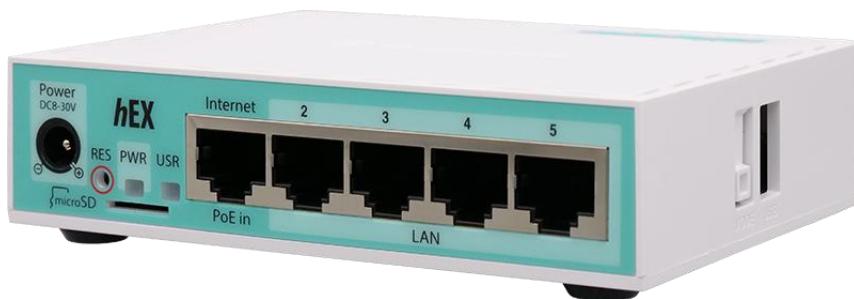




有線 5 ポート VPN ルータ

hEX シリーズ

取扱説明書



HYTEC INTER Co., Ltd.

第 4.2 版

ご注意

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

改版履歴

第1版	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
第4.2版	2025年04月18日	v6.49.18 でのリセットボタンでの初期化時の注意点を追記

ご使用上の注意事項

- 本製品及び付属品をご使用の際は、取扱説明書に従って正しい取り扱いをしてください。
- 本製品は、一般事務用、通常の産業等の一般的用途を想定した製品であり、ハイセイフティ用途*での設備や機器としての使用またはこれらに組込んでの使用は意図されておりません。これらの設備や機器、システムなどに本製品を使用され、本製品の故障等により、人身事故、火災事故、社会的な損害などが生じても当社はいかなる責任も負いかねます。
お客様が、本製品をハイセイフティ用途に使用される場合は、必要な安全性を確保する措置を施す等 十分な配慮をお願いします。
*: 極めて高度な信頼性や安全性が要求され、機器の故障、誤動作により、信頼性や安全性が確保されない場合、生命、身体や財産等に損害を及ぼす恐れがある用途
- 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	8
2. 梱包物一覧	8
3. 製品外観	9
3.1. hEX lite	9
3.2. hEX	10
4. WebFig へのログイン	11
4.1. Quick Set 画面について	13
4.2. インターネットに接続する前に	15
5. CLI(Telnet/SSH)へのログイン	16
5.1. CLI の基本機能について	18
5.2. CLI の一般的なコマンドについて	19
6. 基本設定	22
6.1. イーサネットインターフェースの状態確認	22
6.2. IP アドレスの変更	24
6.3. ログインパスワードの変更	25
6.4. 時刻同期の設定	26
6.5. Firewall の設定方法	28
6.6. タグベース VLAN の設定方法	31
6.7. DHCP サーバの設定方法	40
6.8. 本体の再起動	42
6.9. 本体の初期化方法	42
6.10. 設定のバックアップ	43
6.11. 設定のリストア	44
6.12. RouterOS のアップグレード	46
7. DDNS 機能の設定方法	48
7.1. DDNS 機能の有効(Web の場合)	48
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	51
8.1. ポートフォワーディングの設定(Web の場合)	51
8.2. ポートフォワーディングの設定(CLI の場合)	52
9. L2TP/IPSec を使用したリモートアクセス VPN の設定方法	53
9.1. L2TP/IPSec VPN サーバの設定	53
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	63
10.1. RouterA の設定(Web の場合)	63
10.2. RouterB の設定(Web の場合)	66
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)	71
10.6. ステータスの確認(CLI の場合)	72
11. 動的 IP のモバイルルータを使用した EoIP/IPSec の設定方法	73
11.1. RouterA の設定	74
11.2. RouterB の設定	76
11.3. ステータスの確認	78
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)	83
12.3. RouterA の設定(CLI の場合)	85
12.4. RouterB の設定(CLI の場合)	86
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	87
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	91
15.1. Ethernet スループット	91
15.2. IPsec スループット	92
16. 製品仕様	93

17. 製品保証	95
----------------	----

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。

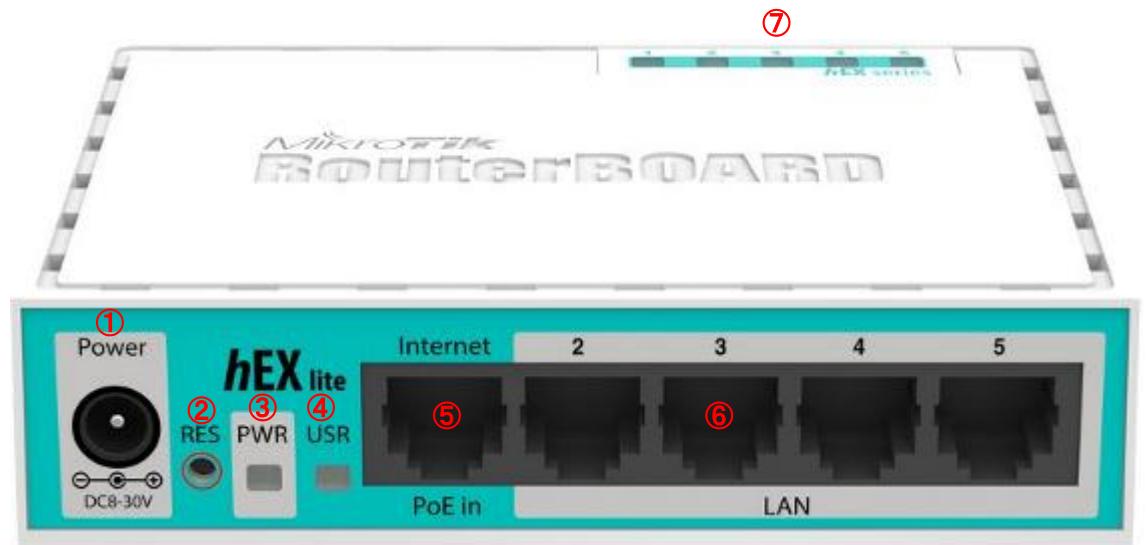
2. 梱包物一覧

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

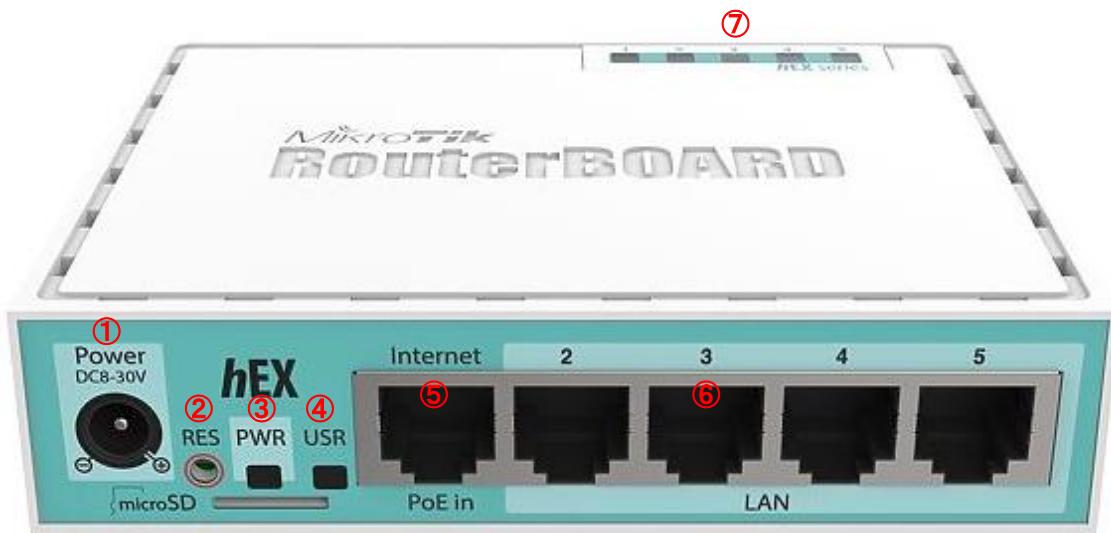


#	表示	説明
①	<u>Power</u>	付属の AC アダプタを接続します。
②	<u>RES</u>	リセットボタンです。
③	<u>PWR</u>	電源 LED です。 電源が ON の時に青点灯します。
④	<u>USR</u>	ユーザに割り当てられた LED です。 <code>/system routerboard leds</code> にて任意のイベントを割り当てることが出来ます。
⑤	<u>Internet</u>	Ether1 ポートです。 WAN ポートとして動作します。
⑥	<u>2~5</u>	Ether2~5 ポートです。 LAN ポートとして動作します。
⑦	<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。
- ※ V6.49.18 以降、リセットボタンによる初期化を行った場合は Current Firmware のバージョンが
が Factory Firmware に戻るため、"6.12. RouterOS のアップグレード" の⑥の手順を行い、再度
Current Firmware のバージョンを変更してください。

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。 <code>/system routerboard leds</code> 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>	Ether1 ポートです。 WAN ポートとして動作します。
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。
- ※ V6.49.18 以降、リセットボタンによる初期化を行った場合は Current Firmware のバージョンが
が Factory Firmware に戻るため、"6.12. RouterOS のアップグレード"の⑥の手順を行い、再度
Current Firmware のバージョンを変更してください。

