

CAPsMANについて

MUM Japan 2015

自己紹介

- ▶ 堀米 義仁 (Horigome Yoshihito)
- ▶ 都内のManaged Service Provider事業な会社に所属
- ▶ Networkの仕事はしたことはありません。
- ▶ Routerboard User Group JPという有志のグループに所属しています
- ▶ ユーザーグループに所属してくれる人募集中



Routerboard User Group JPの活動

RBUG JP Portal Site

Routerboard Users Group JP

[TOP](#) [INFO](#) [BLOG](#) [FORUM](#) [ABOUT](#)



Top



Routerboard User Group JPの活動

- ▶ 新商品ネタの紹介
- ▶ 技術情報の共有
- ▶ バージョンアップ情報
- ▶ Routerboardを使ったネタ
- ▶ などを取り上げています

CAPsMANとは

- ▶ **Overview**
- ▶ Controlled Access Point system Manager (CAPsMAN) allows centralization of wireless network management and if necessary, data processing. When using the CAPsMAN feature, the network will consist of a number of 'Controlled Access Points' (CAP) that provide wireless connectivity and a 'system Manager' (CAPsMAN) that manages the configuration of the APs, it also takes care of client authentication and optionally, data forwarding.
- ▶ 制御されたアクセス ポイント システム マネージャー (CAPsMAN) により、ワイヤレス ネットワークの管理を一元化し、必要に応じて、データ処理します。

CAPsMANの機能

- ▶ RADIUS MAC authentication
- ▶ WPA/WPA2 security
- ▶ CAPsMAN automatic upgrade of all CAP clients (configurable)
- ▶ improved CAP<->CAPsMAN data connection protocol
- ▶ added "Name Format" and "Name Prefix" setting for Provision rules
- ▶ improved logging entries when client roams between the CAPs
- ▶ added L2 Path MTU discovery

CAPsMANってなんぞ？

- ▶ CAPsMAN
 - ▶ Controlled Access Point system Manager
- ▶ CAPs
 - ▶ Controlled Access Point

必須要件

▶ CAPsMAN

- ▶ 1.x86 or RouterBOARD based device
- ▶ 2.RouterOS v6.11以上
- ▶ 3.Wireless-fp パッケージ かWireless-cm2パッケージ (ROS6.22rc7)

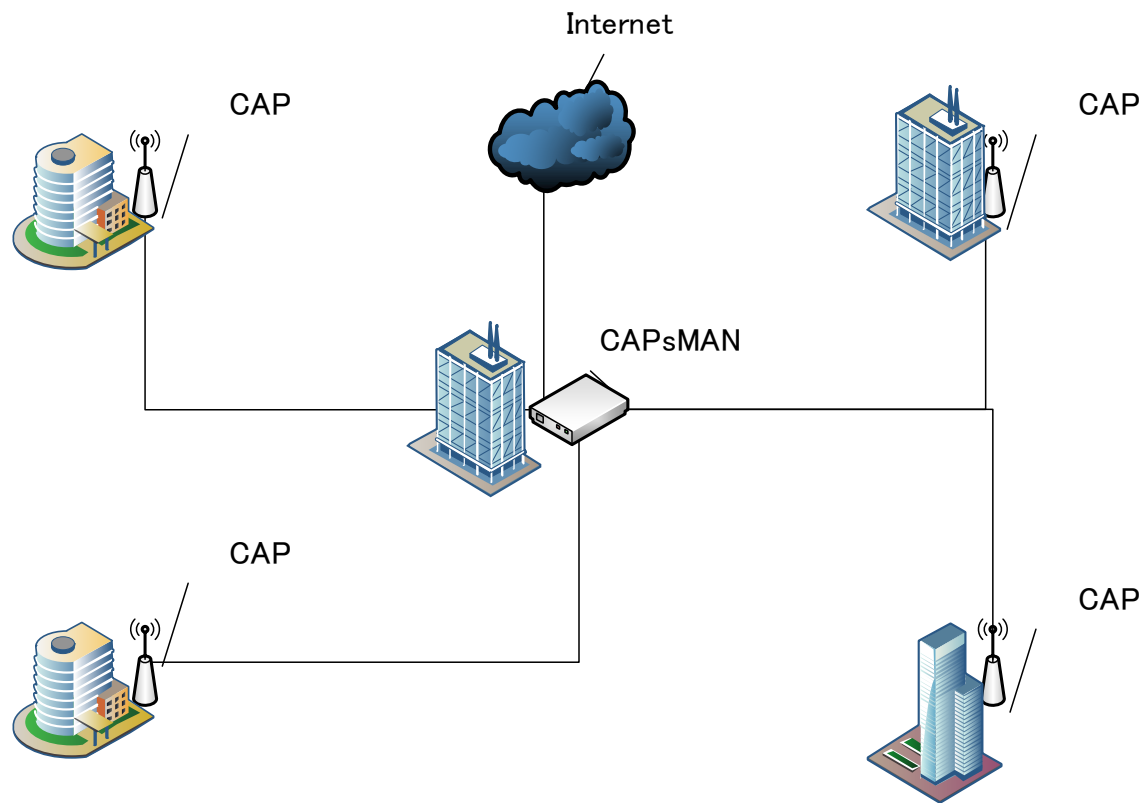
▶ CAPs

- ▶ 1.X86 or RouterBOARD based device
- ▶ 2.RouterOS v6.11以上
- ▶ 3.Atheros chipset (a/b/g/n/ac) wireless card
- ▶ 4.Wireless-fp パッケージ かWireless-cm2パッケージ (ROS6.22rc7)
- ▶ 5. Level4 RouterOS license以上

CAPsMANはv1とv2があります

- ▶ お互いに互換性はありません
- ▶ V2はテストバージョンに位置づけられています
- ▶ 幾つかの機能が追加されています
 - ▶ CAPsMAN automatic upgrade of all CAP clients (configurable)
 - ▶ improved CAP<->CAPsMAN data connection protocol
 - ▶ added "Name Format" and "Name Prefix" setting for Provision rules
 - ▶ improved logging entries when client roams between the CAPs
 - ▶ added L2 Path MTU discovery

