MikroTik

CAPsMAN管理及应用

EDCwifi-LI Bo Zhou

概述

- 控制接入点系统管理（CAPsMAN ）允许无线网络的集中管理和必要时的数据处理。使用CAPsMAN 功能时，该网络将包括大量的“受控接入点”（CAP），提供无线连接和一个“系统管理”（CAPsMAN ）管理AP的配置，它也需要负责客户端认证以及可选的数据转发的。
- 当一个CAP被CAPsMAN控制，只要求需要以允许其建立与CAPsMAN连接的最低配置。这是传统上由一个AP（如访问控制，客户端身份验证）执行的功能现在由CAPsMAN执行。CAP设备现在只要提供的无线链路层加密/解密。
- 根据配置的不同，数据或者转交给集中处理CAPsMAN （默认）或转发在CAP本身（本地转发模式 ）。

- **CAPsMAN的特点**
- RADIUS MAC地址认证
- WPA/WPA2安全
- TBA
- **MISSING CAPsMAN功能**
- 支持Nstreme AP
- 支持NV2 AP
- TBA

软件需求

- CAPsMAN适用于从v6.11任何RouterOS的设备，无线接口不是必需的（因为它管理的无线接口的CAPs ）

CAP连接到CAPsMAN

- 对于CAPsMAN系统功能，并提供无线连接，一个CAP必须建立与CAPsMAN管理连接。一个管理连接可以使用MAC或IP层协议来建立和使用“DTLS'是安全的。
- 一个CAP还可以通过在客户端的数据连接到管理中心，但数据连接并不安全。如果被这样认为是有必要的，那么需要使用，例如IPSec或加密隧道数据的安全性的其他手段。
- CAP到CAPsMAN 连接可以使用两个传输协议建立（通过二层和三层）。

- **MAC层连接的特征：**
  - 没有必要在CAP配置IP地址
  - CAP和CAPsMAN必须在同一个二层网络-无论是物理的还是虚拟的（通过二层隧道的方式）
- **IP层（UDP）连接的特征：**
  - 如果有必要，可以穿透NAT
  - 使用IP协议CAP必须能够到达CAPsMAN
  - 如果CAP不在相同的二层网络内的CAPsMAN，它必须提供CAPsMAN IP地址，因为IP组播无法发现工作在三层网络的设备

- 为了建立与CAPsMAN连接，CAP执行发现过程。在发现过程中，CAP尝试联系CAPsMAN并建立一个可用的CAPsMANs列表。CAP尝试使用接触到可用的CAPsMAN：
- 管理配置的IP地址列表
- 从DHCP服务器获取CAPsMAN IP地址列表
- 同时使用广播上这两种配置的接口 - IP和MAC层协议
- **当可用的CAPsMANs的列表中，CAP选择CAPsMAN 基于以下规则：**
- 如果CAPs名称参数指定允许管理的名称（***/system identity*** of CAPsMAN ），早期在列表中的CAP将优先于CAPsMAN，如果列表为空，它可以连接到任何可用的管理器
- MAC层连接合适的管理更优先与IP管理器连接

- **选择管理器后，CAP尝试建立DTLS连接。可以允许两种认证方式：**

- CAP和CAPsMAN没有证书 - 无验证
- 只有管理器配置了证书 - CAP检查CAPsMAN证书，但如果没有适当的可信CA证书并没有失败， CAPsMAN必须配置 **require-peer-certificate=no** 为了建立连接，CAP不具备的证书
- CAP和CAPsMAN配置了证书 - 相互认证

- 建立后DTLS连接，CAP可选择通过检查提供CAPsMAN证书的CommonName领域。**caps-man-certificate-common-names** 参数包含允许的CommonName值列表。如果该列表不为空， CAPsMAN必须使用证书来配置。如果此列表为空， CAP不检查的CommonName字段。

自动锁定CAPsMAN

- CAP可以配置为自动锁定到特定的CAPsMAN 。锁定是通过记录CAPsMAN证书的CommonName的CAP被锁定并检查这个的CommonName实现所有后续的连接。
- 由于此功能使用证书的CommonName实现，证书的使用是强制性的锁定操作。

自动证书

- 为了简化证书时需要（例如，用于自动锁定功能）CAPsMAN和CAP配置， CAPsMAN可以被配置为自动生成必要的证书和CAP可以被配置为从CAPsMAN申请的证书。
- 自动证书不提供完整的公钥基础设施，并提供简单的设置。如果更复杂的PKI是必要的 - 支持适当的证书有效期，多级CA证书，证书更新 - 其他手段必须使用，如手动证书分发或SCEP 。

- 启用锁定由以下面的命令：
- **[admin@CAP] > /interface wireless cap set lock-to-caps-man=yes**
- 一旦CAP连接到合适的CAPsMAN并锁定了它，它也反映这样的：
- **[admin@wtp] > /interface wireless cap print**
  ...
  locked-caps-man-common-name: CAPsMAN-000C424C30F3
- 从现在开始第只会连接到CAPsMAN与此的CommonName，直到锁定要求被清除，通过设置 **lock-to-caps-man=no**. 这种方法需要被使用，如果有必要，迫使CAP锁定到另一个CAPsMAN - 通过在第一设置**lock-to-caps-man=no** 接着用 **lock-to-caps-man=yes.**
  需要注意的是CAP可手动“锁定”，以CAPsMAN通过设置**caps-man-certificate-common-names**.

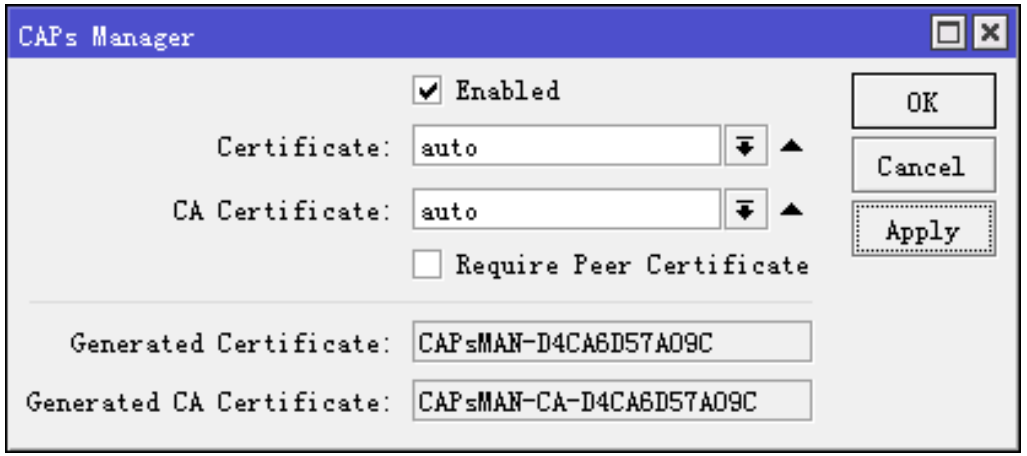
- CAPsMAN具有以下证书设置:
- **certificate -** 这是CAPsMAN证书，私钥必须提供此证书。如果设置为**none**， CAPsMAN将运行在无证书方式，没有证书要求的特性才能工作。如果设置为**auto**， CAPsMAN将尝试使用CA证书颁发证书本身（见CA证书的说明） 。注意的CommonName自动颁发的证书将是“CAPsMAN-<mac address > ”和有效期将是相同的CA证书。

