

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 4.1 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
第 2 版	2021 年 04 月 28 日	PC 経由のファームウェア更新手順、WinBox の説明を追記
第 3 版	2021 年 08 月 11 日	VLAN 設定方法の修正、設定リストアの注意点を追記
第 3.1 版	2023 年 03 月 03 日	EoIP 設定方法の誤字を修正
第 4 版	2024 年 07 月 23 日	パスワードが本体ラベルに記載されている場合のログイン方法を追記
第 4.1 版	2024 年 08 月 14 日	アップグレード方法の変更

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。
- 通気口をふさがらないでください。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纯粹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. hEX lite	8
3.2. hEX.....	9
4. WebFig へのログイン	10
4.1. Quick Set 画面について	12
4.2. インターネットに接続する前に	14
5. CLI(Telnet/SSH)へのログイン	15
5.1. CLI の基本機能について	17
5.2. CLI の一般的なコマンドについて	18
6. 基本設定	21
6.1. イーサネットインタフェースの状態確認.....	21
6.2. IP アドレスの変更	23
6.3. ログインパスワードの変更	24
6.4. 時刻同期の設定	25
6.5. Firewall の設定方法.....	27
6.6. タグベース VLAN の設定方法	30
6.7. DHCP サーバの設定方法	39
6.8. 本体の再起動	41
6.9. 本体の初期化方法.....	41
6.10. 設定のバックアップ	42
6.11. 設定のリストア	43
6.12. RouterOS のアップグレード	45
7. DDNS 機能の設定方法	47
7.1. DDNS 機能の有効(Web の場合).....	47
7.2. DDNS 機能の有効(CLI の場合).....	49

8. ポートフォワーディングの設定方法	50
8.1. ポートフォワーディングの設定(Web の場合)	50
8.2. ポートフォワーディングの設定(CLI の場合)	51
9. L2TP/IPSec を使用したリモートアクセス VPN の設定方法	52
9.1. L2TP/IPSec VPN サーバの設定	52
9.2. L2TP/IPSec VPN クライアントの設定	58
10. EoIP/IPSec を使用した拠点間同一セグメント VPN の設定方法	62
10.1. RouterA の設定 (Web の場合)	62
10.2. RouterB の設定 (Web の場合)	65
10.3. ステータスの確認 (Web の場合)	68
10.4. RouterA の設定 (CLI の場合)	69
10.5. RouterB の設定 (CLI の場合)	70
10.6. ステータスの確認 (CLI の場合)	71
11. 動的 IP のモバイルルータを使用した EoIP/IPSec の設定方法	72
11.1. RouterA の設定	73
11.2. RouterB の設定	75
11.3. ステータスの確認	77
12. L2TP/IPSec を使用した拠点間 VPN の設定方法	78
12.1. RouterA の設定 (Web の場合)	79
12.2. RouterB の設定 (Web の場合)	82
12.3. RouterA の設定 (CLI の場合)	84
12.4. RouterB の設定 (CLI の場合)	85
13. IP アドレスを忘れてしまった、初期化が上手くいかない場合	86
14. より詳細な操作説明について	89
15. 各ルータの処理能力について	90
15.1. Ethernet スループット	90
15.2. IPsec スループット	91
16. 製品仕様	92

17. 製品保証94

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。

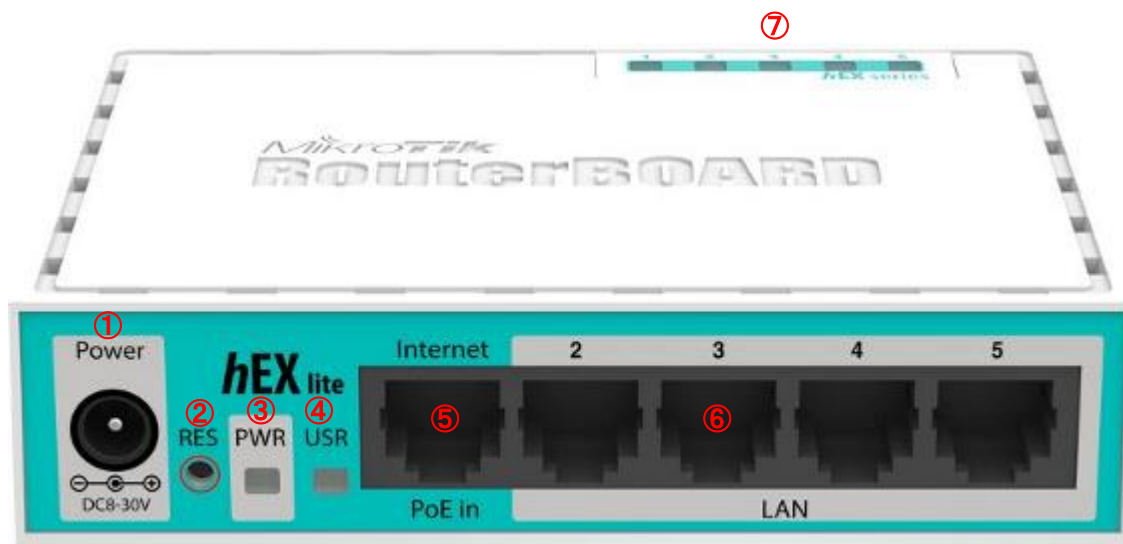
2. 梱包物一覧

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

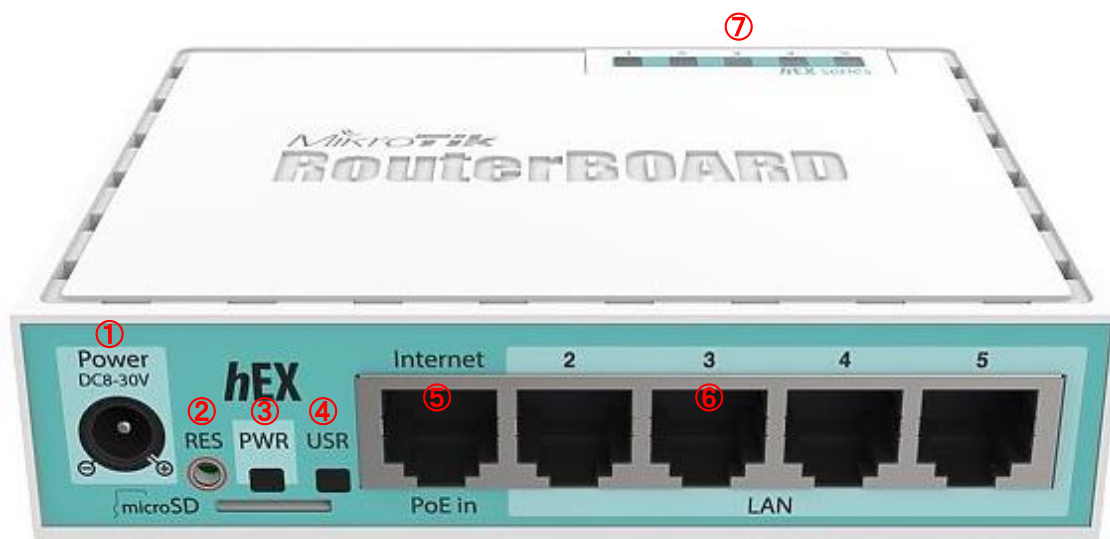


#	表示	説明
①	<u>Power</u>	付属の AC アダプタを接続します。
②	<u>RES</u>	リセットボタンです。
③	<u>PWR</u>	電源 LED です。 電源が ON の時に青点灯します。
④	<u>USR</u>	ユーザに割り当てられた LED です。 /system routerboard leds にて任意のイベントを割り当てることが出来ます。
⑤	<u>Internet</u> <u>(PoE In)</u>	Ether1 ポートです。 WAN ポートとして動作します。 Passive PoE 入力に対応しており、DC8-30V の電源入力でルータを動作させる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

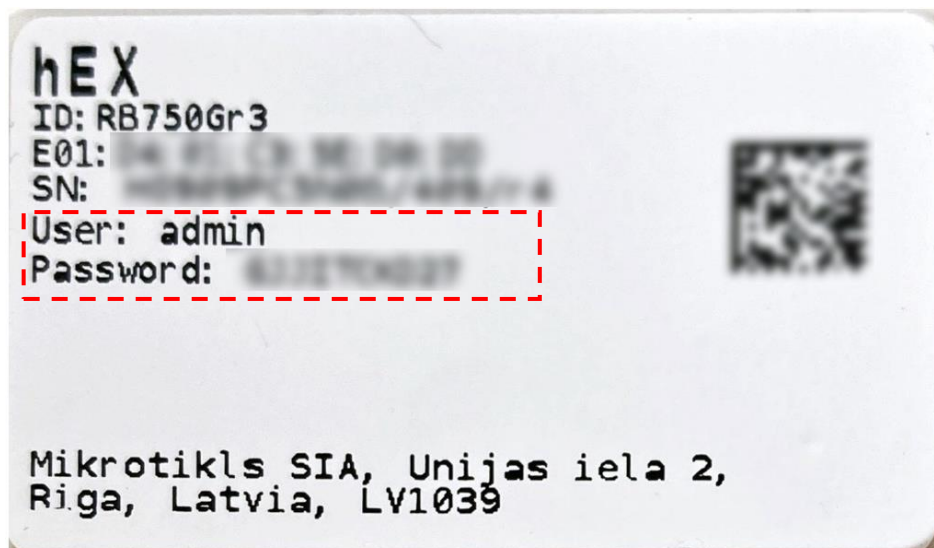
IP アドレス : 192.168.88.1

ユーザ名 : admin

パスワード : 無し※

※ 2024年7月以降にご購入された機器には、セキュリティ強化のため、機器ごとにユニークなパスワードが設定されている場合があります。その場合は本体裏面のラベルの”Password”に記載されたパスワードを入力してログインしてください。(下図の赤枠部分を参照)

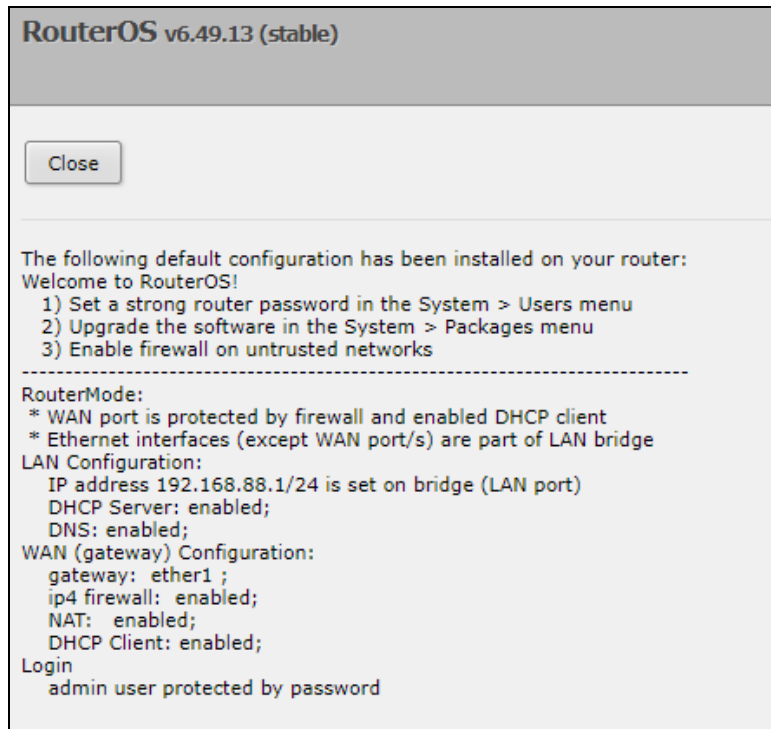
ラベルに Password が記載されていない機器は、初期パスワードは無し(空欄)となります。