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できます。

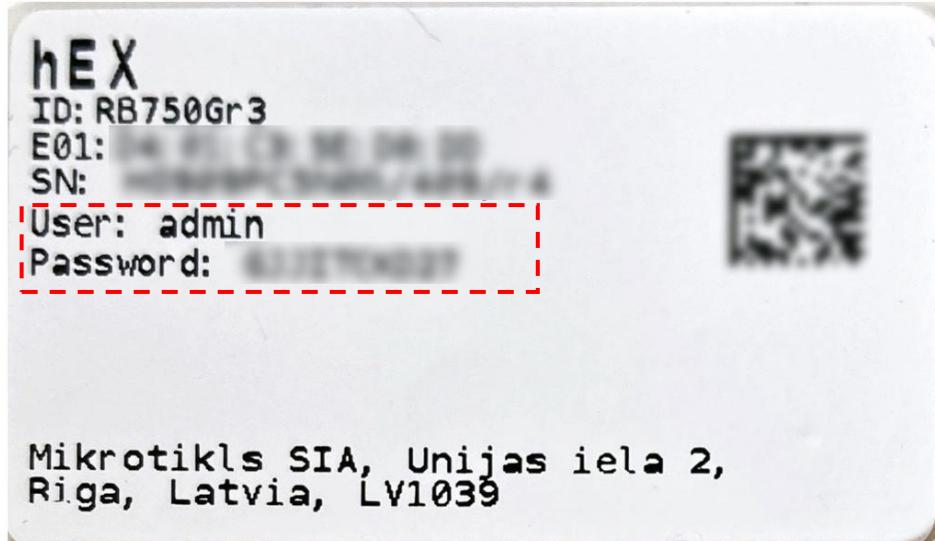
- ログイン初期設定

IP アドレス : 192.168.88.1

ユーザ名 : admin

パスワード : 無し※

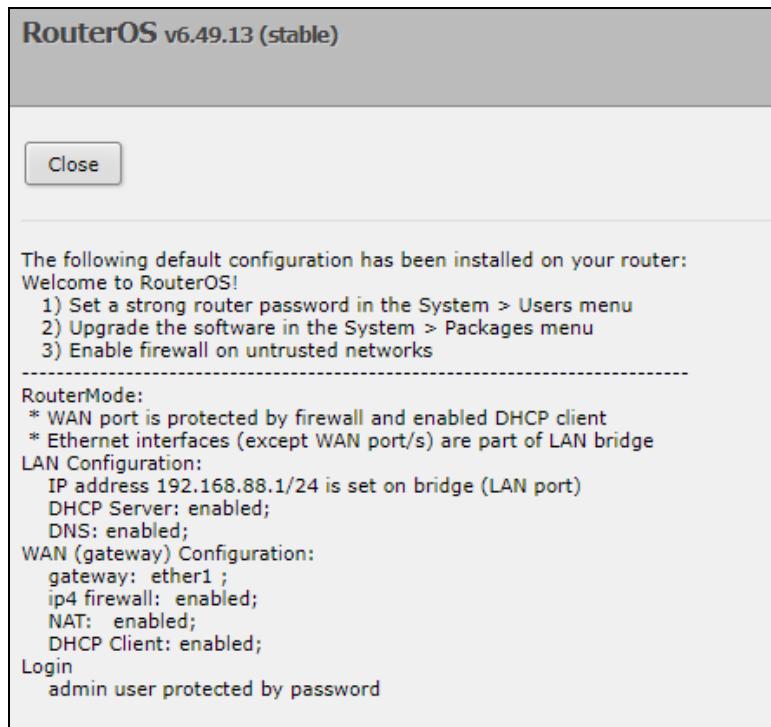
※ 2024 年 7 月以降にご購入された機器には、セキュリティ強化のため、機器ごとにユニークなパスワードが設定されている場合があります。その場合は本体裏面のラベルの”Password”に記載されたパスワードを入力してログインしてください。(下図の赤枠部分を参照)
ラベルに Password が記載されていない機器は、初期パスワードは無し(空欄)となります。



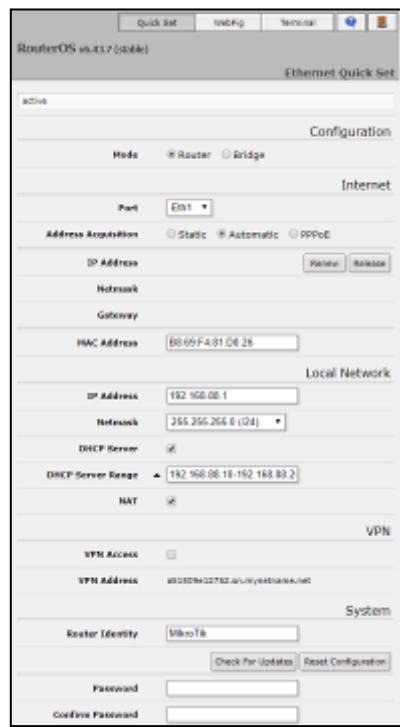
- ログイン手順

- 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。

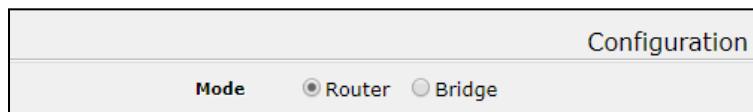


- ⑤ 画面右上の WebFig をクリックすることで、WebFig の画面を開くことが出来ます。

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出来ます。

- ① 使用するモードを Router、Bridge から選択します。



- ② Internet に関する設定を行います。

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	<input checked="" type="checkbox"/>
DHCP Server Range	▲ 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	MikroTik
<input type="button" value="Check For Updates"/> <input type="button" value="Reset Configuration"/>	
Password	<input type="password"/>
Confirm Password	<input type="password"/>
<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。

Old Password	<input type="text"/>
New Password	<input type="password"/>
Confirm Password	<input type="password"/>

② 不必要なサービスの停止

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

		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

		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。

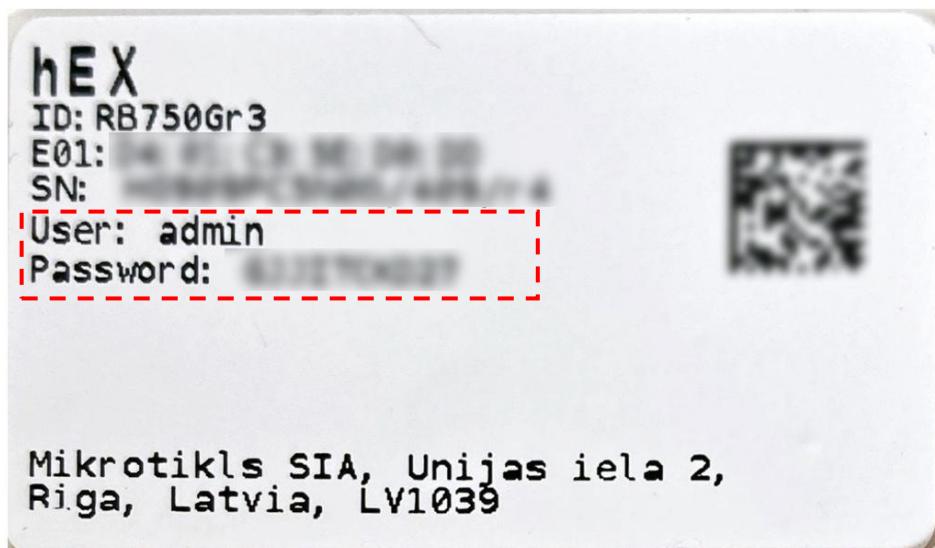
- ② Login に”admin”、Password にパスワードを入力して[Enter]キーを押してログインします。

```
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。

```
      MMMM      MMMM      KKK          TTTTTTTTTTTT      KKK
      Mmmm      Mmmm      Kkk          TTTTTTTTTTTT      Kkk
      MMMM MMMM  III KKK KKK RRRRRR  000000  TTT  III KKK KKK
      MM  MM  III KKKKKK   RRR RRR  000 000  TTT  III KKKKKK
      MM  MM  III KKK KKK RRRRRR  000 000  TTT  III KKK KKK
      MM  MM  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[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      192.168.88.0     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      192.168.88.0     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      192.168.88.0     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できます。