- **ca-certificate** -这是CA证书的CAPsMAN将在必要时签发证书时使用本身（见证书的说明），并自签署证书通行证请求时。如果设置为**none**， CAPsMAN将无法发出证书本身或者通行证签署的证书请求。如果设置为 **auto**， CAPsMAN会产生如CA证书使用自签名的CA证书。CommonName此证书的名称形式将采取“CAPsMAN-CA-<mac address> ”及有效期将从jan/01/1970直到jan/18/2038

当CAPsMAN会自动生成证书，将这样显示：

```
[admin@CM] /caps-man manager> pr
                  enabled: yes
              certificate: auto
           ca-certificate: auto
  require-peer-certificate: no
    generated-certificate: CAPsMAN-000C424C30F3
generated-ca-certificate: CAPsMAN-CA-000C424C30F3
```

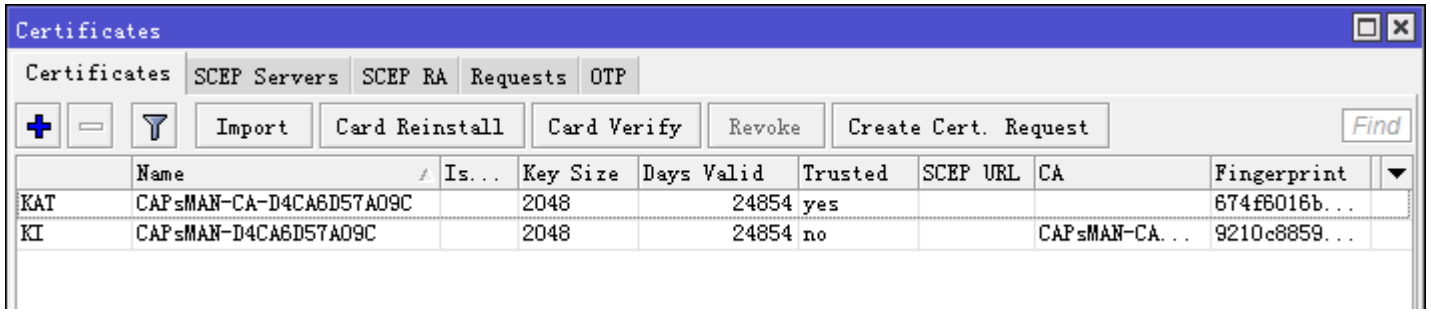
示图：



```
[admin@CM] /certificate> print
detailFlags: K - private-key, D - dsa, L - crl, C - smart-card-key,
A - authority, I - issued, R - revoked, E - expired, T - trusted
 0 K  A T name="CAPsMAN-CA-000C424C30F3" common-name="CAPsMAN-CA-000C424C30F3" key-size=2048
       days-valid=24854 trusted=yes
       key-usage=digital-signature,key-encipherment,data-encipherment,key-cert-sign,crl-sign
       serial-number="1" fingerprint="69d77bbb45c50afd2d6c1785c2a3d72596b8a5f6"
       invalid-before=jan/01/1970 00:00:01 invalid-after=jan/18/2038 03:14:07

 1 K  I  name="CAPsMAN-000C424C30F3" common-name="CAPsMAN-000C424C30F3" key-size=2048
       days-valid=24854 trusted=no key-usage=digital-signature,key-encipherment
       ca=CAPsMAN-CA-000C424C30F3 serial-number="1"
       fingerprint="e853ddb9d41fc139083a176ab164331bc24bc5ed"
       invalid-before=jan/01/1970 00:00:01 invalid-after=jan/18/2038 03:14:07
```

- 示图：



- CAP可从CAPsMAN被配置为要求证书。为了使这项工作，CAP必须配置与设置**certificate=request** 和CAPsMAN必须有CA证书使用（无论是在指定的**CA**证书设置或自动生成）。
- CAP初期将生成私钥和证书请求的CommonName形式“CAP-<mac address> ”。当CAP将建立与CAPsMAN连接，CAP将要求CAPsMAN签署的证书请求。这是否会成功，CAPsMAN将发送CA证书和新发行的证书CAP。CAP将在其证书存储区中导入这些证书：

```
[admin@CAP] > /interface wireless cap print...
          requested-certificate: cert_2
      locked-caps-man-common-name: CAPsMAN-000C424C30F3
[admin@CAP] > /certificate print detail
Flags: K - private-key, D - dsa, L - crl, C - smart-card-key,
A - authority, I - issued, R - revoked, E - expired, T - trusted
 0      T name="cert_1" issuer=CN=CAPsMAN-CA-000C424C30F3 common-name="CAPsMAN-CA-000C424C30F3"
        key-size=2048 days-valid=24837 trusted=yes
        key-usage=digital-signature,key-encipherment,data-encipherment,key-cert-sign,crl-sign
        serial-number="1" fingerprint="69d77bbb45c50afd2d6c1785c2a3d72596b8a5f6"
        invalid-before=jan/01/1970 00:00:01 invalid-after=jan/01/2038 03:14:07

 1 K    T name="cert_2" issuer=CN=CAPsMAN-CA-000C424C30F3 common-name="CAP-000C4200C032"
       key-size=2048 days-valid=24837 trusted=yes
        key-usage=digital-signature,key-encipherment serial-number="2"
        fingerprint="2c85bf2fbc9fc0832e47cd2773a6f4b6af35ef65"
        invalid-before=jan/01/1970 00:00:01 invalid-after=jan/01/2038 03:14:07
```

CAP配置

- 当AP被配置为通过CAPsMAN进行控制，选择的无线接口的配置输入的AP自身被忽略。相反，AP接受来自CAPsMAN选定的无线接口的配置。

- **注意：** CAP无线接口，由CAPsMAN和它的流量被转发到CAPsMAN（即：它们不是在本地转发模式），显示为已禁用，由CAPsMAN管理的注意事项。这是在本地转发模式的接口（流量由CAP本地管理，只有管理是通过CAPsMAN完成）不显示禁用，但注意**通过CAPsMAN管理**显示

- 配置AP的CAP行为 **/interface wireless cap 菜单** 它包含以下设置：

属性	描述
enabled (*yes* | *no*; Default: **no**)	禁用或启用CAP功能
interfaces (*list of interfaces*; Default:**empty**)	要由管理器来控制无线接口列表
certificate (*certificate name* | *none*; Default: **none**)	证书用于验证
discovery-interfaces (*list of interfaces*; Default: **empty**)	接口列表指CAP应该尝试发现管理器
caps-man-addresses (*list of IP addresses*; Default: **empty**)	管理器的IP地址列表CAP将试图发现过程中接触
caps-man-names (*list of allowed CAPs Manager names*; Default: **empty**)	CAP管理器名单列表将尝试连接，如果为空 - CAP不检查管理器名称
caps-man-certificate-common-names (*list of allowed CAPs Manager CommonNames*; Default: **empty**)	管理器证书CommonNames列表CAP将连接到，如果为空 - CAP不检查管理器证书的CommonName
bridge (*bridge interface*; Default: **none**)	当本地转发模式时接口应加桥

