。

```
/interface bridge port  
set 1 bridge=bridge-vlan100 interface=ether3 pvid=100  
add bridge=bridge-vlan100 interface=vlan100  
set 2 bridge=bridge-vlan200 interface=ether4 pvid=200  
add bridge=bridge-vlan200 interface=vlan200
```

- ⑥ 作成した VLAN を LAN のグループに追加します。

```
/interface list member  
add interface=bridge-vlan100 list=LAN  
add interface=bridge-vlan200 list=LAN
```

※ 追加しない場合は、この VLAN からマネージメントアクセス出来ません。

- ⑦ VLAN に IP アドレスを付与します。(必要な場合のみ)

```
/ip address  
add address=192.168.100.1/24 interface=vlan100 network=192.168.100.0  
add address=192.168.200.1/24 interface=vlan200 network=192.168.200.0
```

⑧ DHCP サーバを設定します。(必要な場合のみ)

```
/ip dhcp-server network
add address=192.168.100.0/24 gateway=192.168.100.1 dns-server=8.8.8.8
add address=192.168.200.0/24 gateway=192.168.200.1 dns-server=8.8.8.8

/ip pool
add name=pool_vlan100 ranges=192.168.100.2-192.168.100.50
add name=pool_vlan200 ranges=192.168.200.2-192.168.200.50

/ip dhcp-server
add address-pool=pool_vlan100 disabled=no interface=bridge-vlan100 name=dhcp-vlan100
add address-pool=pool_vlan200 disabled=no interface=bridge-vlan200 name=dhcp-vlan200
```

⑨ VLAN100⇔VLAN200 間のルーティングを遮断する場合は以下のとおりに設定します。
(必要な場合のみ)

```
/ip firewall filter
Chain=forward In int=bridge-vlan200 Out int=bridge-vlan100 Action=drop place-before=1
Chain=forward In int=bridge-vlan100 Out int=bridge-vlan200 Action=drop place-before=1
```

6.7. DHCP サーバの設定方法

- Web による設定方法

- ① IP⇒DHCP Server を選択し、DHCP Setup をクリックします。
- ② DHCP サーバを設定したいインタフェースを選択します。

Select interface to run DHCP server on	
DHCP Server Interface	bridge-vlan100 ▼

- ③ DHCP サーバを設定するインタフェースのネットワークを入力します。

Select network for DHCP addresses	
DHCP Address Space	192.168.100.0/24

- ④ DHCP クライアントに割り当てるゲートウェイのアドレスを入力します。

Select gateway for given network	
Gateway for DHCP Network	192.168.100.1

- ⑤ DHCP 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。

Select pool of ip addresses given out by DHCP server	
Addresses to Give Out ▼	192.168.1.2-192.168.1.10 ▲

- ⑥ DHCP クライアントに割り当てる DNS サーバのアドレスを入力します。

Select DNS servers	
DNS Servers ▼	8.8.8.8 ▲

- ⑦ アドレスのリース時間を設定します。

Select lease time	
Lease Time	00:10:00

- CLI による設定方法

- ① IP アドレスプールを追加します。

```
/ip pool  
add name=vlan_100 ranges=192.168.100.10-192.168.100.100
```

- ② DHCP サーバを設定するインタフェースを設定します。

```
/ip dhcp-server  
add address-pool=pool_vlan100 disabled=no interface=bridge-vlan100 name=dhcp-vlan100
```

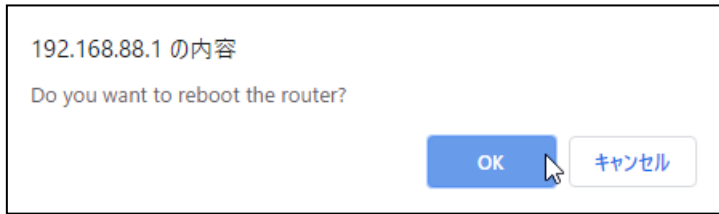
- ③ ネットワークアドレス、デフォルトゲートウェイ、DNS サーバを設定します。

```
/ip dhcp-server network  
add address=192.168.100.0/24 gateway=192.168.100.1 dns-server=8.8.8.8
```

6.8. 本体の再起動

- Web による設定方法

- ① **System⇒Reboot** を選択します。
- ② 確認画面で **OK** をクリックすると本体の再起動が行えます。



- CLI による設定方法

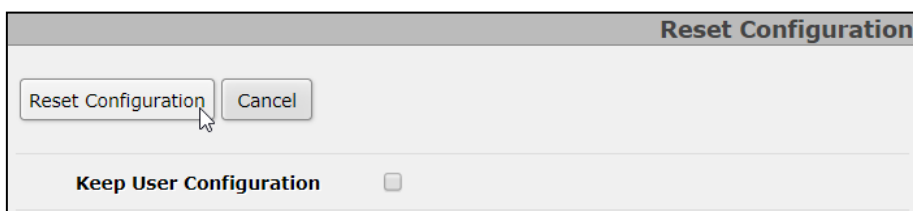
以下のコマンドを入力します。

```
/system reboot
Reboot, yes? [y/N]: y ← 確認要求が表示されたら”y”を入力します。
system will reboot shortly
```

6.9. 本体の初期化方法

- Web による設定方法

- ① **System⇒Reset Configuration** を選択します。
- ② **Rest Configuration** をクリックします。
- ③ 確認画面で **OK** をクリックすると本体の初期化が行えます。
この時 **Keep User Configuration** にチェックを入れると、ユーザアカウント情報を残したままその他の設定を初期化することが出来ます。



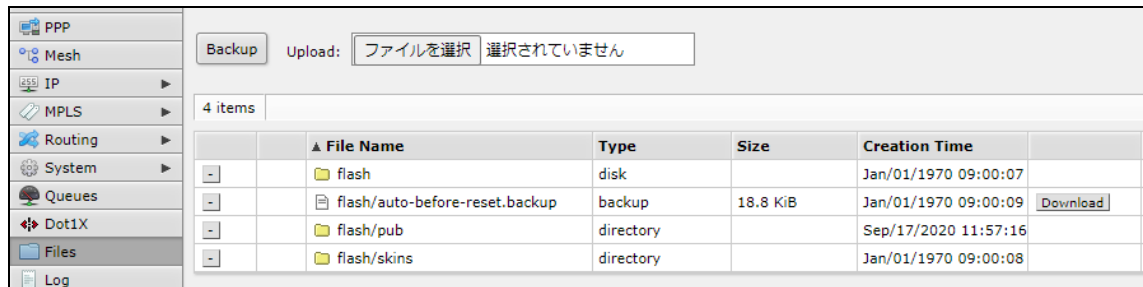
- CLI による設定方法

以下のコマンドを入力します。

```
/system reset-configuration
Dengerous! Reset anyway? [y/N]: y ← 確認要求が表示されたら”y”を入力します。
system configuration will be reset
```

6.10. 設定のバックアップ

- ① **Files**を選択します。
- ② **Backup**をクリックします。



- ③ Name に保存するファイル名を入力して、**Backup**をクリックします。
ファイルを暗号化の場合は、“Don't Encrypt”のチェックを外し、Password を入力します。

Backup Cancel

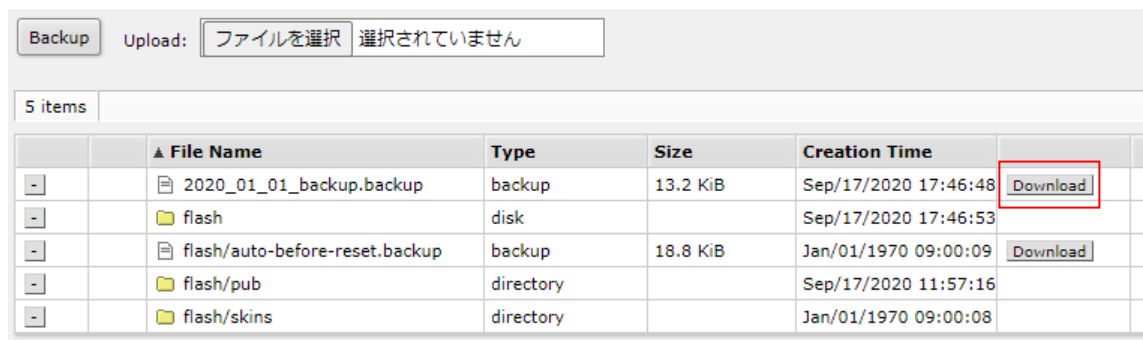
Name ▲ 2020_01_01_backup

Password ▼

Encryption aes-sha256 ▼

Don't Encrypt ☒

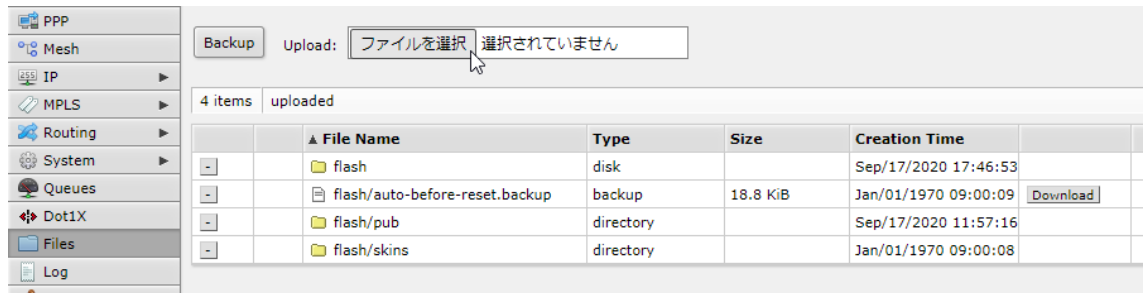
- ④ **Download**をクリックして、バックアップファイルをパソコンにダウンロードします。



