

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)

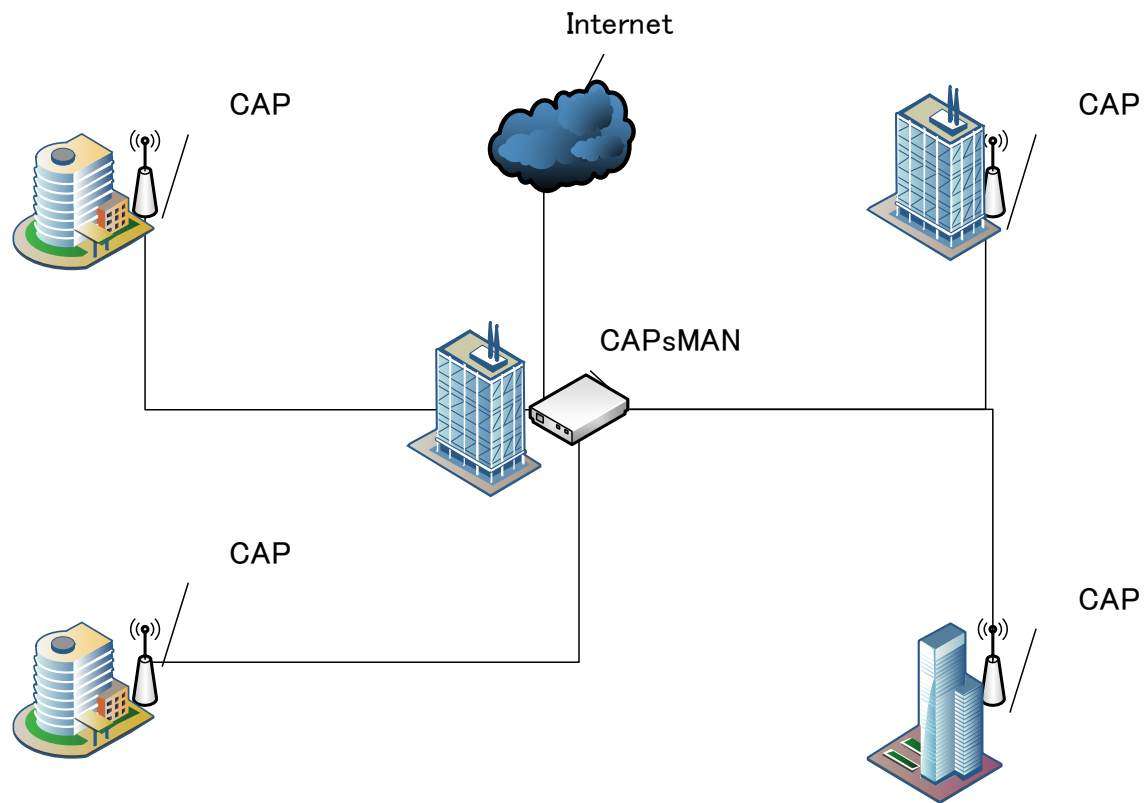
▶ CAPs

- ▶ 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

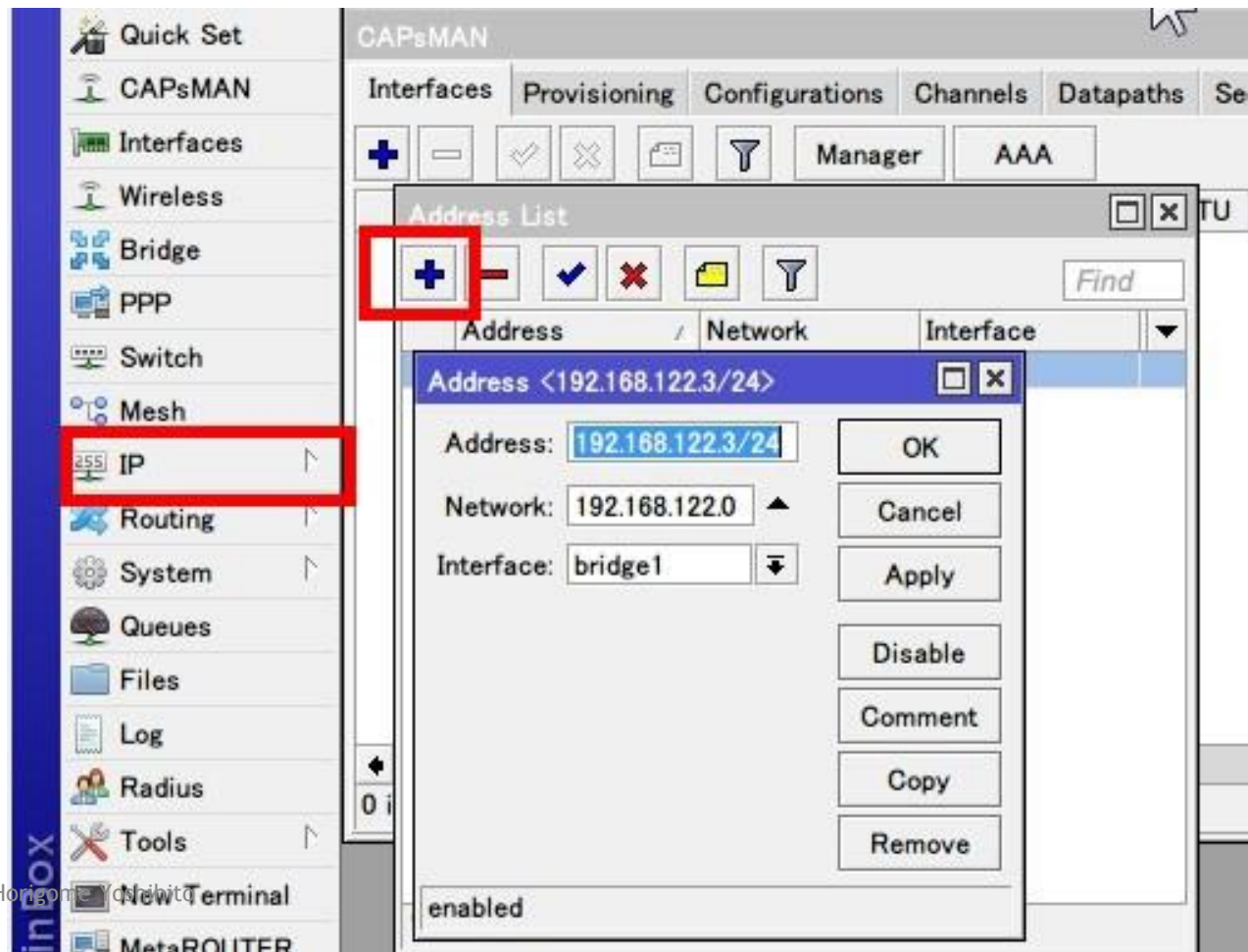
CAPsMANの設定手順

CAPsMANサービスの有効化

The screenshot displays the Mikrotik WinBox interface. On the left sidebar, the 'CAPsMAN' menu item is highlighted with a red box. The main window shows the 'CAPsMAN' configuration page with tabs for 'Interfaces', 'Provisioning', 'Configurations', 'Channels', 'Datapaths', 'Security Cfg.', and 'Access Li'. The 'Manager' button is also highlighted with a red box. A 'CAPs Manager' dialog box is open, showing the 'Enabled' checkbox checked with a red arrow pointing to it. Other fields in the dialog include 'Certificate', 'CA Certificate', 'Require Peer Certificate', 'Generated Certificate', and 'Generated CA Certificate'. Buttons for 'OK', 'Cancel', and 'Apply' are visible on the right side of the dialog.