CAPsMAN配置概念

- 一个CAP是根据CAPsMAN控制每个无线接口出现在CAPsMAN一个虚拟接口。这提供了一种使用常规RouterOS的功能，如路由，桥接，防火墙等等中的数据转发控制最大的灵活性。
- 许多无线接口设置能够被组合成一个名为组（'profiles '），简化了配置的复用 - 例如，常见的配置设置可以在“配置文件”进行配置，然后多个接口可以参考该配置文件。同时，任何配置文件的设置，可直接在接口配置实现最大的灵活性覆盖。

- 目前有以下设置组：
- channel - 信道相关的设置，例如频率和宽度
- datapath - 数据转发相关的设置，如bridge ，其特定的接口应该被自动添加端口
- interworking - IEEE 802.11u，热点2.0相关设置
- security - 安全相关的设置，例如允许的认证类型或密码
- configuration - 主要的无线设置组，包括设置，如SSID，另外其他设置组结合在一起 - 也就是说，配置文件可以参考通道，安全等命名设置组。此外任何设置可以在配置文件直接覆盖。

- 接口设置的所有设置组结合在一起，但另外任何设置可以直接在界面设置所覆盖。
- 通过设置组的方式，配置在组织层次结构与接口（配置的实际用户）为根。为了弄清楚的一些设置有效值这种结构被咨询的实现方式，其中一个更高的级别设置的值将覆盖水平较低值。

- 例如，当需要WPA2密钥要使用一个特定的接口被发现，以下几个地方进行协商，并与配置WPA2密钥首先指定有效的密码。
- “ - >”表示指的是设置配置文件（如果配置）：
- interface passphrase
- interface->security passphrase
- interface->configuration passphrase
- interface->configuration->security passphrase

- 有2种类型的接口上CAPsMAN - “主”和“从”。主界面保存配置一个实际的无线接口（无线），而从接口链接到主界面，目的是保持配置一个虚拟-AP（多SSID支持）。有设置是有意义的，只是对主界面，即主要是硬件设置相关的设置，如无线电信道的设置。请注意，为了用于无线电接受客户端，它的主接口需要启用。只有当启用，主界面启用从接口将投入使用。
- CAPsMAN接口可以是静态的或动态的。静态接口存储在RouterOS的配置，并会持续到重新引导。只有动态接口，同时存在一个特定的CAP连接到CAPsMAN。

CAPsMAN全局配置

- 设置以启用CAPsMAN发现功能 **/caps-manager manager** 菜单：

属性	描述
enabled (*yes* | *no*; Default: **no**)	禁用或启用CAPsMAN功能
certificate (*auto* | *certificate name* | *none*; Default: **none**)	设备证书
ca-certificate (*auto* | *certificate name* | *none*; Default: **none**)	设备CA证书
require-peer-certificate (*yes* | *no*; Default: **no**)	要求所有的连接CAPs有一个有效的证书

无线配置

- **基于标识符区分CAP之间CAPsMAN。根据以下规则产生的标识符：**

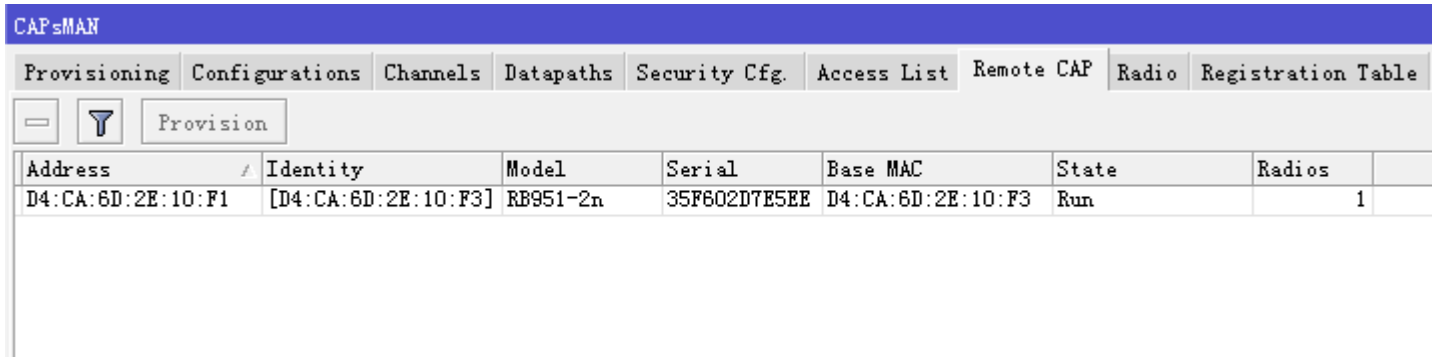
- 如果CAP提供的证书，标识被设置为通用名称字段中输入证书的
- 否则标识符是基于MAC的基础CAP的形式提供： '[XX:XX:XX:XX:XX:XX]'.

- 当成功建立与该第DTLS连接（这意味着第标识符是已知的，有效的），CAPsMAN可以确保有使用CAP相同的标识符不过时的连接。
- 当前连接的CAP列在 **/caps-manager remote-cap** 菜单：

[admin@CM] /caps-manager> remote-cap print

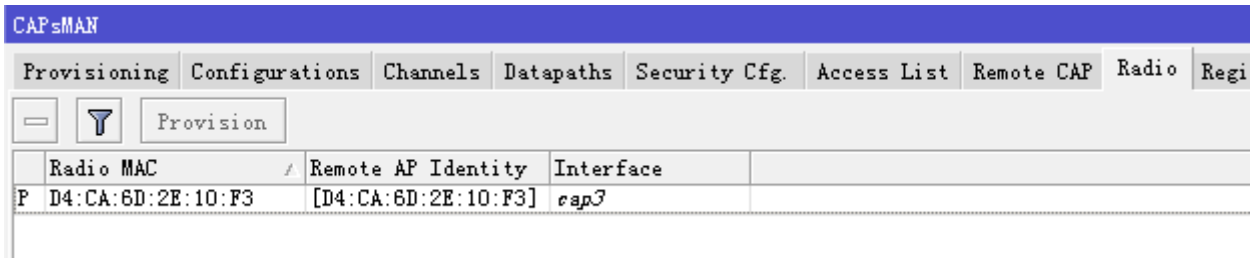
- **# ADDRESS IDENT STATE RADIOS**
  0 00:0C:42:00:C0:32/27044 MT-000C4200C032 Run 1

- 示图：



- 基于其内置的MAC地址（radio-mac ）实际的无线接口（radios ）之间CAPsMAN区分。这意味着它是不可能管理两个无线电与在一个CAPsMAN相同的MAC地址。目前CAPsMAN（通过已连接的CAPs提供）管理无线电列在**/caps-manager radio** 菜单：
  [admin@CM] /caps-manager> radio print
  Flags: L - local, P - provisioned
- **# RADIO-MAC INTERFACE REMOTE-AP-IDENT**
  0 P 00:03:7F:48:CC:07 cap1 MT-000C4200C032