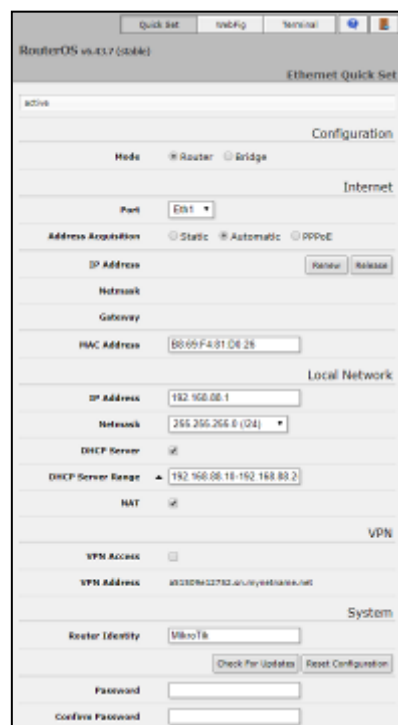
- ログイン手順

- 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 ユーザ名とパスワードを入力して **Log in** をクリックします。

- ③ ログインに成功すると、以下の画面が表示されますので、Close をクリックします。



- ④ Quick Set 画面が表示されます。



- ⑤ 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できます。

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 使用するモードを Mode を Router、Bridge から選択します。

The screenshot shows a configuration window titled "Configuration". At the bottom, 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 the "Internet" configuration screen. It includes the following fields and options:

- Port:** A dropdown menu showing "Eth1".
- Address Acquisition:** Three radio buttons: "Static", "Automatic" (selected), and "PPPoE".
- IP Address:** A text input field with "Renew" and "Release" buttons to its right.
- Netmask:** A text input field.
- Gateway:** A text input field.
- MAC Address:** A text input field containing "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。

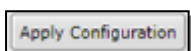
Local Network	
IP Address	<input type="text" value="192.168.88.1"/>
Netmask	<input type="text" value="255.255.255.0 (/24)"/>
DHCP Server	<input checked="" type="checkbox"/>
DHCP Server Range	<input type="text" value="192.168.88.10-192.168.88.2"/>
NAT	<input checked="" type="checkbox"/>

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	<input type="text" value="MikroTik"/>
	<input type="button" value="Check For Updates"/> <input type="button" value="Reset Configuration"/>
Password	<input type="text"/>
Confirm Password	<input type="text"/>
	<input type="button" value="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、Old Password に現在のパスワードを入力し、New Password 及び Confirm Password に新しいパスワードを入力します。

② 不必要なサービスの停止

IP⇒Services を選択し、不必要なサービスは **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。

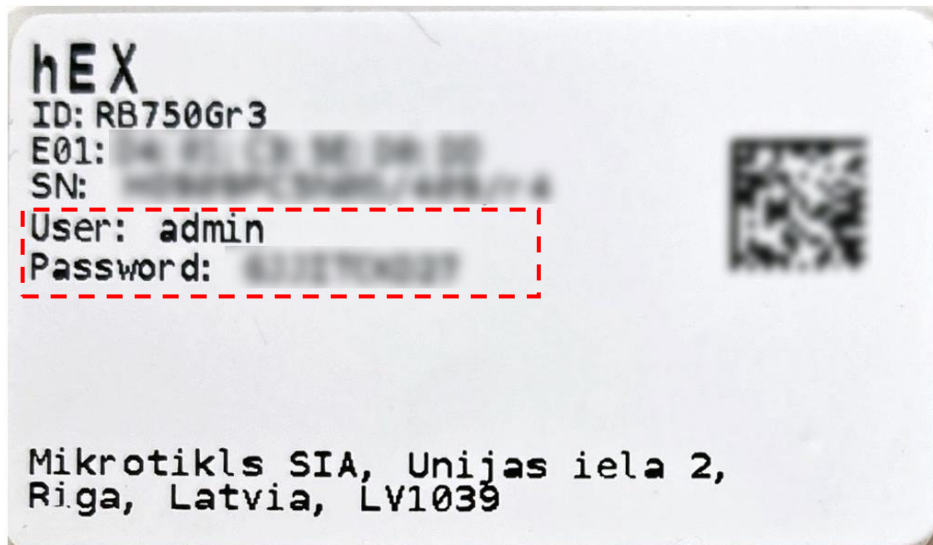
```
telnet 192.168.88.1
```

※ Windows の場合、Telnet クライアントが有効になっている必要があります。

- ② Login に”admin”、Password にパスワードを入力して[Enter]キーを押してログインします。

```
Login: admin  
Password:
```

※ 2024年7月以降にご購入された機器には、セキュリティ強化のため、機器ごとにユニークなパスワードが設定されている場合があります。その場合は本体裏面のラベルの”Password”に記載されたパスワードを入力してログインしてください。(下図の赤枠部分を参照)
ラベルに Password が記載されていない機器は、初期パスワードは無し(空欄)となります。



- ③ ソフトウェアライセンスに関する説明文を読むかどうか表示されますので、不要な場合は”n”キーを押下します。

```
MMM      MMM      KKK      TTTTTTTTTT      KKK
MMMM     MMMM     KKK      TTTTTTTTTT      KKK
MMM MMMM MMM III KKK KKK RRRRRR 000000 TTT III KKK KKK
MMM MM  MMM III KKKKK RRR RRR 000 000 TTT III KKKKK
MMM     MMM III KKK KKK RRRRRR 000 000 TTT III KKK KKK
MMM     MMM III KKK KKK RRR RRR 000000 TTT III KKK KKK

MikroTik RouterOS 6.49.13 (c) 1999-2024 http://www.mikrotik.com/
Do you want to see the software license? [Y/n]: █
```

- ④ “y”キーを押下した場合、“MIKROTIKLS MIKROTIK SOFTWARE END-USER LICENCE AGREEMENT”が表示されます。“ENTER”キーで先に進むか、途中で終わる場合は”q”キーを押下します。

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”の状態では[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
  192.168.88.1/24 192.168.88.0 bridge
1 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
  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
  192.168.88.1/24 192.168.88.0 bridge
1 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できます。

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できます。

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できます。

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						
- D R	bridge	Bridge	1500	1598	68.0 kbps	5.0 kbps
D	ether1	Ethernet	1500	1598	0 bps	0 bps
D	ether2	Ethernet	1500	1598	0 bps	0 bps
D	ether3	Ethernet	1500	1598	0 bps	0 bps
D	ether4	Ethernet	1500	1598	0 bps	0 bps
D	ether5	Ethernet	1500	1598	0 bps	0 bps
D	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。

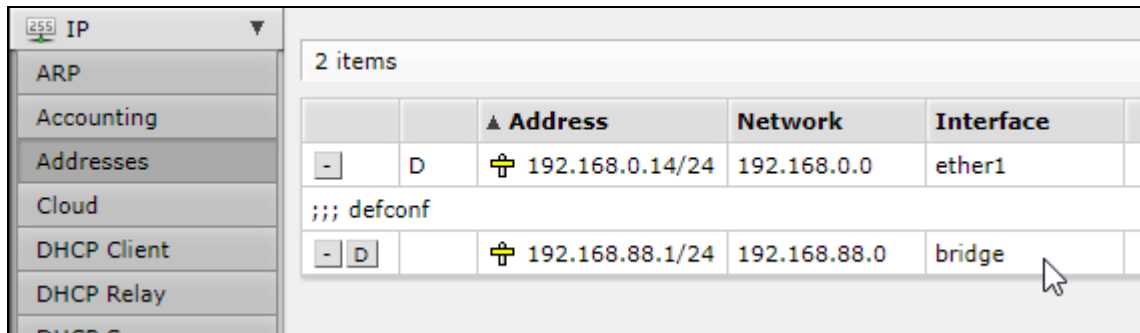
S :ポートがブリッジに所属していることを表します。

```
[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
   bridge
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。

OK Cancel Apply Remove

not invalid

Enabled

Address

Network ▲

Interface

- CLI による設定方法

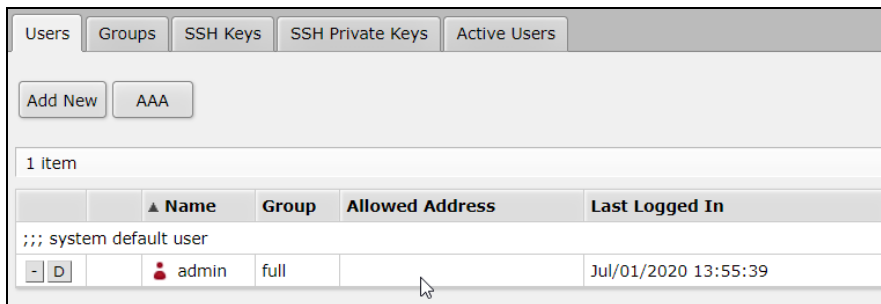
以下のコマンドを入力します。

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

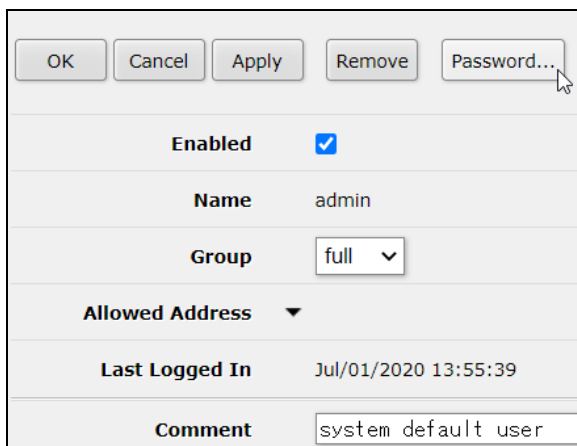
6.3. ログインパスワードの変更

- 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。
(ドメインでの入力は不可)
- ③ 時刻同期が成功すると、各ステータスが表示されます。

The screenshot shows the web interface for configuring the SNTP Client. On the left, a sidebar menu lists various system settings, with 'SNTP Client' highlighted and marked with a red circle and the number 1. The main content area is titled 'SNTP Client' and contains the following configuration options:

- Enabled:** A checkbox that is checked, marked with a red circle and the number 2.
- Mode:** A dropdown menu set to 'unicast'.
- Primary NTP Server:** A text input field containing the IP address '133.243.238.243'.
- Secondary NTP Server:** A dropdown menu.
- Server DNS Names:** A dropdown menu.
- Dynamic Servers:** A section containing several status fields, marked with a red circle and the number 3:
 - Poll Interval:** 512 s
 - Active Server:** 133.243.238.243
 - Last Update From:** 133.243.238.243
 - Last Update:** 00:00:30 ago
 - Last Adjustment:** 929 793 us

- 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。

The screenshot shows the web interface for configuring the Clock. On the left, a sidebar menu lists various system settings, with 'Clock' highlighted. The main content area is titled 'Clock' and contains the following configuration options:

- Time:** A text input field containing '10:15:09'.
- Date:** A text input field containing 'Apr/02/2019'.
- Time Zone Autodetect:** A checkbox that is checked.
- Time Zone Name:** A dropdown menu set to 'Asia/Tokyo', marked with a red circle and the number 4.
- GMT Offset:** +09:00
- DST Active:** A checkbox that is unchecked.

- **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
```