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      192.168.88.0    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できます。

```
[admin@MikroTik] /ip address> print
Flags: X - disabled, I - invalid, D - dynamic
# ADDRESS           NETWORK           INTERFACE
0 ;;; defconf      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      192.168.88.0     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      192.168.88.0     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ーフェースの状態確認

- Web による確認方法

Interface を選択すると、インター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
-	D	RS	ether1	Ethernet	1500	1598	0 bps
-	D	S	ether2	Ethernet	1500	1598	0 bps
-	D	S	ether3	Ethernet	1500	1598	0 bps
-	D	S	ether4	Ethernet	1500	1598	0 bps
-	D	S	ether5	Ethernet	1500	1598	0 bps
-	D	S	sfp1	Ethernet	1500	1600	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、インターフェースの状態を確認することが出来ます。

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。

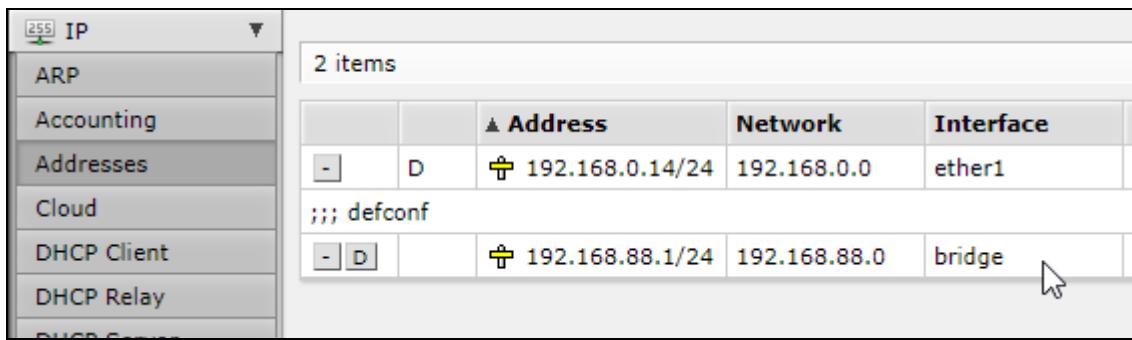
S : ポートがブリッジに所属していることを表します。

#	NAME	TYPE	ACTUAL-MTU	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

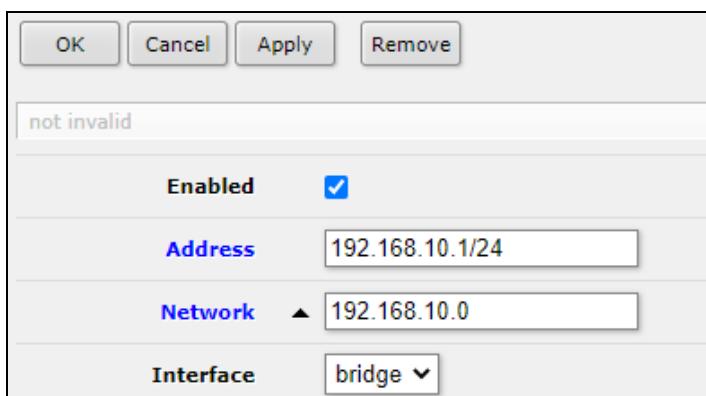
- ① **IP⇒Addresses** を選択します。
- ② bridge インタフェースをクリックします。



The screenshot shows the 'IP' configuration menu on the left with 'Addresses' selected. The main window displays a table titled '2 items' with two entries:

		Address	Network	Interface
-	D	192.168.0.14/24	192.168.0.0	ether1
;;; defconf				
-	D	192.168.88.1/24	192.168.88.0	bridge

- ③ IP アドレスを変更して、OK をクリックします。



The dialog box contains the following fields:

- OK, Cancel, Apply, Remove buttons at the top.
- A status message: "not invalid".
- Enabled**: checked.
- Address**: 192.168.10.1/24
- Network**: 192.168.10.0
- Interface**: bridge

- 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。

	Name	Group	Allowed Address	Last Logged In
;;; system default user	admin	full		Jul/01/2020 13:55:39

- ③ Password..をクリックして、新しいパスワードを設定します。

OK Cancel Apply Remove Password...

Enabled

Name admin

Group full

Allowed Address ▾

Last Logged In Jul/01/2020 13:55:39

Comment system default user

- 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。

- 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。

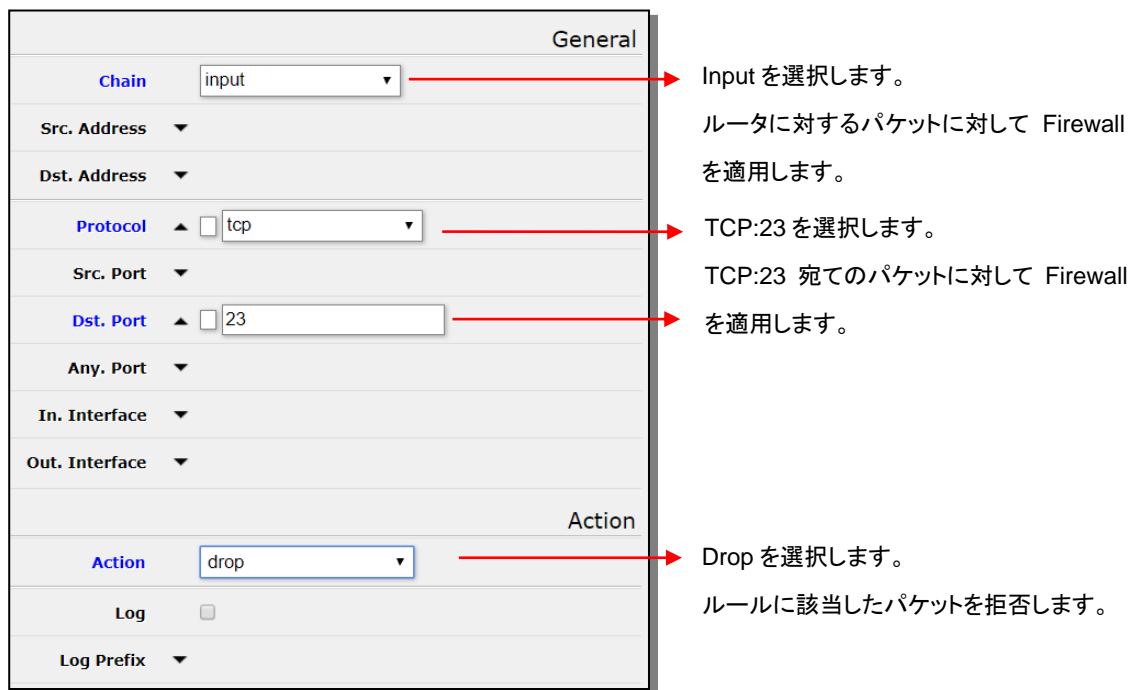
優先順位を変更する場合は、優先順位を変更したいルールをドラッグアンドドロップして移動させます。



The diagram illustrates the priority order of firewall rules. A vertical arrow points upwards, indicating increasing priority. To the right of the arrow, the words "高い" (High) at the top and "低い" (Low) at the bottom are written vertically, corresponding to the rule numbers 1 and 8 respectively.

#	Action	Chain	Src. Address	Dst. Address	Prot...	Src. Port	Dst. Port	Any. Port	In. Interf...	Out. Interf...	Bytes	Packets
::: special dummy rule to show fasttrack counters												
- 0	pastrn 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。



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 を適用するインター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。

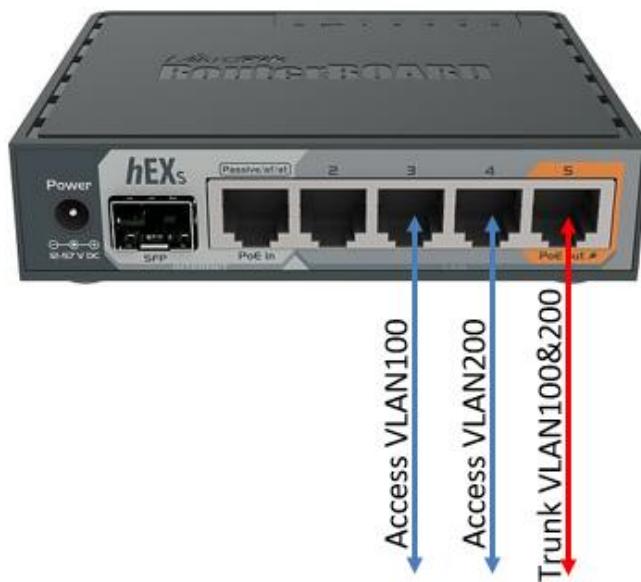
```
/ip firewall filter  
add action=drop chain=input protocol=tcp dst-port=23 place-before=1
```

※ 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できます。

6.6. タグベース VLAN の設定方法

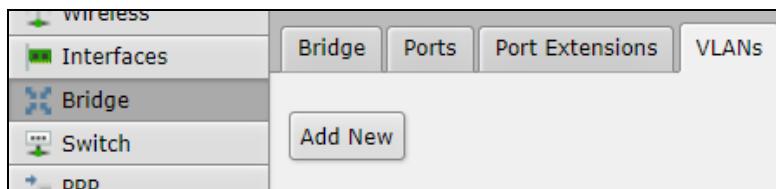
以下の例のように VLAN 設定を行う方法を説明します。

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



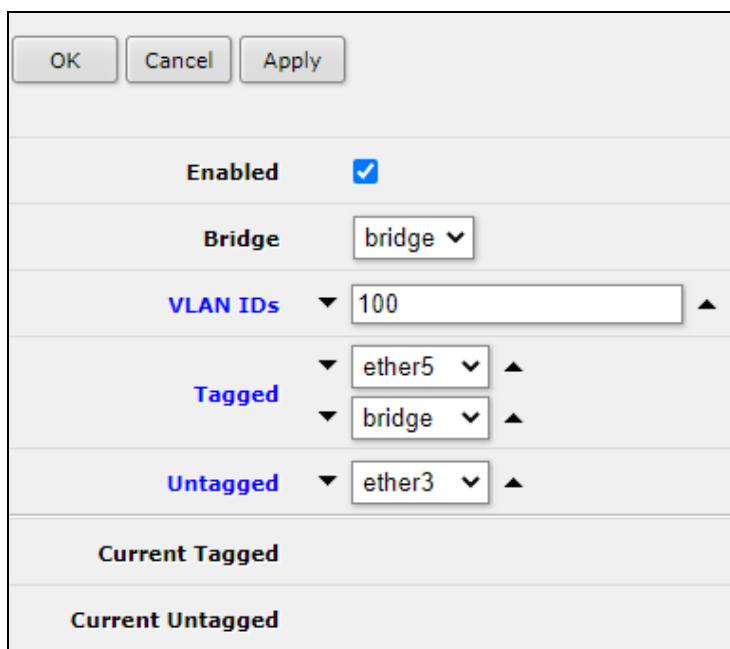
- Web による設定方法

- 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。

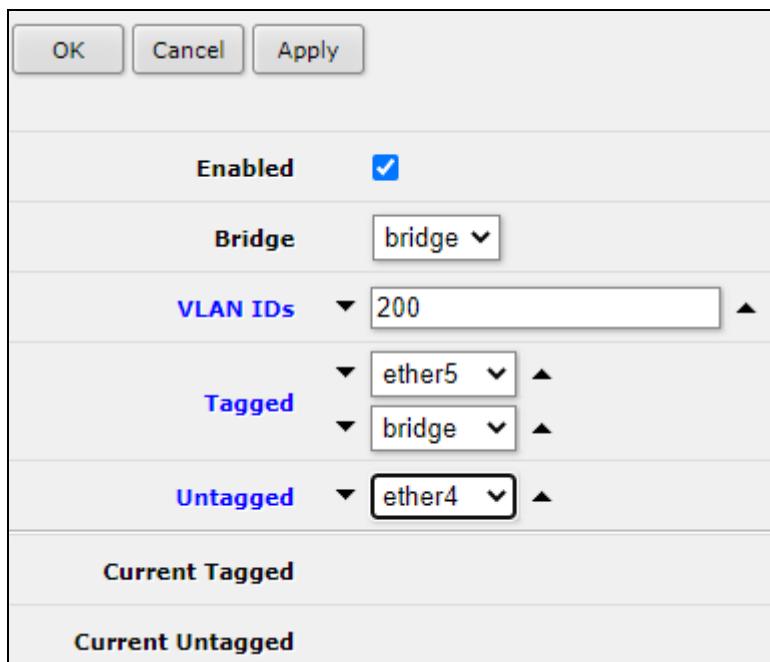
VLAN IDs に 100 と入力、Tagged に ether5 と bridge、Untagged に ether3 を選択し、OK をクリックします。



Enabled	<input checked="" type="checkbox"/>
Bridge	bridge
VLAN IDs	100
Tagged	ether5 bridge
Untagged	ether3
Current Tagged	
Current Untagged	

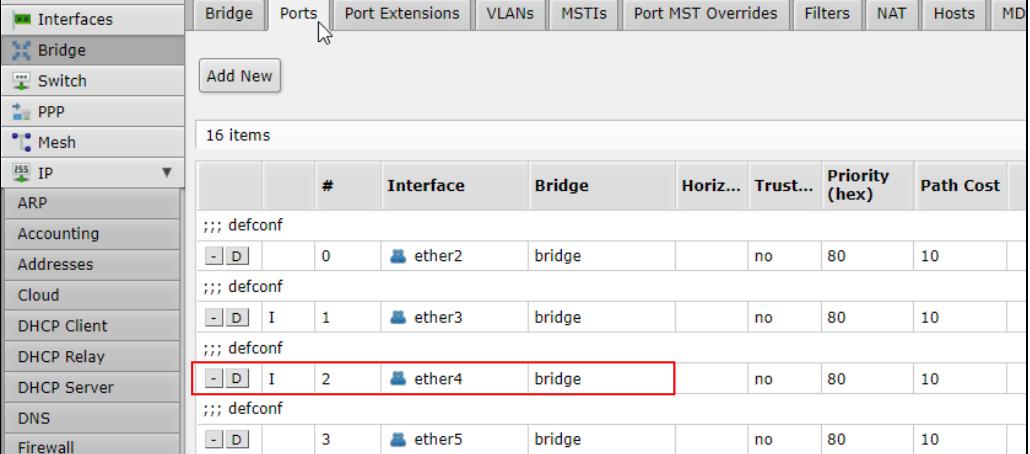
- ③ VLAN200 を作成します。

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。



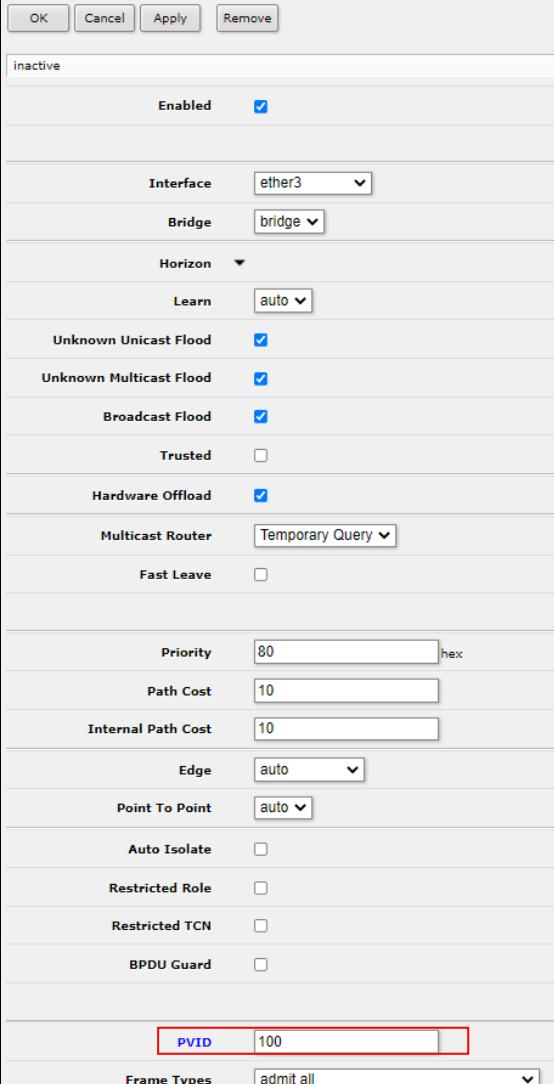
④ ether3 の PVID を設定します。

