无线集中管理

CAPsMAN基础搭建

深圳捷联讯通科技有限公司

陈树远

概述

- CAPsMAN功能的角色组成：
  - CAPsMAN——受控接入点系统管理器
    - 集中管理无线网络，在必要时进行数据处理。负责客户端的身份验证和数据转发。
  - CAP——受控接入点
    - 根据配置信息提供无线覆盖，只负责无线链路层加密/解密。
- 功能支持
  - 支持RADIUS MAC认证
  - 支持WPA/WPA 2安全
  - 不支持Nstreme、Nv2协议，仅支持802.11协议
  - 不支持WDS和MESH组网管理
- 版本差异性
  - CAPsMAN v2（RouterOS v6.22rc7起）与CAPsMAN v1（RouterOS V6.11起）互不兼容
  - 早期无线功能分为多个wireless包，使用CAPsMAN功能需启用wireless-cm2包，默认为禁用
  - 目前所有无线功能已整合为一个wireless包

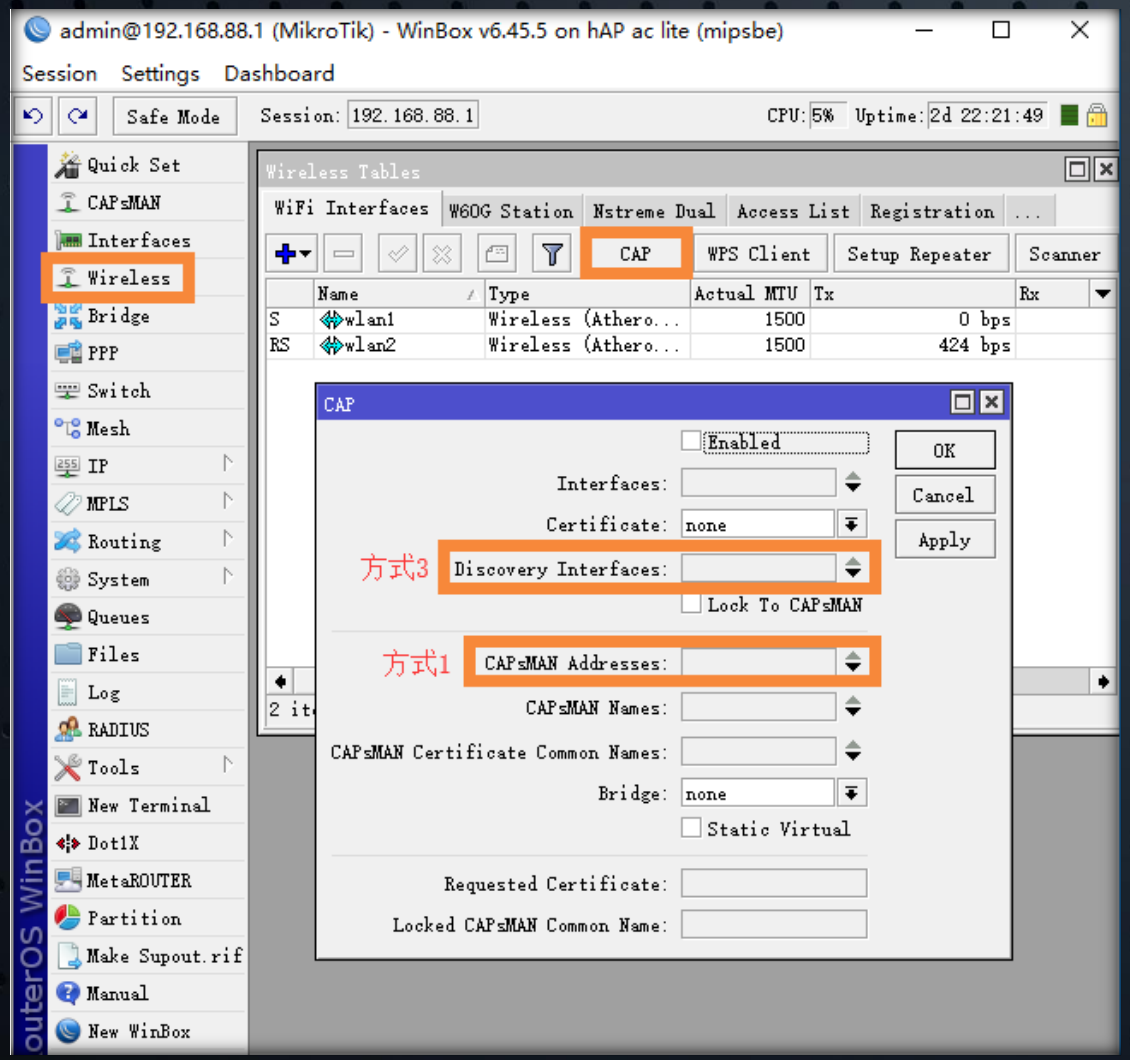