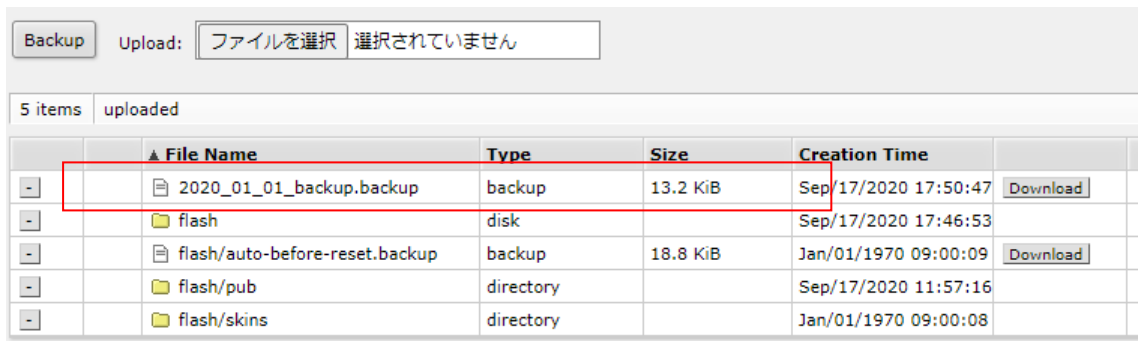
※ 設定を初期化すると、バックアップファイルはルータから削除されますので、必ずダウンロードしてください。

6.11. 設定のリストア

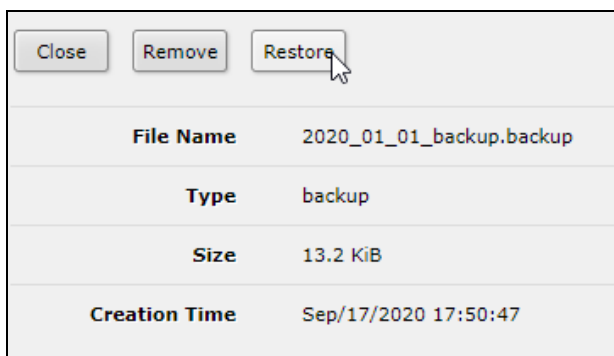
- ① **Files** を選択します。
- ② **ファイルを選択** をクリックして、パソコン上のバックアップファイルをルータにアップロードします。



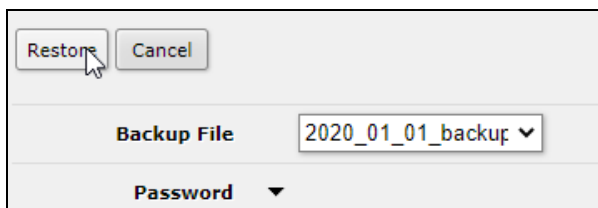
- ③ アップロードが完了したら、リストに追加されたバックアップファイルをクリックします。



- ④ **Restore** をクリックします。



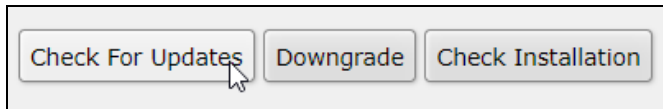
- ⑤ **Restore** をクリックします。暗号化を行っている場合は Password を入力します。



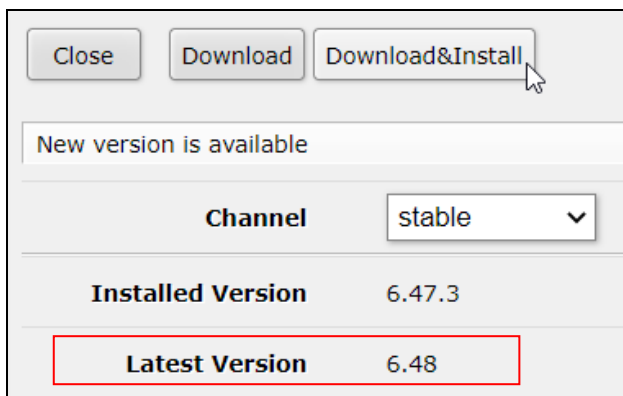
- ⑥ 確認画面で OK をクリックすると、リストアを開始し自動で再起動します。

6.12. RouterOS のアップグレード

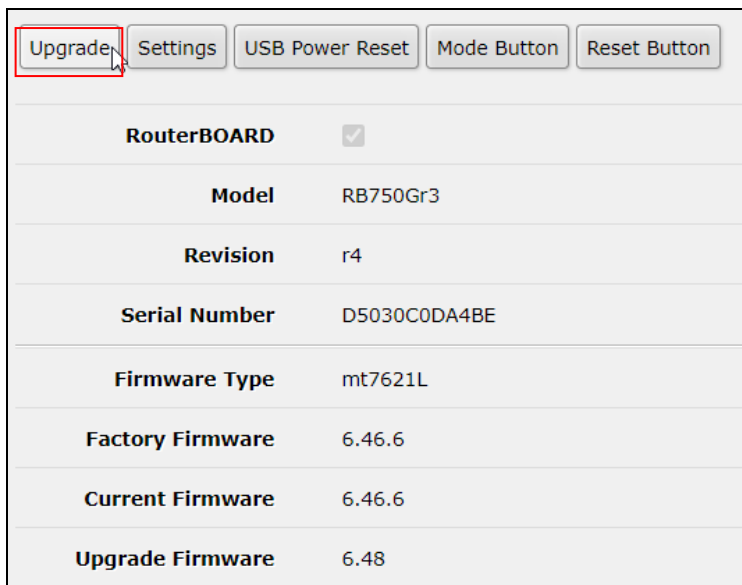
- ① System⇒Packages を選択します。
- ② Check For Updates をクリックします。



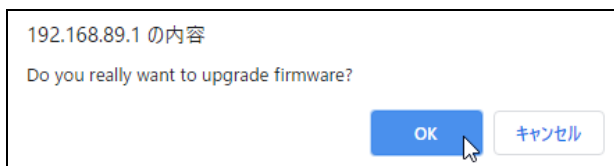
- ③ Channel は Stable を選択し、Installed Version と Latest Version が違う場合は Download&Install をクリックすると、最新バージョンのダウンロード/インストールと再起動が行われます。



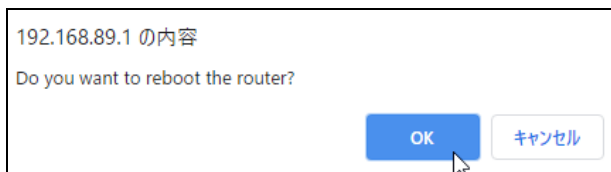
- ④ System⇒RouterBOARD を選択し、Upgrade をクリックします。



- ⑤ 確認画面が表示されますので、OK をクリックします。



- ⑥ System⇒Reboot をクリックし、確認画面で OK をクリックします。



- ⑦ System⇒RouterBOARD を選択し、Current Firmware が最新バージョンに切り替わっていることを確認しています。

Upgrade	Settings	USB Power Reset	Mode Button	Reset Button
RouterBOARD		☒		
Model		RB750Gr3		
Revision		r4		
Serial Number		D5030C0DA4BE		
Firmware Type		mt7621L		
Factory Firmware		6.46.6		
Current Firmware		6.48		
Upgrade Firmware		6.48		

7. DDNS 機能の設定方法

本機がインターネットに接続されている場合、DDNS を設定して固定ドメイン名を取得することが出来ます。

この DDNS サービスは Mikrotik 社が提供しているサービスで、利用料金は発生しません。

7.1. DDNS 機能の有効(Web の場合)

- ① **IP⇒Cloud** を選択し、**DDNS Enabled** にチェックを入れます。

The screenshot shows the 'Cloud' configuration window. At the top, there are 'Apply' and 'Force Update' buttons. Below them is a status bar that says 'updating...'. The main configuration area includes:

- DDNS Enabled**: Checked with a blue checkbox.
- DDNS Update Interval**: A dropdown menu.
- Update Time**: Checked with a blue checkbox.
- Public Address**: Displayed as 0.0.0.0.
- DNS Name**: A text field.
- Use Local Address**: An unchecked checkbox.