CAPsMAN設定手順

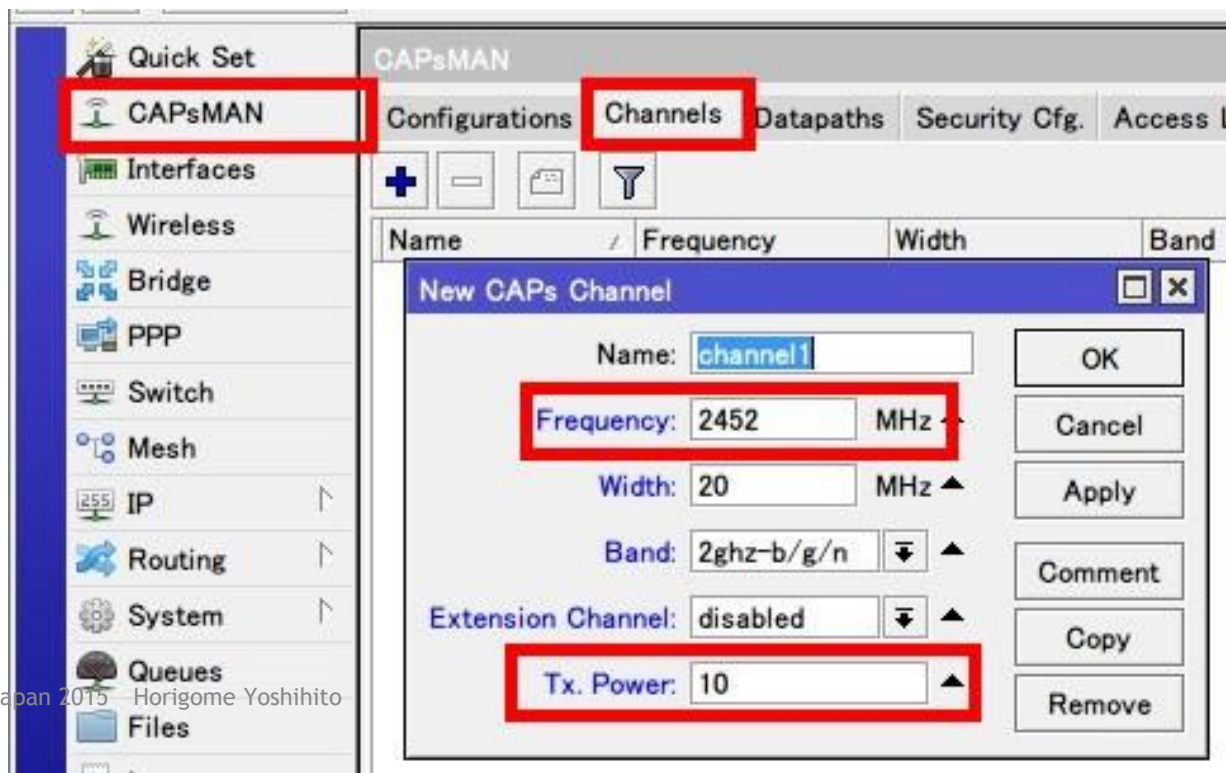
BridgeインターフェイスへのIPアドレス設定



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

The screenshot shows the Mikrotik WinBox interface for configuring CAPsMAN. The left sidebar contains various configuration categories, with 'CAPsMAN' highlighted. The main window displays the 'Configurations' tab, which includes a table of existing configurations and a '+ Add' button. A 'New CAPs Configuration' dialog box is open, allowing for the creation of a new configuration. The dialog has tabs for 'Wireless', 'Channel', 'Datapath', and 'Security'. The 'Wireless' tab is selected, and the following fields are visible: Name (cfg1), Mode (dropdown), SSID (MikrotikUserMeeting), Hide SSID (dropdown), Load Balancing Group (dropdown), Country (japan), and Max Station Count (dropdown). Red boxes highlight the 'Configurations' tab, the '+' button, the Name field, the SSID field, and the Country field. A red arrow points to the Country field.