CAPsMAN v2新特性及使用注意事项

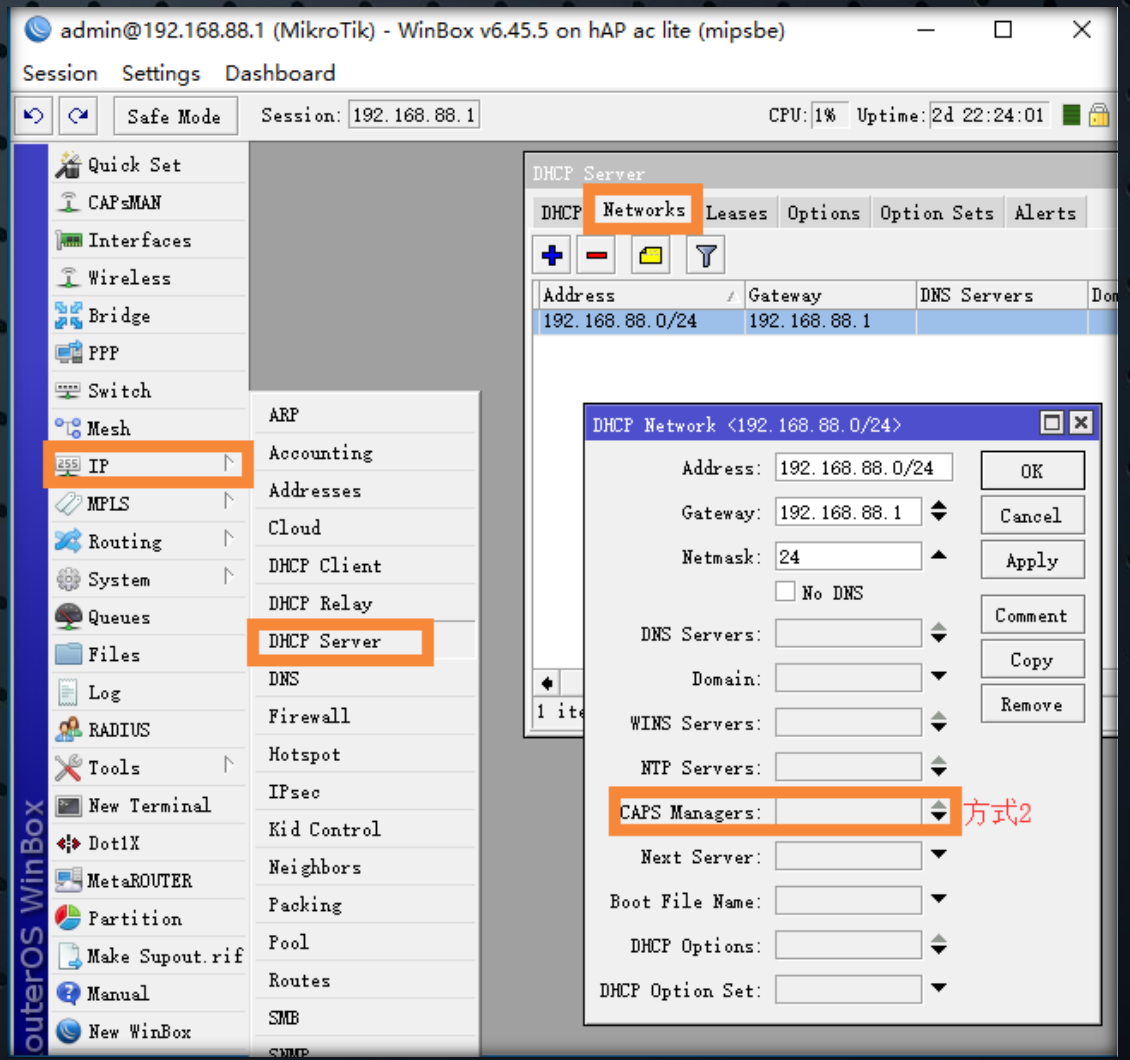
- CAPsMAN v2新特性
  - CAPsMAN可为所有CAP客户端配置自动升级
  - 改进了CAP和CAPsMAN的数据连接协议
  - 为Provision（供应）规则添加了“Name Format”（名称格式）和“Name Prefix”（名称前缀）设置
  - 改进了客户端在CAP之间漫游时的日志记录条目
  - 添加了L2路径MTU发现
- CAPsMAM功能使用条件及限制
  - CAPsMAN可配置于指定版本后的任何RouterOS设备（没有授权限制，无需无线接口）
  - CAP设备至少应具有L4 RouterOS授权
  - 理论上CAPsMAN没有限制接入的CAP（接入点）数量
  - 每个CAP支持被管理32个无线网卡
  - 每个主接口支持被管理32个虚拟无线接口
  - ROS客户端不能以station bridge模式连接AP