- ② **DDNS Update Interval** には、IP アドレスに変化がないか確認する間隔を入力します。
本機能を NAT 配下で使用する場合は、必ず必要な設定となります。

The screenshot shows the 'Cloud' configuration window after updates. At the top, there are 'Apply' and 'Force Update' buttons. Below them is a status bar that says 'updated Router is behind a NAT. Remote connection might not work.'. The main configuration area includes:

- DDNS Enabled**: Checked with a blue checkbox.
- DDNS Update Interval**: Set to 00:00:10 in a text input field.
- Update Time**: An unchecked checkbox.
- Public Address**: A blacked-out field.
- DNS Name**: A blacked-out field followed by '.mynetname.net'.
- Use Local Address**: An unchecked checkbox.

※ 指定した間隔で、“cloud2.mikrotik.com”に UDP:15252 のパケット(100byte 程度)を送信するようになります。

- ③ ルータがインターネットに接続されている場合、数秒待つか **Force Update** をクリックすることで固定ドメイン名を取得出来ます。

固定ドメイン名は必ず以下のようになります。

[本体のシリアル番号].sn.mynetname.net

Cloud

Apply

Force Update

updated

DDNS Enabled	☒
DDNS Update Interval	▼
Update Time	☒
Public Address	146.99.216.76
DNS Name	a515 [REDACTED].sn.mynetname.net
Use Local Address	☐

7.2. DDNS 機能の有効(CLI の場合)

- ① DDNS 機能を有効にして、IP アドレスに変化がないか確認する間隔を入力します。

```
/ip cloud  
set ddns-enabled=yes ddns-update-interval=30s
```

- ② ステータスを確認します。

```
/ip cloud  
print
```

```
[admin@MikroTik] > /ip cloud  
[admin@MikroTik] /ip cloud> print  
      ddns-enabled: yes  
ddns-update-interval: 10s  
      update-time: no  
      public-address: [REDACTED]  
          dns-name: [REDACTED].mynetname.net  
          status: updated  
      warning: Router is behind a NAT. Remote connection might not work.
```

8. ポートフォワーディングの設定方法

ポートフォワーディングの設定方法を説明します。

8.1. ポートフォワーディングの設定(Web の場合)

- ① IP⇒Firewall⇒NAT を選択し、Add New をクリックします。
- ② NAT のルールを追加します。(例: TCP:50000 を 192.168.88.253 にフォワードする)

not invalid

Enabled ☒

Chain Chain は dstnat を選択します。

Src. Address ▼

Dst. Address ▼

Protocol ▲ ☐ 6 (tcp) ▼ プロトコルを選択します。

Src. Port ▼

Dst. Port ▲ ☐ 50000 ポート番号を設定します。

Action Action は dst-nat を選択します。

Log ☐

Log Prefix ▼

To Addresses ▲ フォワード先の IP アドレスを入力します。

To Ports ▲ フォワード先のポート番号を入力します。

- ③ NAT のルールを追加します。(TCP:50000 を 192.168.88.253 にフォワードする)

8.2. ポートフォワーディングの設定(CLI の場合)

- ① NAT のルールを追加します。(TCP:50000 を 192.168.88.253 にフォワードする)

```
/ip firewall nat  
add action=dst-nat chain=dstnat dst-port=50000 protocol=tcp to-addresses=192.168.88.253  
to-ports=50000
```

9. L2TP/IPSec を使用したリモートアクセス VPN の設定方法

本機にてリモートアクセス VPN を実現する方法を説明します。

9.1. L2TP/IPSec VPN サーバの設定

◆ ルータの設定 (Web の場合)

- ① **IP⇒Pool** を選択し、**Add New** をクリックします。
- ② Pool 名と Addresses を設定し、**OK** をクリックします。

この時 Addresses には、VPN 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。

The screenshot shows the 'IP Pool <RoadWarrior>' configuration window. At the top are buttons for OK, Cancel, Apply, and Remove. Below these are four rows of configuration fields: 'Name' with the value 'RoadWarrior', 'Addresses' with a dropdown menu showing '192.168.89.10-192.168.89.1', 'Next Pool' with a dropdown menu showing 'none', and 'Comment' with an empty text box.

- ③ **PPP⇒Profile** を選択し、**Add New** をクリックします。
- ④ 下図を参考に設定します。

The screenshot shows the 'PPP Profile <RW-cfg>' configuration window. It has buttons for OK, Cancel, Apply, and Remove at the top. The 'General' tab is selected. The configuration fields include: 'Name' (RW-cfg), 'Local Address' (192.168.89.1), 'Remote Address' (RoadWarrior), 'Bridge' (dropdown), 'Bridge Port Priority' (dropdown), 'Bridge Path Cost' (dropdown), 'Bridge Horizon' (dropdown), 'Incoming Filter' (dropdown), 'Outgoing Filter' (dropdown), 'Address List' (dropdown), 'Interface List' (dropdown), and 'DNS Server' (8.8.8.8). Red arrows point from the text on the right to the 'Name', 'Remote Address', 'Remote Address' dropdown, and 'DNS Server' fields.

プロファイル名を設定します。

VPN クライアントに設定されるデフォルトゲートウェイを設定します。

VPN クライアントに割り当てる IP アドレスの Pool を指定します。
②の手順で作成した Pool を選択します。

VPN クライアントに設定される DNS サーバを設定します。

- ⑤ PPP⇒Interface を選択し、L2TP Server をクリックします。
- ⑥ 下図を参考に設定します。

The screenshot shows the 'L2TP Server' configuration window. It has a title bar 'L2TP Server' and buttons 'OK', 'Cancel', and 'Apply' at the top left. The settings are as follows:

Setting	Value
Enabled	☒
Max MTU	1450
Max MRU	1450
MRRU	▼
Keepalive Timeout	▲ 30
Default Profile	RW-cfg ▼
Max Sessions	▼
Authentication	☒ mschap2 ☐ mschap1 ☐ chap ☐ pap
Use IPsec	yes ▼
IPsec Secret	
Caller ID Type	ip address ▼

Annotations with red arrows point to the following settings:

- Enabled**: チェックを入れます。
- Default Profile**: ④の手順で作成したプロファイルを選択します。
- Authentication**: 認証方式を選択します。
- Use IPsec**: Yes を選択し、シークレット (事前共有キー) を設定します。

- ⑦ IP⇒IPSec を選択し、Proposals をクリックします。
- ⑧ Default をクリックし、下図を参考に設定します。

default	
Enabled	☒
Name	default
Auth. Algorithms	☐ md5 ☒ sha1 ☐ null ☐ sha256 ☐ sha512
Encr. Algorithms	☐ null ☐ des ☒ 3des ☐ aes-128 cbc ☐ aes-192 cbc ☒ aes-256 cbc ☐ blowfish ☐ twofish ☐ camellia-128 ☐ camellia-192 ☐ camellia-256 ☐ aes-128 ctr ☐ aes-192 ctr ☐ aes-256 ctr ☐ aes-128 gcm ☐ aes-192 gcm ☐ aes-256 gcm
Lifetime	▼
PFS Group	none ▼

→ 3des と aes-256cbc
を選択します。

→ None を選択します。

⑨ IP⇒IPSec を選択し、Profiles をクリックします。

⑩ Default をクリックし、下図を参考に設定します。

default

Name	default
Hash Algorithms	sha1
Encryption Algorithm	☐ des ☒ 3des ☐ aes-128 ☐ aes-192 ☒ aes-256 ☐ blowfish ☐ camellia-128 ☐ camellia-192 ☐ camellia-256
DH Group	☐ modp768 ☒ modp1024 ☐ ec2n155 ☐ ec2n185 ☐ modp1536 ☐ modp2048 ☐ modp3072 ☐ modp4096 ☐ modp6144 ☐ modp8192 ☐ ecp256 ☐ ecp384 ☐ ecp521
Proposal Check	obey
Lifetime	1d 00:00:00
Lifebytes	
NAT Traversal	☒
DPD Interval	120 s
DPD Maximum Failures	5

3des と aes-256
を選択します。

⑪ PPP⇒Secrets を選択し、Add New をクリックします。

⑫ 下図を参考に設定します。

PPP Secret <user>

OK Cancel Apply Remove

Enabled	☒
Name	user
Password	
Service	l2tp
Caller ID	
Profile	RW-cfg

ユーザ名、パスワードを設
定します。

L2TP を選択します。

④の手順で作成したプロファ
イルを選択します。

- ⑬ IP⇒Firewall を選択し、Add New をクリックします。
- ⑭ 以下の通りにルールを追記し、デフォルトで存在する drop all not coming from LAN のルールよりも上にドラッグして配置します。

```
add action=accept chain=input dst-port=500,1701,4500 protocol=udp
```

Enabled	☒
Chain	input
Src. Address	
Dst. Address	
Protocol	17 (udp)
Src. Port	
Dst. Port	500,1701,4500

⑭の手順で作成したルール

☐	D	11	✓ accept	input		17 (udp)	500,1701,4500
;;; defconf: drop all not coming from LAN							
☐	D	12	✗ drop	input			

defconf: drop all not coming from LAN のルールよりも上に配置する。

◆ ルータの設定 (CLI の場合)