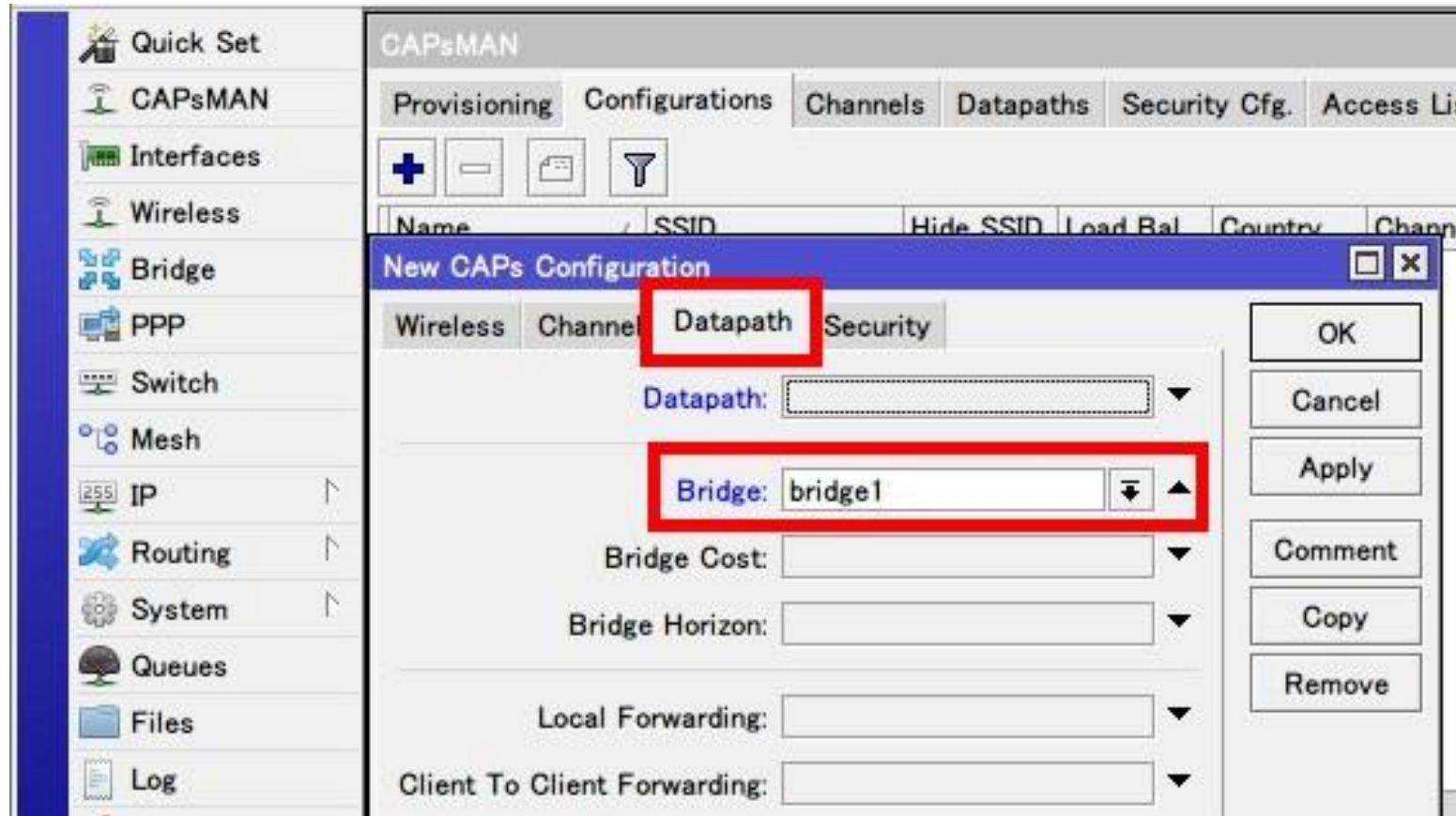
CAPsMAN設定手順

CAPsMAN設定の追加

The screenshot shows the Mikrotik WinBox interface for CAPsMAN configuration. The left sidebar contains a navigation menu with items like Quick Set, CAPsMAN, Interfaces, Wireless, Bridge, PPP, Switch, Mesh, IP, Routing, System, Queues, Files, and Log. The main window is titled 'CAPsMAN' and has several tabs: Provisioning, Configurations, Channels, Datapaths, Security Cfg., Access List, and Remote. The 'Configurations' tab is active, showing a table of configurations. Below the table, there are sub-tabs for 'Wireless', 'Channel', 'Datapath', and 'Security'. The 'Channel' sub-tab is selected, and the 'Channel' dropdown menu is set to 'channel1'. The 'Channel' sub-tab and the dropdown menu are highlighted with red boxes. Below the dropdown menu, there are input fields for Frequency, Width, Band, Extension Channel, and Tx. Power.