CAPsMAN与CAP的关联

- 使用MAC或IP层协议建立管理连接，并使用“DTLS”进行安全保护。
  - Mac层连接特性：
    - CAP上不需要IP配置
    - CAP和CAPsMAN必须位于相同2层子网-物理或虚拟(通过二层隧道)
  - IP层(UDP)连接特性：
    - 必要时可以穿透NAT
    - CAP必须能够使用IP协议与CAPsMAN通信
    - 必须提供CAPsMAN的IP地址，因为IP组播发现不能在L3上工作
- 初始由CAP执行发现过程。在发现期间，CAP尝试使用以下方式联系可用的CAPsMAN：
  - 1、已配置的Manager IP地址列表
  - 2、从DHCP服务器获得的CAPsMAN IP地址列表
  - 3、使用IP和MAC层协议在配置的接口上进行广播发现

Winbox上CAP发现方式路径





CAP选择CAPsMAN的优先级与身份验证模式

- 如果CAPsMAN-Names参数被指定，则会匹配CAPsMAN设备的系统标识名（System-Identity）
- MAC层连接的管理器优先于IP连接的管理器（符合指定参数前提）

- 选中管理器后，CAP尝试建立DTLS连接。可选择证书身份验证模式：
  - CAP和CAPsMAN上没有配置证书参数 - 不进行身份验证
  - 只有CAPsMAN配置了证书 - CAP检查CAPsMAN证书，且CAPsMAN必须配置require-peer-certificate = no（如果填证书选项那么必须是由受信任的CA证书颁发，如果填CA证书选项即使没有信任也不会建立失败）
  - CAP和CAPsMAN都配置了证书 - 相互身份验证

- 建立DTLS连接后，CAP可以选择检查CAPsMAN提供的证书CommonName字段。caps-man-certificate-common-names参数包含允许的CommonName值列表。（如果此列表不为空，则CAPsMAN必须使用证书配置）
- 如果CAPsMAN或CAP从网络断开，CAP和CAPsMAN之间的连接丢失将在大约10-20秒内检测到。