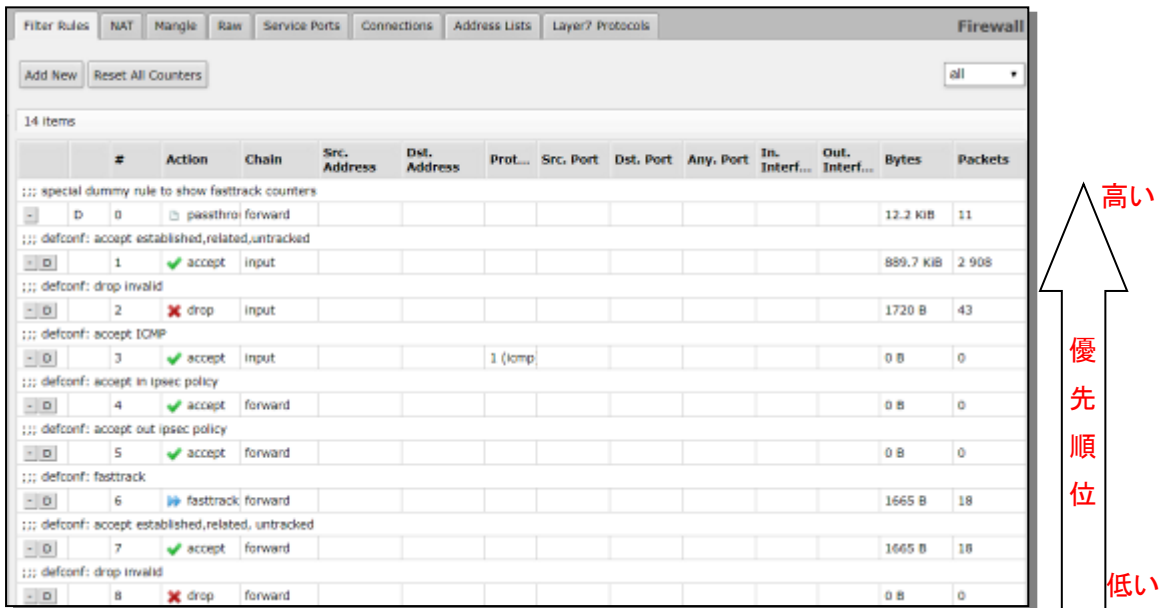
6.5. Firewall の設定方法

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。



#	Action	Chain	Src. Address	Dst. Address	Prot...	Src. Port	Dst. Port	Any. Port	In. Interf...	Out. Interf...	Bytes	Packets
0	passthro	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

高い
優先順位
低い

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。

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

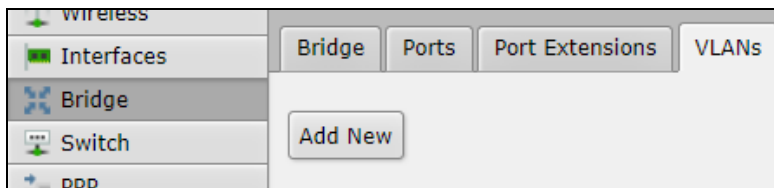
以下の例のように VLAN 設定を行う方法を説明します。

- 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 Bridge⇒VLANs を選択し、Add New をクリックします。



② VLAN100 を作成します。

VLAN IDs に 100 と入力、Tagged に ether5 と bridge、Untagged に ether3 を選択し、OK をクリックします。

The screenshot shows a configuration dialog box for creating a new VLAN. At the top are three buttons: 'OK', 'Cancel', and 'Apply'. Below them is a section with the following settings:

- Enabled:** A checkbox that is checked.
- Bridge:** A dropdown menu set to 'bridge'.
- VLAN IDs:** A text input field containing '100'.
- Tagged:** A section with two dropdown menus. The first is set to 'ether5' and the second is set to 'bridge'.
- Untagged:** A dropdown menu set to 'ether3'.

At the bottom of the dialog are two sections: 'Current Tagged' and 'Current Untagged', which are currently empty.

③ VLAN200 を作成します。

VLAN IDs に 200 と入力、Tagged に ether5 と bridge、Untagged に ether4 を選択し、OK をクリックします。

OK		Cancel	Apply
Enabled	<input checked="" type="checkbox"/>		
Bridge	bridge ▼		
VLAN IDs	▼ 200 ▲		
Tagged	▼ ether5 ▼ ▲		
	▼ bridge ▼ ▲		
Untagged	▼ ether4 ▼ ▲		
Current Tagged			
Current Untagged			

- ④ ether3 の PVID を設定します。

Bridge⇒Ports を選択し、ether3 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

PVID を 100 に設定し、OK をクリックします。

OK Cancel Apply Remove

inactive

Enabled

Interface ether3

Bridge bridge

Horizon

Learn auto

Unknown Unicast Flood

Unknown Multicast Flood

Broadcast Flood

Trusted

Hardware Offload

Multicast Router Temporary Query

Fast Leave

Priority 80 hex

Path Cost 10

Internal Path Cost 10

Edge auto

Point To Point auto

Auto Isolate

Restricted Role

Restricted TCN

BPDU Guard

PVID 100

Frame Types admit all

- ⑤ ether4 の PVID を設定します。

Bridge⇒Ports を選択し、ether4 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

PVID を 200 に設定し、OK をクリックします。

OK Cancel Apply Remove

Inactive

Enabled

Interface: ether4

Bridge: bridge

Horizon: auto

Learn: auto

Unknown Unicast Flood:

Unknown Multicast Flood:

Broadcast Flood:

Trusted:

Hardware Offload:

Multicast Router: Temporary Query

Fast Leave:

Priority: 80 hex

Path Cost: 10

Internal Path Cost: 10

Edge: auto

Point To Point: auto

Auto Isolate:

Restricted Role:

Restricted TCN:

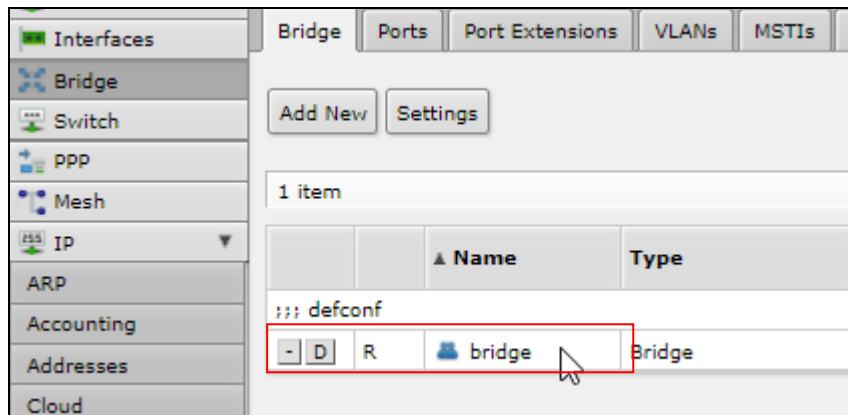
BPDU Guard:

PVID: 200

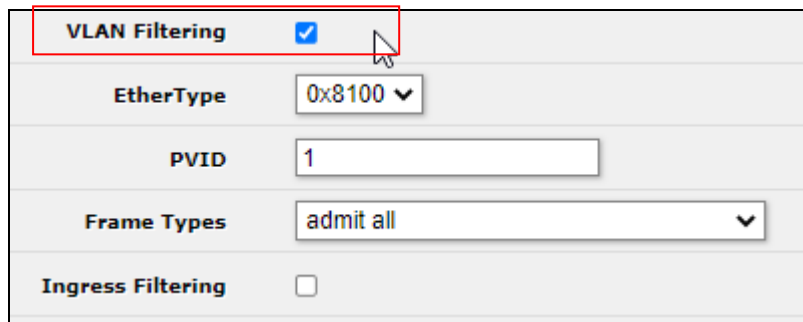
Frame Types: sdmit all

- ⑥ Tag VLAN 機能を有効にします。

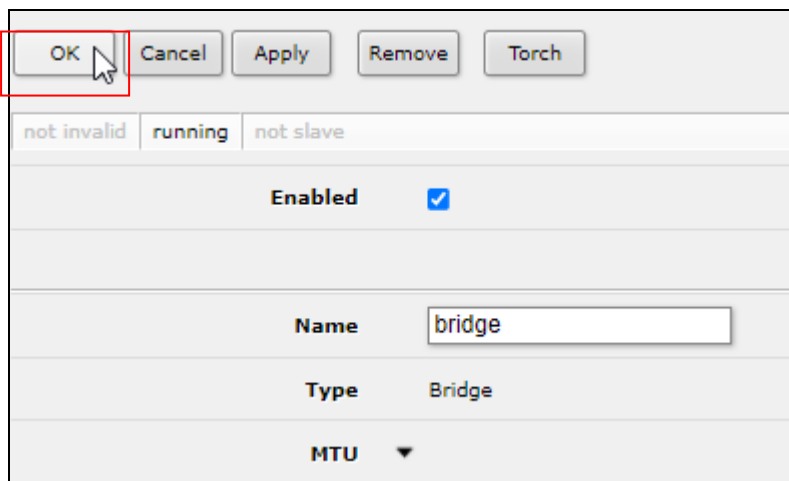
Bridge⇒Bridge を選択し、bridge をクリックします。



表示される画面を下にスクロールして、VLAN Filtering にチェックを入れます。

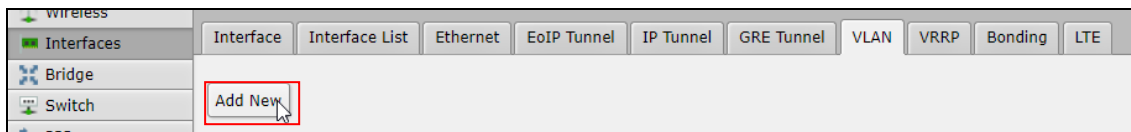


その後、OK をクリックします。



必要に応じて、VLAN に IP アドレスを設定します。

- ⑦ Interface ⇒ VLAN を選択し、Add New をクリックします。



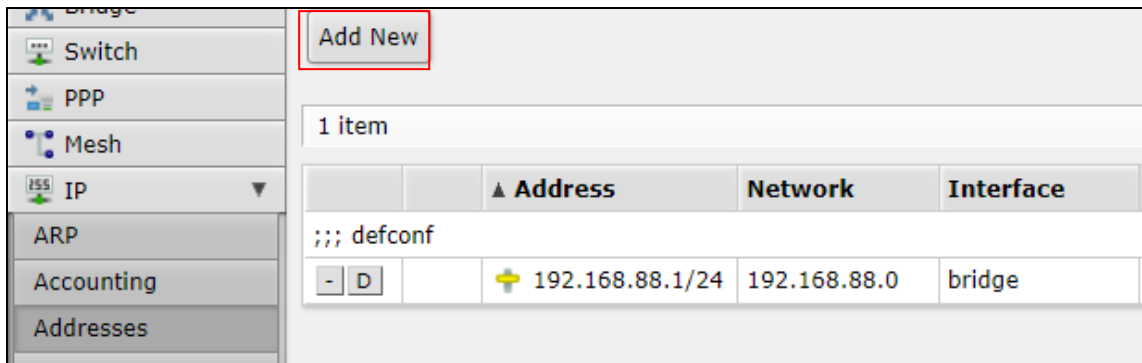
- ⑧ Name に任意の名前、VLAN ID に 100 と入力し、OK をクリックします。