CAPsMAN設定手順

CAPsMAN設定の追加



CAPsMAN設定手順

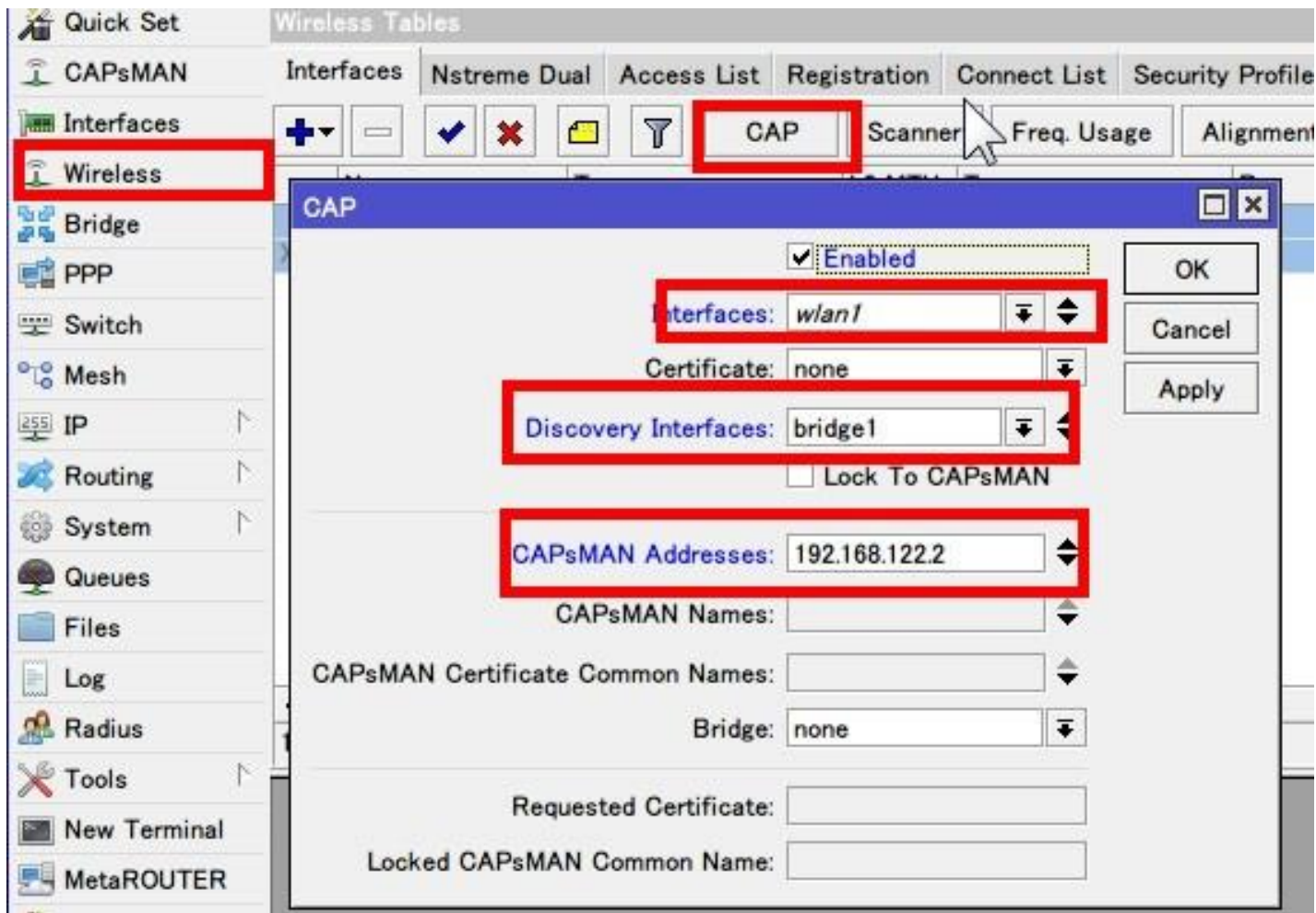
CAPsMAN設定の追加

The screenshot shows the Mikrotik WinBox interface for configuring CAPsMAN. The left sidebar contains various system settings like Quick Set, CAPsMAN, Interfaces, Wireless, Bridge, PPP, Switch, Mesh, IP, Routing, System, Queues, Files, Log, Radius, Tools, New Terminal, and MetaROUTER. The main window is titled 'CAPsMAN' and has tabs for Provisioning, Configurations, Channels, Datapaths, Security Cfg., Access List, Remote CAP, and Radio. A 'New CAPs Configuration' dialog box is open, with the 'Security' tab selected. The 'Security' dropdown is empty. Under 'Authentication Type', 'WPA2 PSK' is selected. Under 'Encryption', 'aes