構成イメージ図



今回は、以下の構成で。

- ▶ CAPsMAN

- ▶ RB951G-2HnD
- ▶ RouterOS 6.32.2
- ▶ 192.168.122.2/24

- ▶ CAPs

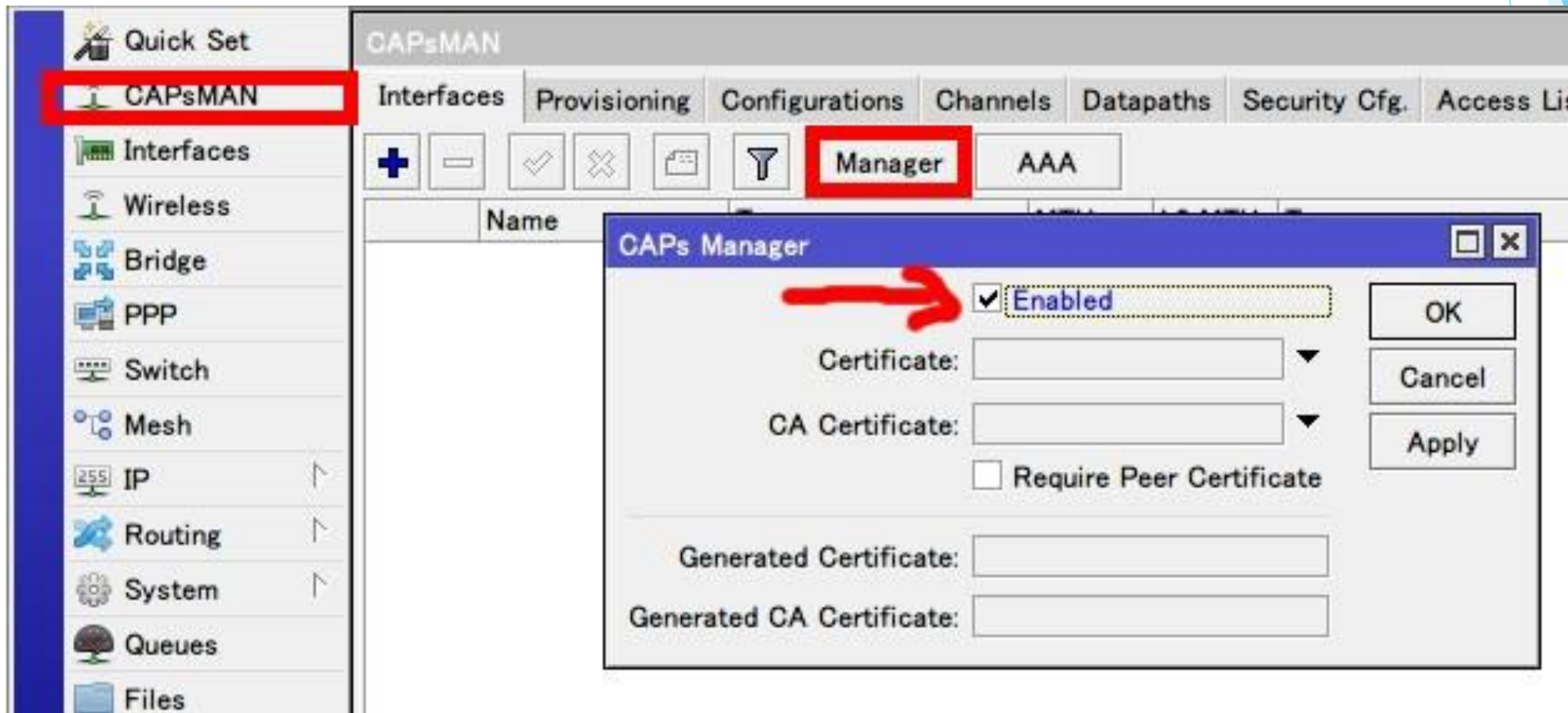
- ▶ RB951Ui-2HnD
- ▶ RouterOS 6.32.2
- ▶ 192.168.122.3/24

CAPsMANのセットアップ手順

- ▶ CAPsMANサービスの有効化
- ▶ Bridgeインターフェイスの作成（CAPがここにぶら下がる格好になります）
- ▶ BridgeインターフェイスへのIPアドレス設定
- ▶ CAPsMAN設定の追加
- ▶ CAPの接続について
- ▶ APのCAPモードの有効化