Bridge⇒Ports を選択し、ether3 をクリックします。



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

PVID を 100 に設定し、OK をクリックします。



OK	Cancel	Apply	Remove
inactive			
<input checked="" type="checkbox"/> Enabled			
Interface: <input type="button" value="ether3"/> Bridge: <input type="button" value="bridge"/>			
Horizon: <input type="button" value="auto"/> Learn: <input type="button" value="auto"/>			
Unknown Unicast Flood: <input checked="" type="checkbox"/> Unknown Multicast Flood: <input checked="" type="checkbox"/> Broadcast Flood: <input checked="" type="checkbox"/>			
Trusted: <input type="checkbox"/>			
Hardware Offload: <input checked="" type="checkbox"/>			
Multicast Router: <input type="button" value="Temporary Query"/>			
Fast Leave: <input type="checkbox"/>			
Priority: <input type="text" value="80"/> hex			
Path Cost: <input type="text" value="10"/>			
Internal Path Cost: <input type="text" value="10"/>			
Edge: <input type="button" value="auto"/>			
Point To Point: <input type="button" value="auto"/>			
Auto Isolate: <input type="checkbox"/>			
Restricted Role: <input type="checkbox"/>			
Restricted TCN: <input type="checkbox"/>			
BPDU Guard: <input type="checkbox"/>			
PVID: <input type="text" value="100"/>			
Frame Types: <input type="button" value="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							
-	D	0	ether2	bridge		no 80	10
;;; defconf							
-	D	I	1	ether3	bridge		no 80 10
;;; defconf							
-	D	I	2	ether4	bridge		no 80 10
;;; defconf							
-	D		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

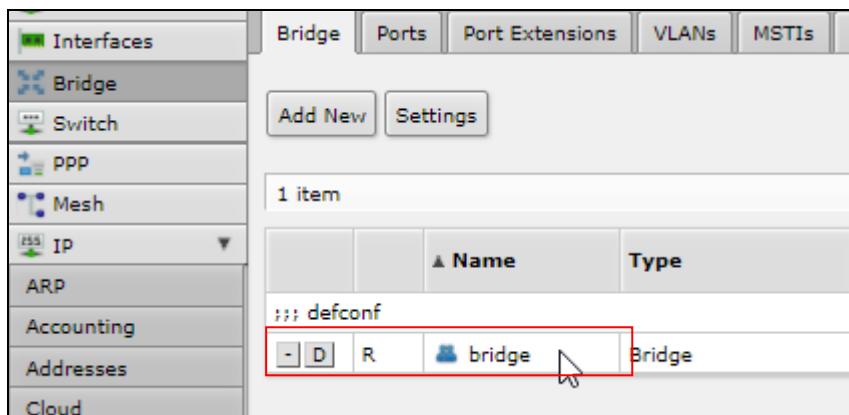
BPDUs Guard

PVID **200**

Frame Types **admin 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。

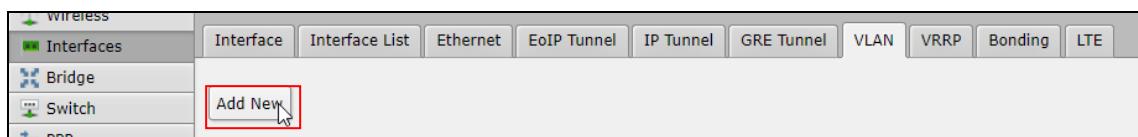
VLAN Filtering	<input checked="" type="checkbox"/>
EtherType	0x8100
PVID	1
Frame Types	admit all
Ingress Filtering	<input type="checkbox"/>

その後、OK をクリックします。

OK	<input style="outline: none; border: none; background-color: transparent; color: inherit; font-size: inherit; font-weight: inherit; padding: 0; margin: 0;" type="button" value="OK"/>	Cancel	Apply	Remove	Torch
not invalid running not slave					
Enabled <input checked="" type="checkbox"/>					
Name	bridge				
Type	Bridge				
MTU	<input style="outline: none; border: none; background-color: transparent; color: inherit; font-size: inherit; font-weight: inherit; padding: 0; margin: 0;" type="button" value="▼"/>				

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。



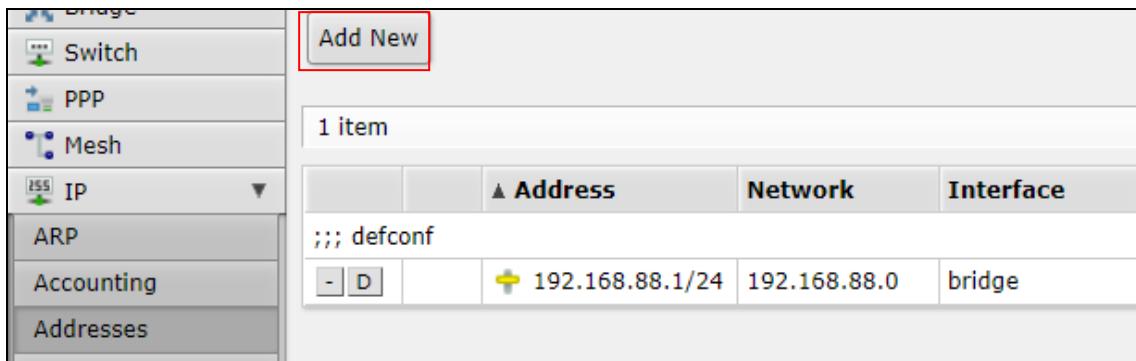
- ⑧ Name に任意の名前、VLAN ID に 100 と入力し、OK をクリックします。

		OK	Cancel	Apply	Torch
not invalid not running not slave					
Enabled <input checked="" type="checkbox"/>					
Name	<input type="text" value="vlan100"/>				
Type	VLAN				
MTU	<input type="text" value="1500"/>				
Actual MTU					
L2 MTU					
MAC Address					
ARP	<input type="button" value="enabled"/>				
ARP Timeout	<input type="button" value="▼"/>				
VLAN ID	<input type="text" value="100"/>				
Interface	<input type="button" value="bridge"/>				

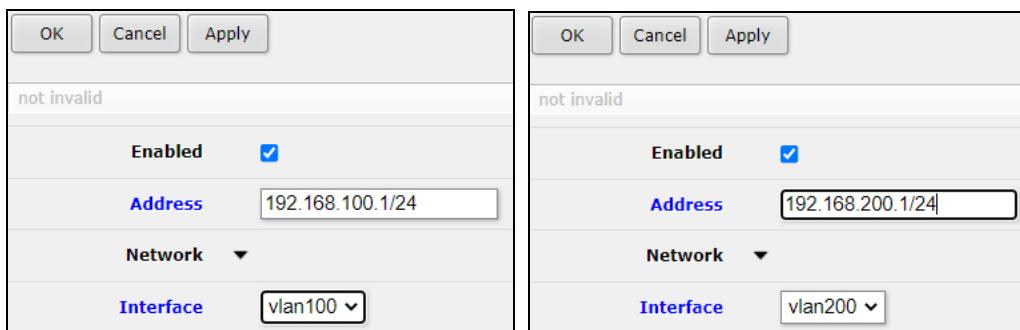
- ⑨ 同様の手順で VLAN 200 を作成します。

		OK	Cancel	Apply	Torch
not invalid not running not slave					
Enabled <input checked="" type="checkbox"/>					
Name	<input type="text" value="vlan200"/>				
Type	VLAN				
MTU	<input type="text" value="1500"/>				
Actual MTU					
L2 MTU					
MAC Address					
ARP	<input type="button" value="enabled"/>				
ARP Timeout	<input type="button" value="▼"/>				
VLAN ID	<input type="text" value="200"/>				
Interface	<input type="button" value="bridge"/>				

- 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...
<i>;;; special dummy rule to show fasttrack counters</i>										
-	D	0	passthru	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ー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ー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ー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
```