The screenshot shows a configuration dialog box for a new VLAN. At the top are buttons for 'OK', 'Cancel', 'Apply', and 'Torch'. Below are status indicators: 'not invalid', 'not running', and 'not slave'. The 'Enabled' checkbox is checked. The 'Name' field contains 'vlan100'. The 'Type' is set to 'VLAN'. The 'MTU' field contains '1500'. The 'Actual MTU' and 'L2 MTU' fields are empty. The 'MAC Address' section is empty. The 'ARP' dropdown is set to 'enabled'. The 'ARP Timeout' dropdown is set to a default value. The 'VLAN ID' field contains '100'. The 'Interface' dropdown is set to 'bridge'.

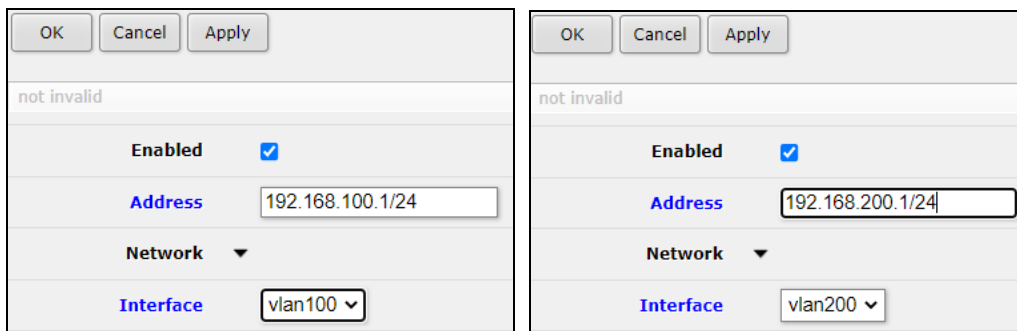
- ⑨ 同様の手順で VLAN 200 を作成します。

The screenshot shows a configuration dialog box for a new VLAN, similar to the previous one. The 'Name' field contains 'vlan200'. The 'VLAN ID' field contains '200'. All other settings (Type, MTU, ARP, Interface) are the same as in the previous dialog.

- ⑩ IP⇒Addresses を選択し、Add New をクリックします。



- ⑪ Address に IP アドレス/サブネットマスクを入力し、Interface に VLAN を選択し、OK をクリックします。



VLAN 間ルーティングを無効にする場合は Firewall に以下のルールを追加します。

Action=drop Chain=forward in-interface=all-vlan out-interface=all-vlan

	#	Action	Chain	Src. Address	Dst. Address	Prot...	Src. Port	Dst. Port	Any. Port	In. Interf...	Out. Interf...
;;; special dummy rule to show fasttrack counters											
-	D	0	passthro	forward							
-	D	1	drop	forward						all vlan	all vlan

- **CLI による設定方法**

- ① VLAN を作成します。

```
/interface bridge vlan
add bridge=bridge tagged=ether5,bridge untagged=ether3 vlan-ids=100
add bridge=bridge tagged=ether5,bridge untagged=ether4 vlan-ids=200
```

- ② PVID を設定します。

```
/interface bridge port
set numbers=1 pvid=100
set numbers=2 pvid=200
```

- ③ Tag VLAN を有効にします。

```
/interface bridge
set numbers=0 vlan-filtering=yes
```

必要に応じて、VLAN に IP アドレスを設定します。

- ④ VLAN インタフェースを作成します。

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

- ⑤ VLAN インタフェースに IP アドレスを設定します。

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

VLAN 間ルーティングを無効にする場合は以下を設定します。(必要な場合のみ)

```
/ip firewall filter
add action=drop chain=forward in-interface=all-vlan out-interface=all-vlan place-before=0
```

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
```

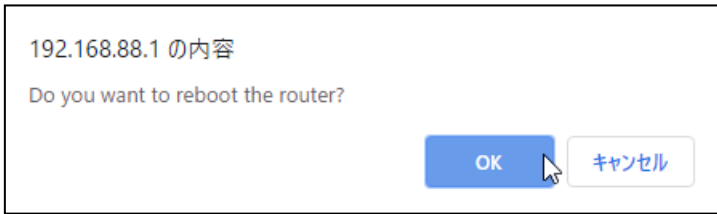
- ③ ネットワークアドレス、デフォルトゲートウェイ、DNS サーバを設定します。

```
/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

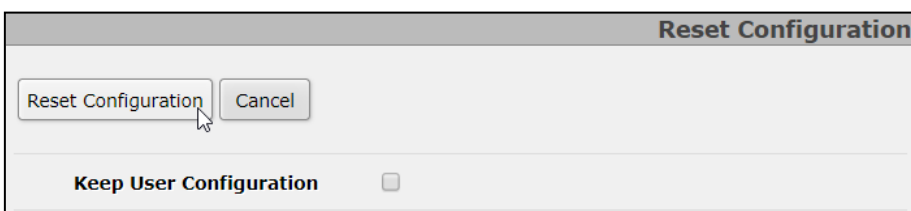
以下のコマンドを入力します。

```
/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。



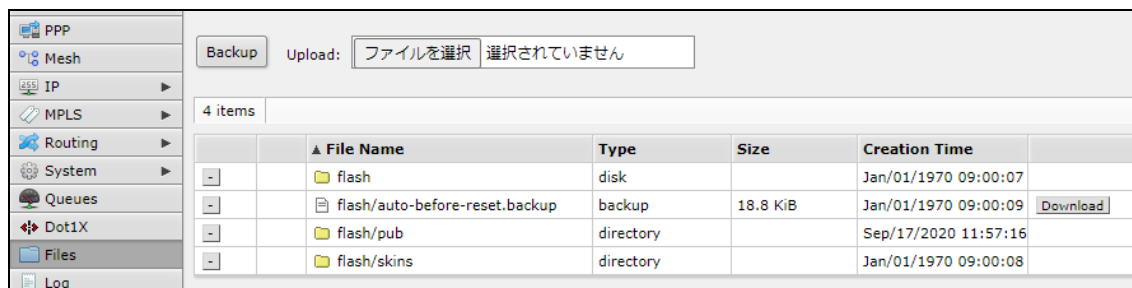
- CLI による設定方法

以下のコマンドを入力します。

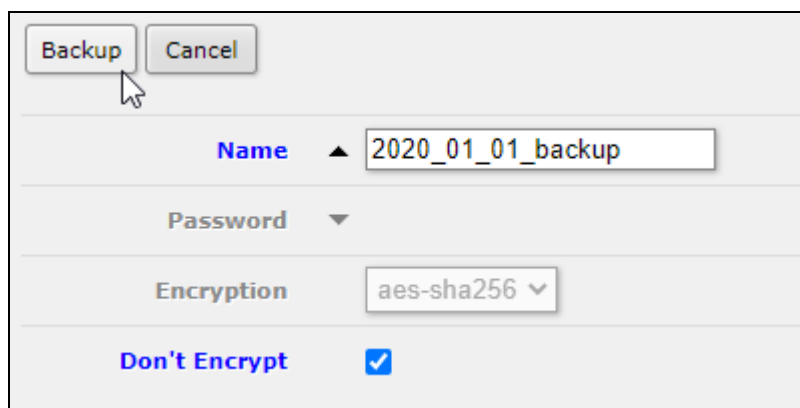
```
/system reset-configuration
Dengerous! Reset anyway? [y/N]: y ← 確認要求が表示されたら”y”を入力します。
system configuration will be reset
```

6.10. 設定のバックアップ

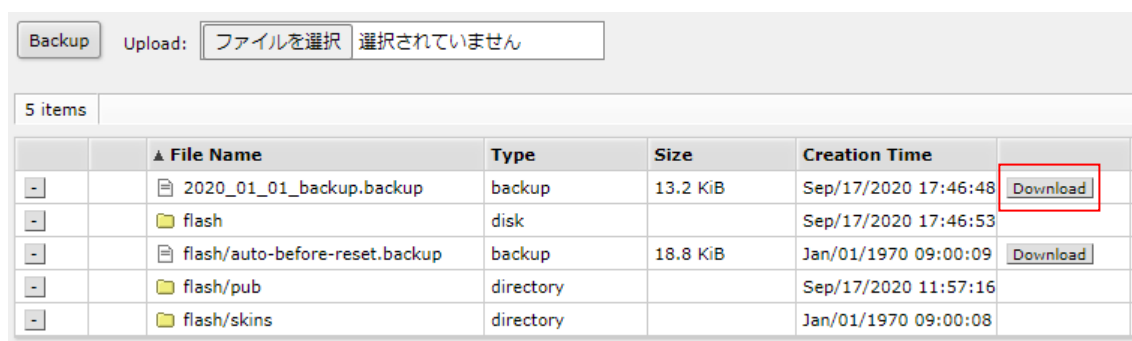
- ① **Files** を選択します。
- ② **Backup** をクリックします。



- 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。
ファイルを暗号化する場合は、「Don't Encrypt」のチェックを外し、Password を入力します。



- 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。

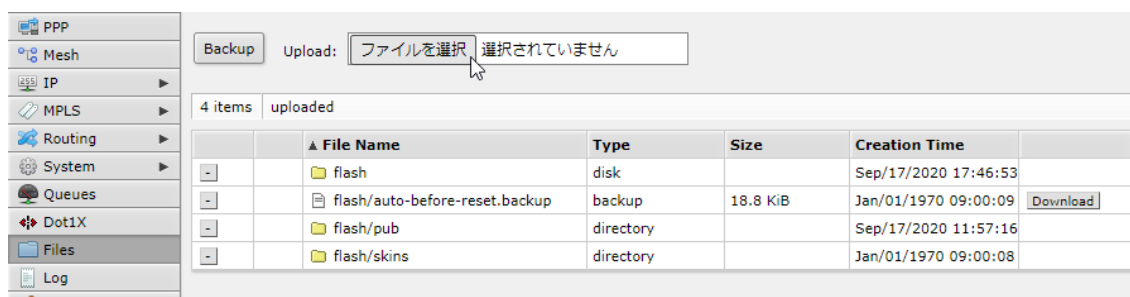


※ 設定を初期化すると、バックアップファイルはルータから削除されますので、必ずダウンロードしてください。

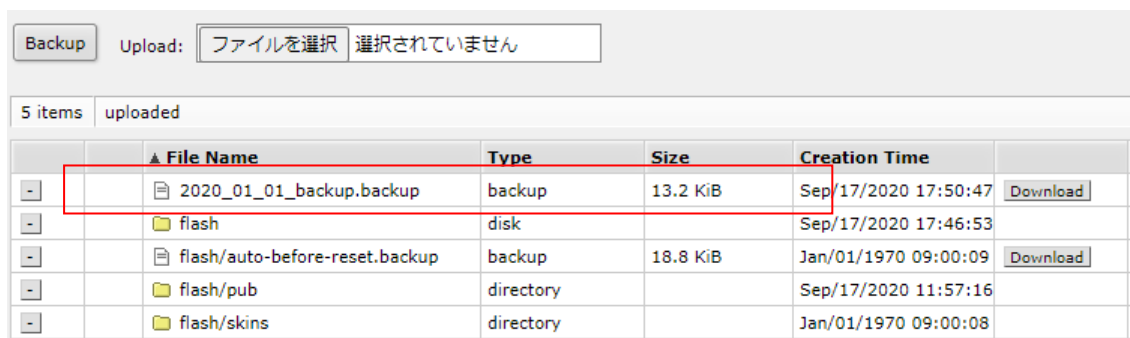
6.11. 設定のリストア

設定のバックアップ・リストアは、バックアップ元の MAC アドレス情報までバックアップされるため、バックアップ元のルータとリストア先のルータが別の機器の場合、リストア先のルータの MAC アドレス情報が上書きされます。

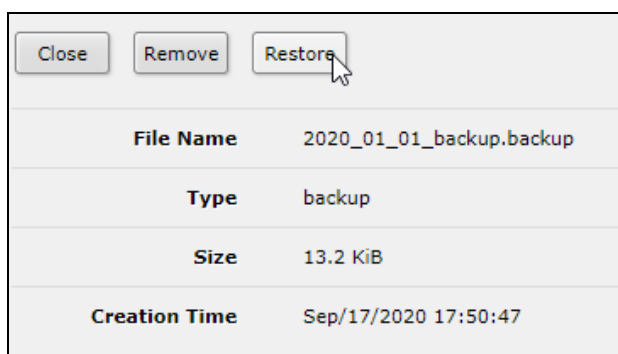
- ① **Files** を選択します。
- ② **ファイルを選択** をクリックして、パソコン上のバックアップファイルをルータにアップロードします。



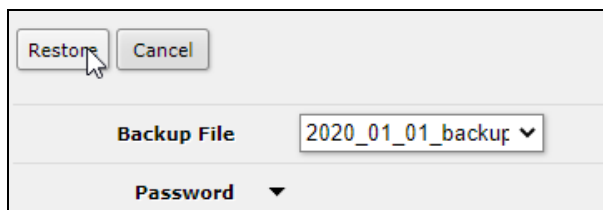
- ③ アップロードが完了したら、リストに追加されたバックアップファイルをクリックします。



- 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。
- ⑦ 再起動が完了したら、画面右上から **Terminal** を選択して、以下のコマンドを入力します。