- ① VPN で接続したユーザに割り当てる IP アドレスのプールを作成します

```
/ip pool  
add name=RoadWarrior ranges=192.168.89.10-192.168.89.20
```

- ② PPP プロファイルを作成します。

```
/ppp profile  
add name=RW-cfg local-address=192.168.89.1 remote-address=RoadWarrior dns-server=8.8.8.8
```

- ③ L2TP サーバインタフェースを設定します。

```
/interface l2tp-server server  
set enabled=yes authentication=mschap2 default-profile=RW-cfg ipsec-secret=123456  
use-ipsec=yes
```

- ④ IPsec の proposal 設定を変更します。

```
/ip ipsec proposal  
set auth-algorithms=sha1 enc-algorithms=aes-256-cbc,3des pfs-group=none
```

- ⑤ IPsec の profile 設定を変更します。

```
/ip ipsec profile  
set hash-algorithm=sha1 enc-algorithm=aes-256,3des dh-group=modp1024 nat-traversal=yes
```

- ⑥ PPP ユーザを追加します。

```
/ppp secret  
add name=user password=password profile=RW-cfg service=l2tp
```

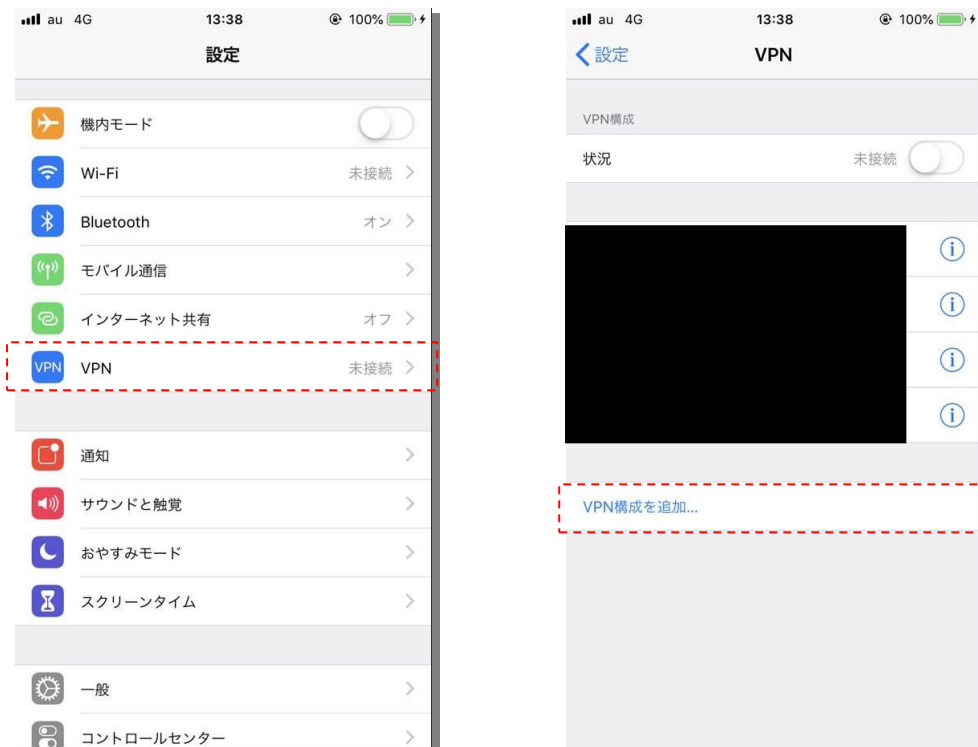
- ⑦ ファイアウォールのルールを追加します。

```
/ip firewall filter  
add action=accept chain=input dst-port=500,1701,4500 protocol=udp place-before=1
```

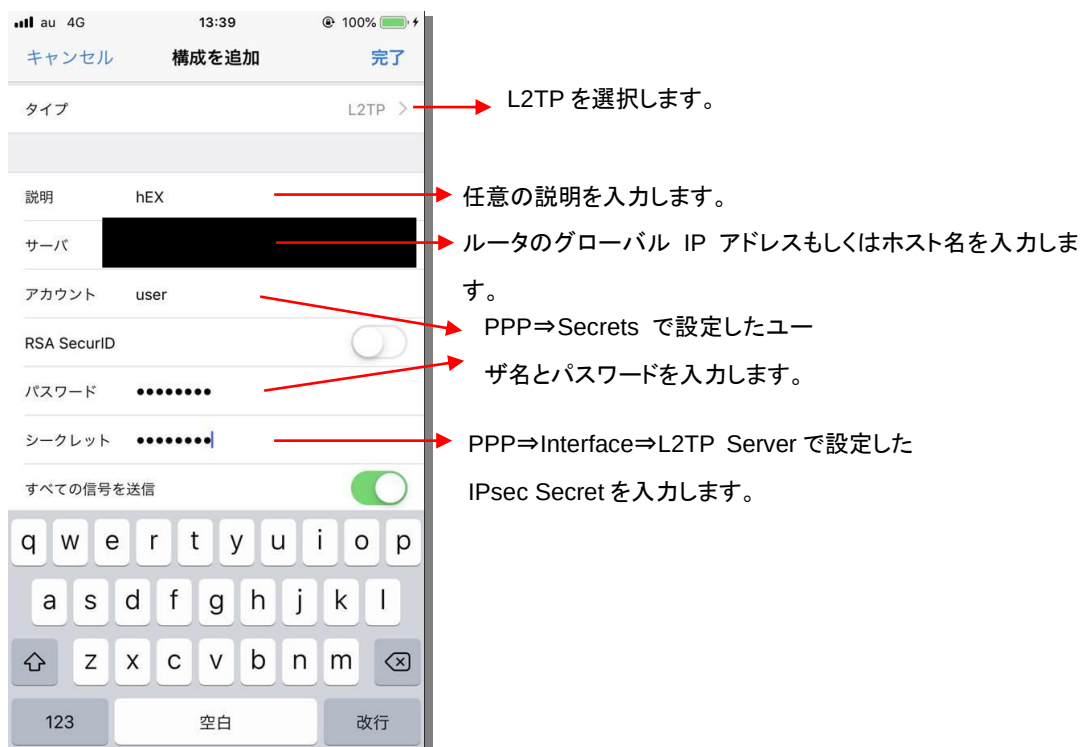
9.2. L2TP/IPSec VPN クライアントの設定

◆ スマートフォンの場合(iPhone)

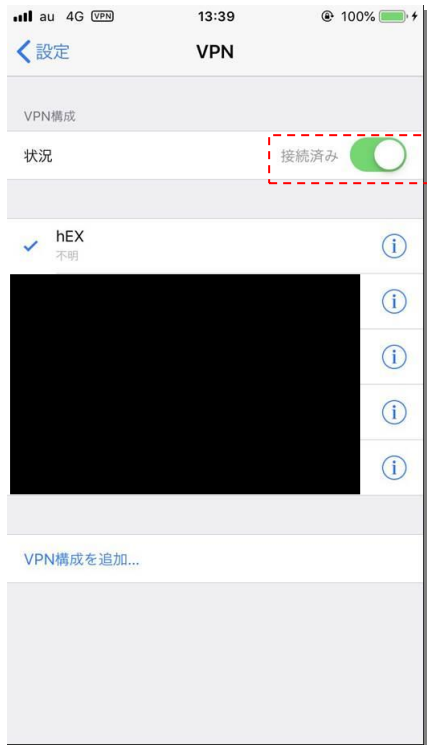
- ① **設定⇒VPN**を選択し、**VPN 構成を追加…**をタップします。



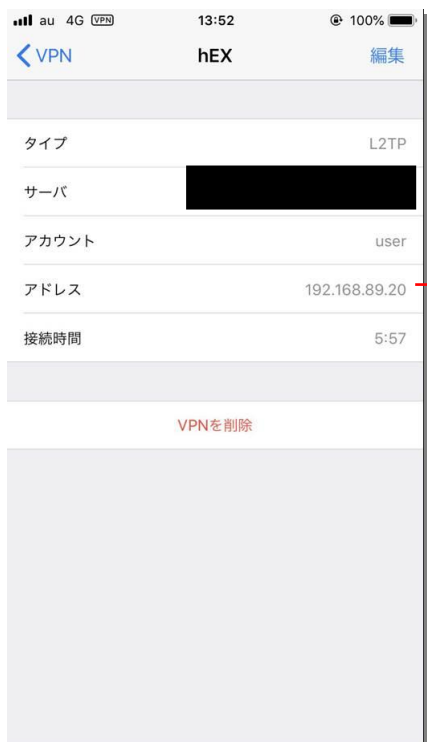
- ② 下図を参考に設定します。



- ③ VPN 構成⇒状況の右側にあるボタンをタップすると、VPN サーバと接続されます。



- ④ ⓘ をタップすると、ステータスが確認できます。



→ IP⇒Pool および PPP⇒Profile で設定した範囲の IP アドレスが割り当てられる。

◆ Windows10 の場合

- ① **設定⇒ネットワークとインターネット⇒VPN** を選択し、**VPN 接続を追加する** をクリックします。
- ② 下図を参考に設定します。

VPN接続を追加

VPN プロバイダー
Windows (ビルトイン)