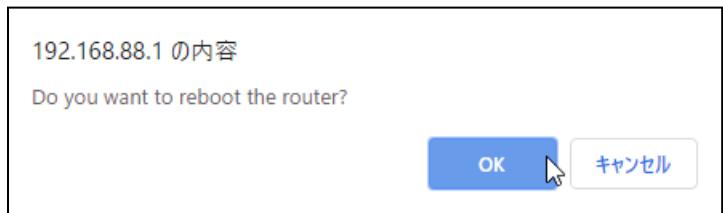
- ③ ネットワークアドレス、デフォルトゲートウェイ、DNS サーバを設定します。

```
/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。

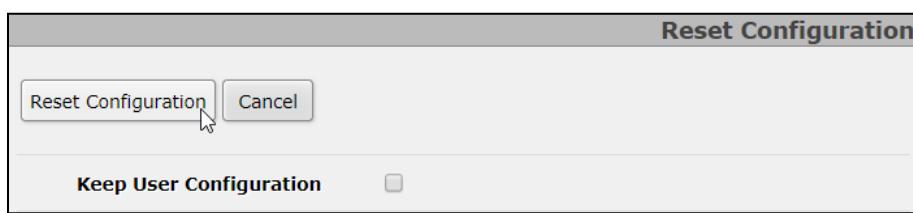
```
/system reboot
Reboot, yes? [y/N]: y ←確認要求が表示されたら”y”を入力します。
system will reboot shortly
```

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、ユーザー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できます。



- CLI による設定方法

以下のコマンドを入力します。

```
/system reset-configuration
Dangerous! 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。

	File Name	Type	Size	Creation Time	
-	flash	disk		Jan/01/1970 09:00:07	
-	flash/auto-before-reset.backup	backup	18.8 KiB	Jan/01/1970 09:00:09	Download
-	flash/pub	directory		Sep/17/2020 11:57:16	
-	flash/skins	directory		Jan/01/1970 09:00:08	

- 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。

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。

	File Name	Type	Size	Creation Time	
-	2020_01_01_backup.backup	backup	13.2 KiB	Sep/17/2020 17:46:48	Download
-	flash	disk		Sep/17/2020 17:46:53	
-	flash/auto-before-reset.backup	backup	18.8 KiB	Jan/01/1970 09:00:09	Download
-	flash/pub	directory		Sep/17/2020 11:57:16	
-	flash/skins	directory		Jan/01/1970 09:00:08	

※ 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。



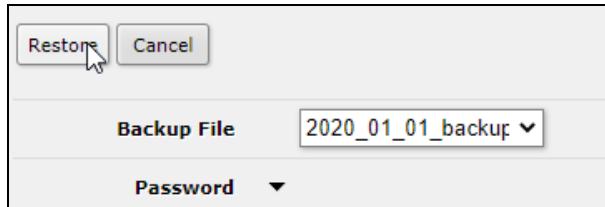
- ③ アップロードが完了したら、リストに追加されたバックアップファイルをクリックします。