```
interface ethernet reset-mac-address 0,1,2,3,4
```



```
[admin@MikroTik] > interface ethernet reset-mac-address 0,1,2,3,4
[admin@MikroTik] > |
```

このコマンドを実行することで、MAC アドレス情報まで上書きされていた場合も、機器本来の MAC アドレスに戻すことができます。

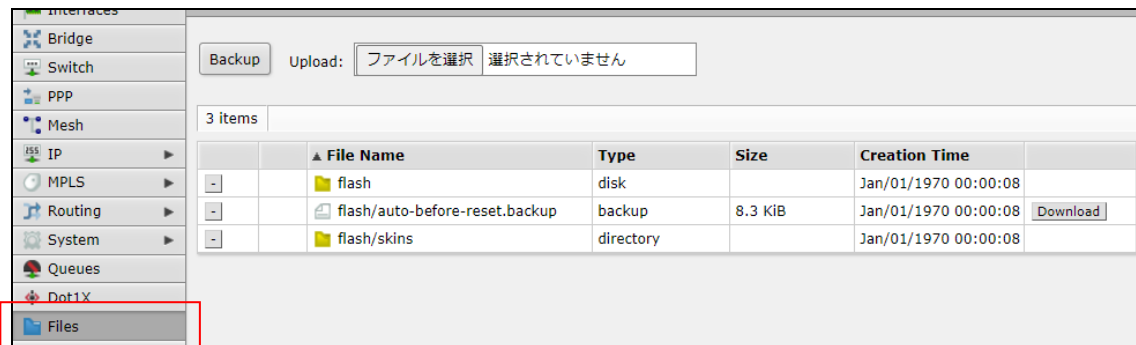
- ※ Bonding Interface を作成していた場合は、この手順で MAC アドレスが初期化されませんので、Bonding インタフェースを一旦 Disable にし、再度 Enable にしてください。

Interfaces		Interface	Interface List	Ethernet	EoIP Tunnel	IP Tunnel	GRE Tunnel	VLAN	VRRP	Bonding	LTE
Bridge Switch PPP Mesh IP MPLS Routing		Add New Monitor Slaves		1 item							
		▲ Name	Type	MTU	Actual MTU	L2 MTU	Tx	Rx			
	R	bonding1	Bonding	1500	1500	1596	0 bps	512			

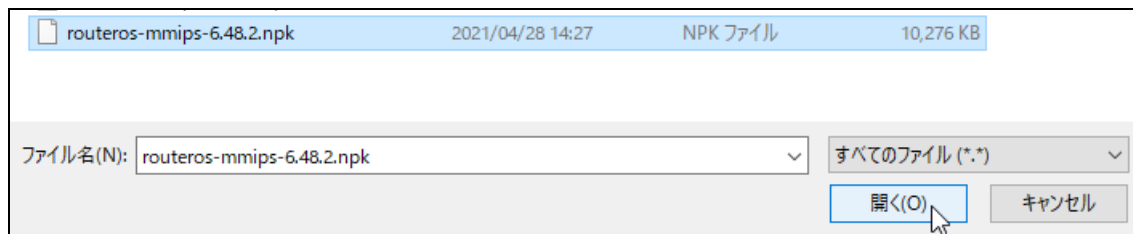
6.12. RouterOS のアップグレード

- ① **Files** を選択します。

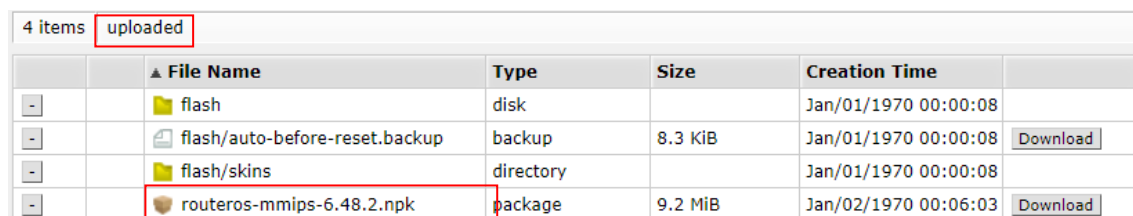
※アップグレードファイルは必ず弊社 HP のダウンロードページのものをご利用ください。



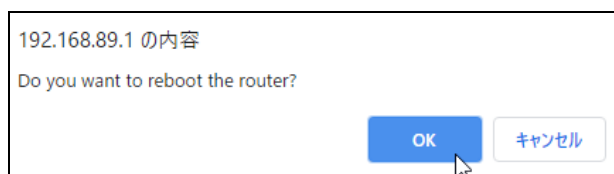
- ② **ファイルを選択** をクリックします。
 ③ ファームウェアファイルを選択して、**開く** をクリックします。



- ④ アップロードしたファイルが画面上に追加され、"uploaded"と表示されたことを確認します。



- ⑤ **System⇒Reboot** をクリックし、確認画面で **OK** をクリックします。



- ⑥ System⇒RouterBOARD を選択し、Upgrade をクリックします。

Upgrade	Settings	USB Power Reset	Mode Button	Reset Button
RouterBOARD	<input checked="" type="checkbox"/>			
Model	RB750Gr3			
Revision	r4			
Serial Number	D5030C0DA4BE			
Firmware Type	mt7621L			
Factory Firmware	6.46.6			
Current Firmware	6.46.6			
Upgrade Firmware	6.48.2			

- ⑦ 確認画面が表示されますので、OK をクリックします。

192.168.89.1 の内容
Do you really want to upgrade firmware?
OK <input type="button" value="キャンセル"/>

- ⑧ System⇒Reboot をクリックし、確認画面で OK をクリックします。

192.168.89.1 の内容
Do you want to reboot the router?
OK <input type="button" value="キャンセル"/>

- ⑨ 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。

RouterBOARD	<input checked="" type="checkbox"/>
Model	RB750Gr3
Revision	r4
Serial Number	D5030C0DA4BE
Firmware Type	mt7621L
Factory Firmware	6.46.6
Current Firmware	6.48.2
Upgrade Firmware	6.48.2

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できます。

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。

- 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。

※ 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	<input checked="" type="checkbox"/>
DDNS Update Interval	▼
Update Time	<input checked="" type="checkbox"/>
Public Address	146.99.216.76
DNS Name	a515 [REDACTED].sn.mynetname.net
Use Local Address	<input type="checkbox"/>

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:
      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)

The screenshot shows the configuration interface for a NAT rule. The top section is titled "not invalid" and contains the following fields:

- Enabled:** A checkbox that is checked.
- Chain:** A dropdown menu set to "dstnat".
- Src. Address:** A dropdown menu.
- Dst. Address:** A dropdown menu.
- Protocol:** A dropdown menu set to "6 (tcp)".
- Src. Port:** A dropdown menu.
- Dst. Port:** A text input field set to "50000".

The bottom section is for the action configuration and contains the following fields:

- Action:** A dropdown menu set to "dst-nat".
- Log:** An unchecked checkbox.
- Log Prefix:** A dropdown menu.
- To Addresses:** A text input field set to "192.168.88.253".
- To Ports:** A text input field set to "50000".

Red arrows point from the following Japanese text to the corresponding fields in the screenshot:

- Chain は dstnat を選択します。
- プロトコルを選択します。
- ポート番号を設定します。
- Action は dst-nat を選択します。
- フォワード先の IP アドレスを入力します。
- 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。

- 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。

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 contains several settings with red arrows pointing to them from the right side of the page:

- Enabled:** A checkbox that is checked. An arrow points to it with the text 'チェックを入れます。' (Check this).
- Max MTU:** A text box containing the value '1450'.
- Max MRU:** A text box containing the value '1450'.
- MRRU:** A dropdown menu.
- Keepalive Timeout:** A text box containing the value '30'.
- Default Profile:** A dropdown menu showing 'RW-cfg'. An arrow points to it with the text '④の手順で作成したプロファイルを選択します。' (Select the profile created in step 4).
- Authentication:** A group of radio buttons. 'mschap2' is selected. An arrow points to this group with the text '認証方式を選択します。' (Select the authentication method).
- Use IPsec:** A dropdown menu showing 'yes'. An arrow points to it with the text 'Yesを選択し、シークレット(事前共有キー)を設定します。' (Select Yes and set the secret (pre-shared key)).
- IPsec Secret:** A text box containing several asterisks '*****'.
- Caller ID Type:** A dropdown menu showing 'ip address'.

- 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	<input checked="" type="checkbox"/>
Name	<input type="text" value="default"/>
Auth. Algorithms	<input type="checkbox"/> md5 <input checked="" type="checkbox"/> sha1 <input type="checkbox"/> null <input type="checkbox"/> sha256 <input type="checkbox"/> sha512
Encr. Algorithms	<input type="checkbox"/> null <input type="checkbox"/> des <input checked="" type="checkbox"/> 3des <input type="checkbox"/> aes-128 cbc <input type="checkbox"/> aes-192 cbc <input checked="" type="checkbox"/> aes-256 cbc <input type="checkbox"/> blowfish <input type="checkbox"/> twofish <input type="checkbox"/> camellia-128 <input type="checkbox"/> camellia-192 <input type="checkbox"/> camellia-256 <input type="checkbox"/> aes-128 ctr <input type="checkbox"/> aes-192 ctr <input type="checkbox"/> aes-256 ctr <input type="checkbox"/> aes-128 gcm <input type="checkbox"/> aes-192 gcm <input type="checkbox"/> aes-256 gcm
Lifetime	▼
PFS Group	<input type="text" value="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。

The screenshot shows the configuration window for a default IPsec profile. The settings are as follows:

- Name:** default
- Hash Algorithms:** sha1
- Encryption Algorithm:**
 - des
 - aes-256
 - camellia-128
 - camellia-256
 - 3des
 - aes-192
 - blowfish
 - camellia-192
- DH Group:**
 - modp768
 - ec2n155
 - modp1536
 - modp3072
 - modp6144
 - ecp256
 - ecp521
 - modp1024
 - ec2n185
 - modp2048
 - modp4096
 - modp8192
 - ecp384
- Proposal Check:** obey
- Lifetime:** 1d 00:00:00
- Lifebytes:** (dropdown arrow)
- 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。

The screenshot shows the configuration window for a new PPP Secret profile. The settings are as follows:

- Enabled:**
- Name:** user
- Password:** (masked with dots)
- Service:** l2tp
- Caller ID:** (dropdown arrow)
- 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	<input checked="" type="checkbox"/>
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

11	accept	Input	17 (udp)	500,1701,4500
;;; defconf: drop all not coming from LAN				
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
```