- 示图：



- 当CAP连接，CAPsMAN在首先尝试每个CAP无线电绑定到CAPsMAN主界面基于无线MAC。如果找到一个合适的接口，无线电被设置成使用主界面的配置和引用特定的主接口从接口的配置。此时接口（包括主站和从站）被认为是绑定到无线，被认为是无线电置备。

- 如果没有找到匹配的主接口的无线电，CAPsMAN执行“配置规则”。配置规则是一个有序的规则列表，包含设置，指定无线匹配设置，如果无线电匹配指定要采取什么行动。

- 匹配无线电配置规则配置在**/caps-manager provisioning** 菜单：

属性	描述
action (*create-disabled* | *create-enabled* | *create-dynamic-enabled* | *none*; Default:**none**)	如果行动规则匹配由以下设置规定采取： **create-disabled** - 创建禁用静态接口的无线电。也就是说，该接口将被绑定到无线，但无线不会操作，直到接口手动启用; **create-enabled** - 启用创建静态接口。也就是说，该接口将被绑定到广播电台将投入运营; **create-dynamic-enabled** - 创建启用了动态接口。也就是说，该接口将被绑定到无线，无线电将业务; **none** - 什么都不做，离开无线电无配置状态;
master-configuration (; Default:)	**如果动作指定要创建的接口，然后用它的配置设置为这个配置文件一个新的主界面将被创建**
slave-configurations (; Default:)	**如果动作指定要创建的接口，然后在这个列表中的新从属接口为每个配置文件被创建。**
radio-mac (*MAC address*; Default:**00:00:00:00:00:00**)	**无线MAC地址进行匹配，空的MAC（00:00:00:00:00:00）表示匹配所有MAC地址**
? (*?*; Default: **?**)	**（更多的匹配可能在将来的版本中提供）**

- 注意： 如果没有规则匹配无线，然后用行动隐含的默认规则创建功能，没有配置设置被执行。

  为了得到有效配置匹配器：
  [admin@CM] /caps-manager provisioning> print
- **Flags: X - disabled**
  0 radio-mac=00:00:00:00:00:00 action=create-enabled master-configuration=main-cfg
  slave-configurations=virtual-ap-cfg

  为了用户的方便有命令，允许重新执行配置过程中的一些广播或通过某些AP提供的所有无线：

  [admin@CM] > caps-manager radio provision 0

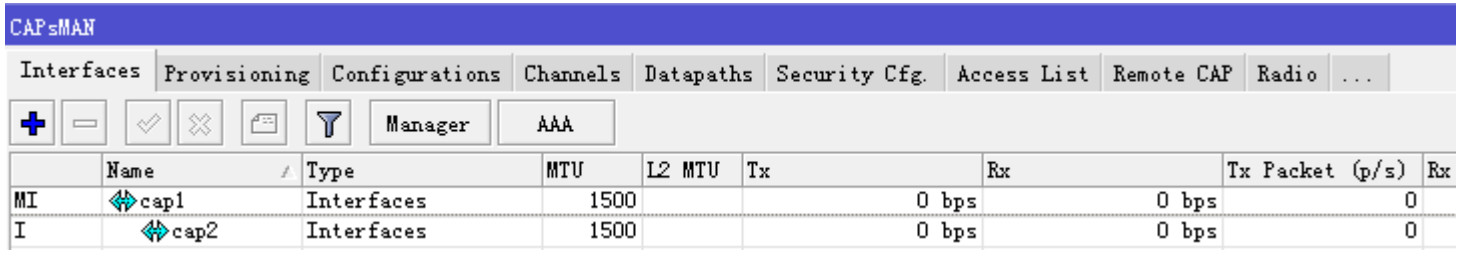
  和

  [admin@CM] > caps-manager remote-cap provision 0

接口配置

- CAPsMAN接口管理**/caps-manager interface** 菜单:
- **[admin@CM] > /caps-manager interface print**
  Flags: M - master, D - dynamic, B - bound, X - disabled, I - inactive, R - running
  # NAME RADIO-MAC MASTER-INTERFACE
  0 M BR cap2 00:0C:42:1B:4E:F5 none
  1 B cap3 00:00:00:00:00:00 cap2

  示图：



数据路径配置

- 数据路径设置控制数据转发相关方面。在CAPsMAN数据路径设定是在数据通路配置菜单**/caps-manager datapath** 或直接在一个配置文件或界面菜单设置为**datapath**。
- 主要有两个转发模式：

- 本地转发模式，无线接口并从其中CAP本地转发数据
- 管理转发模式，其中CAP发送到CAPsMAN收到了无线的所有数据，只发送了从CAPsMAN接收到的无线数据。在这种模式下，即使客户端 - 客户端转发进行控制和由CAPsMAN执行。

- 转发模式为基于每个接口进行配置 - 所以，如果一个CAP提供了2个无线接口，可以配置为在本地转发模式，另一个在管理的转发模式。这同样适用于虚拟-AP接口 - 每一个都可以由主接口或其他虚拟-AP接口具有不同的转发模式。
- 大部分的数据路径设置仅适用于管理转发模式，因为在本地转发模式CAPsMAN不具有对数据转发控制。

- 有下面的数据路径设置：

- bridge -- 启用时，interface 加入桥 ，作为一个网桥端口
- bridge-cost -- 网桥端口为网桥端口增加时使用
- bridge-horizon -- bridge horizon 网桥端口增加时使用
- client-to-client-forwarding -- 控制如果连接到接口的无线客户端之间的客户端 - 客户端转发应该允许在本地转发模式下，该功能是通过CAP进行，否则它是由CAPsMAN执行。
- local-forwarding -- 转发的控制模式
- openflow-switch -- OpenFlow的交换机接口加入，端口为启用时
- vlan-id -- VLAN ID分配给接口，如果VLAN模式允许使用VLAN标记
- vlan-mode -- VLAN标记模式，如果指定的VLAN标记应分配给接口（导致所有接收到的数据，以得到标有VLAN标签，并允许接口只发送了标有特定标记的数据）

本地转发模式

- 在这种模式下，对CAP无线接口相当于一个正常的界面，并参与正常的数据转发。无线接口将接受/传递数据到CAP网络堆栈。CAPsMAN不会参与数据转发，不会处理任何数据帧的，它只会控制接口的配置和客户端的关联过程。
- 在CAP无线接口将改变其配置为“"enabled ”，其状态和一些相关参数（如MAC地址，ARP，MTU）将反映在CAPsMAN的接口。需要注意的是无线相关的配置将不会应用于由CAPsMAN不代表实际的接口配置：

- **[admin@CAP] /interface wireless> pr**
  Flags: X - disabled, R - running
  0 R ;;; managed by CAPsMAN
  ;;; channel: 5180/20-Ceee/ac, SSID: master, local forwarding
  name="wlan2" mtu=1500 mac-address=00:03:7F:48:CC:07 arp=enabled
  interface-type=Atheros AR9888 mode=ap-bridge ssid="merlin"
  frequency=5240 band=5ghz-a/n channel-width=20/40mhz-eC scan-list=default