CAP锁定CAPsMAN和自动证书配置

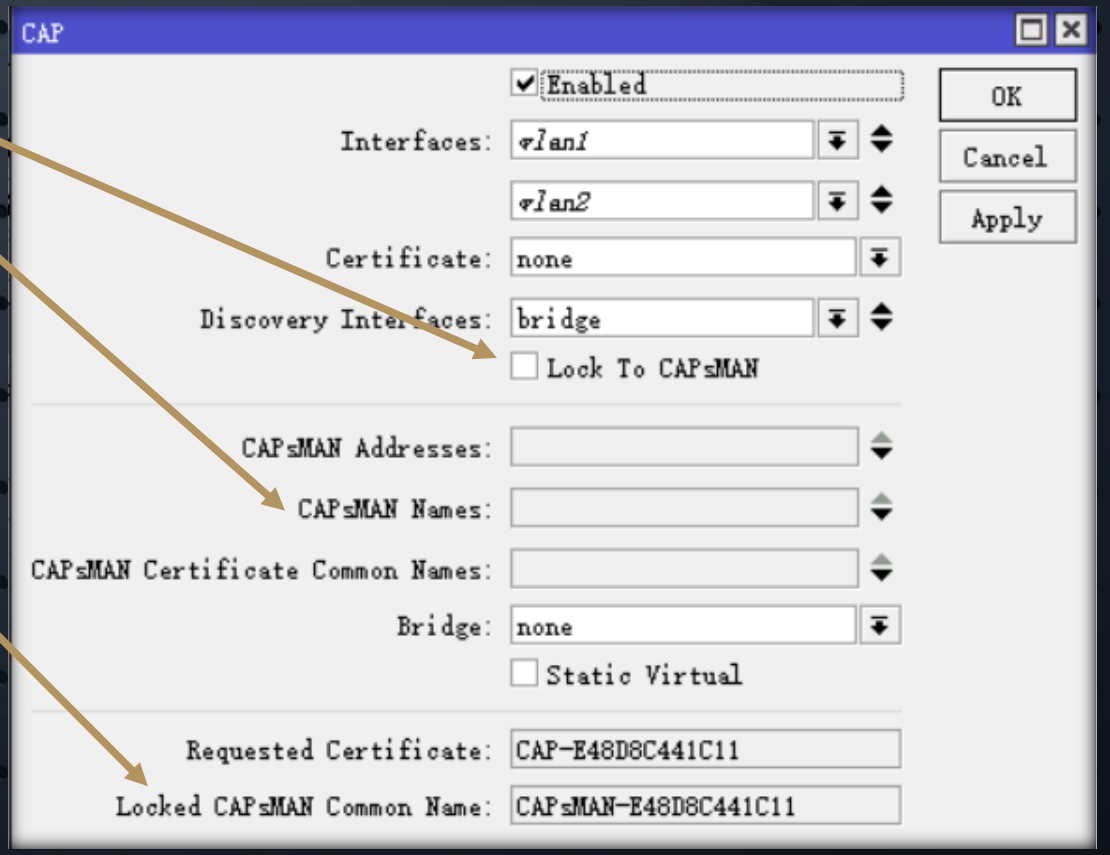
- CAP可以配置锁定到特定的CAPsMAN。通过记录CAPsMAN证书CommonName并检查所有后续连接的CommonName来实现的（CAMsMAN必须使用证书）。
  - 通过设置lock-to-caps-man = yes，