ccm' is selected. The 'Group Encryption' dropdown is set to 'aes ccm'. The 'Passphrase' field contains asterisks and a red note '8文字以上' (8 characters or more). Other fields like 'EAP Methods', 'TLS Mode', and 'TLS Certificate' are empty. Buttons for OK, Cancel, Apply, Comment, Copy, and Remove are on the right.

CAPの接続について

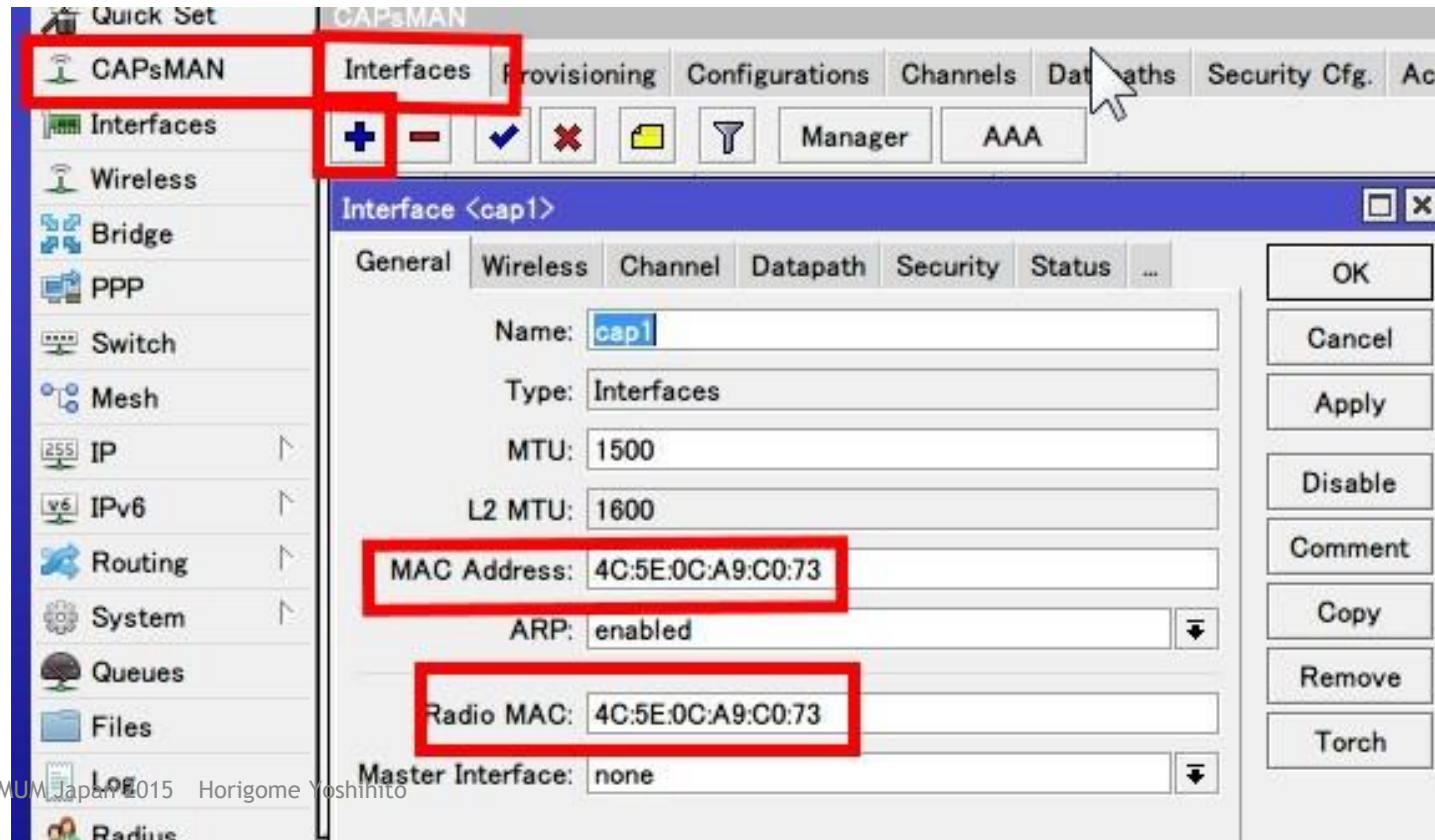
- ▶ <http://wiki.mikrotik.com/wiki/Manual:CAPsMAN>
- ▶ MAC layer connection features:
 - ▶ CAPにIPアドレスの設定が必要ない
 - ▶ 物理、または仮想（L2トンネル）により、CAPとCAPsMANが同じL2セグメントにいる必要がある。
- ▶ IP layer (UDP) connection features:
 - ▶ 必要に応じてNATを通過できます
 - ▶ CAPとCAPsMANは、IPプロトコルで到達出来る必要があります
 - ▶ CAPはCAPsMANと同じL2セグメント上にない場合は、IP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