- 在本地转发模式虚拟AP接口将显示为enabled 和 dynamic 虚拟-AP接口：

```
[admin@CAP] /interface> pr
Flags: D - dynamic, X - disabled, R - running, S - slave
 #     NAME                            TYPE        MTU L2MTU  MAX-L2MTU
...
2  RS ;;; managed by CAPsMAN
       ;;; channel: 5180/20-Ceee/ac, SSID: master, local forwarding
       wlan2                           wlan        1500  1600
3 DRS ;;; managed by CAPsMAN
       ;;; SSID: slave, local forwarding
       wlan6                           wlan        1500  1600
...
[admin@CAP] /interface> wireless pr
  Flags: X - disabled, R - running
 ...
2  R ;;; managed by CAPsMAN
     ;;; SSID: slave, local forwarding
     name="wlan6" mtu=1500 mac-address=00:00:00:00:00:00 arp=enabled
     interface-type=virtual-AP master-interface=wlan2
```

- 该虚拟-AP接口添加为动态的，事实上有些CAP上进行数据转发限制静态配置的可能性，如地址分配给虚拟-AP接口。这不适用于掌握无线接口。
  为了便于数据转发的配置，CAP可以与桥，其接口为连接时，接口由CAPsMAN启用自动添加配置。这可以做 **/interface wireless cap** 菜单。

管理转发模式

- 在这种模式下发送CAP接收到无线到CAPsMAN所有数据，只发送了超过无线，从CAPsMAN接收到的数据。CAPsMAN拥有完全控制权，包括客户端 - 客户端转发数据的转发。在CAP无线接口被禁用，并且不参与网络：

...

- **1 X ;;; managed by CAPsMAN**
  ;;; channel: 5180/20-Ceee/ac, SSID: master, manager forwarding
  name="wlan2" mtu=1500 mac-address=00:03:7F:48:CC:07 arp=enabled
  interface-type=Atheros AR9888 mode=ap-bridge ssid="merlin"

- 虚拟AP接口也是创建为“disabled ”，不参与对CAP数据转发。

访问列表

- 在CAPsMAN访问列表规则中，用于允许/拒绝客户端连接到下CAPsMAN控制任何第一个有序列表。当客户端试图连接到由CAPsMAN控制的CAP，CAP请求转发到CAPsMAN 。作为注册过程的一部分，CAPsMAN咨询访问列表，以确定客户端是否应该允许进行连接。
- 直到匹配规则被发现访问列表规则的处理一个接一个。然后执行在匹配规则的动作。如果行动指定客户端应该被接受，客户端被接受，可能覆盖它与在访问列表中规则中指定的那些默认的连接参数。

- 访问列表配置在**/caps-manager access-list** 的菜单。有访问列表的规则如下参数：
- **客户端匹配参数：**
  - address - 客户端的MAC地址
  - mask - 用客户端地址和MAC地址掩码来进行比较
  - interface - 可选的接口与接口可比性，后者的客户端实际上是连接到
  - time - 规则匹配的时间为一天
  - signal-range - 范围，其中客户端信号必须适合规则匹配
- **action parameter - 指定动作，当客户端匹配采取：**
  - accept - 接受客户端
  - reject - 拒绝客户端
  - query-radius - 查询RADIUS服务器，如果特定的客户端允许连接

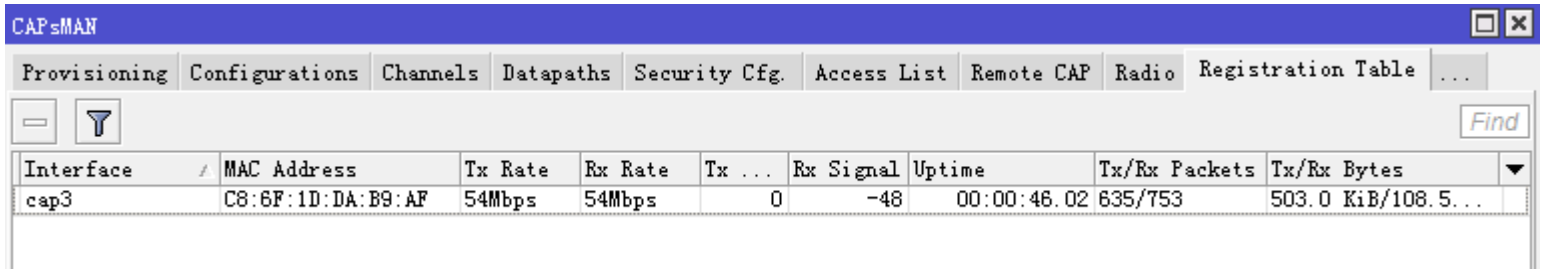
- 连接参数：

- ap-tx-limit - 以客户端TX限速的方向
- client-tx-limit - 在管理TX速度限制（仅适用于RouterOS的客户端）
- client-to-client-forwarding - 指定是否允许从该客户机接收到连接到同一接口的其他客户端转发数据
- private-passphrase - 如果使用PSK认证算法，客户端使用PSK密码
- radius-accounting - 指定是否应使用RADIUS流量计费，如果RADIUS身份验证获取此客户端完成
- vlan-mode - VLAN标记模式指定，如果流量从客户端来应该得到标记（和未标记的客户端）。
- vlan-id - VLAN ID来使用，如果这样做VLAN标记。