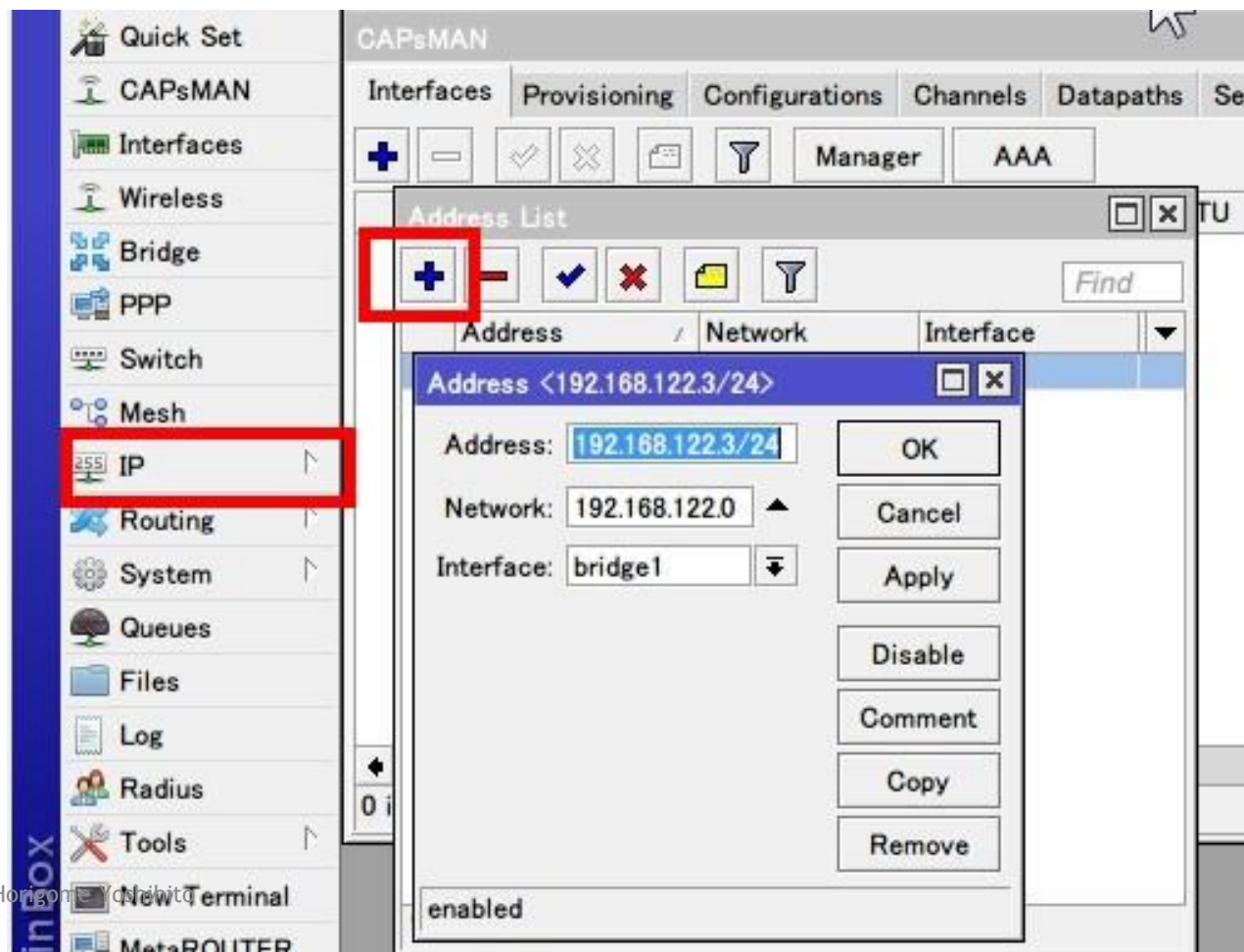
CAPsMANの設定手順

CAPsMANサービスの有効化



CAPsMAN設定手順

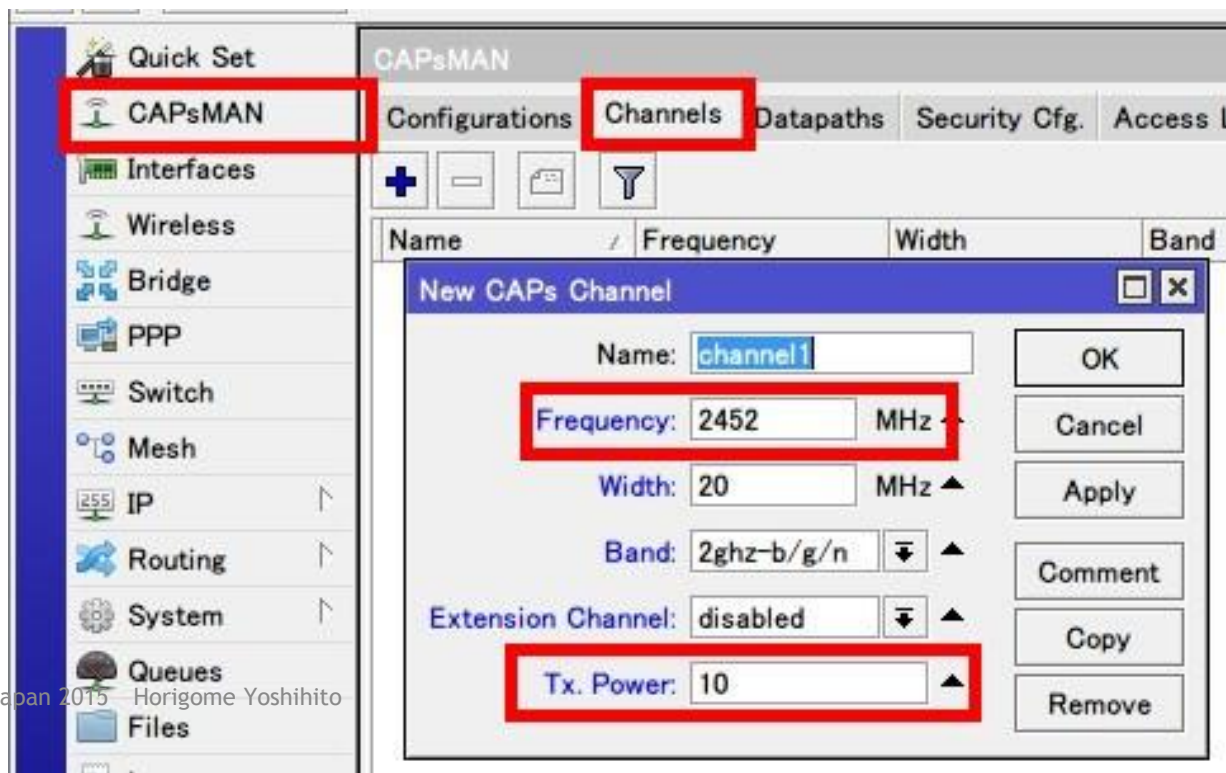
BridgeインターフェイスへのIPアドレス設定



CAPsMAN設定手順

CAPsMAN設定の追加

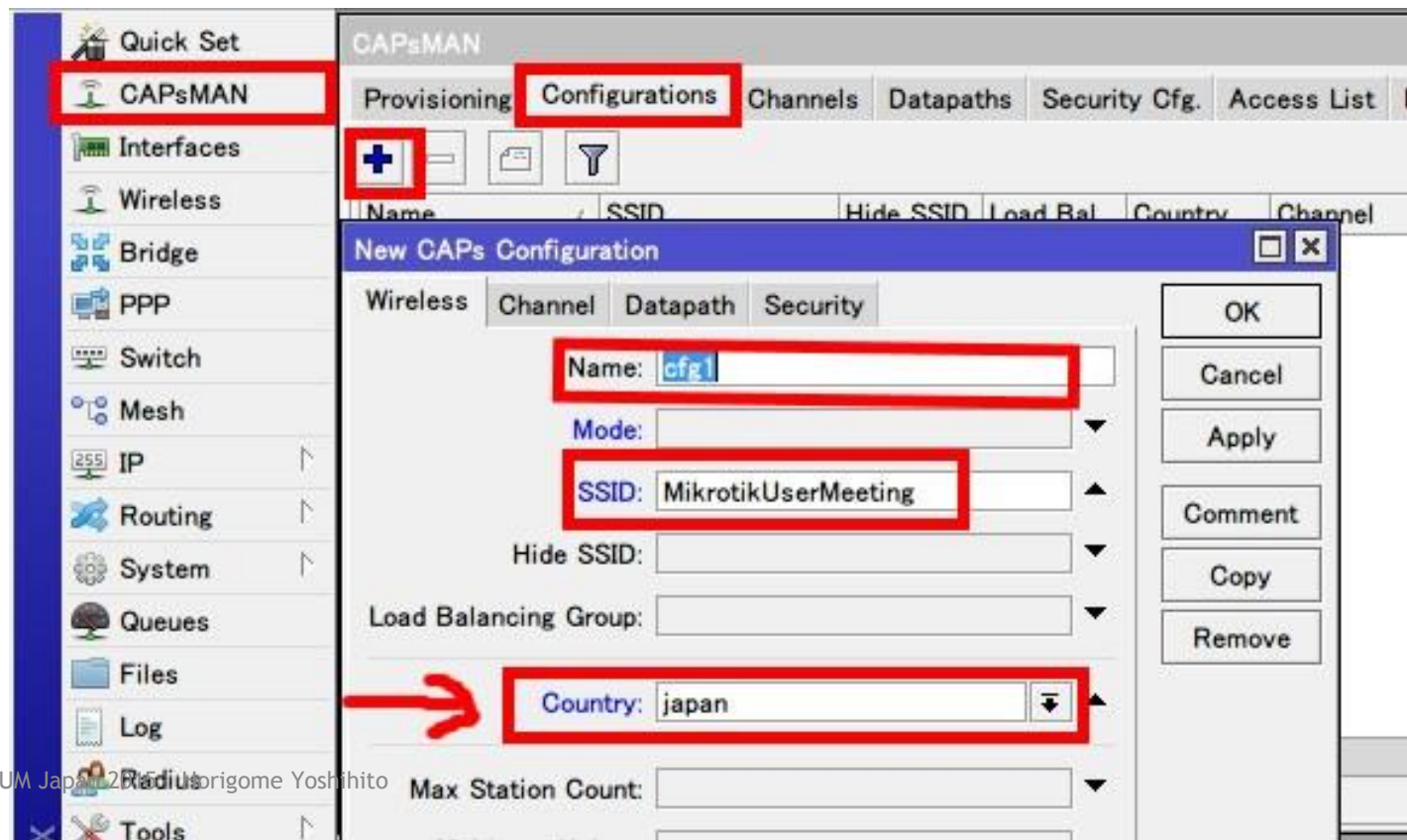
- ▶ この辺りを参考に：<http://michisugara.jp/archives/2014/wifi.html>
- ▶ Tx Powerは10dBmに（電波法違反になります）