    来实现自动锁定。（CAP需设置证书）
  - 通过设置caps-man-certificate-common-names

    手动“锁定”到CAPsMAN。（CAP可不设置证书）
- 关闭锁定：设置lock-to-caps-man = no。

  （关闭锁定不会使上一次锁定失效）
- 强制CAP锁定另一个CAPsMAN：关闭锁定之后

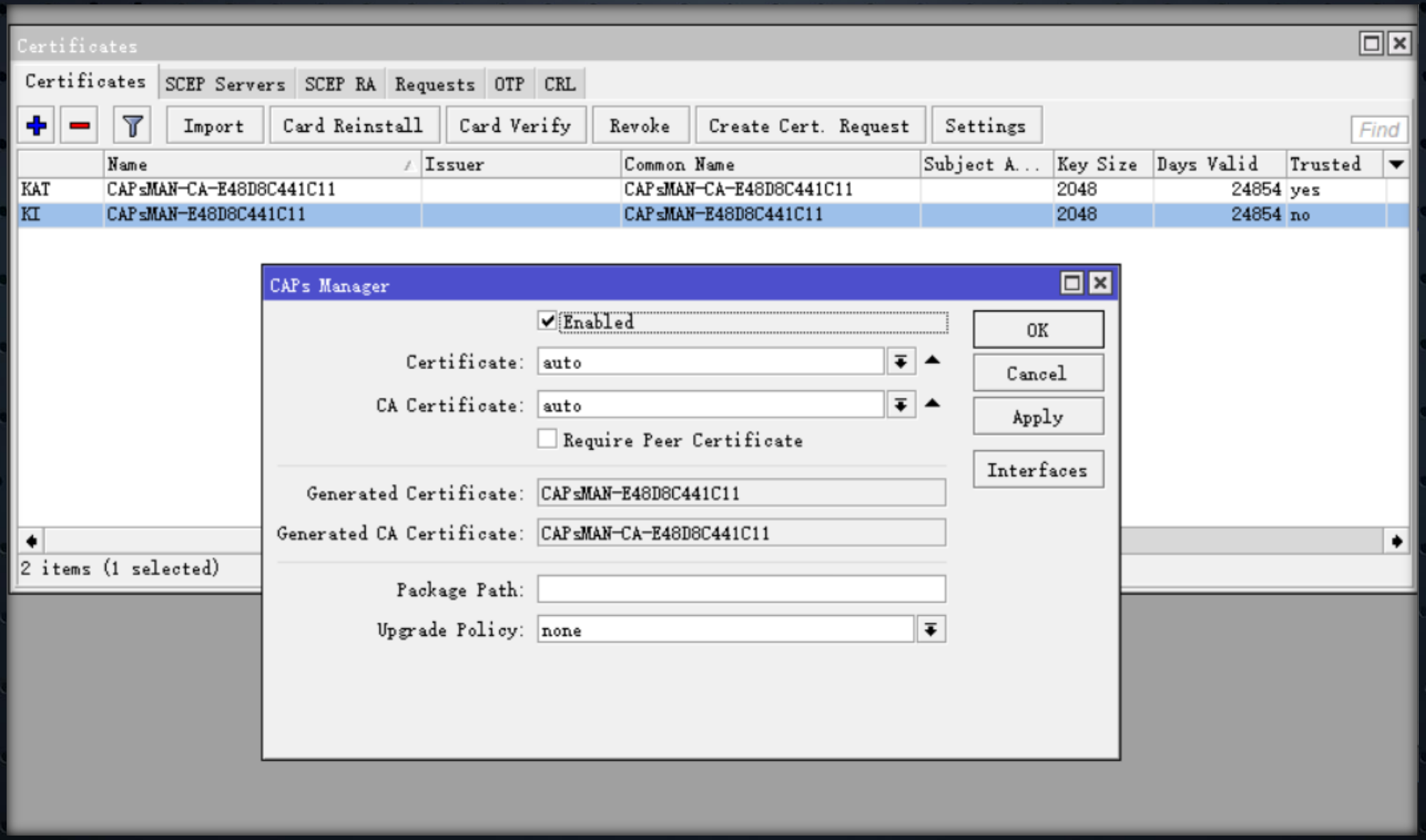
  （必要时需修改CAP证书）重新开启锁定



CAP锁定CAPsMAN和自动证书配置

- 为了简化CAPsMAN和CAP使用证书时的配置(例如，对于自动锁定功能)，可以将CAPsMAN配置为自动生成必要的证书，而CAP可以配置为从CAPsMAN请求证书。
- 自动证书不提供完整的公钥基础结构，仅提供简单的设置。如果需要更复杂的PKI - 如支持证书有效期，多级CA证书，证书续订，则必须使用其他方法，例如手动证书分发或SCEP。
- CAPsMAN具有以下证书设置：
  - certificate - CAPsMAN的证书参数，必须提供该证书的私钥。如果设置为auto，CAPsMAN将尝试使用CA证书向自己颁发证书。自动颁发的证书CommonName将为“CAPsMAN- <mac address>”，有效期将与CA证书相同。
  - ca-certificate - CAPsMAN在必要时为自己颁发证书及签署来自CAP证书请求时使用的CA证书。如果设置为auto，CAPsMAN将生成自签名CA证书以用作CA证书。此证书的CommonName形式为“CAPsMAN-CA-<mac Address>”，有效期为1970年1月1日至2038年1月18日。
- 当CAPsMAN配置了CA证书，CAP可以配置从CAPsMAN请求证书，使用设置certificate = request。
- CAP将首先使用“CAP- <mac address>”形式的CommonName生成私钥和证书请求。当CAP与CAPsMAN建立连接时，CAP将请求CAPsMAN签署其证书请求。如果成功，CAPsMAN将向CAP发送CA证书和新颁发的证书。CAP将在其证书存储中导入这些证书，在随后与CAPsMAN的连接上，CAP将使用生成的证书。