接続名
hEX

サーバー名またはアドレス
[Redacted]

VPNの種類
事前共有キーを使った L2TP/IPsec

事前共有キー
●●●●●●●●

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)
user

パスワード (オプション)
●●●●●●●●

☒ サインイン情報を保存する

保存 キャンセル

任意の名前を入力します。

事前共有キーを使った L2TP/IPsec を選択します。

PPP ⇒ Interface ⇒ L2TP Server で設定した IPsec Secret を入力します。

PPP⇒Secrets で設定したユーザー名とパスワードを入力します。

- ③ **アダプタのオプションを変更する** をクリックします。

関連設定

アダプターのオプションを変更する

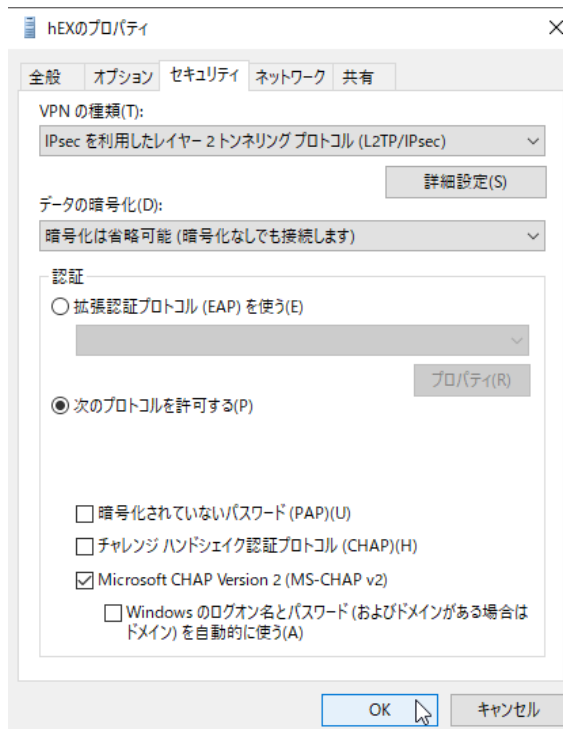
共有の詳細オプションを変更する

ネットワークと共有センター

Windows ファイアウォール

- ④ 先ほど作成した VPN 接続のプロパティを開きます。

- ⑤ セキュリティタブにて、“次のプロトコルを許可する”を選択し、
Microsoft CHAP version 2(MS-CHAP v2)にチェックを入れて、OK をクリックします。

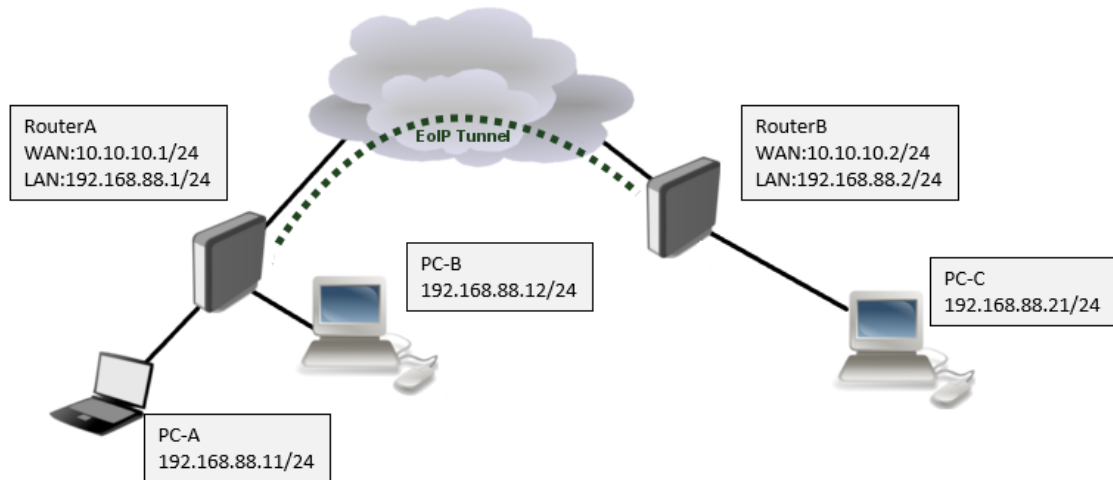


- ⑥ 接続します。



10.EoIP/IPSec を使用した拠点間同一セグメント VPN の設定方法

以下のネットワーク図を参考に、Mikrotik の独自 VPN である EoIP と IPsec を使用して2拠点間で同一セグメントの VPN を構築する方法を説明します。



10.1. RouterA の設定(Web の場合)

- ① Quick Set にて IP アドレスを設定します。

Mode	☒ Router ☐ Bridge
Port	Eth1 ▼
Address Acquisition	☒ Static ☐ Automatic ☐ PPPoE
IP Address	10.10.10.1
Netmask	255.255.255.0 (/24) ▼
Gateway	10.10.10.254
DNS Servers	▼
MAC Address	B8:69:F4:86:71:84
IP Address	192.168.88.1
Netmask	255.255.255.0 (/24) ▼
DHCP Server	☐
NAT	☒

- ② **Interface⇒EoIP Tunnel** を選択し、**Add New** をクリックします。
- ③ 下図を参考に設定します。

Enabled	☒
Name	eoip-tunnel1
Type	EoIP Tunnel
MTU	▼
Actual MTU	1408
L2 MTU	65535
MAC Address	FE:0D:FA:A5:83:9F
ARP	enabled ▼
ARP Timeout	▼
Local Address	▼
Remote Address	10.10.10.2
Tunnel ID	1
IPsec Secret	
Keepalive	00:00:10 10
DSCP	inherit ▼
Dont Fragment	no ▼
Clamp TCP MSS	☒
Allow Fast Path	☐

- Router A の WAN 側アドレスを入力します。
- Router B の WAN 側アドレスを入力します。
- 任意のトンネル ID を入力します。
- Tunnel ID と IPsec Secret は両方のルータで同じ値にする必要があります。
- チェックを外します。

- ④ **Bridge⇒Ports** を選択し、**Add New** をクリックします。
- ⑤ 下図を参考に設定します。

Enabled	☒
Interface	eoip-tunnel1 ▼
Bridge	bridge ▼
Horizon	▼
Learn	auto ▼

- 作成した EoIP インタフェースを、使用する eth ポートが所属するブリッジと同じブリッジに配置します。

- ⑥ IP⇒Firewall 選択し、Add New をクリックします。
- ⑦ 以下の通りにルールを追記し、デフォルトで存在する drop all not coming from LAN のルールよりも上にドラッグして配置します。

Enabled	☒
Chain	input ▼
Src. Address	▼
Dst. Address	▼
Protocol	47 (gre) ▼

	#	Action	Chain	Src. Address	Dst. Address	Prot...	S
;;; special dummy rule to show fasttrack counters							
-	D	0	passthro	forward			
;;; defconf: accept established,related,untracked							
-	D	1	✓ accept	input			
;;; defconf: drop invalid							
-	D	2	✗ drop	input			
;;; defconf: accept ICMP							
-	D	3	✓ accept	input		1 (icmp)	
-	D	4	✓ accept	input		47 (gre)	
;;; defconf: drop all not coming from LAN							
-	D	5	✗ drop	input			

drop all not coming from LAN のルールより上に配置する。

10.2. RouterB の設定(Web の場合)

- ① Quick Set にて IP アドレスを設定します。

Mode	☒ Router ☐ Bridge
Port	Eth1 ▼
Address Acquisition	☒ Static ☐ Automatic ☐ PPPoE
IP Address	10.10.10.2
Netmask	255.0.0.0 (/8) ▼
Gateway	10.10.10.254
DNS Servers	▼
MAC Address	B8:69:F4:81:D0:26
IP Address	192.168.88.2
Netmask	255.255.255.0 (/24) ▼
DHCP Server	☐
NAT	☒

10.3. ステータスの確認(Web の場合)

Bridge⇒EoIP Tunnelを選択し、以下の画面を確認します。

- ① EoIPトンネル正常時(Running の表示がある)

		▲ Name	Type	Actual MTU	L2 MTU	Tx	Rx	
-	D	RS	eoip-tunnel1	EoIP Tunnel	1408	65535	62.7 kbps	5.4 kbps

- ② EoIPトンネル障害発生時(Running の表示がない)

		▲ Name	Type	Actual MTU	L2 MTU	Tx	Rx	
-	D	S	eoip-tunnel1	EoIP Tunnel	1408	65535	0 bps	0 bps