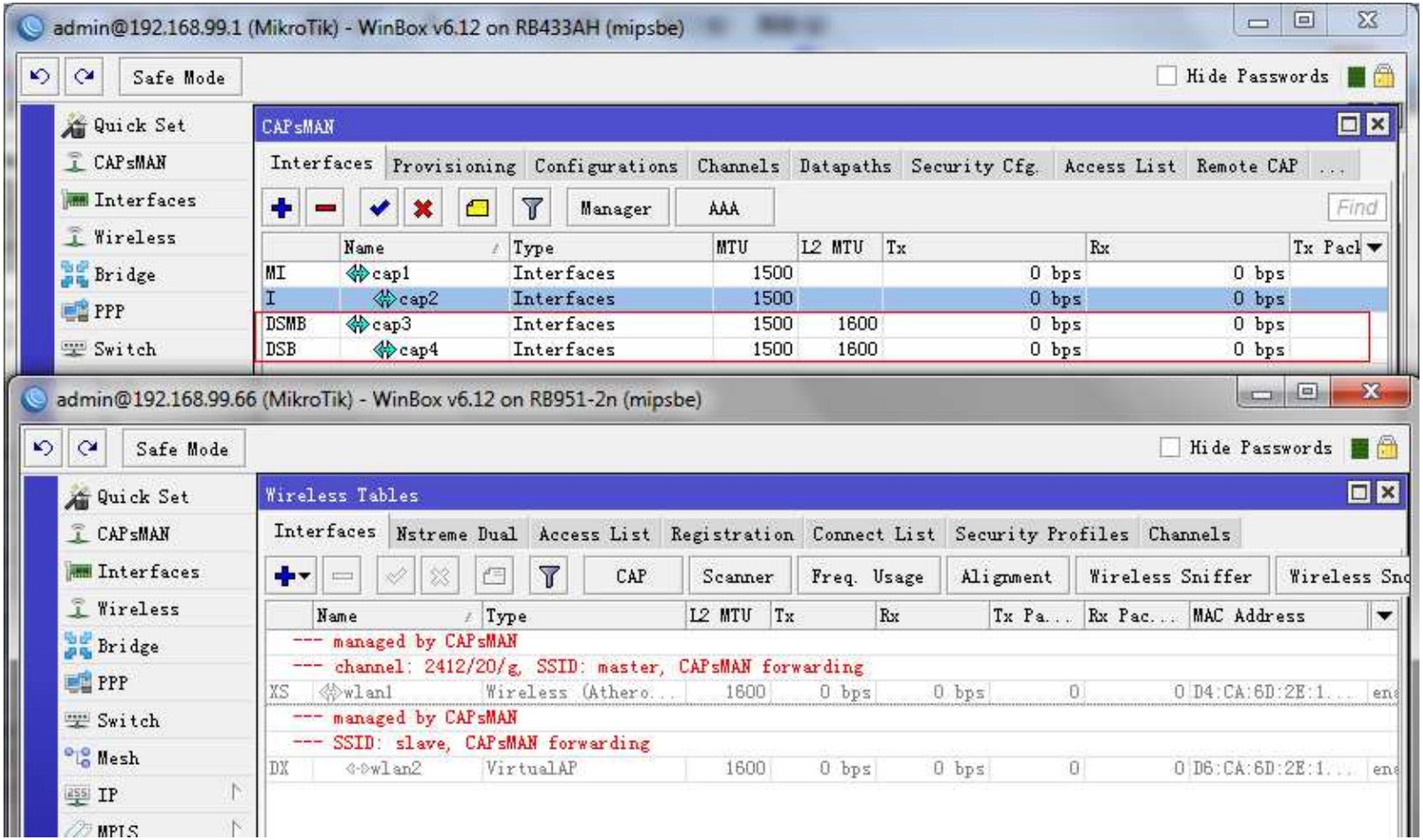
登记表

- 登记表中包含了连接到由CAPsMAN控制的无线，可在客户端列表 **/caps-manager registration-table** 菜单：

- **[admin@CM] /caps-manager> registration-table print**
  # INTERFACE MAC-ADDRESS UPTIME RX-SIGNAL
  0 cap1 00:03:7F:48:CC:0B 1h38m9s210ms -36
- 示图：