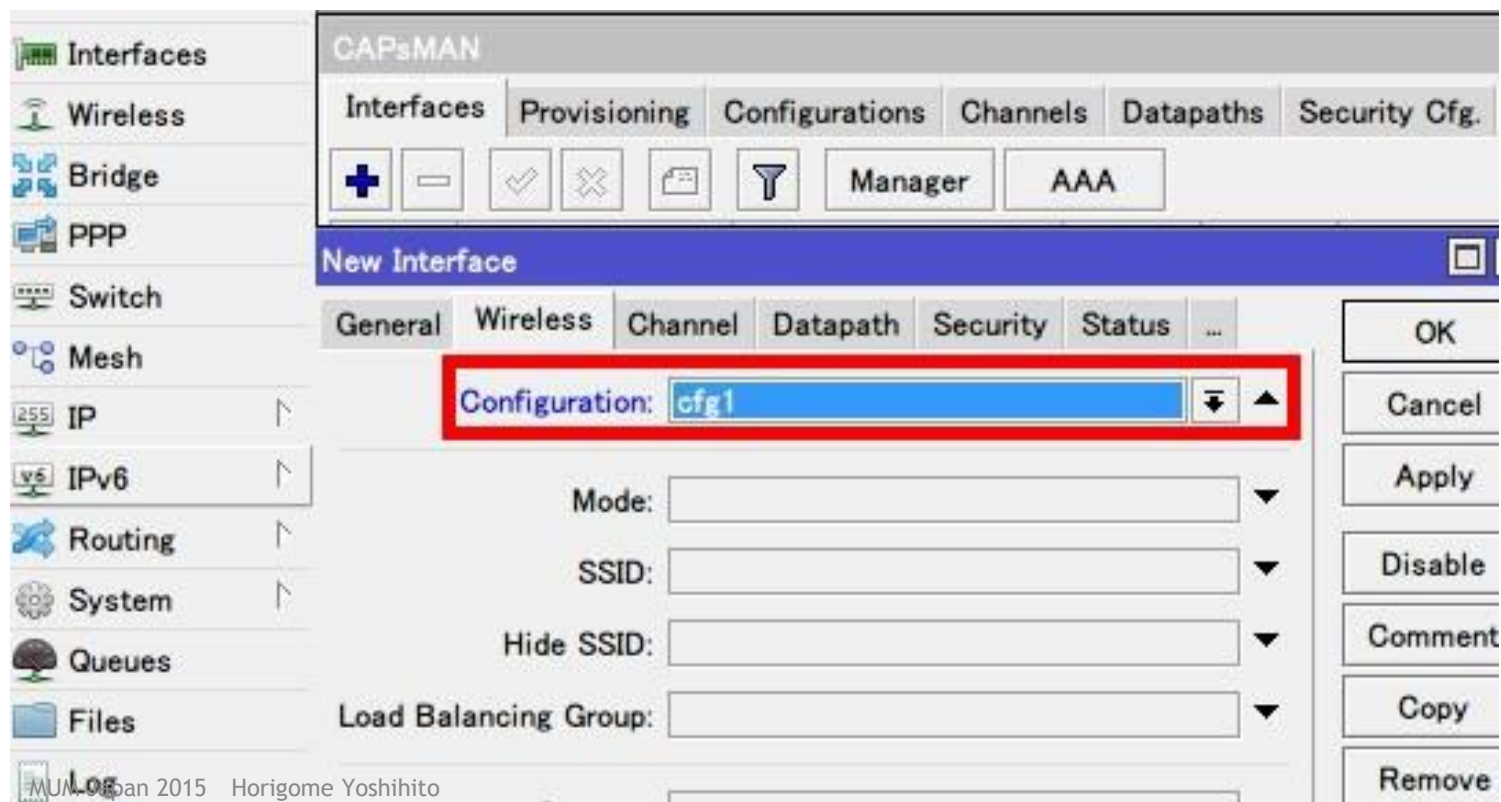
CAPのCAPsMAN設定の有効化

- ▶ 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. On the left, the 'Interface <cap1>' configuration window is open, showing various settings. On the right, the 'Wireless Tables' window is open, displaying a table of wireless interfaces.