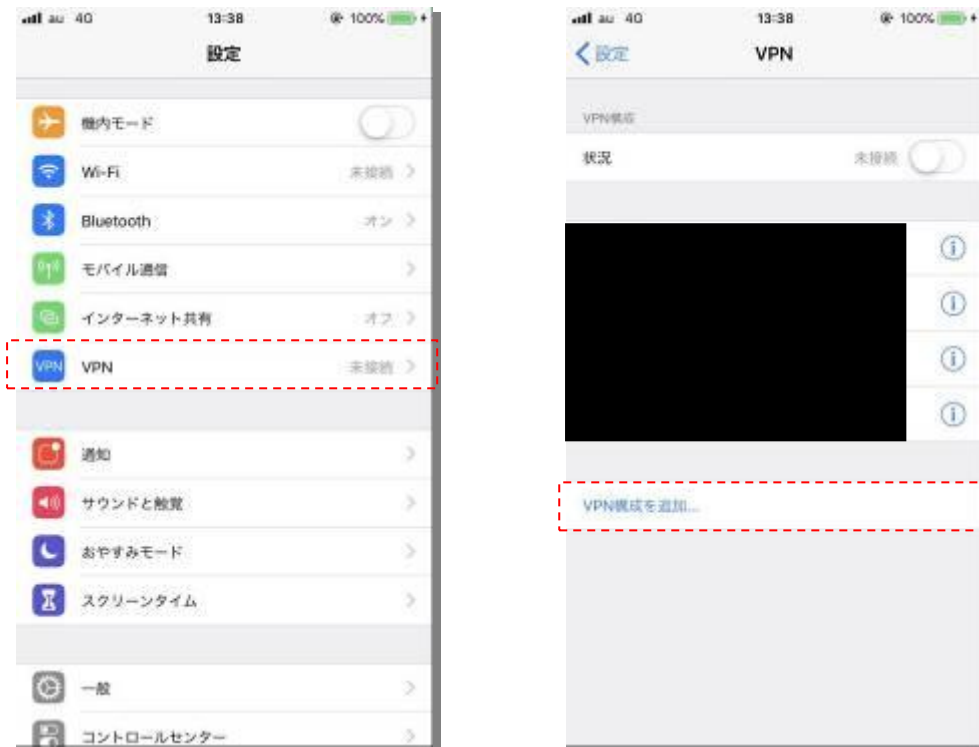
- ⑦ ファイアウォールのルールを追加します。

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

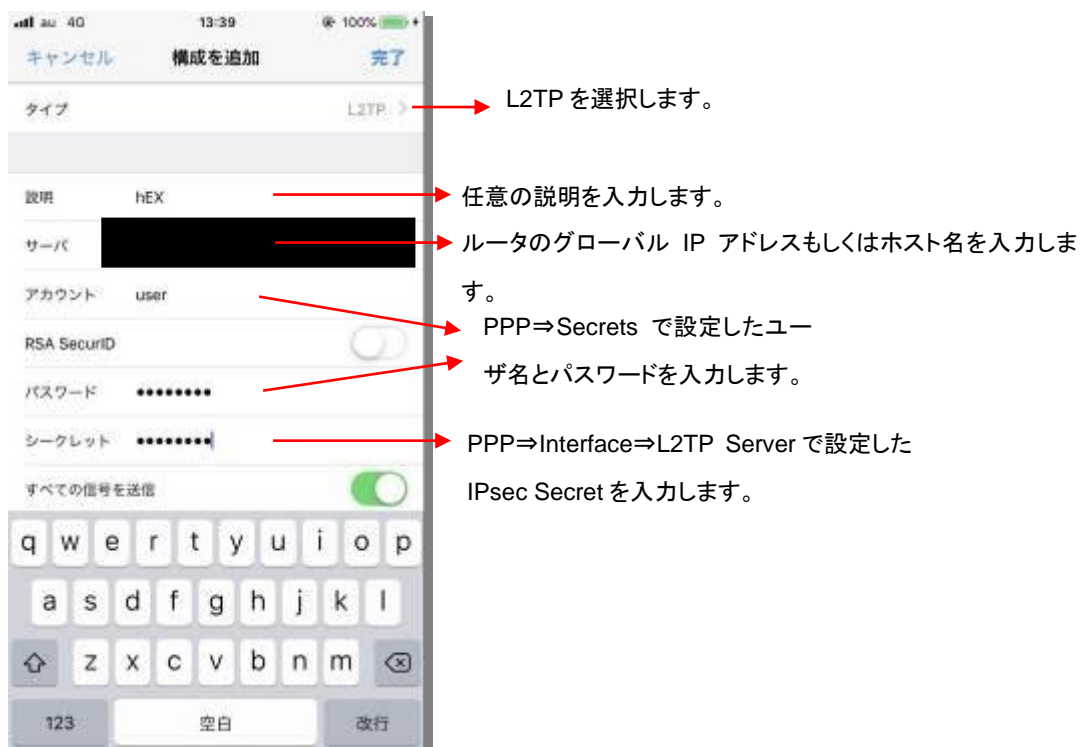
9.2. L2TP/IPSec VPN クライアントの設定

◆ スマートフォンの場合(iPhone)

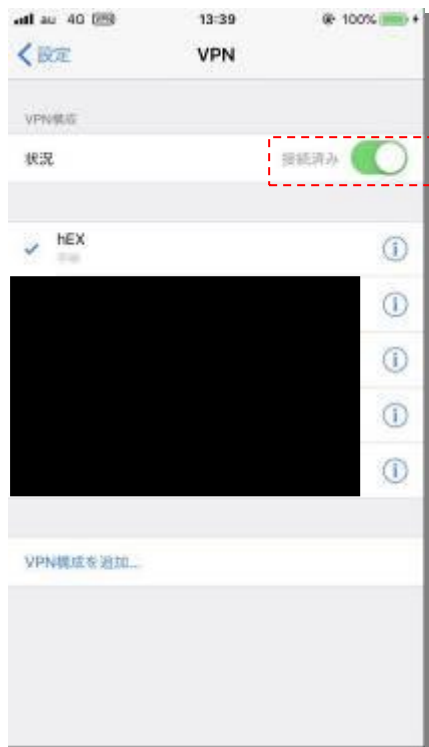
- ① **設定⇒VPN**を選択し、**VPN 構成を追加…**をタップします。



- 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
[blacked out]

VPNの種類
事前共有キーを使った L2TP/IPsec

事前共有キー
[blacked out]

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)
[blacked out]