CAPsMAN設定手順

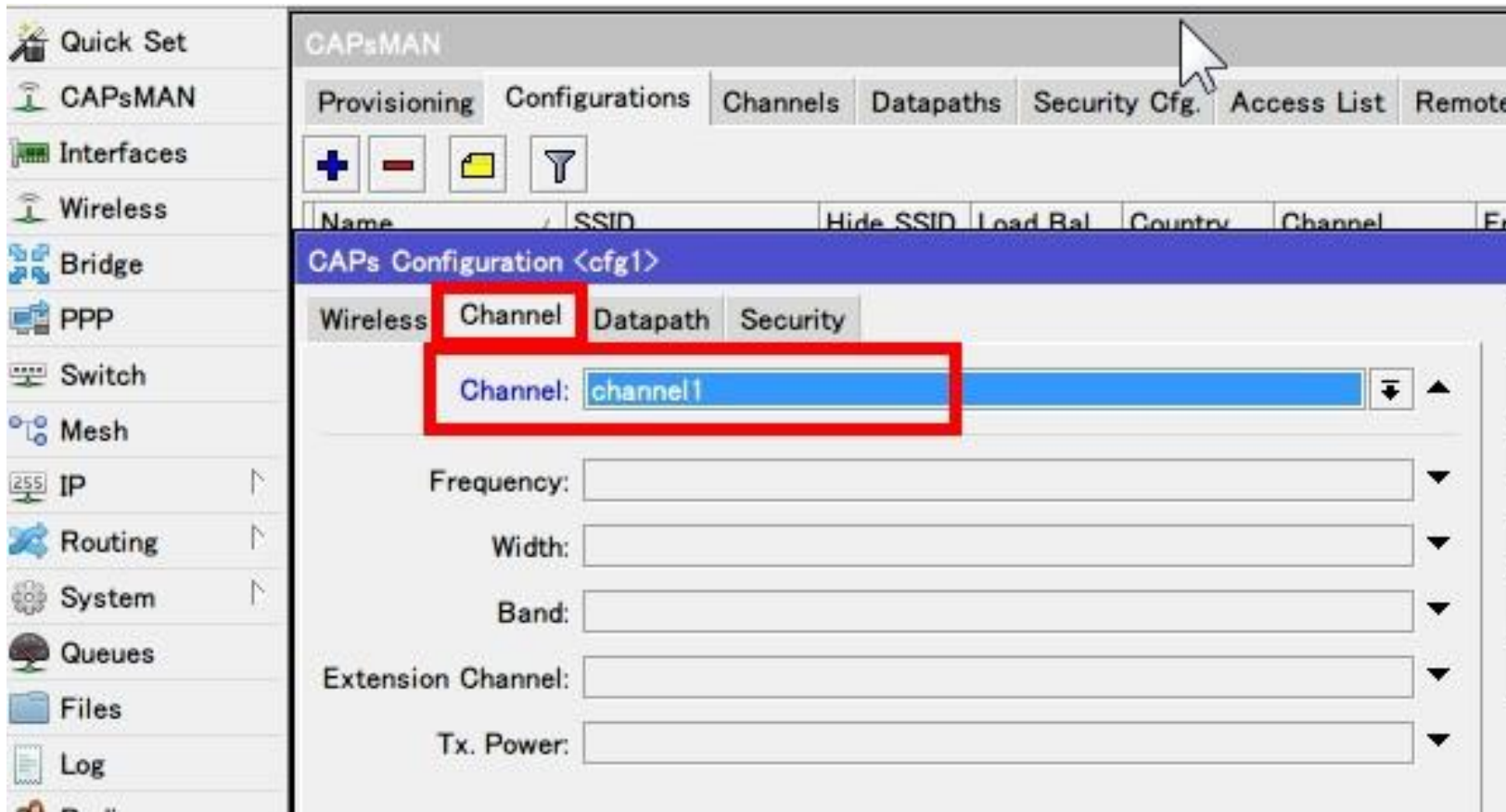
CAPsMAN設定の追加

- ▶ CountryはJapanを設定してください



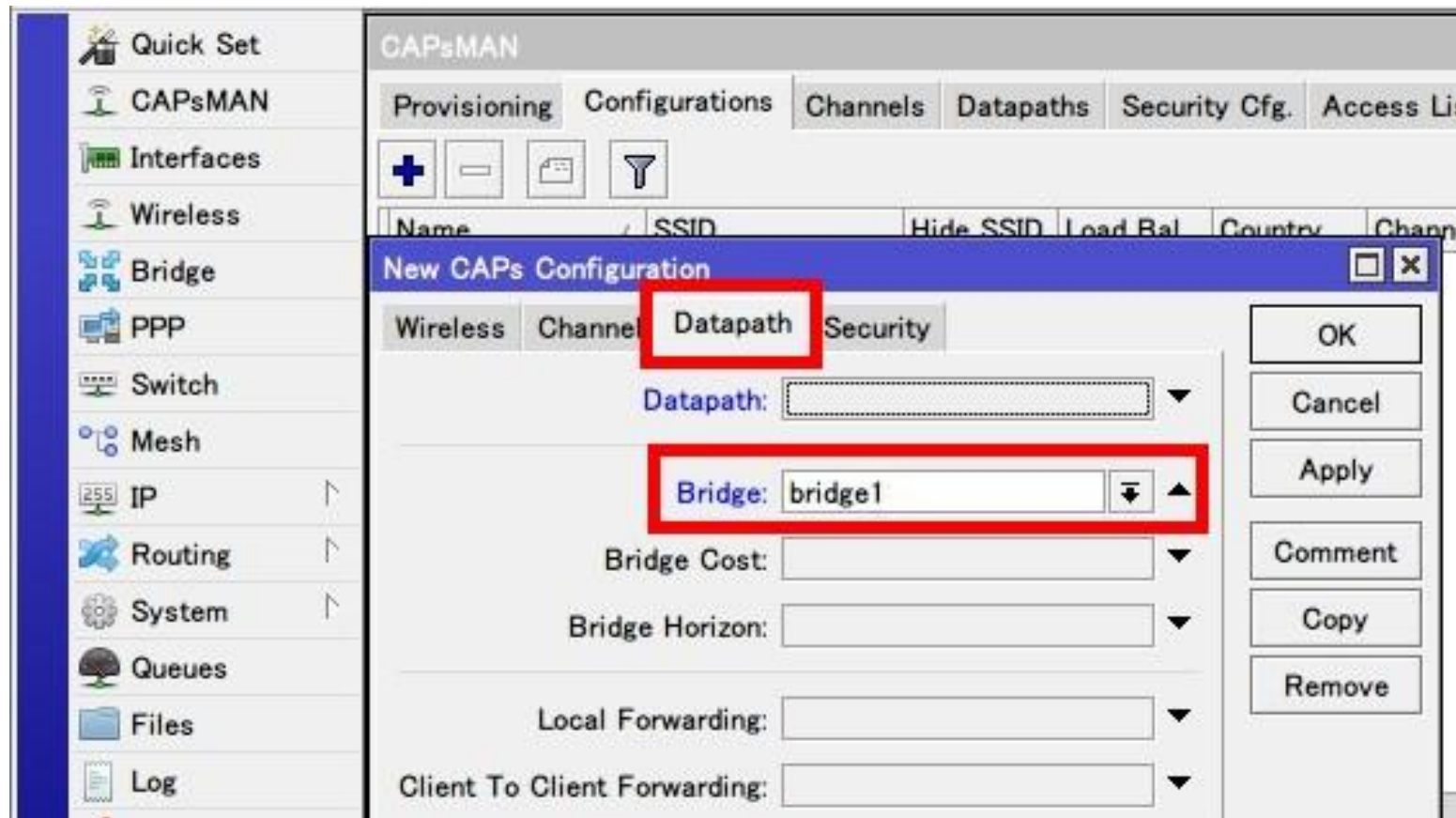
CAPsMAN設定手順

CAPsMAN設定の追加



CAPsMAN設定手順

CAPsMAN設定の追加



CAPsMAN設定手順

CAPsMAN設定の追加

The screenshot displays the CAPsMAN configuration window with the 'Security' tab selected. The 'Authentication Type' section has 'WPA2 PSK' checked. The 'Encryption' section has 'aes ccm' selected. The 'Group Encryption' dropdown is set to 'aes ccm'. The 'Passphrase' field is highlighted with a red box and contains a red annotation '8文字以上' (8 characters or more). The left sidebar shows the navigation menu with 'CAPsMAN' selected. The top