Interface <cap1> Configuration:

- Wireless: Channel, Datapath, Security, Status, Traffic, ...
- Last Link Down Time: []
- Last Link Up Time: []
- Link Downs: 0
- Current State: running-ap
- Current Channel: 2452/20-eC/gn(10dBm)
- Current Rate Set: CCK:1-11 OFDM:6-54 BW:1x-2x HT:0-15
- Current Basic Rate Set: CCK:1-11

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

The screenshot shows the CAPsMAN configuration interface. The 'Registration Table' tab is selected and highlighted with a red box. Below the tabs, there are minus and plus icons. A table displays the registration information:

| 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... |

A modal window titled 'CAPs AP Client <50:A7:2B:6C:ED:9D>' is open, showing the configuration for the selected entry:

- 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

Buttons for 'OK', 'Remove', and 'Copy to Access List' are visible on the right side of the modal window.

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 configuration interface. The left sidebar contains navigation options: Quick Set, CAPsMAN, Interfaces, Wireless, Bridge, PPP, Switch, Mesh, IP, IPv6, Routing, System, Queues, Files, and Log. The main window is titled 'CAPsMAN' and has several tabs: Provisioning, Configurations, Channels, Datapaths, Security, Config, Access List, and Remote Config. The 'Configurations' tab is active and highlighted with a red box. Below the tabs, there are icons for adding (+), removing (-), saving (floppy), and filtering (funnel). A table lists existing configurations:

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

Below the table, a 'New CAPs Configuration' dialog is open with the 'Wireless' tab selected. The fields are:

- Name:
- Mode:
- SSID: (highlighted with a red box)
- Hide SSID:
- Load Balancing Group:
- Country: (highlighted with a red box)