Backup					
Upload: ファイルを選択 選択されていません					
5 items uploaded					
	File Name	Type	Size	Creation Time	
-	2020_01_01_backup.backup	backup	13.2 KiB	Sep/17/2020 17:50:47	Download
-	flash	disk		Sep/17/2020 17:46:53	
-	flash/auto-before-reset.backup	backup	18.8 KiB	Jan/01/1970 09:00:09	Download
-	flash/pub	directory		Sep/17/2020 11:57:16	
-	flashskins	directory		Jan/01/1970 09:00:08	

- ④ **Restore** をクリックします。

Close	Remove	Restore
File Name 2020_01_01_backup.backup		
Type backup		
Size 13.2 KiB		
Creation Time Sep/17/2020 17:50:47		

- 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出来ます。

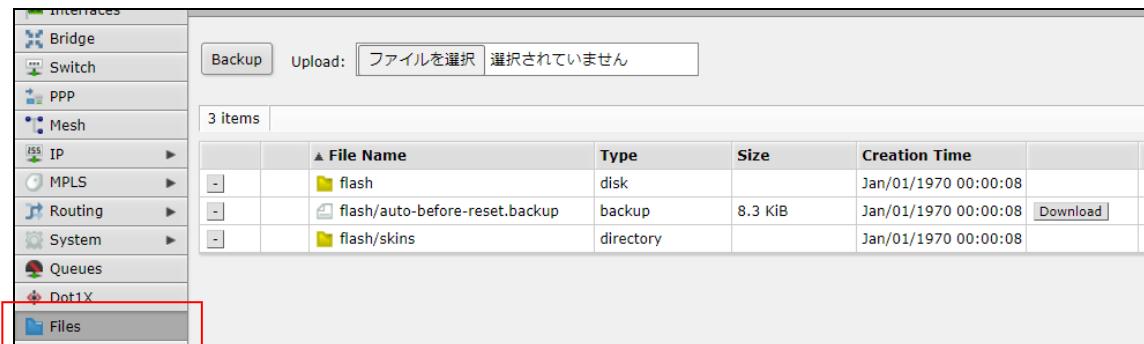
※ Bonding Interface を作成していた場合は、この手順で MAC アドレスが初期化されませんので、Bonding インタフェースを一旦 Disable にし、再度 Enable にしてください。

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																														
<table border="1"> <thead> <tr> <th></th> <th></th> <th>Name</th> <th>Type</th> <th>MTU</th> <th>Actual MTU</th> <th>L2 MTU</th> <th>Tx</th> <th></th> <th>Rx</th> </tr> </thead> <tbody> <tr> <td><input type="button" value="[-]"/></td> <td>D</td> <td>bonding1</td> <td>Bonding</td> <td>1500</td> <td>1500</td> <td>1596</td> <td>0 bps</td> <td></td> <td>512</td> </tr> </tbody> </table>													Name	Type	MTU	Actual MTU	L2 MTU	Tx		Rx	<input type="button" value="[-]"/>	D	bonding1	Bonding	1500	1500	1596	0 bps		512
		Name	Type	MTU	Actual MTU	L2 MTU	Tx		Rx																					
<input type="button" value="[-]"/>	D	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。

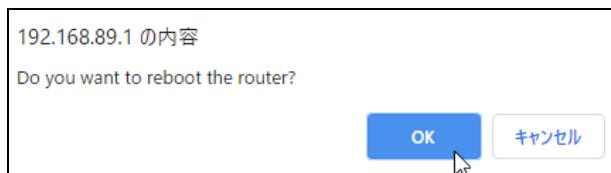
- ③ フームウェアファイルを選択して、**開く**をクリックします。



- 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。

4 items uploaded				
	File Name	Type	Size	Creation Time
-	flash	disk		Jan/01/1970 00:00:08
-	flash/auto-before-reset.backup	backup	8.3 KiB	Jan/01/1970 00:00:08
-	flash/skins	directory		Jan/01/1970 00:00:08
-	routeros-mmips-6.48.2.npk	package	9.2 MiB	Jan/02/1970 00:06:03

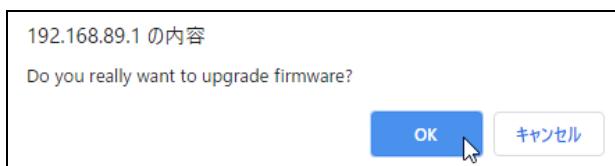
- ⑤ **System⇒Reboot**をクリックし、確認画面で OK をクリックします。



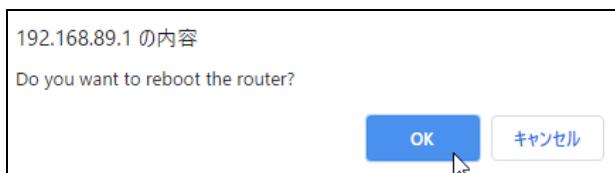
- ⑥ System⇒RouterBOARD を選択し、Upgrade をクリックします。

RouterBOARD	
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。



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



- 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	
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。

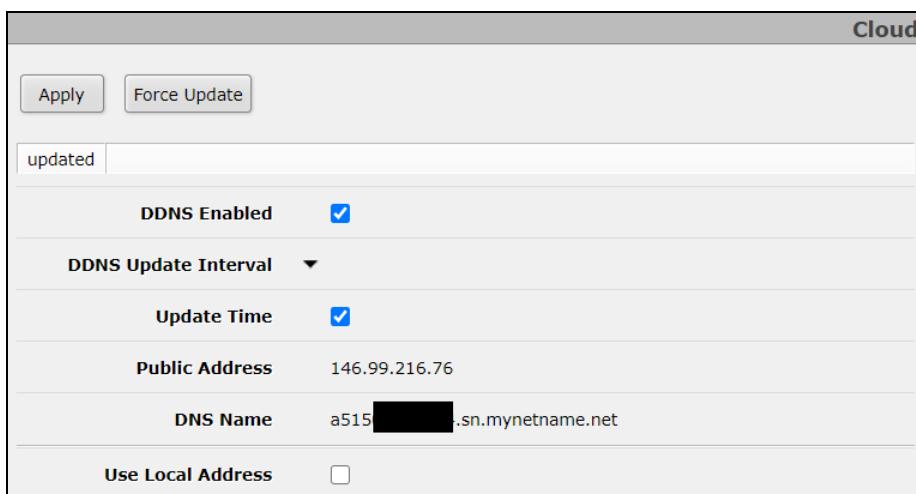
7.1. DDNS 機能の有効(Web の場合)

- 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



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)

General Settings	
Enabled	<input checked="" type="checkbox"/>
Chain	dstnat
Src. Address	▼
Dst. Address	▼
Protocol	▲ □ 6 (tcp)
Src. Port	▼
Dst. Port	▲ □ 50000

Forwarding Details	
Action	dst-nat
Log	<input type="checkbox"/>
Log Prefix	▼
To Addresses	▲ 192.168.88.253
To Ports	▲ 50000

- 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
```

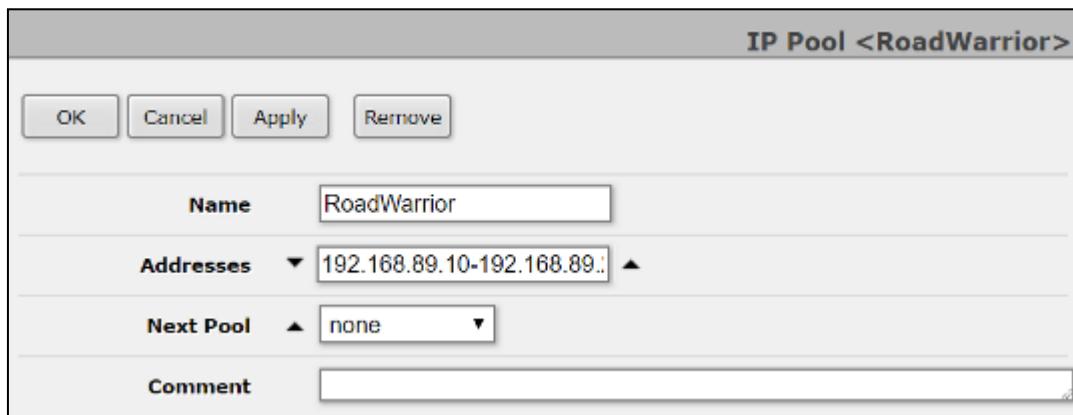
9. L2TP/IPSec を使用したリモートアクセス VPN の設定方法

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。

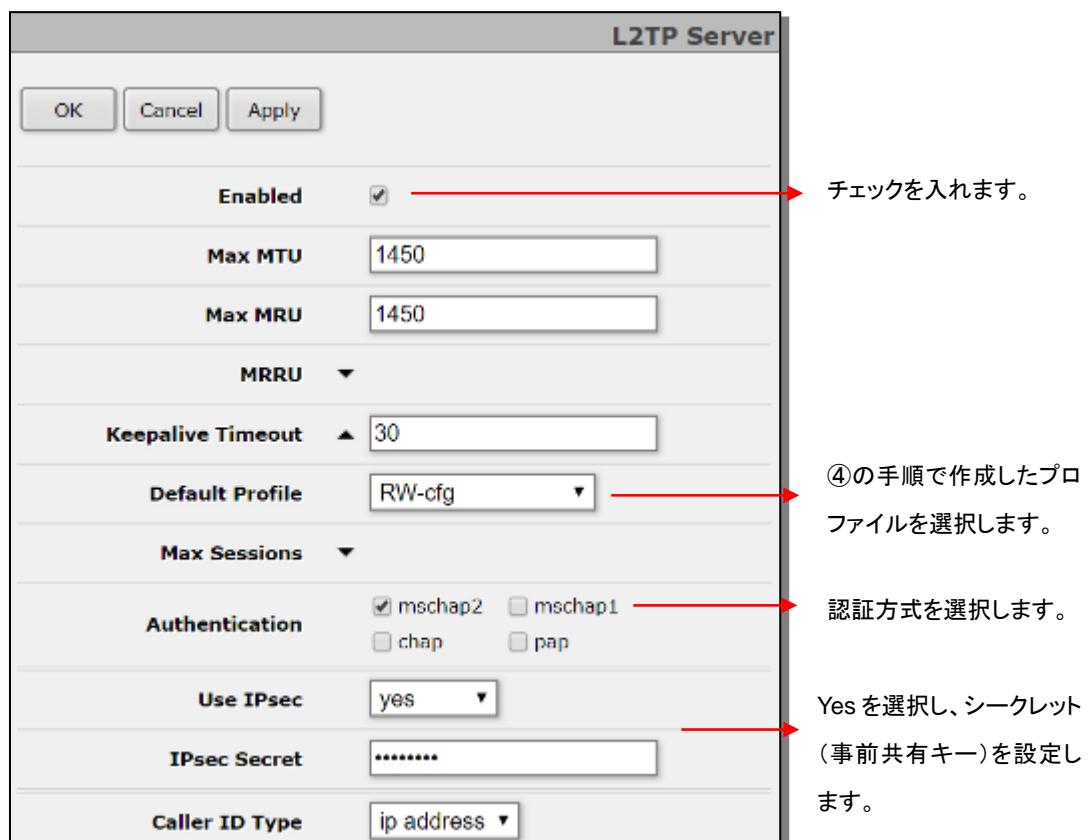


- ③ [PPP⇒Profile]を選択し、[Add New]をクリックします。
- ④ 下図を参考に設定します。



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。



⑦ [P⇒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	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	none

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。

Name	
default	

Hash Algorithms	
sha1	

Encryption Algorithm	
<input type="checkbox"/> des	<input checked="" type="checkbox"/> 3des
<input type="checkbox"/> aes-128	<input type="checkbox"/> aes-192
<input checked="" type="checkbox"/> aes-256	<input type="checkbox"/> blowfish
<input type="checkbox"/> camellia-128	<input type="checkbox"/> camellia-192
<input type="checkbox"/> camellia-256	

DH Group	
<input type="checkbox"/> modp768	<input checked="" type="checkbox"/> modp1024
<input type="checkbox"/> ec2n155	<input type="checkbox"/> ec2n185
<input type="checkbox"/> modp1536	<input type="checkbox"/> modp2048
<input type="checkbox"/> modp3072	<input type="checkbox"/> modp4096
<input type="checkbox"/> modp6144	<input type="checkbox"/> modp8192
<input type="checkbox"/> ecp256	<input type="checkbox"/> ecp384
<input type="checkbox"/> ecp521	

Proposal Check	
obey	

Lifetime	
1d 00:00:00	

Lifebytes	
▼	

NAT Traversal	
<input checked="" type="checkbox"/>	

DPD Interval	
120	s

DPD Maximum Failures	
5	

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 <input checked="" type="checkbox"/>	
Name	user
Password
Service	l2tp
Caller ID	▼
Profile	RW-cfg

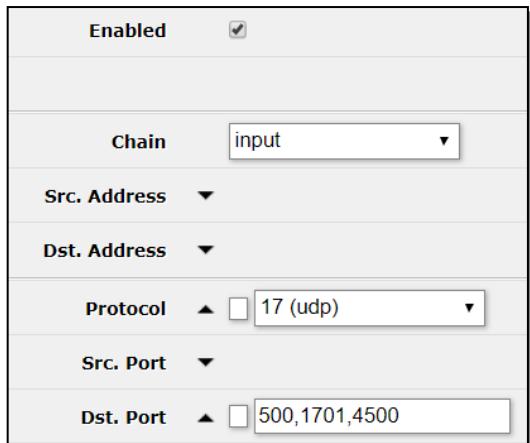
ユーザ名、パスワードを設定します。

L2TP を選択します。

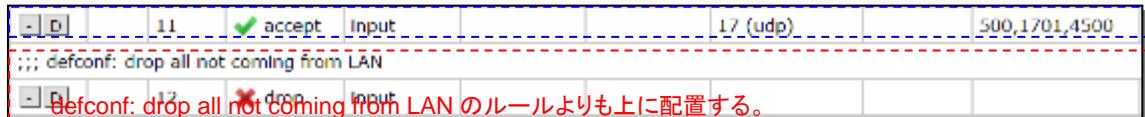
④の手順で作成したプロファイルを選択します。

- 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
```