tabs include 'Provisioning', 'Configurations', 'Channels', 'Datapaths', 'Security Cfg.', 'Access List', 'Remote CAP', and 'Radio'.

inBox

Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
MetaROUTER

CAPsMAN

Provisioning Configurations Channels Datapaths Security Cfg. Access List Remote CAP Radio

New CAPs Configuration

Wireless Channel Datapaths **Security**

Security: [Dropdown]

Authentication Type: ☐ WPA PSK ☒ **WPA2 PSK** ☐ WPA EAP ☐ WPA2 EAP

Encryption: ☒ **aes ccm** ☐ tkip

Group Encryption: aes ccm

Passphrase: ***** 8文字以上

EAP Methods: [Dropdown]

TLS Mode: [Dropdown]

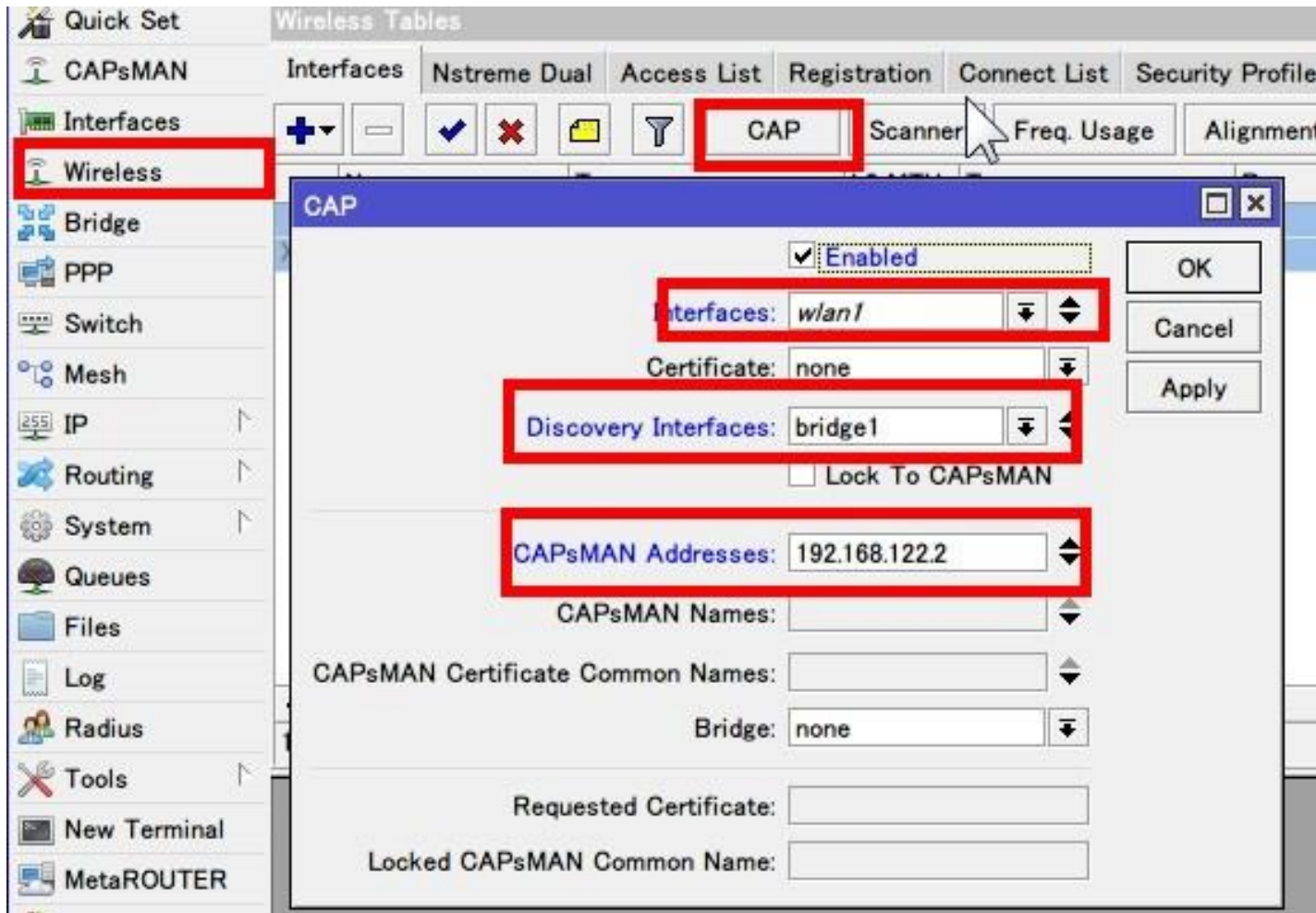
TLS Certificate: [Dropdown]