- ② **Interface⇒EoIP Tunnel** を選択し、**Add New** をクリックします。
- ③ 下図を参考に設定します。

Enabled	☒	
Name	eoip-tunnel1	
Type	EoIP Tunnel	
MTU	▼	
Actual MTU	1408	
L2 MTU	65535	
MAC Address	FE:DC:CE:60:67:13	
ARP	enabled ▼	
ARP Timeout	▼	
Local Address	▼	Router B の WAN 側アドレスを入力します。
Remote Address	10.10.10.1	Router A の WAN 側アドレスを入力します。
Tunnel ID	1	任意のトンネル ID を入力します。
IPsec Secret		Tunnel ID と IPsec Secret は両方のルータで同じ値にする必要があります。
Keepalive	00:00:10 10	
DSCP	inherit ▼	
Dont Fragment	no ▼	
Clamp TCP MSS	☒	
Allow Fast Path	☐	チェックを外します。

- ④ **Bridge⇒Ports** を選択し、**Add New** をクリックします。
- ⑤ 下図を参考に設定します。

Enabled	☒	
Interface	eoip-tunnel1 ▼	作成した EoIP インタフェースを、使用する eth ポートが所属するブリッジと同じブリッジに配置します。
Bridge	bridge ▼	
Horizon	▼	
Learn	auto ▼	

- ⑥ IP⇒Firewall 選択し、Add New をクリックします。
- ⑦ 以下の通りにルールを追記し、デフォルトで存在する drop all not coming from LAN のルールよりも上にドラッグして配置します。

	#	Action	Chain	Src. Address	Dst. Address	Prot...	S
;;; special dummy rule to show fasttrack counters							
- D	0	passthro	forward				
;;; defconf: accept established,related,untracked							
- D	1	✓ accept	input				
;;; defconf: drop invalid							
- D	2	✗ drop	input				
;;; defconf: accept ICMP							
- D	3	✓ accept	input			1 (icmp)	
- D	4	✓ accept	input			47 (gre)	
;;; defconf: drop all not coming from LAN							
- D	5	✗ drop	input				

drop all not coming from LAN のルールより上に配置する。

注意点: EoIP Tunnel 作成時に IPsec Secret を入力しなかった場合、暗号化無しで EoIP を構築出来ますが、拠点間のトラフィックが暗号化無しで送受信されます。

◆ 参考: EoIP Tunnel 実効スループット

モード	暗号化	RouterA⇒RouterB	RouterB⇒RouterA
EoIP	無し	585Mbps	545Mbps
EoIP/IPsec	有り	36.7Mbps	36.9Mbps

10.4. RouterA の設定 (CLI の場合)

- ① LAN の IP アドレスと WAN の IP アドレスを設定します。

```
/ip address  
set numbers=0 address=192.168.88.1/24  
add address=10.10.10.1/24 interface=ether1 network=10.10.10.0
```

- ② WAN の DHCP-client 機能を無効にします。

```
/ip dhcp-client  
set numbers=0 disable=yes
```

- ③ LAN の DHCP-Server 機能を無効にします。

```
/ip dhcp-server  
set numbers=0 disable=yes
```

- ④ EoIP トンネルを作成します。

```
/interface eoip  
add name=eoip-tunnel1 remote-address=10.10.10.2 tunnel-id=1 ipsec-secret=123456  
allow-fast-path=no
```

注意点:

- 1) Fast-path 機能は IPsec が有効の場合には使用出来ません。
- 2) 暗号化 (IPsec) が不要の場合は、ipsec-secret を省略します。
- 3) remote-address は必ず入力しなければなりません。
- 4) tunnel-id は RouterA と RouterB で必ず同じにしてください。

- ⑤ EoIP を Bridge に追加します。

```
/interface bridge port  
add bridge=bridge interface=eoip-tunnel1
```

- ⑥ ファイアウォールにルールを追加します。

```
/ip firewall filter  
add action=accept chain=input protocol=gre place-before=1
```

10.5. RouterB の設定 (CLI の場合)

- ① LAN の IP アドレスと WAN の IP アドレスを設定します。

```
/ip address  
set numbers=0 address=192.168.88.2/24  
add address=10.10.10.2/24 interface=ether1 network=10.10.10.0
```

- ② WAN の DHCP-client 機能を無効にします。

```
/ip dhcp-client  
set numbers=0 disable=yes
```

- ③ LAN の DHCP-Server 機能を無効にします。

```
/ip dhcp-server  
set numbers=0 disable=yes
```

- ④ EoIP トンネルを作成します。

```
/interface eoip  
add name=eoip-tunnel1 remote-address=10.10.10.1 tunnel-id=1 ipsec-secret=123456  
allow-fast-path=no
```

注意点:

- 1) Fast-path 機能は IPsec が有効の場合には使用出来ません。
- 2) 暗号化 (IPsec) が不要の場合は、ipsec-secret を省略します。
- 3) remote-address は必ず入力しなければなりません。
- 4) tunnel-id は RouterA と RouterB で必ず同じにしてください。

- ⑤ EoIP を Bridge に追加します。

```
/interface bridge port  
add bridge=bridge interface=eoip-tunnel1
```

- ⑥ ファイアウォールにルールを追加します。

```
/ip firewall filter  
add action=accept chain=input protocol=gre place-before=1
```


10.6. ステータスの確認(CLI の場合)

以下のコマンドを入力します。

```
/interface eoip print
```

① EoIP トンネル正常時(Running の表示がある)

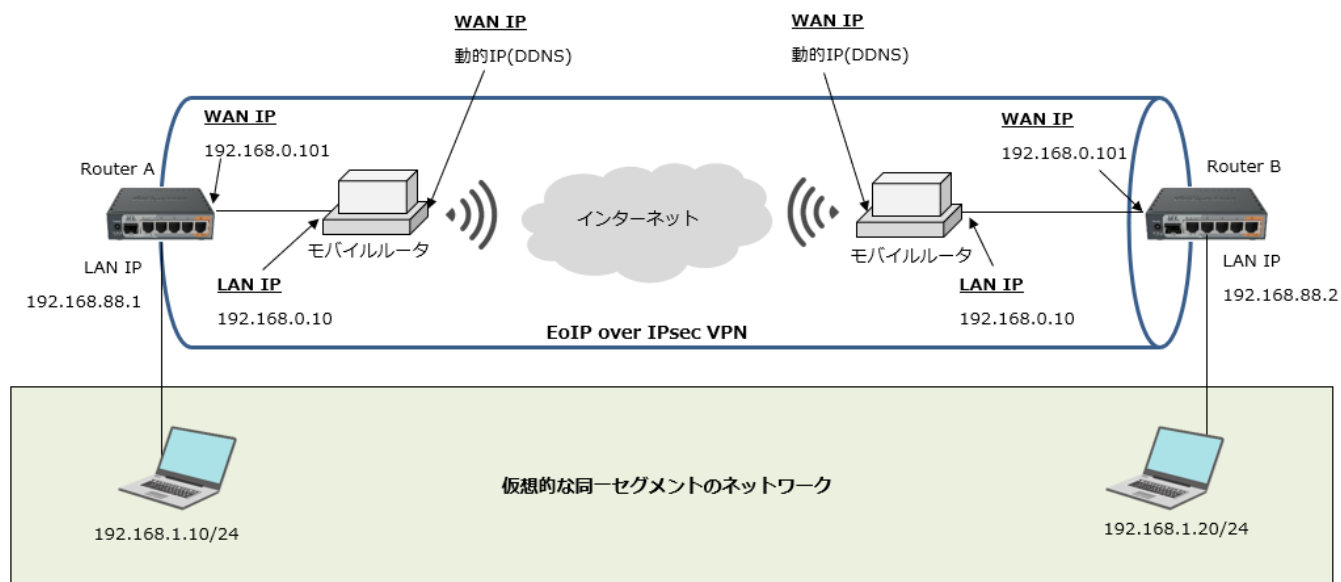
```
[admin@MikroTik] > /interface eoip print
Flags: X - disabled, R - running
0 R name="eoip-tunnel1" mtu=auto actual-mtu=1408 l2mtu=65535
  mac-address=FE:0D:FA:A5:83:9F arp=enabled arp-timeout=auto loop-protect=default
  loop-protect-status=off loop-protect-send-interval=5s loop-protect-disable-time=5m
  local-address=0.0.0.0 remote-address=192.168.0.102 tunnel-id=1 keepalive=10s,10
  dscp=inherit clamp-tcp-mss=yes dont-fragment=no ipsec-secret="123456"
  allow-fast-path=no
```

② EoIP トンネル障害発生時(Running の表示がない)

```
[admin@MikroTik] > /interface eoip
[admin@MikroTik] /interface eoip> print
Flags: X - disabled, R - running
0  name="eoip-tunnel1" mtu=auto actual-mtu=1408 l2mtu=65535
  mac-address=FE:0D:FA:A5:83:9F arp=enabled arp-timeout=auto loop-protect=default
  loop-protect-status=off loop-protect-send-interval=5s loop-protect-disable-time=5m
  local-address=0.0.0.0 remote-address=192.168.0.102 tunnel-id=1 keepalive=10s,10
  dscp=inherit clamp-tcp-mss=yes dont-fragment=no ipsec-secret="123456"
  allow-fast-path=no
```