⑫の手順で作成したルール



◆ 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 サーバインター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
```

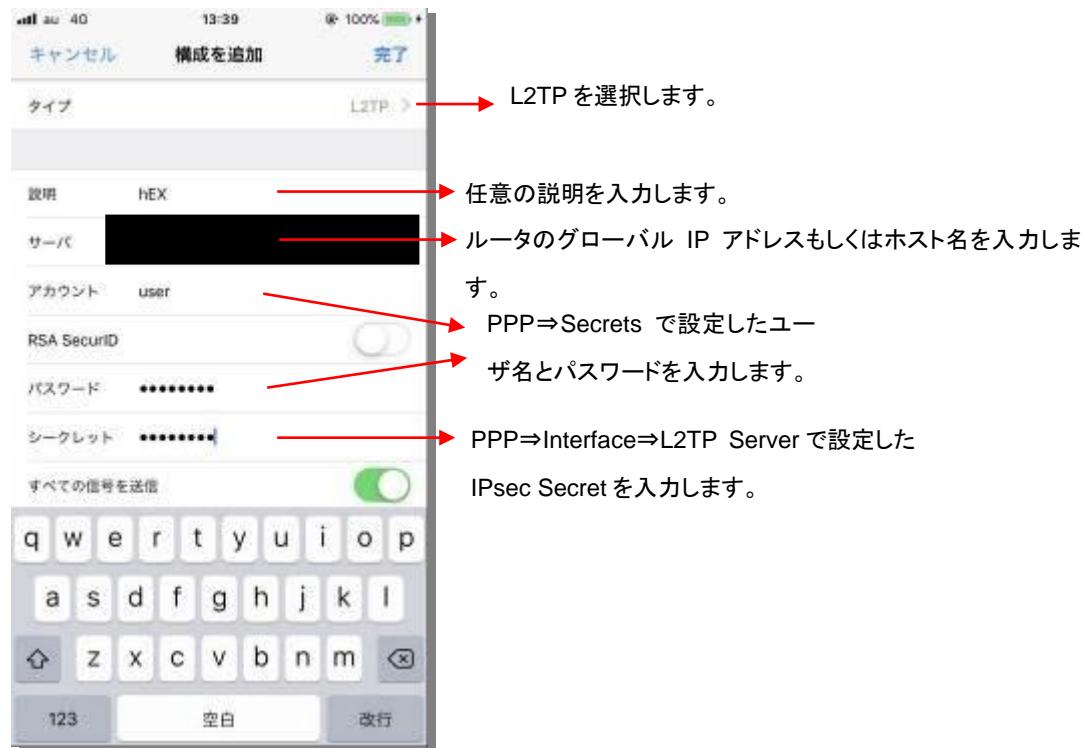
9.2. L2TP/IPSec VPN クライアントの設定

◆ スマートフォンの場合(iPhone)

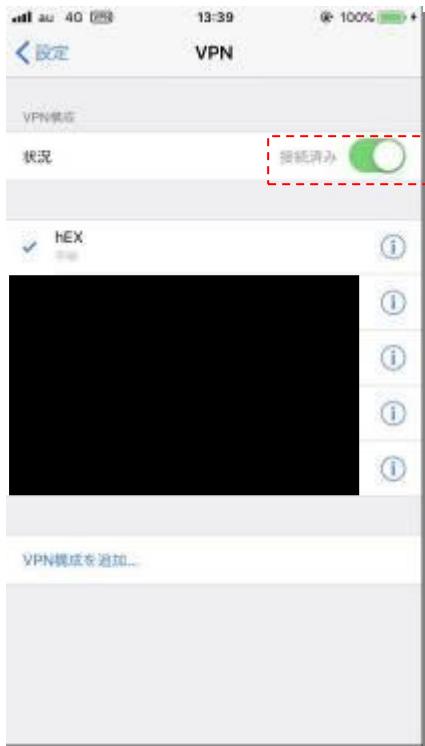
- ① 設定⇒VPNを選択し、VPN構成を追加…をタップします。



- 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。

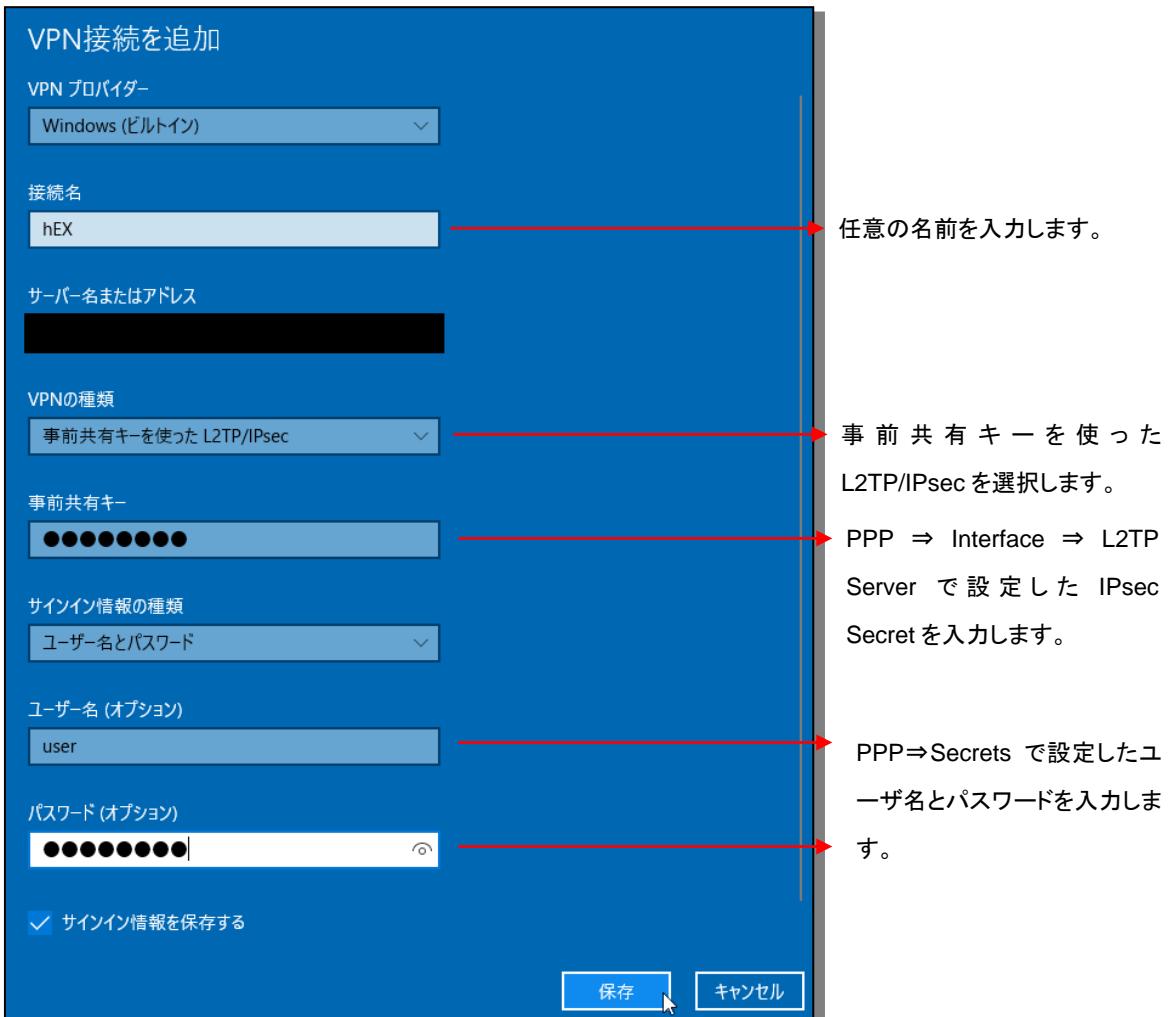


- ④ ① をタップすると、ステータスが確認できます。



◆ 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。

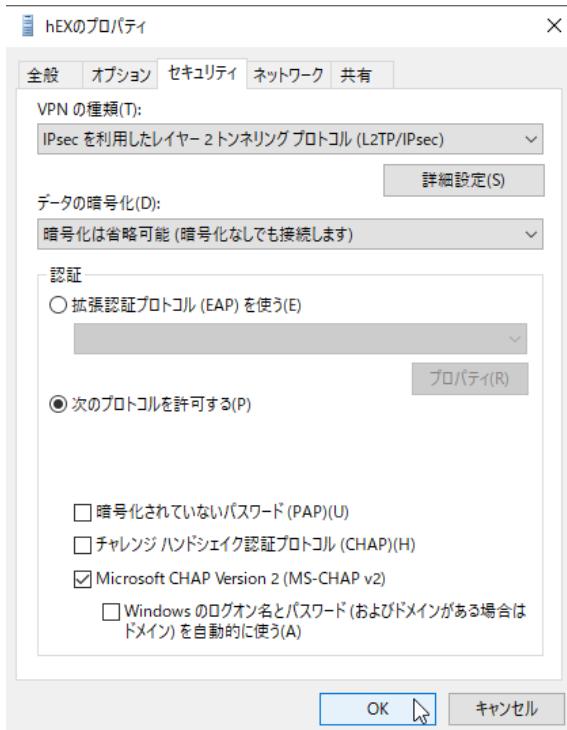


- ③ **アダプタのオプションを変更する** をクリックします。



- 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。

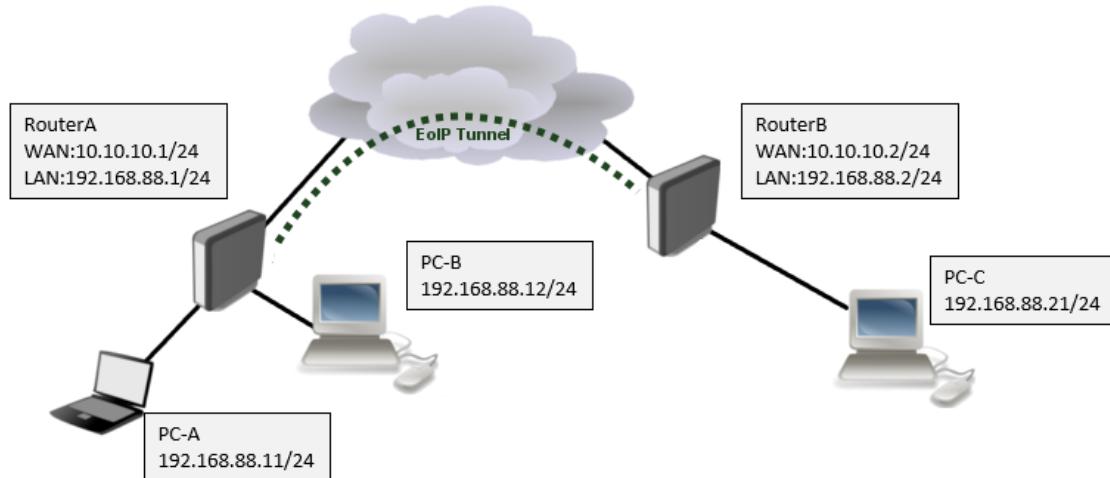


- ⑥ 接続します。



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

Name

Type EoIP Tunnel

MTU ▾

Actual MTU 1408

L2 MTU 65535

MAC Address

ARP

ARP Timeout ▾

Local Address ▾

Remote Address

Tunnel ID

IPsec Secret

Keepalive

DSCP

Dont Fragment

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

Bridge

Horizon ▾

Learn

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	▲ □ 47 (gre)

	#	Action	Chain	Src. Address	Dst. Address	Prot...	\$
;;; special dummy rule to show fasttrack counters							
-	D	0	passthru	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

Name

Type

MTU

Actual MTU

L2 MTU

MAC Address

ARP

ARP Timeout

Local Address

Remote Address

Tunnel ID

IPsec Secret

Keepalive

DSCP

Dont Fragment

Clamp TCP MSS

Allow Fast Path

Router B の WAN 側アドレスを入力します。
 Router A 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

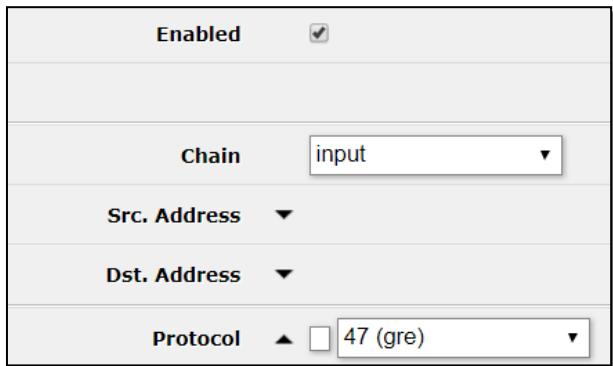
Bridge

Horizon

Learn

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。



	#	Action	Chain	Src. Address	Dst. Address	Prot...	...
;;; special dummy rule to show fasttrack counters							
-	D	0	passthru	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	eoip-tunnel1	EoIP Tunnel	1408	65535	62.7 kbps
	RS					

- 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	eoip-tunnel1	EoIP Tunnel	1408	65535	0 bps
	S					

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)

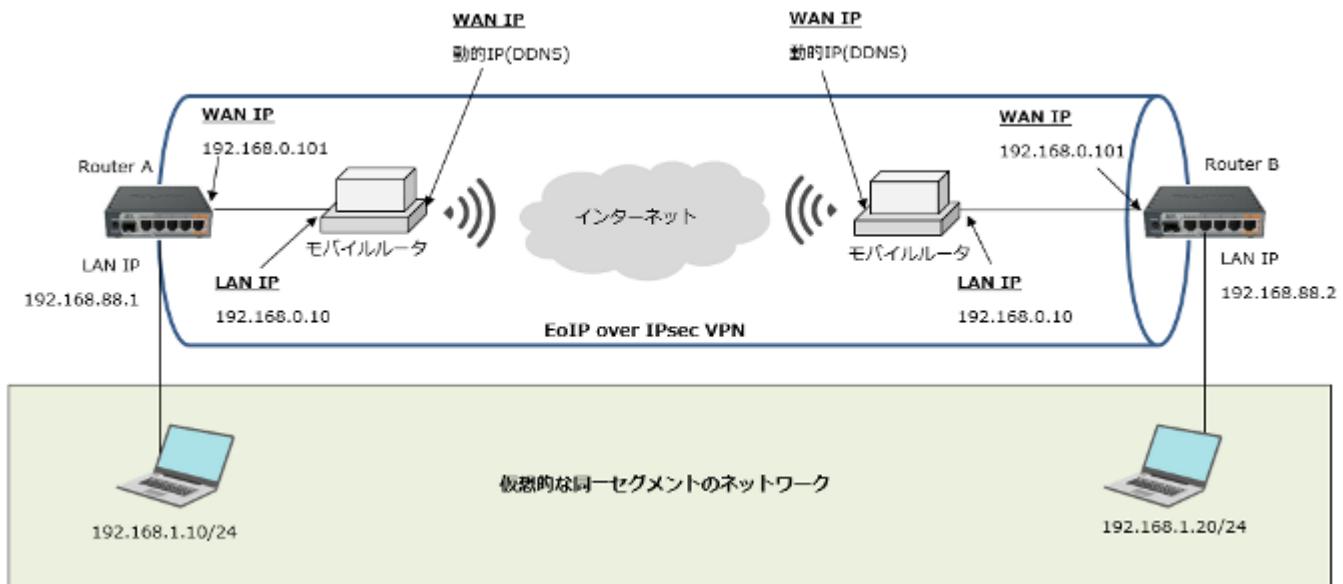
```
[admin@MikroTik] > /interface eoip print
Flags: X - disabled, R - running
0 [R] name="eoip-tunnel1" mtu=auto actual-mtu=1408 l2mtu=65535
    mac-address=FE:0D:FA:A5:83:9F arp=enabled arp-timeout=auto loop-protect=default
    loop-protect-status=off loop-protect-send-interval=5s loop-protect-disable-time=5m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

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出来ます。

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)

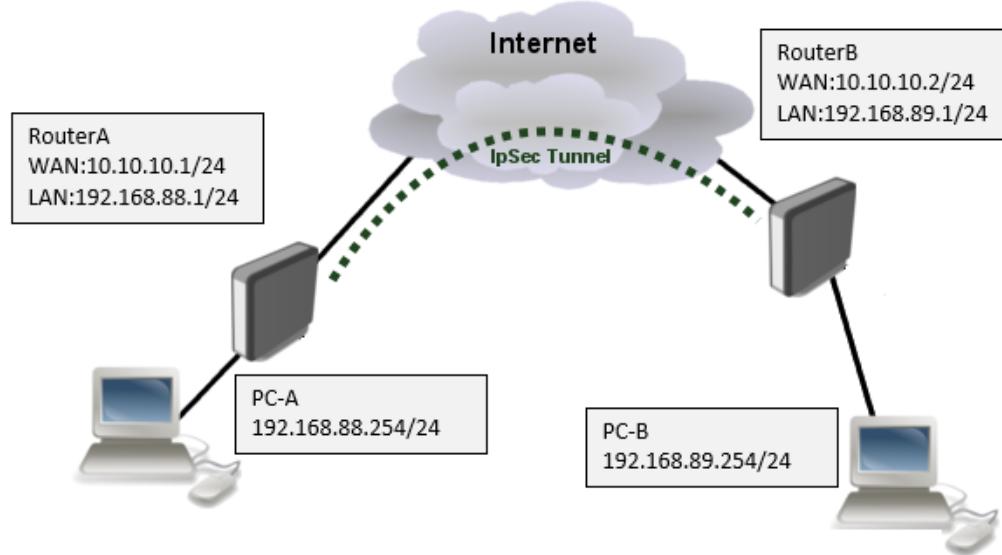
```
[admin@MikroTik] > /interface eoip print
Flags: X - disabled, R - running
0 [R] name="eoip-tunnel1" mtu=auto actual-mtu=1408 l2mtu=65535
    mac-address=FE:0D:FA:A5:83:9F arp=enabled arp-timeout=auto loop-protect=default
    loop-protect-status=off loop-protect-send-interval=5s loop-protect-disable-time=5m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

- 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。

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。

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	1450	
Max MRU	1450	
MRRU	▼	
Keepalive Timeout	▲ 30	
Default Profile	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	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	<input checked="" type="checkbox"/>	
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	I2tp	I2tp 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	<input checked="" type="checkbox"/>
Chain	input
Src. Address	▼
Dst. Address	▼
Protocol	▲ □ 17 (udp)
Src. Port	▼
Dst. Port	▲ □ 50,1701,500,4500

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	passthru	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。

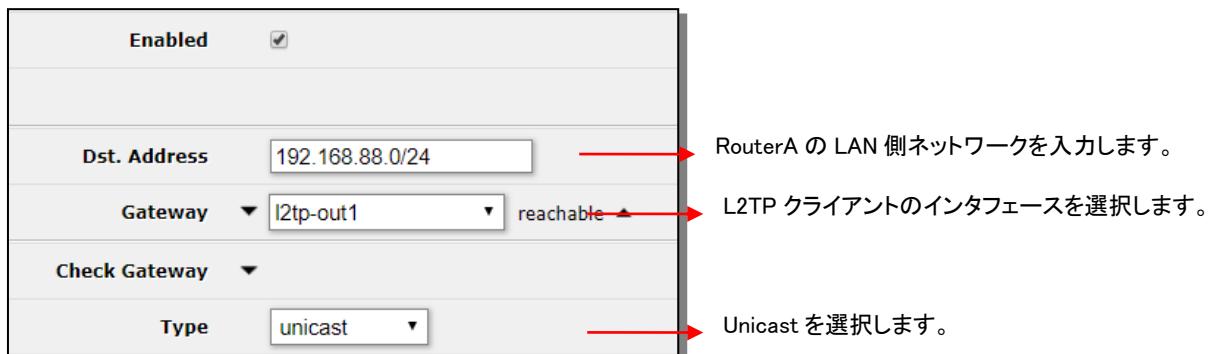
Port	Eth1
Address Acquisition	<input checked="" type="radio"/> Static <input type="radio"/> Automatic <input type="radio"/> PPPoE
IP Address	10.10.10.2
Netmask	255.255.255.0 (/24)
Gateway	10.10.10.254
DNS Servers	
MAC Address	B8:69:F4:81:D0:26
IP Address	192.168.89.1
Netmask	255.255.255.0 (/24)
DHCP 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"/>	
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。



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ー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
```