OK
Cancel
Apply
Comment
Copy
Remove

CAPの接続について

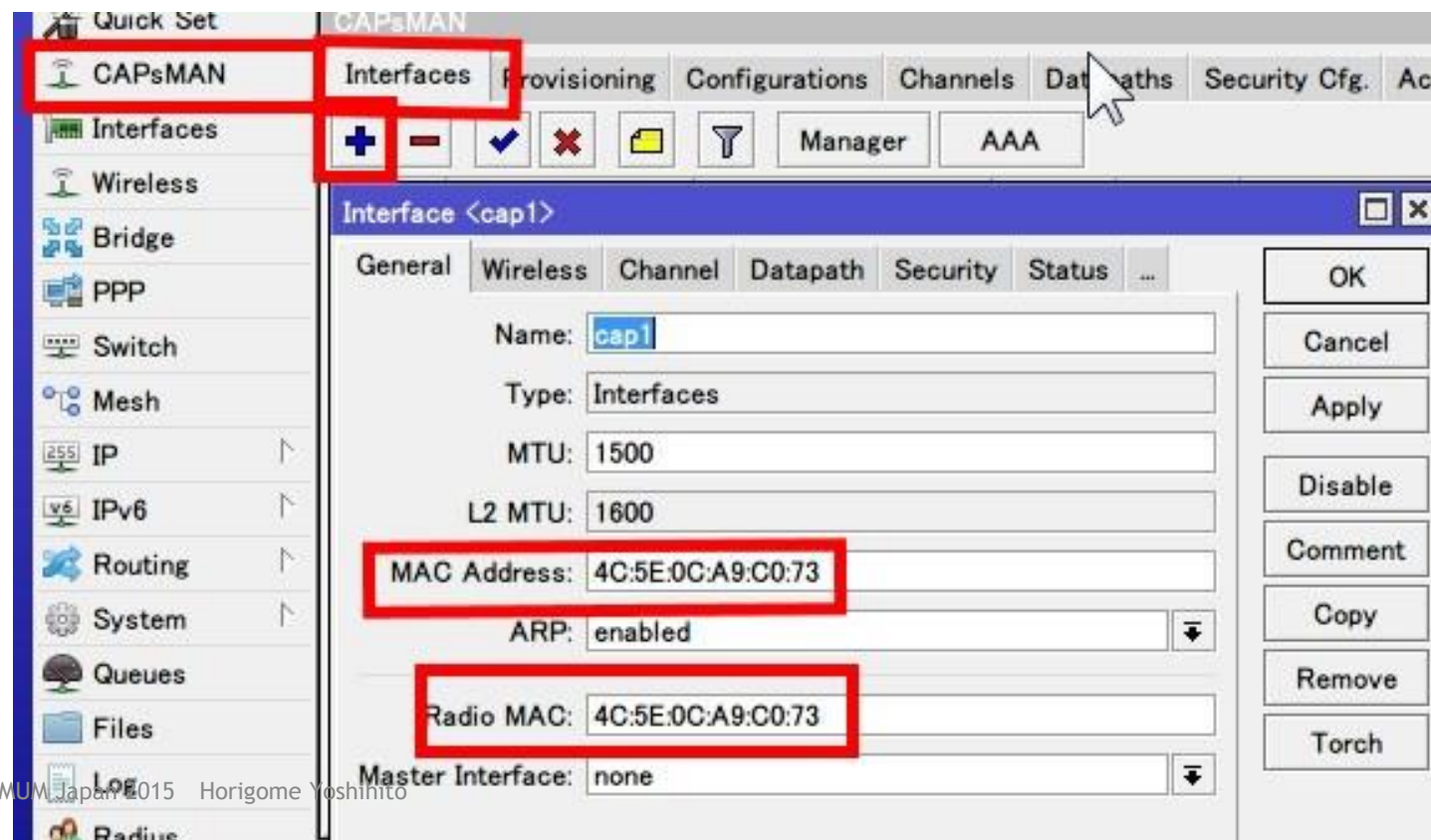
- ▶ <http://wiki.mikrotik.com/wiki/Manual:CAPsMAN>
- ▶ MAC layer connection features:
 - ▶ CAPにIPアドレスの設定が必要ない
 - ▶ 物理、または仮想（L2トンネル）により、CAPとCAPsMANが同じL2セグメントにいる必要がある。
- ▶ IP layer (UDP) connection features:
 - ▶ 必要に応じてNATを通過できます
 - ▶ CAPとCAPsMANは、IPプロトコルで到達出来る必要があります
 - ▶ CAPはCAPsMANと同じL2セグメント上にない場合は、IPマルチキャストベースの検出ではレイヤ3上において動作しないので、CAPsMANはIPアドレスを使用してプロビジョニングする必要があります