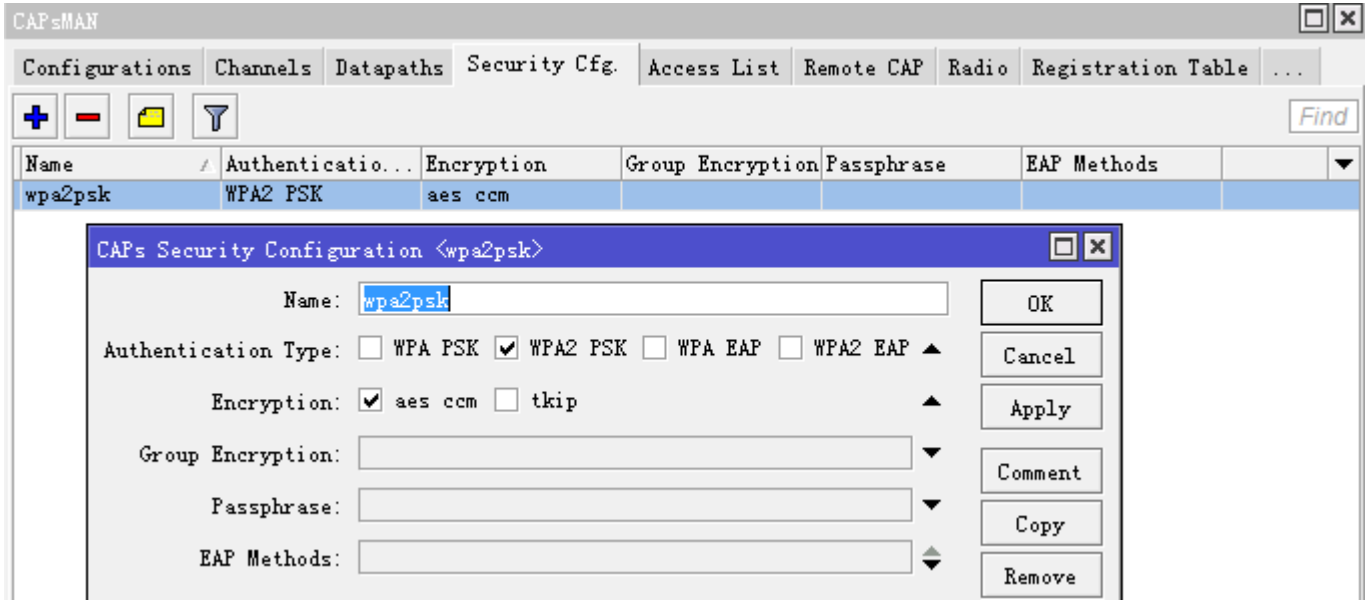


实例

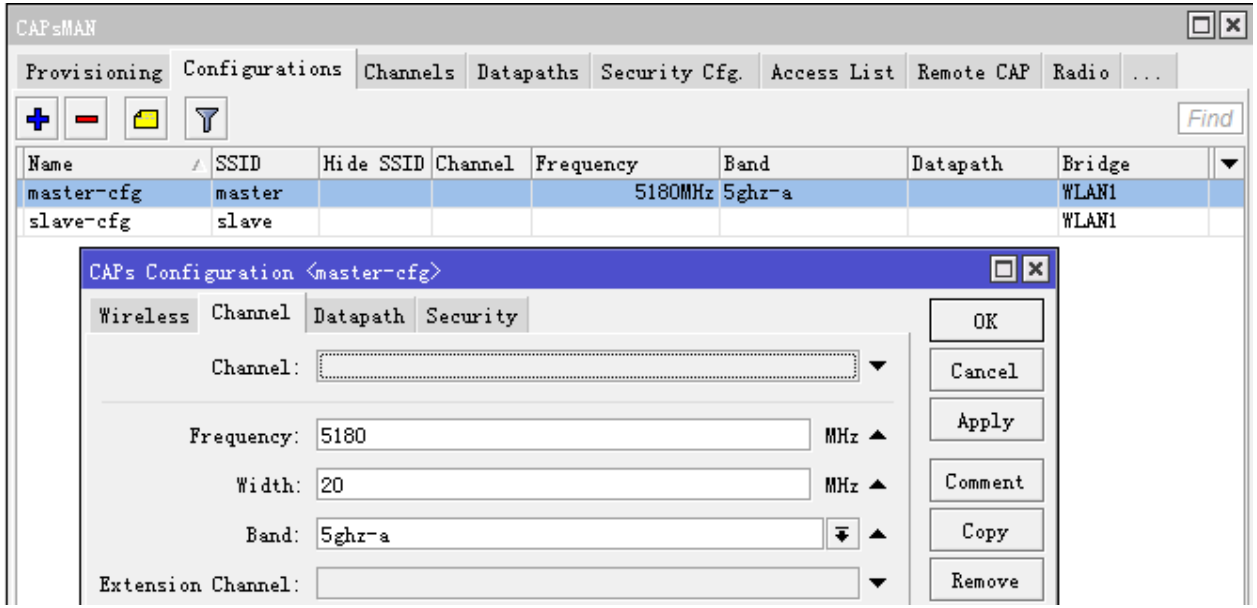

admin@192.168.99.1 (MikroTik) - WinBox v6.12 on RB433AH (mipsbe)
Safe Mode
Hide Passwords
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
CAPsMAN
Interfaces
Provisioning
Configurations
Channels
Datapaths
Security Cfg.
Access List
Remote CAP
Manager
AAA
Find
Name
Type
MTU
L2 MTU
Tx
Rx
Tx Pacl
MI cap1 Interfaces 1500 0 bps 0 bps
I cap2 Interfaces 1500 0 bps 0 bps
DSMB cap3 Interfaces 1500 1600 0 bps 0 bps
DSB cap4 Interfaces 1500 1600 0 bps 0 bps
admin@192.168.99.66 (MikroTik) - WinBox v6.12 on RB951-2n (mipsbe)
Safe Mode
Hide Passwords
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
MPLS
Wireless Tables
Interfaces
Nstreme Dual
Access List
Registration
Connect List
Security Profiles
Channels
CAP
Scanner
Freq. Usage
Alignment
Wireless Sniffer
Wireless Snc
Name
Type
L2 MTU
Tx
Rx
Tx Pa...
Rx Pac...
MAC Address
--- managed by CAPsMAN
--- channel: 2412/20/g, SSID: master, CAPsMAN forwarding
XS wlan1 Wireless (Athero... 1600 0 bps 0 bps 0 0 D4:CA:6D:2E:1...
--- managed by CAPsMAN
--- SSID: slave, CAPsMAN forwarding
DX wlan2 VirtualAP 1600 0 bps 0 bps 0 0 D6:CA:6D:2E:1...

- 创建**WPA2 PSK**安全配置文件，而无需指定口令：

[admin@CM] /caps-manager security>add name="wpa2psk" authentication-types=wpa2-psk encryption=aes-ccm



- 创建配置文件要使用的主界面
- 在配置中指定WPA2密钥
- 在配置中指定通道的设置：
- **[admin@CM] /caps-manager configuration> add name=master-cfg ssid=master security=wpa2psk security.passphrase=12345678 channel.frequency=5180 channel.width=20 channel.band=5ghz-a**

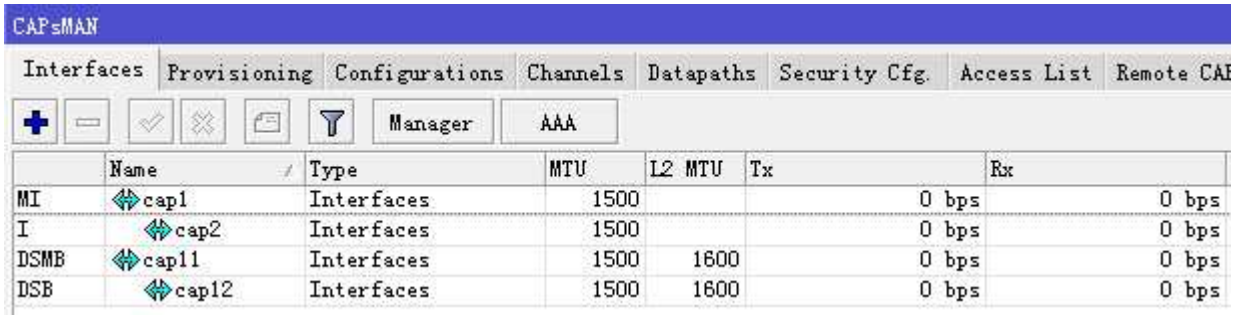


- 创建配置文件要使用虚拟AP接口
- 在配置中指定不同的WPA2密钥：
- **[admin@CM] /caps-manager configuration> add name=slave-cfg ssid=slave security=wpa2psk security.passphrase=87654321**

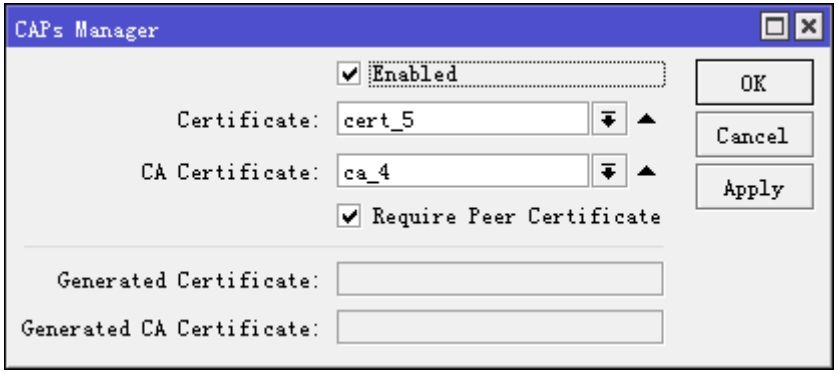
  创建配置规则匹配的任何无线电和采用master-cfg 和 slave-cfg 创建动态界面：
- **[admin@CM] /caps-manager provisioning> add action=create-dynamic-enabled master-configuration=master-cfg slave-configurations=slave-cfg**

- 现在，当AP连接，并置备2动态接口（一个主机和一个从机）将获得创建：
- **[admin@CM] /caps-manager interface> print detail Flags: M - master, D - dynamic, B - bound, X - disabled, I - inactive, R - running**

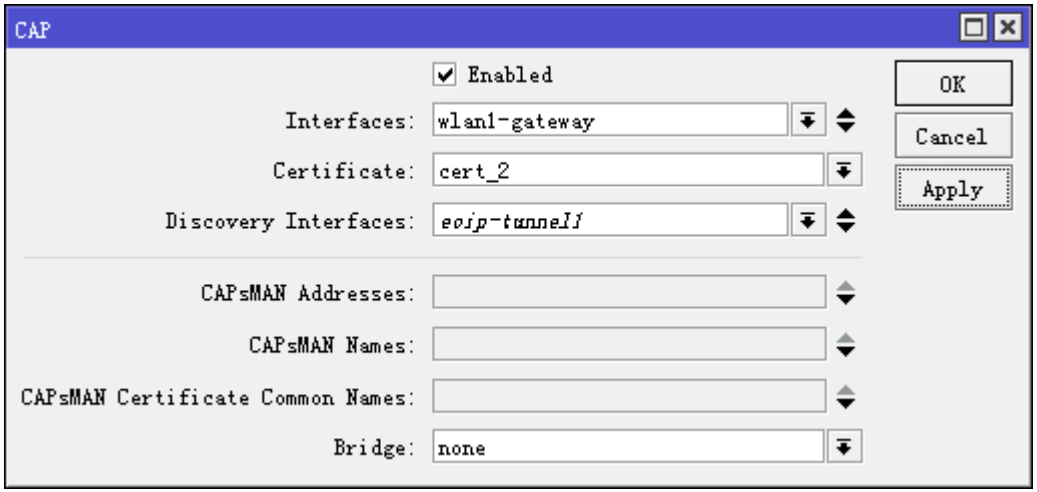
- **0 MDB name="cap1" mtu=1500 l2mtu=2300 radio-mac=00:0C:42:1B:4E:F5 master-interface=none configuration=master-cfg**
- **1 DB name="cap2" mtu=1500 l2mtu=2300 radio-mac=00:00:00:00:00:00 master-interface=cap1 configuration=slave-cfg**