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

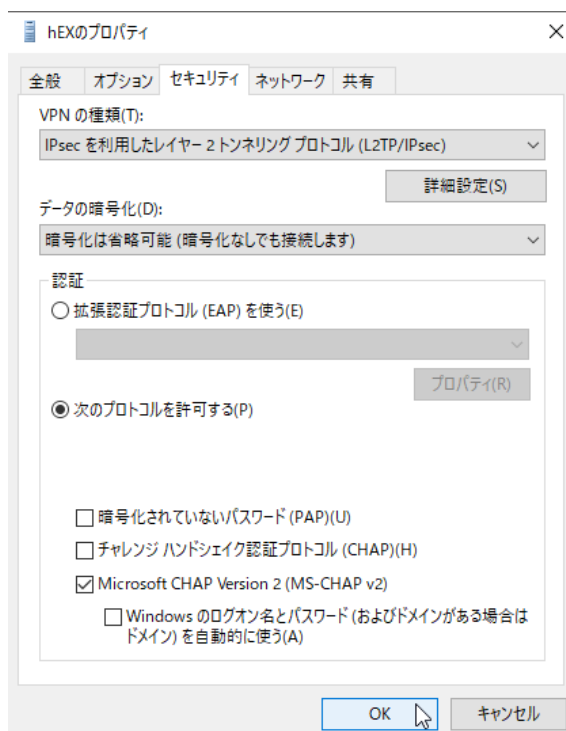
共有の詳細オプションを変更する

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。

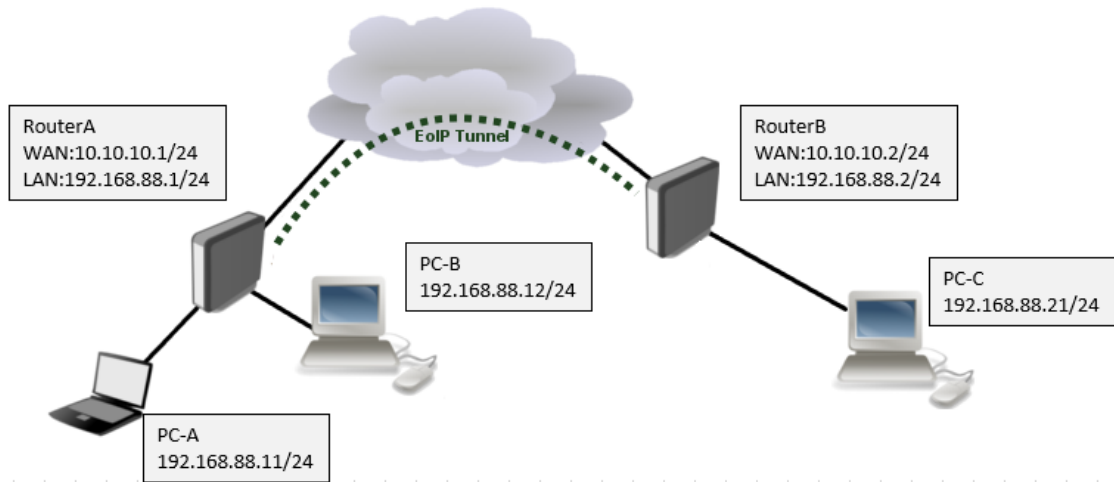


- ⑥ 接続します。



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	<input checked="" type="radio"/> Router <input type="radio"/> Bridge
Port	Eth1
Address Acquisition	<input checked="" type="radio"/> Static <input type="radio"/> Automatic <input type="radio"/> 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	<input type="checkbox"/>
NAT	<input checked="" type="checkbox"/>

- 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	<input checked="" type="checkbox"/>
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	<input checked="" type="checkbox"/>
Allow Fast Path	<input type="checkbox"/>

- 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	<input checked="" type="checkbox"/>
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	<input checked="" type="checkbox"/>
Chain	input
Src. Address	▼
Dst. Address	▼
Protocol	<input type="checkbox"/> 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	<input checked="" type="radio"/> Router <input type="radio"/> Bridge
Port	Eth1 ▼
Address Acquisition	<input checked="" type="radio"/> Static <input type="radio"/> Automatic <input type="radio"/> 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	<input type="checkbox"/>
NAT	<input checked="" type="checkbox"/>

- 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	<input checked="" type="checkbox"/>	
Name	<input type="text" value="eoip-tunnel1"/>	
Type	EoIP Tunnel	
MTU	▼	
Actual MTU	1408	
L2 MTU	65535	
MAC Address	<input type="text" value="FE:DC:CE:60:67:13"/>	
ARP	<input type="text" value="enabled"/>	
ARP Timeout	▼	
Local Address	▼	→ Router B の WAN 側アドレスを入力します。
Remote Address	<input type="text" value="10.10.10.1"/>	→ Router A の WAN 側アドレスを入力します。
Tunnel ID	<input type="text" value="1"/>	→ 任意のトンネル ID を入力します。
IPsec Secret	<input type="text" value="*****"/>	→ 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	<input type="text" value="00:00:10"/> <input type="text" value="10"/>	
DSCP	<input type="text" value="inherit"/>	
Dont Fragment	<input type="text" value="no"/>	
Clamp TCP MSS	<input checked="" type="checkbox"/>	→ チェックを外します。
Allow Fast Path	<input type="checkbox"/>	

- 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	<input checked="" type="checkbox"/>	
Interface	<input type="text" value="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	<input type="text" value="bridge"/>	
Horizon	▼	
Learn	<input type="text" value="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...
;;; 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

10.3. ステータスの確認(Web の場合)

Interface⇒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

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 keepalive=10s,10
```

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
```

- ⑦ NTP クライアントの設定を追加します。(例では、ntp.nict.jp を使用)

```
/system ntp client  
set enabled=yes primary-ntp=61.205.120.130
```

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 keepalive=10s,10
```

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
```

- ⑦ NTP クライアントの設定を追加します。(例では、ntp.nict.jp を使用)

```
/system ntp client  
set enabled=yes primary-ntp=61.205.120.130
```

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)

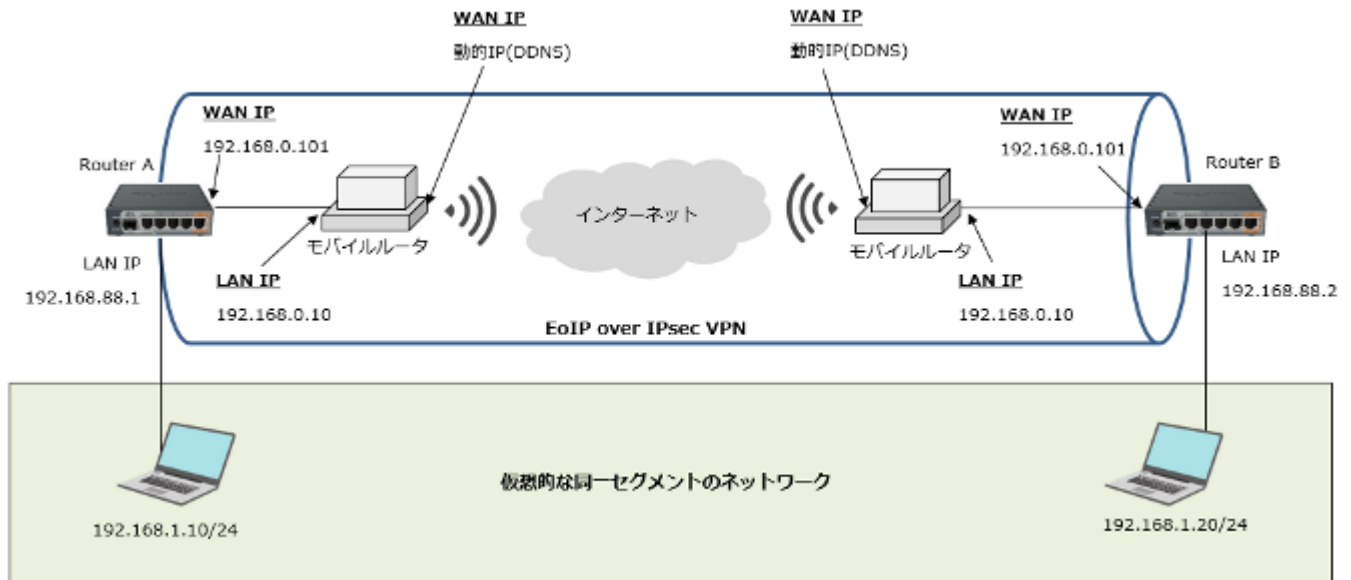
```
[admin@MikroTik] > /interface eoip print
Flags: X - disabled, R - running
0 R name="eoip-tunnel1" mtu=auto actual-mtu=1408 l2mtu=65535
  mac-address=FE:0D:FA:A5:83:9F arp=enabled arp-timeout=auto loop-protect=default
  loop-protect-status=off loop-protect-send-interval=5s loop-protect-disable-time=5m
  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

- ⑧ 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
```

- ⑨ 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
```

- ⑩ WAN の DHCP-client 機能を無効にします。

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

- ⑪ LAN の DHCP-Server 機能を無効にします。

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

- ⑫ DNS Server を設定します。

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

- ⑬ 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。

- ⑭ 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 clamp-tcp-mss=no keepalive=10s,5
```

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。

- ⑮ EoIP を Bridge に追加します。

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

- ⑯ 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
```

- ⑰ NTP クライアントの設定を追加します。(例では、ntp.nict.jp を使用)

```
/system ntp client
set enabled=yes primary-ntp=61.205.120.130
```

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 clamp-tcp-mss=no keepalive=10s,5
```

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
```

- ⑩ NTP クライアントの設定を追加します。(例では、ntp.nict.jp を使用)

```
/system ntp client
set enabled=yes primary-ntp=61.205.120.130
```

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)

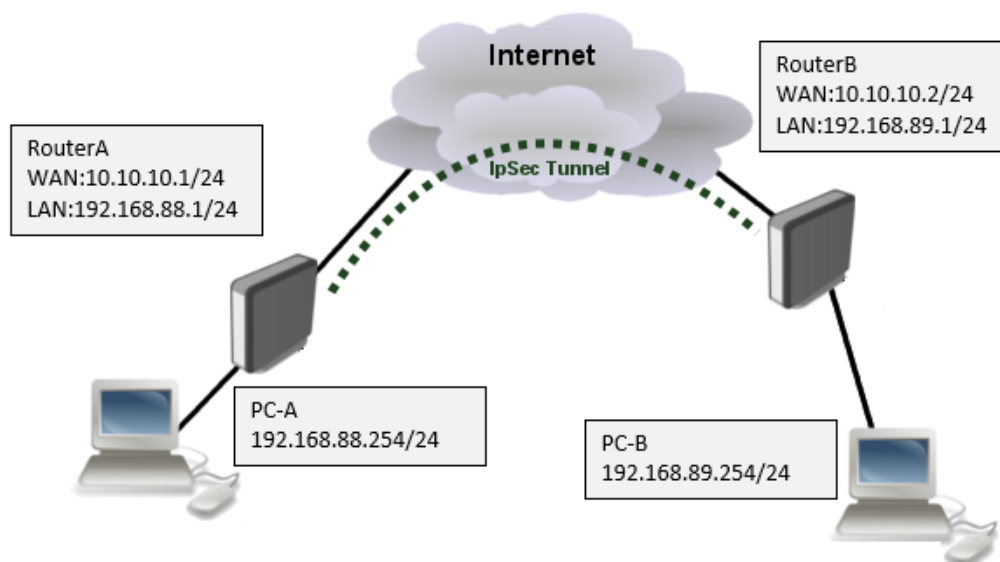
```
[admin@MikroTik] > /interface eoip print
Flags: X - disabled, R - running
0 R name="eoip-tunnel1" mtu=auto actual-mtu=1408 l2mtu=65535
  mac-address=FE:0D:FA:A5:83:9F arp=enabled arp-timeout=auto loop-protect=default
  loop-protect-status=off loop-protect-send-interval=5s loop-protect-disable-time=5m
  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	<input checked="" type="radio"/> Router <input type="radio"/> Bridge
Port	Eth1 ▼
Address Acquisition	<input checked="" type="radio"/> Static <input type="radio"/> Automatic <input type="radio"/> 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	<input type="checkbox"/>
NAT	<input checked="" type="checkbox"/>