CAPの接続について



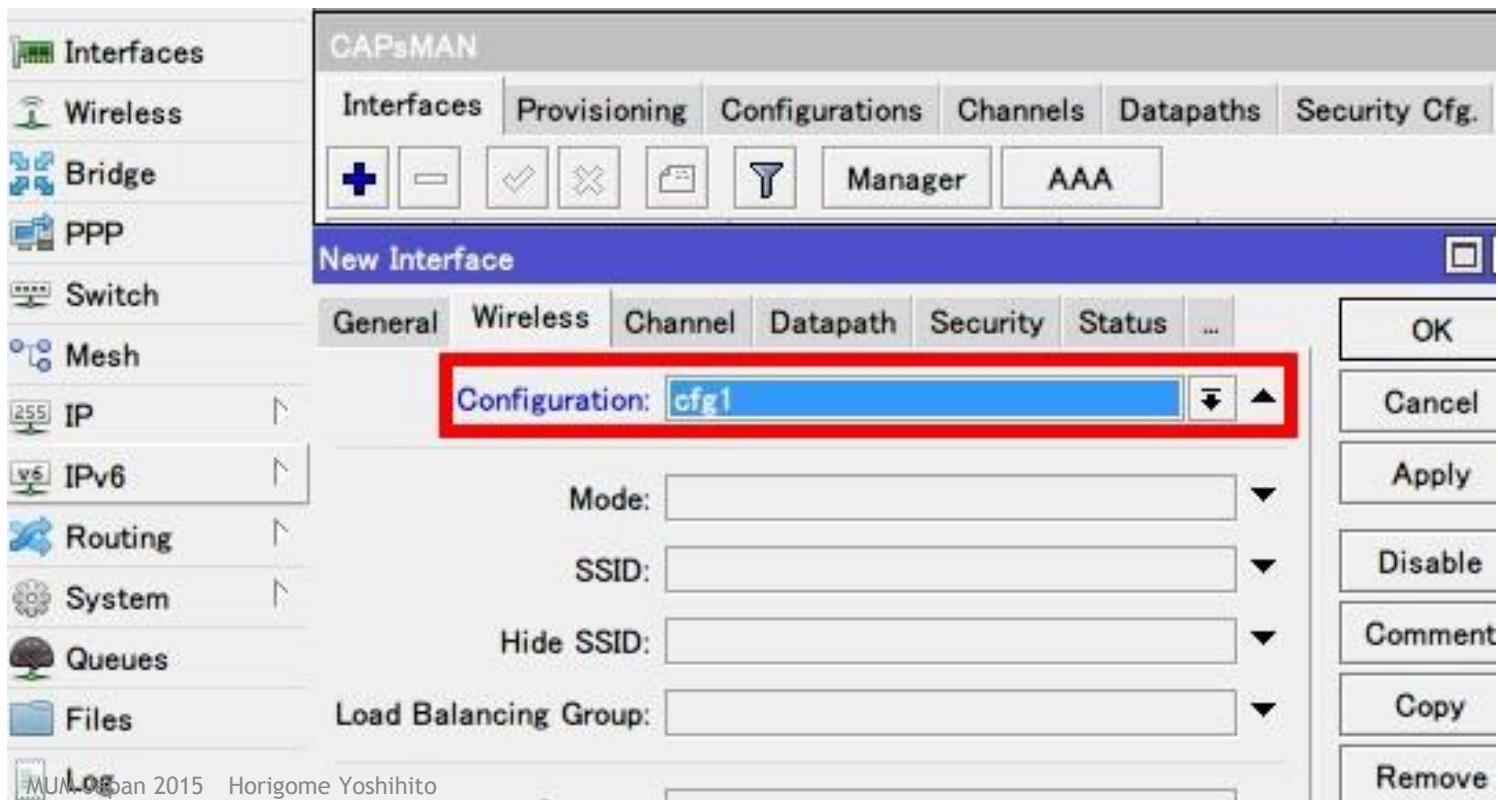
CAPのCAPsMAN設定の有効化

- ▶ MACアドレスはCAPの無線LANのMACアドレスをコピーする必要があります。



CAPのCAPsMAN設定の有効化

- ▶ 先に作ったConfigurationを設定します。



CAPのCAPsMAN設定の有効化

The screenshot displays the Mikrotik WinBox interface for configuring a CAP (Client Access Point) under the CAPsMAN (Centralized Authentication and Provisioning for Management of Access Network) framework.

Interface <cap1>

Wireless | Channel | Datapath | Security | Status | Traffic | ...

Last Link Down Time:

Last Link Up Time:

Link Downs:

Current State:

Current Channel:

Current Rate Set:

Current Basic Rate Set:

Wireless Tables

Interfaces | Nstreme Dual | Access List | Registration | Connect List | Security Profiles | ...

+ - ✓ ✗ 📁 📶 CAP Scanner Freq. Usage Alignment

Name	Type	L2 MTU	Tx	Rx
— managed by CAPsMAN				
— channel: 2452/20-eC/gn(10dBm), SSID: MikrotikUserMeeting, CAPsMAN forwarding				
X wlan1	Wireless (Atheros A...	1600		0 bps

Torch

Registration Tableの確認

CAPsMAN

Channels Datapaths Security Cfg. Access List Remote CAP Radio **Registration Table**

Interface	MAC Address	Tx Rate	Rx Rate	Tx Signal	Rx Signal	Uptime	T...
cap1	50:A7:2B:6C:ED:9D	11Mbps	65Mbps-...	0	-67	00:00:17.90	5...

CAPs AP Client <50:A7:2B:6C:ED:9D>

Interface: cap1

MAC Address: 50:A7:2B:6C:ED:9D

Tx Rate: 11Mbps

Rx Rate: 65Mbps-20MHz/1S

Tx Rate Set: CCK:1-11 OFDM:6-54 BW:1x HT:0-7

Tx Signal: 0

Rx Signal: -67

Uptime: 00:00:17.90

Tx/Rx Packets: 57/96

Tx/Rx Bytes: 11.8 KiB/12.2 KiB

OK

Remove

Copy to Access List

1 item (1 se

Virtual APを使った別APの作成

- ▶ 別AP用の設定を作成します（Country設定を忘れずに）

The screenshot shows the Mikrotik WinBox CAPsMAN interface. The left sidebar contains a menu with items: Quick Set, CAPsMAN, Interfaces, Wireless, Bridge, PPP, Switch, Mesh, IP, IPv6, Routing, System, Queues, Files, and Log. The main window has a tabbed interface with 'Configurations' selected. Below the tabs, there is a table of existing configurations. A 'New CAPs Configuration' dialog is open, showing fields for Name, Mode, SSID, Hide SSID, Load Balancing Group, and Country. The 'Country' field is set to 'japan'.

Name	SSID	Hide SSID	Load Bal...	Country	Channel	Freq
cfg1	MikrotikUserMee...			japan	channel1	

New CAPs Configuration

Wireless | Channel | Datapath | Security

Name:

Mode:

SSID:

Hide SSID:

Load Balancing Group:

Country:

Virtual APを使った別APの作成

- ▶ Master Interfaceを指定します。

CAPsMAN

Interfaces Provisioning Configurations Channels Datapaths Security Cfg. Access

+ - ✓ ✗ 📁 🔍 Manager AAA

New Interface

General Wireless Channel Datapath Security Status ...

Name: cap2

Type: Interfaces

MTU: 1500

L2 MTU:

MAC Address: 00:00:00:00:00:00

ARP: enabled

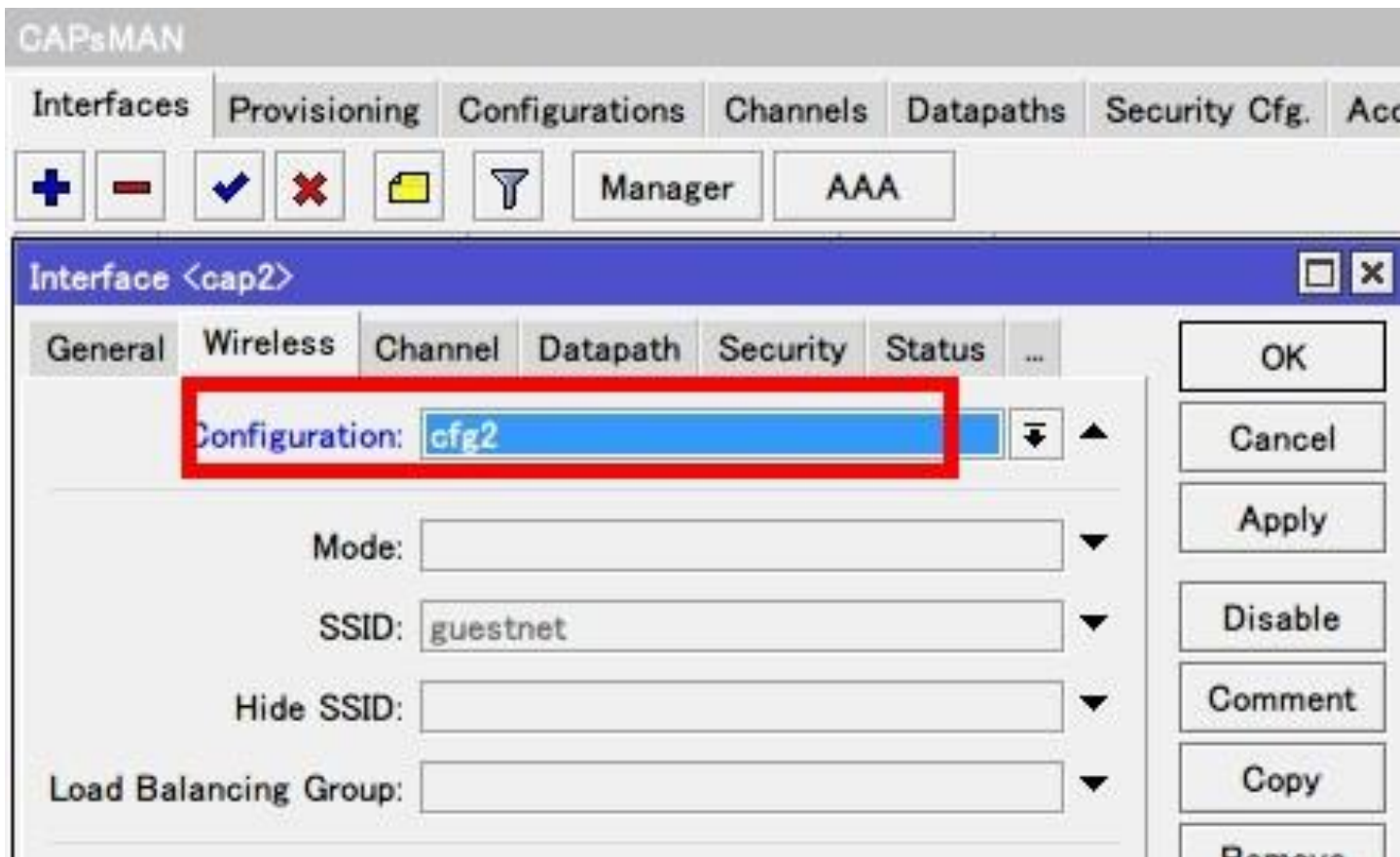
Radio MAC: 00:00:00:00:00:00

Master Interface: cap1

OK Cancel Apply Disable Comment Copy Remove Torch

Virtual APを使った別APの作成

- ▶ 先ほど作成した別AP用の設定を追加します。



Virtual APを使った別APの作成

Wireless Tables										
Interfaces		Nstreme Dual	Access List	Registration	Connect List	Security Profiles	Ch...			
						CAP	Scanner	Freq. Usage	Alignment	W...
	Name	Type	L2 MTU	Tx	Rx					
— managed by CAPsMAN										
— channel: 2452/20-eC/gn(10dBm), SSID: MikrotikUserMeeting, CAPsMAN forwarding										
X	 wlan1	Wireless (Atheros A...	1600		0 bps					
— managed by CAPsMAN										
— SSID: guestnet, CAPsMAN forwarding										
DX	 wlan3	VirtualAP	1600		0 bps					

Access List機能について

- ▶ MAC Authentication
- ▶ Radius Query support
- ▶ MAC Mask support
- ▶ Signal Range
- ▶ Time
- ▶ Private Passphrase
- ▶ VLAN ID assignment

New CAPs Access Rule

MAC Address: ▼

MAC Mask: ▼

Interface: ▼

Signal Range: ▼

▼ Time

Action: ▼

AP Tx Limit: ▼

Client Tx Limit: ▼

Private Passphrase: ▼

Client To Client Forwarding: ▼

RADIUS Accounting: ▼

VLAN Mode: ▼

VLAN ID: ▼

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove

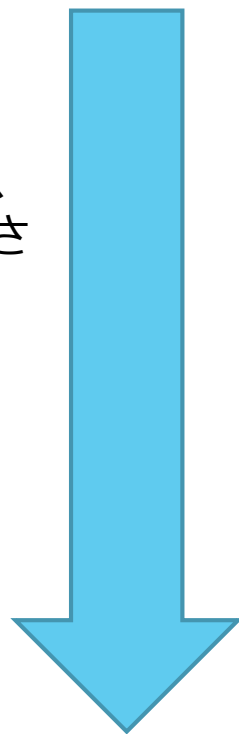
enabled 30

Access List機能について

- ▶ MAC AddressとNetMaskを組み合わせることで、Apple製品だけを接続許可したり、拒否したり出来るようになります。
 - ▶ Device mac address: 18:34:51
 - ▶ Base16 encoding: 183451
 - ▶ vendor name: Apple, Inc.
 - ▶ NetMaskをFF:FF:FF:00:00:00で指定する

CAPsMAN設定は上書きされます

- Channelを参考にとすると、Channelで設定したものはConfigurationで上書きされ、Interfaceで最終的に上書きされます。



The image displays three overlapping screenshots from the Mikrotik WinBox interface, illustrating the configuration hierarchy for CAPsMAN:

- New CAPs Channel:** Shows the initial configuration for a new channel. The 'Name' field is set to 'channel2', 'Frequency' is 2412 MHz, and 'Width' is empty. Buttons for 'OK', 'Cancel', and 'Apply' are visible.
- New CAPs Configuration:** Shows the configuration for a new CAPs configuration. The 'Channel' dropdown is set to 'channel2', 'Frequency' is 2437 MHz, and 'Width' is empty. Tabs for 'Wireless', 'Channel', 'Datapath', and 'Security' are shown.
- Interface <cap2>:** Shows the configuration for a specific interface. The 'Channel' dropdown is set to 'channel2', and 'Frequency' is 2462 MHz. Tabs for 'Wireless', 'Channel', 'Datapath', 'Security', 'Status', and 'Traffic' are shown.

Provisioningについて

CAPs Provisioning <4C:5E:0C:A9:C0:73>

Radio MAC: 4C:5E:0C:A9:C0:73

Hw. Supported Modes: []

Action: create dynamic enabled

Master Configuration: cfg1

Slave Configuration: cfg2

Name Prefix: []

enabled

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove

Provisioningについて

- ▶ Provisioningとは、
 - ▶ 以下の情報に基づいて、先ほどまで設定した内容を自動的に、CAPに適用できるものです。
 - ▶ Identifiersにもとづいて識別できます。
 - ▶ MACアドレスでも出来ます。
 - ▶ CAPsMANv2では、Identifiersや証明書のcommon nameを正規表現で規定することができ、適用することができます。
 - ▶ さらに自動的に作成されるCAPの命名規則なども設定することができます。

Provisioningについて

- ▶ 自動適用については、以下のActionが設定できます
 - ▶ create-disabled : 予め無効のインタフェースを作成します。すなわち、インタフェースはCAPにバインドされますが、インターフェイスを手動で有効にするまで無線は動作しない。
 - ▶ create-enabled : 有効なインタフェースを作成します。
 - ▶ create-dynamic-enabled : 有効なインターフェイスを作成しますが、CAPが接続されない状態（非Provisioning状態）では、インターフェイス設定を削除し、残しておくことはしません。

まとめ

- ▶ 他社のように高いワイヤレスコントローラーを購入しなくても、同じようなことがCAPsManager機能を使って、安価に実現できます。
- ▶ 複数台の無線LAN-APの構築をする際には、Provisioning機能を使うのが便利。
- ▶ 設定をTemplate化しておけるので、設定適用の可視化がしやすくなります。

一方で・・・ (機能要望)

- ▶ HW Protection Modeが設定できないなどの、細かいところに手が届かないとか、
- ▶ 複数台設置のときに、必ずと言って必要になってくる、Data Rates設定が無効化されるとか、
- ▶ Proxy-ARPが、一部の条件下の時に使用できないとか、
- ▶ ということがあるので、是非ともこの辺りは、CAPsMANの制御下から外してもらるか、CAPsMANから設定できるようになってほしいと思っています。

- ▶ ご清聴ありがとうございました。
- ▶ 質問疑問があればどうぞ！