- **CAPsMAN管理端设置:**
- 启用CAPsMAN功能
- 启用CA证书验证功能



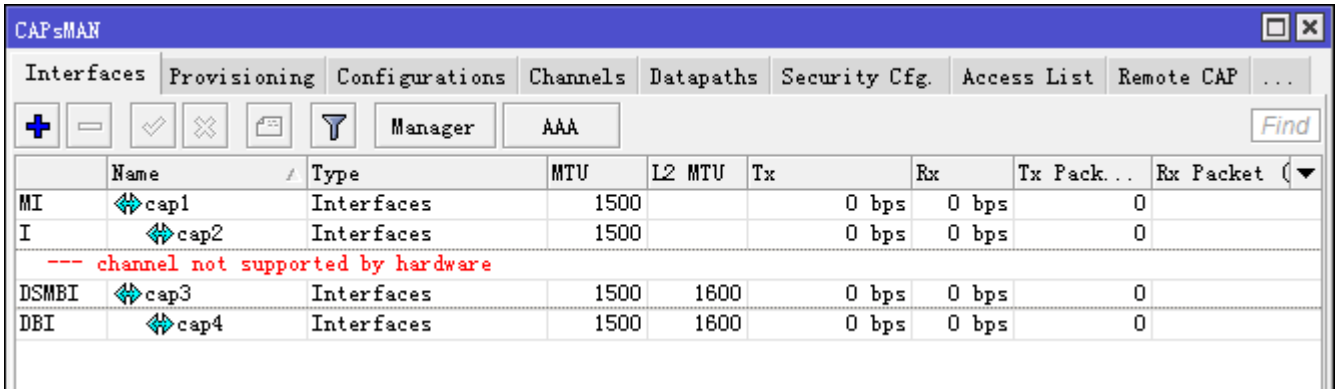
- **CAP客户端设置:**
- 启用CAP功能
- 启用CA证书验证功能
- CAPsMAN接口设置



- 当一个AP，不支持配置的频率连接并不能成为操作：
- **[admin@CM] /caps-manager interface> pr**
  Flags: M - master, D - dynamic, B - bound, X - disabled, I - inactive, R - running

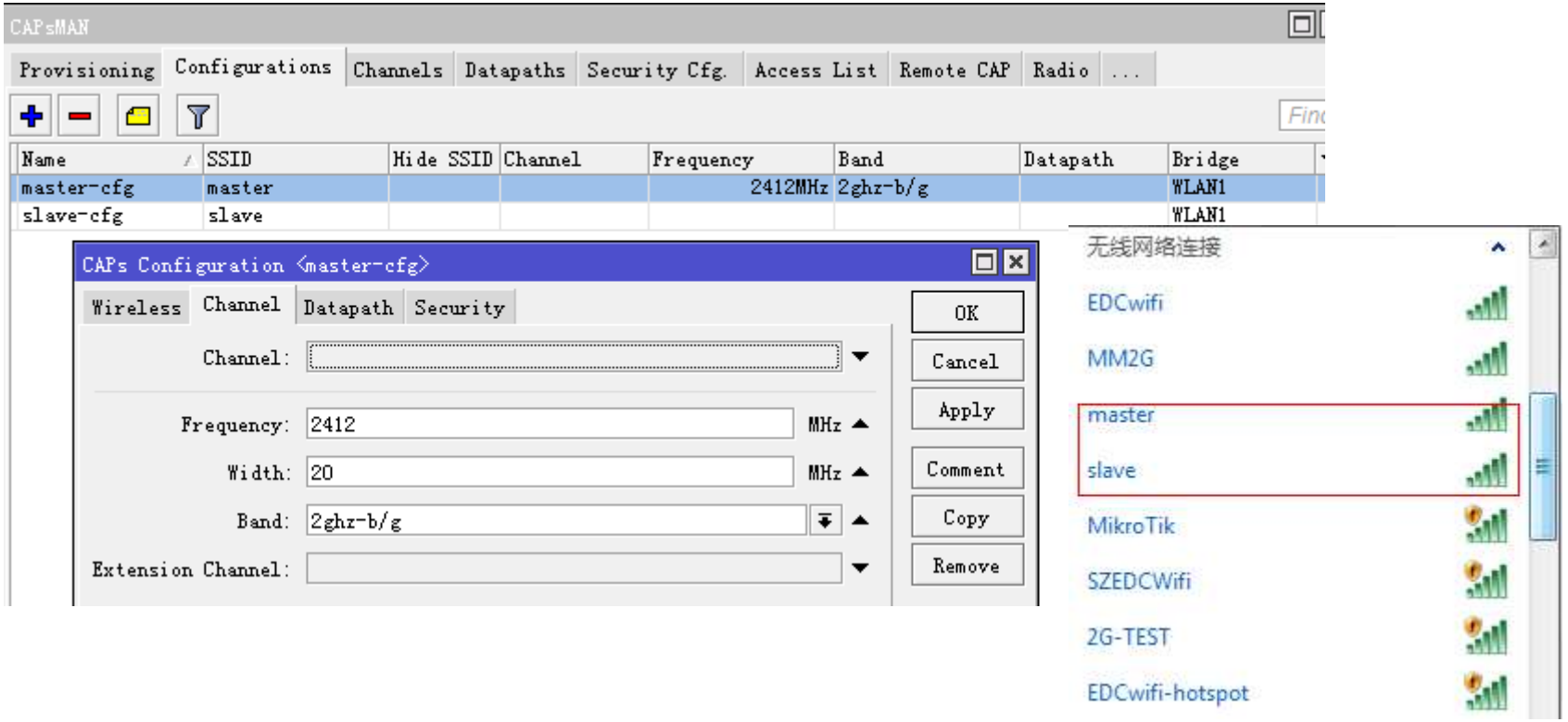
  # NAME RADIO-MAC MASTER-INTERFACE
  0 MDB ;;; unsupported band or channel
  cap3 00:0C:42:1B:4E:FF none

  …



- 我们可以覆盖在接口设置这个特殊的无线电频道设置，在不影响master-cfg 配置文件：

[admin@CM] /caps-manager interface> set cap3 channel.frequency=2142 channel.band=2ghz-b/g



- Thank You !