- 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	<input checked="" type="checkbox"/>	チェックを入れて、L2TP サーバを有効にします。
Max MTU	<input type="text" value="1450"/>	
Max MRU	<input type="text" value="1450"/>	
MRRU	▼	
Keepalive Timeout	<input type="text" value="30"/>	
Default Profile	<input type="text" value="default"/>	
Max Sessions	▼	
Authentication	<input checked="" type="checkbox"/> mschap2 <input checked="" type="checkbox"/> mschap1 <input checked="" type="checkbox"/> chap <input checked="" type="checkbox"/> pap	
Use IPsec	<input type="text" value="required"/>	required を選択し、IPsec での暗号化を有効にします。
IPsec Secret	<input type="text" value="secret"/>	IPsec Secret を入力します。
Caller ID Type	<input type="text" value="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	<input checked="" type="checkbox"/>	
Name	<input type="text" value="L2TP-01"/>	任意のユーザ名を設定します。
Password	<input type="text" value="testtest"/>	任意のパスワードを設定します。
Service	<input type="text" value="l2tp"/>	l2tpを選択します。
Caller ID	▼	
Profile	<input type="text" value="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	<input type="text" value="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

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	<input checked="" type="radio"/> Static <input type="radio"/> Automatic <input type="radio"/> 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	<input checked="" type="checkbox"/>
DHCP Server Range	▲ 192.168.89.10-192.168.89
NAT	<input type="checkbox"/>

- 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	<input checked="" type="checkbox"/>	
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	<input checked="" type="checkbox"/>	RouterA 側で設定した IPsec Secret を入力します。
IPsec Secret	secret	

- 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	<input checked="" type="checkbox"/>	
Dst. Address	<input type="text" value="192.168.88.0/24"/>	RouterA の LAN 側ネットワークを入力します。
Gateway	<input type="text" value="l2tp-out1"/> reachable	L2TP クライアントのインターフェースを選択します。
Check Gateway	<input type="text"/>	
Type	<input type="text" value="unicast"/>	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。

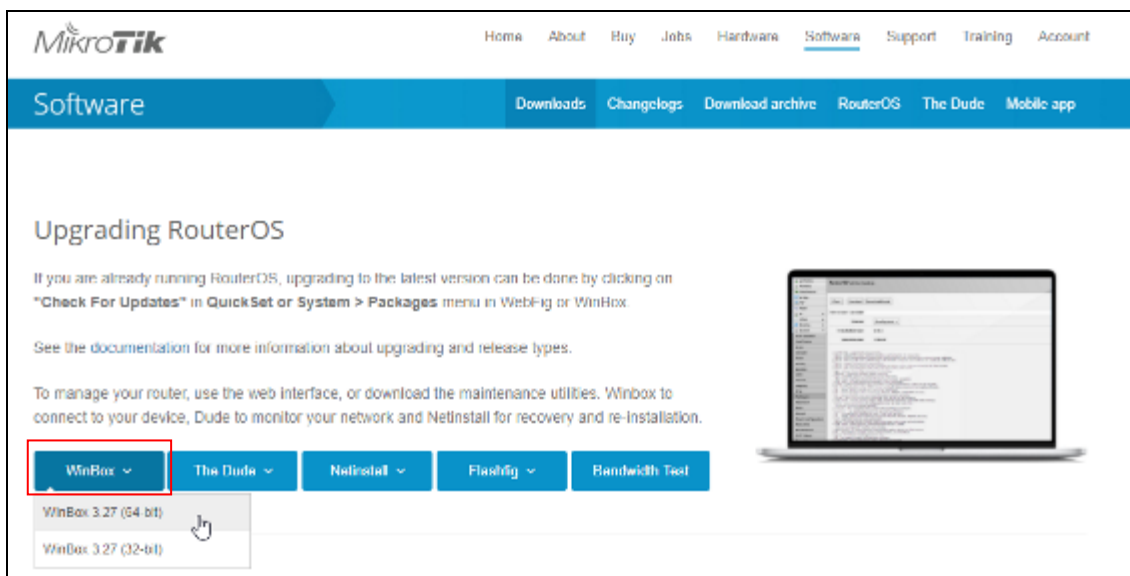
```
/ip route  
add distance=1 gateway=192.168.0.10  
add distance=1 dst-address=192.168.88.0/24 gateway=l2tp-out1
```

13.IP アドレスを忘れてしまった、初期化が上手くいかない場合

もし、IP アドレスを忘れてしまった場合や初期化してもログイン出来ない場合は、Mikrotik のルータ管理ツールである WinBox をお試しください。

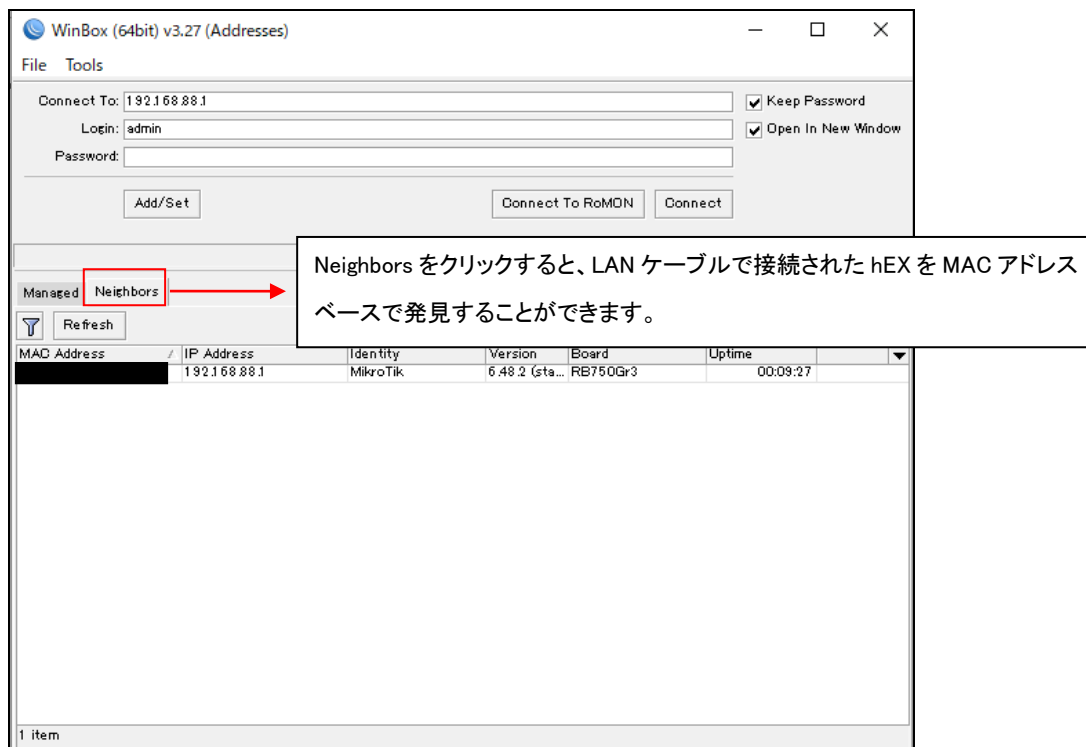
WinBox では、IP アドレスを持っていないルータであっても、MAC アドレス経由で設定変更を行うことが出来ます。

- ① Mikrotik の HP (<https://mikrotik.com/download>) から、WinBox をダウンロードします。
お使いの Windows のバージョンに合わせて 32bit/64bit を選択してください。

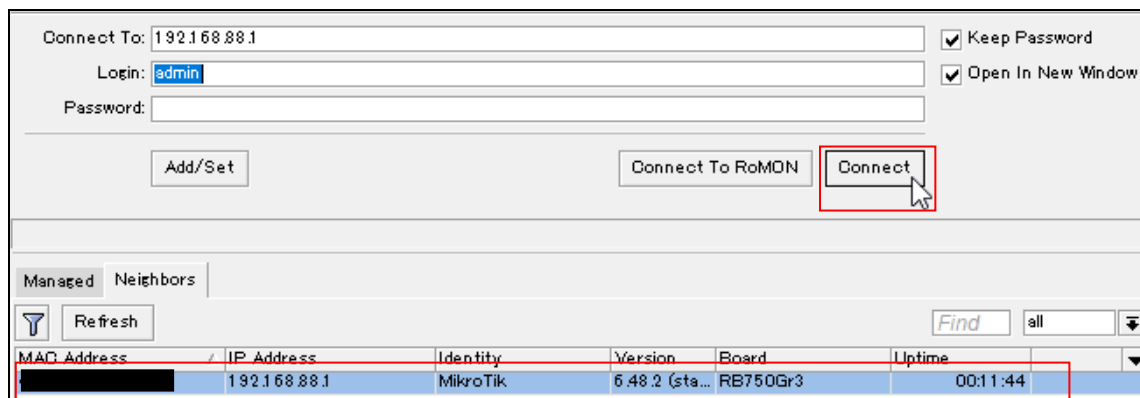


- ② ダウンロードしたファイル (WinBox64.exe または WinBox.exe) をダブルクリックして起動します。

- ③ 起動後の画面は以下の通りとなります。



- ④ 発見した hEX をクリックし、**Connect** ボタンをクリックすることで GUI を開くことができます。



- ⑤ その後の基本的な操作は WEBFig(WEBGUI)と相違ありません。

admin@192.168.88.1 (MikroTik) - WinBox (64bit) v6.48.2 on hEX (mmips)

Session Settings Dashboard

Safe Mode Session: 192.168.88.1

Interface List

Interface Interface List Ethernet EoIP Tunnel IP Tunnel GRE Tunnel VLAN VRRP Bonding LTE

+ - ✓ ✕ 📄 🗑️ Detect Internet

	Name	Type	Actual MTU	L2 MTU	Tx	Rx
::: de foon f						
R	bridge	Bridge	1500	1536	57.8 kbps	
	ether1	Ethernet	1500	1536	0 bps	
RS	ether2	Ethernet	1500	1536	58.5 kbps	
S	ether3	Ethernet	1500	1536	0 bps	
S	ether4	Ethernet	1500	1536	0 bps	
S	ether5	Ethernet	1500	1536	0 bps	

Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
MPLS
Routing
System
Queues
Files
Log
RADIUS
Tools
New Terminal
Dot1X
Partition
Make Supoutrif
Manual
New WinBox
Exit

14. 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>

15. 各ルータの処理能力について

15.1. 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

15.2. 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

16. 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°C
規格・認定	VCCI Class A、RoHS10 物質
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°C
規格・認定	VCCI Class A、RoHS10 物質
製品保証期間	1 年間

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

受付時間：平日(土日祝日、年末年始、当社休業日を除く) 9:00～17:00

TEL: 0570-060030

問合せフォーム: https://hytec.co.jp/contact/technical_support_form.html