11. 動的 IP のモバイルルータを使用した EoIP/IPSec の設定方法

以下のネットワーク図を参考に、Mikrotik の独自 VPN である EoIP と IPsec を使用して動的 IP を持つモバイルルータ経由での VPN を構築する方法を説明します。



※ 使用するモバイルルータが Symmetric NAT モードの場合、Cone NAT モードに変更する必要があります。

11.1. RouterA の設定

- ① LAN の IP アドレスと WAN の IP アドレスを設定します。

```
/ip address  
set numbers=0 address=192.168.88.1/24  
add address=192.168.0.101/24 interface=ether1 network=192.168.0.0
```

- ② デフォルトゲートウェイにモバイルルータの LAN 側 IP を入力します。

```
/ip route  
add distance=1 gateway=192.168.0.10
```

- ③ WAN の DHCP-client 機能を無効にします。

```
/ip dhcp-client  
set numbers=0 disable=yes
```

- ④ LAN の DHCP-Server 機能を無効にします。

```
/ip dhcp-server  
set numbers=0 disable=yes
```

- ⑤ DNS Server を設定します。

```
/ip dns  
set servers=8.8.8.8
```

- ⑥ DDNS 機能を有効にします。

```
/ip cloud  
set ddns-enabled=yes ddns-update-interval=1m
```

DDNS 機能を有効にすることで、動的グローバル IP を固定のホスト名で繋ぐことができます。
ホスト名は固定で、〈ルータのシリアル番号〉.sn.mynetname.net が割り当てられます。

⑦ EoIP トンネルを作成します。

```
/interface eoip  
add name=eoip-tunnel1 remote-address=<Router B のシリアル番号>.sn.mynetname.net  
tunnel-id=1 ipsec-secret=123456 allow-fast-path=no
```

注意点:

- 1) Fast-path 機能は使用出来ません。
- 2) ipsec-secret には、より強固なパスワードを入力してください。
- 3) tunnel-id は RouterA と RouterB で必ず同じにしてください。

⑧ EoIP を Bridge に追加します。

```
/interface bridge port  
add bridge=bridge interface=eoip-tunnel1
```

⑨ ファイアウォールにルールを追加します。

```
/ip firewall filter  
add action=accept chain=input protocol=gre place-before=1
```

11.2. RouterB の設定

- ① LAN の IP アドレスと WAN の IP アドレスを設定します。

```
/ip address  
set numbers=0 address=192.168.88.2/24  
add address=192.168.0.101/24 interface=ether1 network=192.168.0.0
```

- ② デフォルトゲートウェイにモバイルルータの LAN 側 IP を入力します。

```
/ip route  
add distance=1 gateway=192.168.0.10
```

- ③ WAN の DHCP-client 機能を無効にします。

```
/ip dhcp-client  
set numbers=0 disable=yes
```

- ④ LAN の DHCP-Server 機能を無効にします。

```
/ip dhcp-server  
set numbers=0 disable=yes
```

- ⑤ DNS Server を設定します。

```
/ip dns  
set servers=8.8.8.8
```

- ⑥ DDNS 機能を有効にします。

```
/ip cloud  
set ddns-enabled=yes ddns-update-interval=1m
```

DDNS 機能を有効にすることで、動的グローバル IP を固定のホスト名で繋ぐことができます。
ホスト名は固定で、〈ルータのシリアル番号〉.sn.mynetname.net が割り当てられます。

⑦ EoIP トンネルを作成します。

```
/interface eoip
add name=eoip-tunnel1 remote-address=<Router A のシリアル番号>.sn.mynetname.net
tunnel-id=1 ipsec-secret=123456 allow-fast-path=no
```

注意点:

- 1) Fast-path 機能は使用出来ません。
- 2) ipsec-secret には、より強固なパスワードを入力してください。
- 3) tunnel-id は RouterA と RouterB で必ず同じにしてください。

⑧ EoIP を Bridge に追加します。

```
/interface bridge port
add bridge=bridge interface=eoip-tunnel1
```

⑨ ファイアウォールにルールを追加します。

```
/ip firewall filter
add action=accept chain=input protocol=gre place-before=1
```

11.3. ステータスの確認

以下のコマンドを入力します。

```
/interface eoip print
```

① EoIP トンネル正常時 (Running の表示がある)

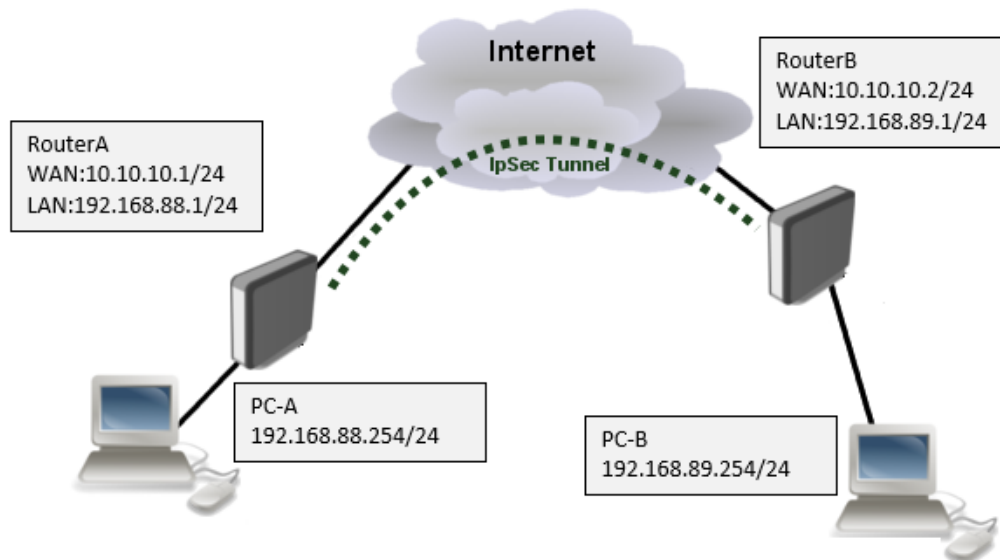
```
[admin@MikroTik] > /interface eoip print
Flags: X - disabled, R - running
0 R name="eoip-tunnel1" mtu=auto actual-mtu=1408 l2mtu=65535
   mac-address=FE:0D:FA:A5:83:9F arp=enabled arp-timeout=auto loop-protect=default
   loop-protect-status=off loop-protect-send-interval=5s loop-protect-disable-time=5m
   local-address=0.0.0.0 remote-address=192.168.0.102 tunnel-id=1 keepalive=10s,10
   dscp=inherit clamp-tcp-mss=yes dont-fragment=no ipsec-secret="123456"
   allow-fast-path=no
```

② EoIP トンネル障害発生時 (Running の表示がない)

```
[admin@MikroTik] > /interface eoip
[admin@MikroTik] /interface eoip> print
Flags: X - disabled, R - running
0  name="eoip-tunnel1" mtu=auto actual-mtu=1408 l2mtu=65535
   mac-address=FE:0D:FA:A5:83:9F arp=enabled arp-timeout=auto loop-protect=default
   loop-protect-status=off loop-protect-send-interval=5s loop-protect-disable-time=5m
   local-address=0.0.0.0 remote-address=192.168.0.102 tunnel-id=1 keepalive=10s,10
   dscp=inherit clamp-tcp-mss=yes dont-fragment=no ipsec-secret="123456"
   allow-fast-path=no
```

12.L2TP/IPSec を使用した拠点間 VPN の設定方法

以下のネットワーク図を参考に、L2TP/IPsec を使用して2拠点間の VPN を構築する方法を説明します。



12.1. RouterA の設定(Web の場合)

- ① Quick Set にて IP アドレスを設定します。

Mode	☒ Router ☐ Bridge
Port	Eth1 ▼
Address Acquisition	☒ Static ☐ Automatic ☐ PPPoE
IP Address	10.10.10.1
Netmask	255.255.255.0 (/24) ▼
Gateway	10.10.10.254
DNS Servers	▼
MAC Address	B8:69:F4:86:71:84
IP Address	192.168.88.1
Netmask	255.255.255.0 (/24) ▼
DHCP Server	☐
NAT	☒

- ② IP⇒Pool を選択し、Add New をクリックします。

- ③ 下図を参考に設定します。

Name	L2TP-Pool
Addresses	1.1.1.1-1.1.1.100 ▲▼
Next Pool	none ▼

任意の名前と任意のアドレス範囲で設定します。
このアドレスが L2TP クライアントに割り振られます。

- ④ PPP⇒Profiles を選択し、Add New をクリックします。

- ⑤ 下図を参考に設定します。

Name	L2TP-Profile
Local Address	L2TP-Pool ▼
Remote Address	L2TP-Pool ▼

任意の名前を設定します。

作成した IPPool を選択します。

- ⑥ PPP⇒Interface を選択し、L2TP Server をクリックします。
- ⑦ 下図を参考に設定します。

Enabled	☒	チェックを入れて、L2TP サーバを有効にします。
Max MTU	1450	
Max MRU	1450	
MRRU	▼	
Keepalive Timeout	▲ 30	
Default Profile	default ▼	
Max Sessions	▼	
Authentication	☒ mschap2 ☒ mschap1 ☒ chap ☒ pap	
Use IPsec	required ▼	required を選択し、IPsec での暗号化を有効にします。
IPsec Secret	secret	IPsec Secret を入力します。
Caller ID Type	ip address ▼	