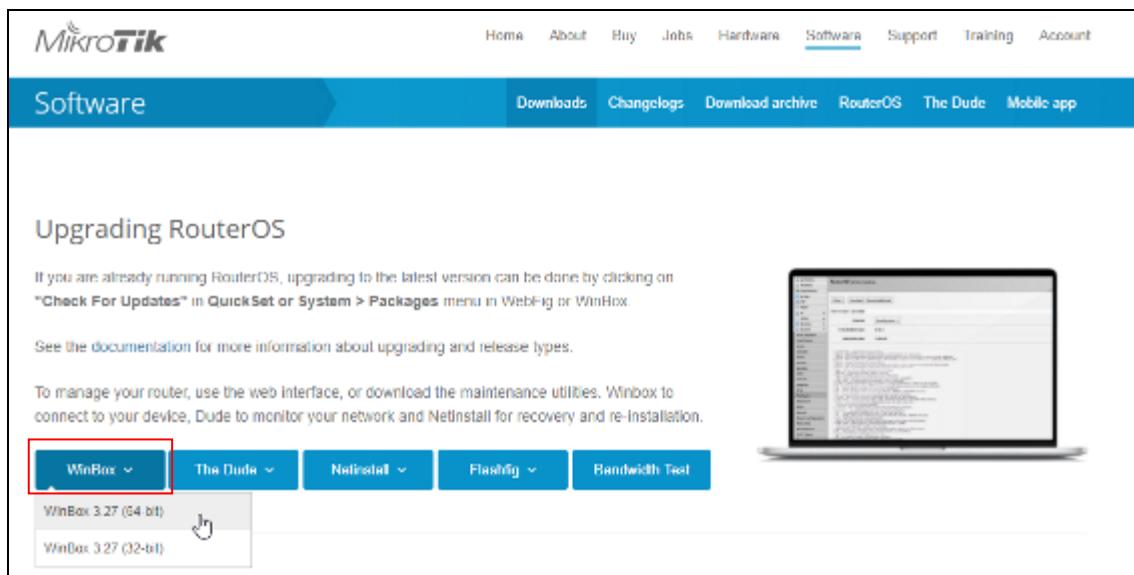
13. IP アドレスを忘れてしまった、初期化が上手くいかない場合

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。

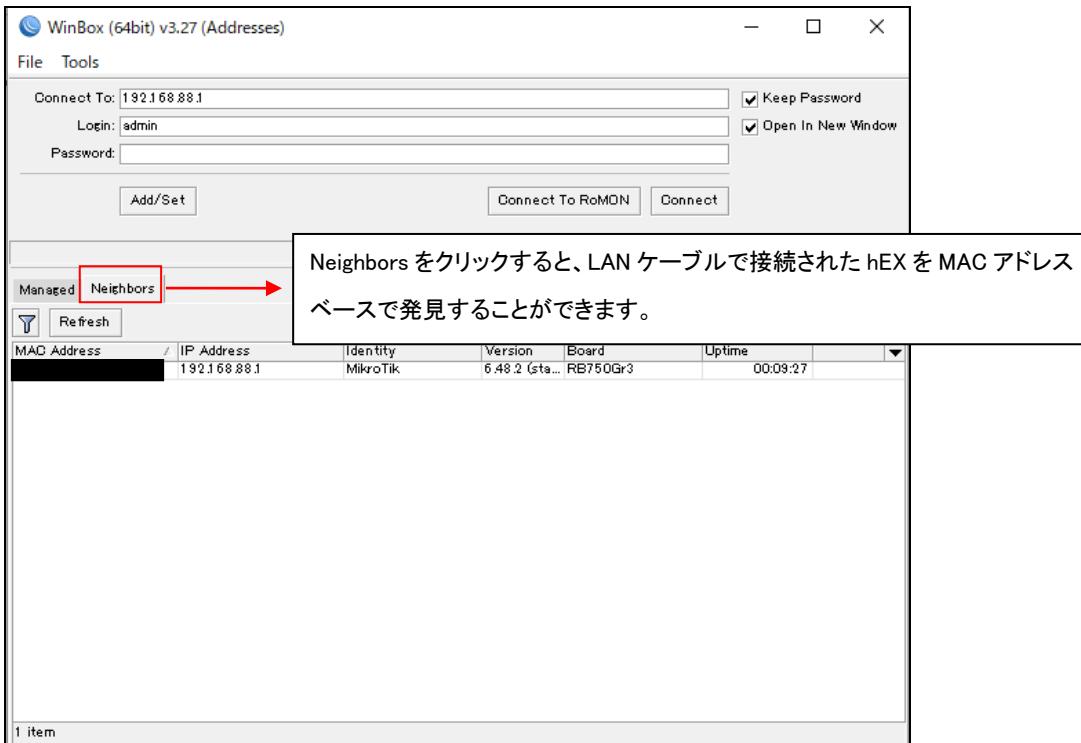
- ① Mikrotik の HP(<https://mikrotik.com/download>) から、WinBox をダウンロードします。

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。

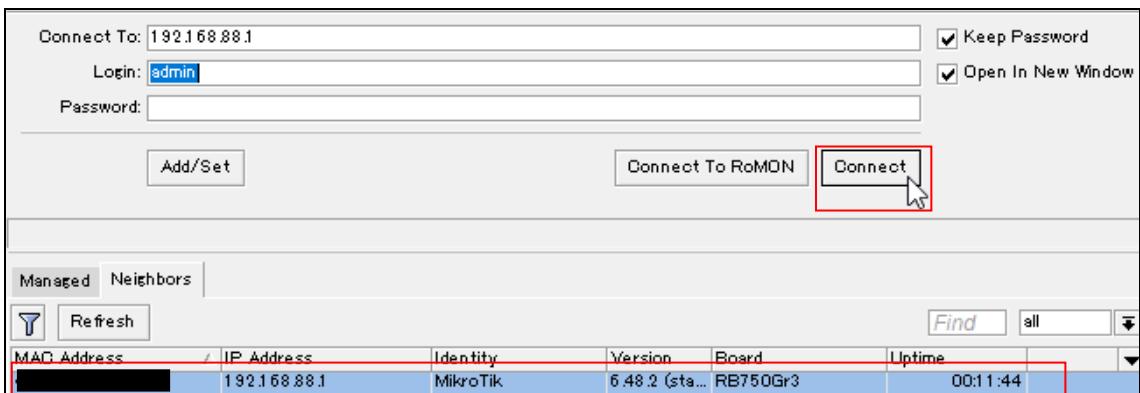


- ② ダウンロードしたファイル(WinBox64.exe または WinBox.exe)をダブルクリックして起動します。

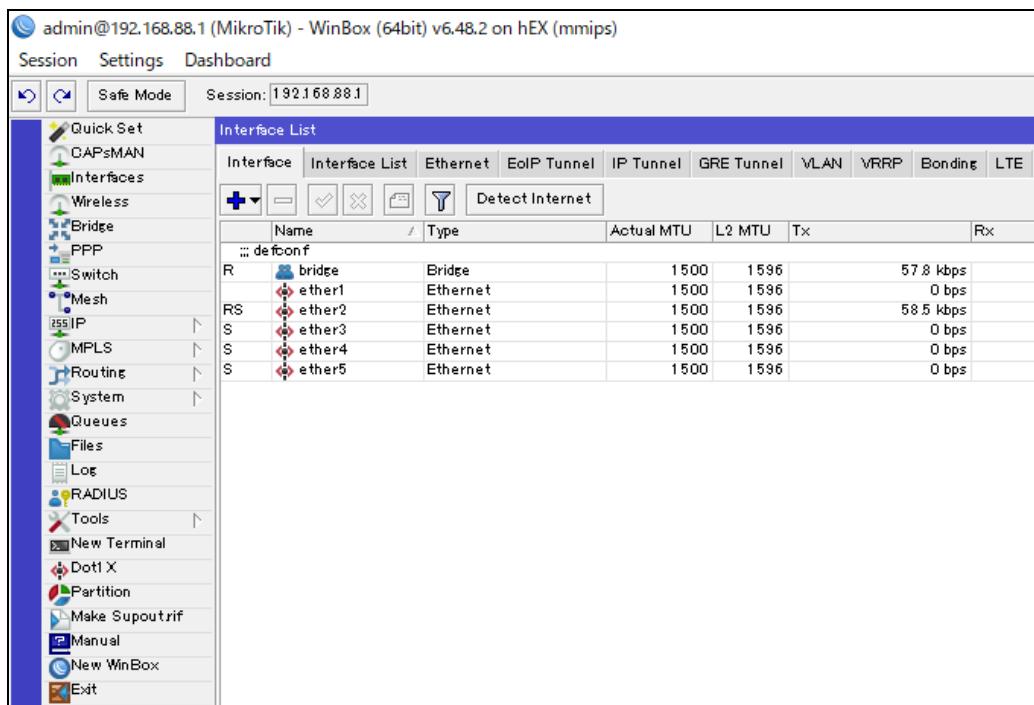
- ③ 起動後の画面は以下の通りとなります。



- 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。



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/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

※ 記載の通信速度についてはテスト環境でのデータのため、お客様環境下での速度を保証するものではありません。

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

※ 記載の通信速度についてはテスト環境でのデータのため、お客様環境下での速度を保証するものではありません。

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
インターフェース	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
インターフェース	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頂きます。
 - 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頂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頂きます。
(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



Copyright © 2025

HYTEC INTER Co., Ltd.