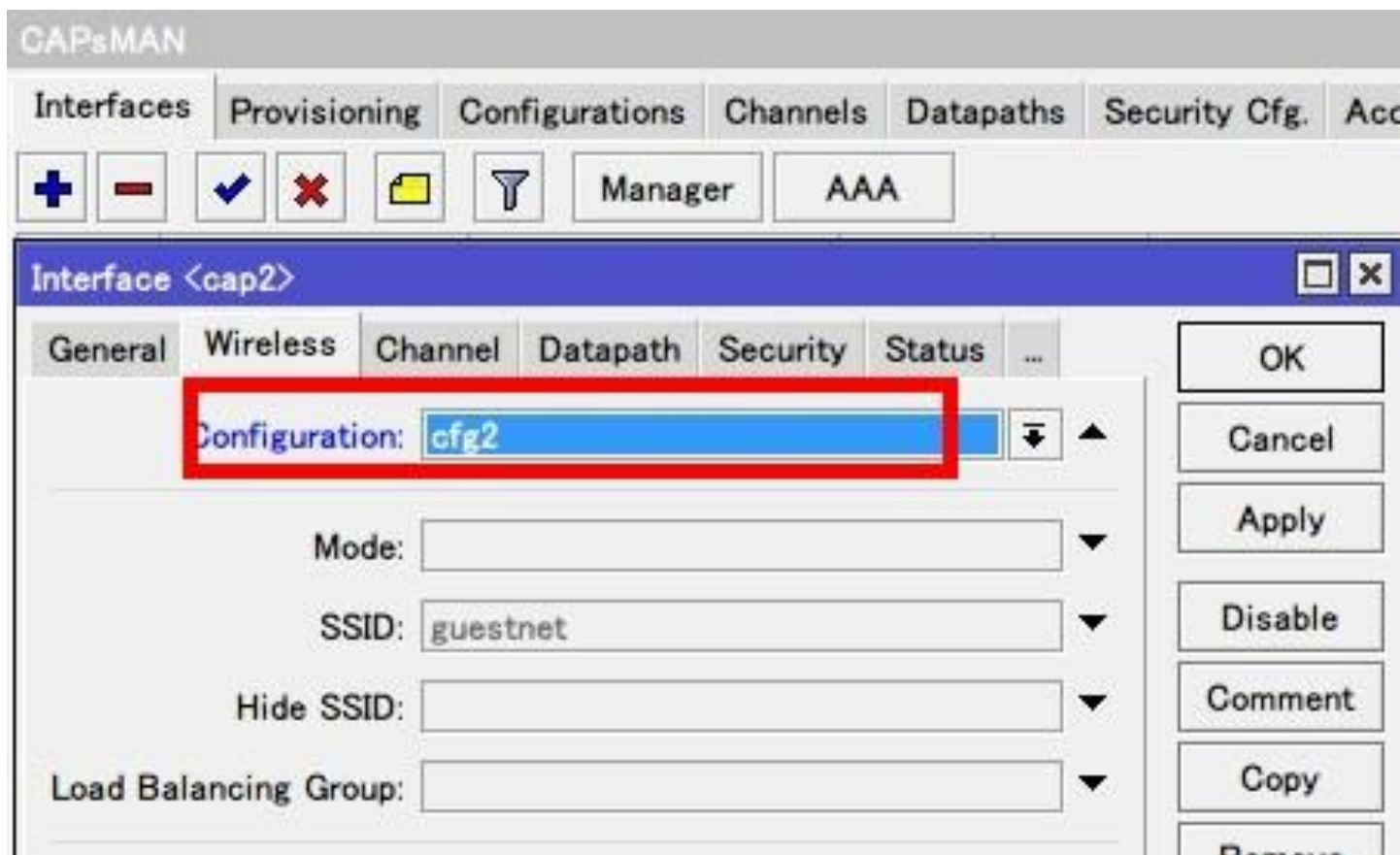
Virtual APを使った別APの作成

- ▶ Master Interfaceを指定します。

The screenshot shows the CAPsMAN configuration interface. The 'New Interface' dialog box is open, displaying the 'General' tab. The 'Name' field is set to 'cap2'. The 'Type' is 'Interfaces', 'MTU' is 1500, 'L2 MTU' is empty, 'MAC Address' is 00:00:00:00:00:00, and 'ARP' is enabled. The 'Radio MAC' is also 00:00:00:00:00:00. The 'Master Interface' field is highlighted with a red box and contains the value 'cap1'. The 'AAA' button in the top toolbar is being clicked by a mouse cursor.

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...

+ - ✓ ✗ [Icon] [Icon] 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 GAPS 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

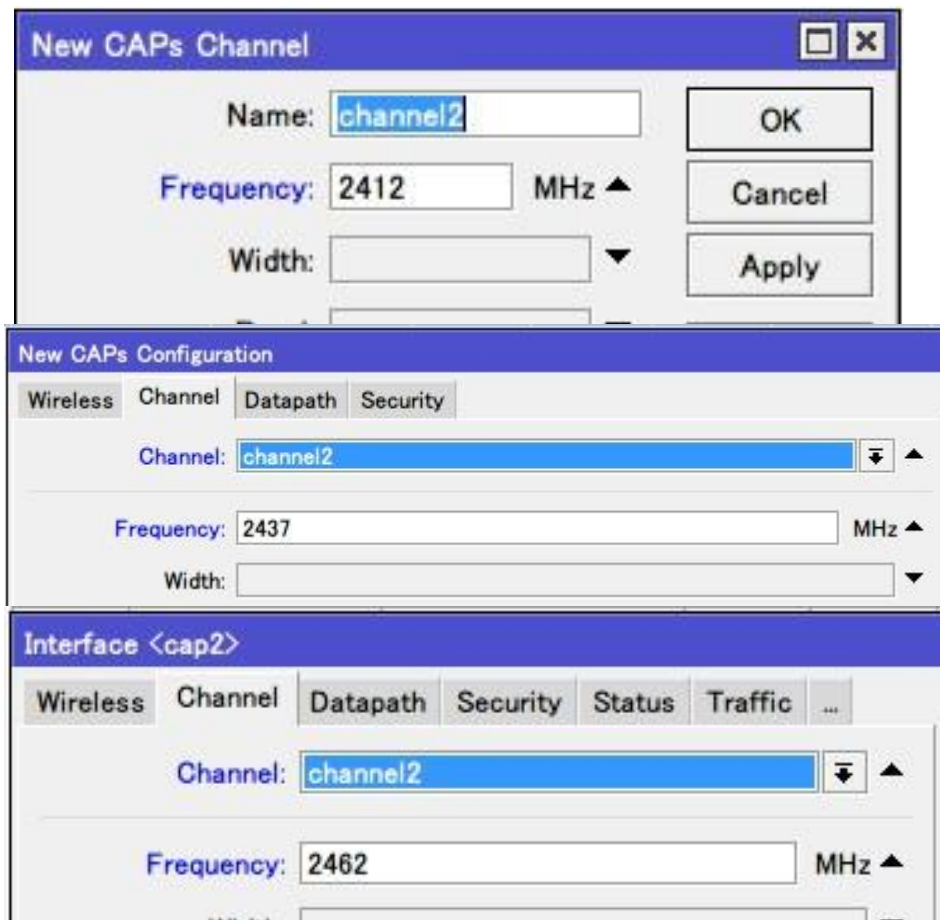
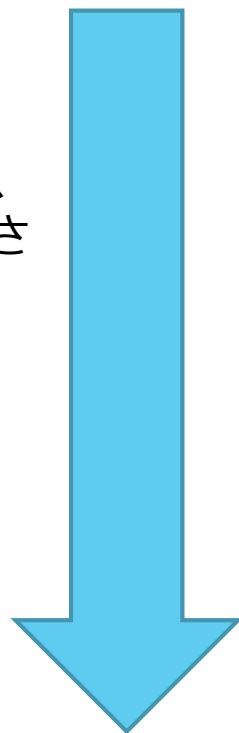
enabled 30

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。



Provisioningについて

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

Radio MAC:

Hw. Supported Modes:

Action:

Master Configuration:

Slave Configuration:

Name Prefix:

enabled

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、インタフェー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 : 有効なインタフェースを作成しますが、CAPが接続されない状態（非Provisioning状態）では、インタフェース設定を削除し、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おうか、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！