- ⑧ PPP⇒Secrets を選択し、Add New をクリックします。
- ⑨ 下図を参考に設定します。

Enabled	☒	
Name	L2TP-01	任意のユーザ名を設定します。
Password	▲ testtest	任意のパスワードを設定します。
Service	l2tp ▼	l2tpを選択します。
Caller ID	▼	
Profile	L2TP-Profile ▼	先ほど作成したプロファイルを選択します。
Local Address	▼	
Remote Address	▼	
Routes	▲ 192.168.89.0/24	RouterB の LAN 側ネットワークを入力します。

⑩ IP⇒Firewall を選択し、Add New をクリックします。

⑪ 下図を参考に設定します。

add action=accept chain=input dst-port=50,500,1701,4500 protocol=udp

Enabled ☒

Chain

Src. Address

Dst. Address

Protocol

Src. Port

Dst. Port

⑫ 作成したルールを”defconf: drop all not coming from LAN”のルールよりも上に配置します。

	#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port
;;; special dummy rule to show fasttrack counters								
- D	0	passthro	forward					
;;; defconf: accept established,related,untracked								
- D	1	✓ accept	input					
;;; defconf: drop invalid								
- D	2	✗ drop	input					
;;; defconf: accept ICMP								
- D	3	✓ accept	input			1 (icmp)		
- D	4	✓ accept	input			17 (udp)		50,1701,500,4500
;;; defconf: drop all not coming from LAN								
- D	4	✗ drop	input					

drop all not coming from LAN のルールより上に配置する。

12.2 RouterB の設定(Web の場合)

- ① Quick Set にて IP アドレスを設定します。

Port	Eth1 ▼
Address Acquisition	☒ Static ☐ Automatic ☐ PPPoE
IP Address	10.10.10.2
Netmask	255.255.255.0 (/24) ▼
Gateway	10.10.10.254
DNS Servers	▼
MAC Address	B8:69:F4:81:D0:26
IP Address	192.168.89.1
Netmask	255.255.255.0 (/24) ▼
DHCP Server	☒
DHCP Server Range	▲ 192.168.89.10-192.168.89
NAT	☐

- ② Interfaces⇒Interface を選択し、Add New⇒L2TP Client をクリックします。

- ③ 下図を参考に設定します。

Enabled	☒	
Name	l2tp-out1	任意の名前を設定します。
Type	L2TP Client	
Actual MTU		
Max MTU	1450	
Max MRU	1450	
MRRU	▼	
Connect To	10.10.10.1	RouterA のグローバル IP アドレスを指定します。
User	L2TP-01	RouterA 側で設定したユーザ名とパスワードを入力
Password	▲ testtest	します。
Profile	default-encryption ▼	
Keepalive Timeout	▼	
Use IPsec	☒	
IPsec Secret	secret	RouterA 側で設定した IPsec Secret を入力します。

- ④ IP⇒Routes を選択し、Add New をクリックします。
- ⑤ 下図を参考に設定します。

Enabled ☒	
Dst. Address	192.168.88.0/24
Gateway	l2tp-out1 reachable
Check Gateway	
Type	unicast

RouterA の LAN 側ネットワークを入力します。

L2TP クライアントのインターフェースを選択します。

Unicast を選択します。

12.3. RouterA の設定 (CLI の場合)

- ① LAN の IP アドレスと WAN の IP アドレスを設定します。

```
/ip address  
set numbers=0 address=192.168.88.1/24  
add address=10.10.10.1/24 interface=ether1 network=10.10.10.0
```

- ② L2TP 用の IP アドレスプールを作成します。

```
/ip pool  
add name=default-dhcp ranges=192.168.88.10-192.168.88.254  
add name=L2TP-pool ranges=1.1.1.1-1.1.1.100
```

- ③ L2TP のプロファイルを作成します。

```
/ppp profile  
add local-address=L2TP-pool name=L2TP-Profile remote-address=L2TP-pool
```

- ④ L2TP サーバを設定します。

```
/interface l2tp-server server  
set enabled=yes ipsec-secret=123456 use-ipsec=required
```

※ Ipsec-secret には、より強固なシークレットキーを入力してください。

- ⑤ PPP Secret を設定します。

```
/ppp secret  
add name=L2TP-01 password=testtest profile=L2TP-Profile routes=192.168.89.0/24 service=l2tp
```

※ password には、より強固なパスワードを入力してください。

- ⑥ Firewall にて UDP:50,500,1701,4500 を許可します。

```
add action=accept chain=input dst-port=50,500,1701,4500 protocol=udp
```

12. 4. RouterB の設定 (CLI の場合)

- ① LAN の IP アドレスと WAN の IP アドレスを設定します。

```
/ip address  
set numbers=0 address=192.168.89.1/24  
add address=10.10.10.2/24 interface=ether1 network=10.10.10.0
```

- ② L2TP クライアントのインタフェースを作成します。

```
/interface l2tp-client  
add connect-to=d5030c395e67.sn.mynetname.net disabled=no ipsec-secret=123456 ¥  
keepalive-timeout=disabled name=l2tp-out1 password=testtest use-ipsec=yes user=L2TP-01
```

- ③ サーバの LAN 側ネットワークへのルートをルーティングテーブルに追加します。

```
/ip route  
add distance=1 gateway=192.168.0.10  
add distance=1 dst-address=192.168.88.0/24 gateway=l2tp-out1
```

13. より詳細な操作説明について

Router OS の詳細なマニュアルについては、以下のリンクから Mikrotik の Wiki をご参照ください。

[URL] <https://wiki.mikrotik.com/wiki/Manual:TOC>

14. 各ルータの処理能力について

14.1. Ethernet スループット

hEX lite (RB750r2)				
モード	設定	1518 byte	512 byte	64 byte
		Mbps	Mbps	Mbps
Bridging	無し	493.0	480.9	120.2
	25 bridge filter rules	493.0	370.3	48.3
Routing	無し	493.0	480.9	111.5
	25 simple queues	493.0	405.1	51.8
	25 ip filter rules	493.0	213.0	27.0

hEX (RB750Gr3)				
モード	設定	1518 byte	512 byte	64 byte
		Mbps	Mbps	Mbps
Bridging	無し	1,972.2	1,817.4	532.0
	25 bridge filter rules	1,972.2	688.5	89.2
Routing	無し	1,972.2	1,820.3	529.9
	25 simple queues	1,972.2	735.6	87.8
	25 ip filter rules	1,128.2	385.4	48.0

14. 2. IPsec スループット

hEX (RB750Gr3)				
モード	設定	1400 byte	512 byte	64 byte
		Mbps	Mbps	Mbps
Single tunnel	AES-128-CBC + SHA1	469.3	173.3	21.2
256 tunnels	AES-128-CBC + SHA1	469.3	179	21.9
256 tunnels	AES-128-CBC + SHA256	472.6	181.9	21.9
256 tunnels	AES-256-CBC + SHA1	358.4	163.8	20.7
256 tunnels	AES-256-CBC + SHA256	359.5	162.6	20.7

15. 製品仕様

製品名	hEX lite (RB750r2)
CPU	QCA9533
CPU 周波数	850MHz
CPU コア数	1
メモリ	64MB
ストレージ容量	16MB
OS	RouterOS (License Level 4)
VPN	IPsec, L2TP, PPTP, GRE, OpenVPN, SSTP, EoIP
セキュリティ	ファイアウォール
管理機能	WEB GUI, Telnet, SSH, SNMP
インタフェース	LAN ポート RJ-45 10/100BASE-TX x4
	WAN ポート RJ-45 10/100BASE-TX x1
寸法	(W)113 x (H)28 x (D)89mm (突起部含まず)
本体重量	130g
電源	DC8~30V
最大消費電力	2W
動作温度	-40~+70℃
規格・認定	VCCI Class A、RoHS
製品保証期間	1 年間

製品名	hEX (RB750Gr3)
CPU	MT7621A
CPU 周波数	880MHz
CPU コア数	2
CPU スレッド	4
CPU	MT7621A
メモリ	256MB
ストレージ容量	16MB
OS	RouterOS (License Level 4)
VPN	IPsec, L2TP, PPTP, GRE, OpenVPN, SSTP, EoIP
セキュリティ	ファイアウォール
管理機能	WEB GUI, Telnet, SSH, SNMP
インタフェース	LAN ポート RJ-45 10/100/1000BASE-T x4
	WAN ポート RJ-45 10/100/1000BASE-T x1
寸法	(W)113 x (H)28 x (D)89mm (突起部含まず)
本体重量	150g
電源	DC8～30V
最大消費電力	10W
動作温度	-40～+60℃
規格・認定	VCCI Class A、RoHS
製品保証期間	1 年間

16. 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