ROS的证书功能

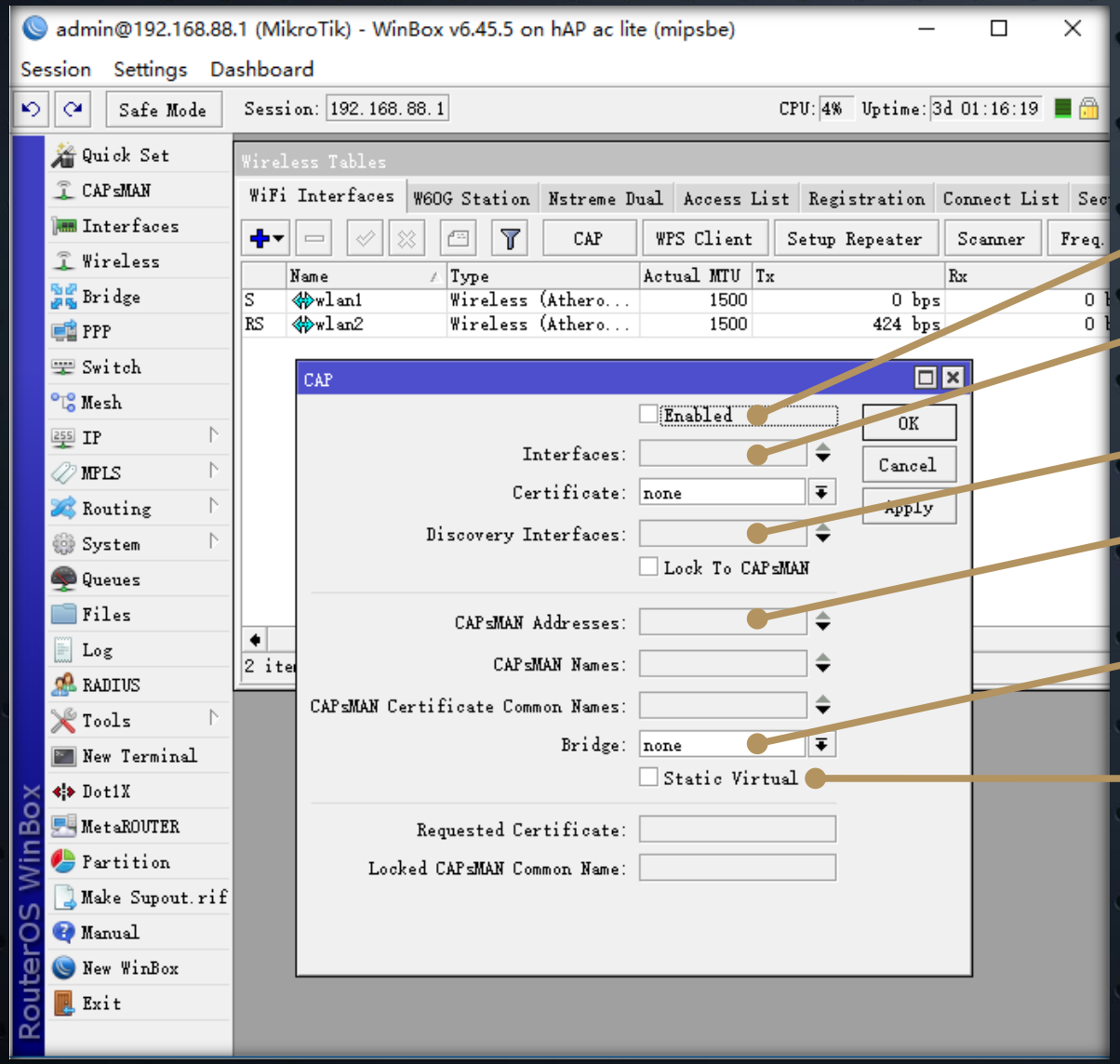

Certificates
Certificates
SCEP Servers
SCEP RA
Requests
OTP
CRL
Import
Card Reinstall
Card Verify
Revoke
Create Cert. Request
Settings
Find
Name
Issuer
Common Name
Subject A...
Key Size
Days Valid
Trusted
KAT
CAPsMAN-CA-E48D8C441C11
CAPsMAN-CA-E48D8C441C11
2048
24854
yes
KI
CAPsMAN-E48D8C441C11
CAPsMAN-E48D8C441C11
2048
24854
no
2 items (1 selected)
CAPs Manager
Enabled
Certificate:
auto
CA Certificate:
auto
Require Peer Certificate
Generated Certificate:
CAPsMAN-E48D8C441C11
Generated CA Certificate:
CAPsMAN-CA-E48D8C441C11
Package Path:
Upgrade Policy:
none
OK
Cancel
Apply
Interfaces

CAP全局配置

- 当AP配置为由CAPsMAN控制时，AP上受管理无线接口的配置将被忽略（例外：天线增益，天线模式），将接受来自CAPsMAN托管接口的配置。
- CAP流量转发模式分两种：
  - 集中转发：由CAPsMAN管理的CAP无线接口，默认其流量被转发到CAPsMAN，接口显示为禁用。
  - 本地转发：流量由CAP本地管理，仅控制接口配置和客户端关联过程，接口未显示禁用。
- 验证本地转发和集中转发时，同等测试条件下CAPsMAN和CAP的负载情况
  - 二层集中转发：CAP CPU达35-45%左右，CAPsMAN CPU达45-55%
  - 二层本地转发：CAP CPU达20-30%左右，CAPsMAN CPU达35-45%

	Name	Type	Actual MTU	Tx	Rx
	;;; managed by CAPsMAN				
	;;; channel: 2412/20-Ce/gn(20dBm), SSID: CAP-2G, CAPsMAN forwarding				
X	wlan1	Wireless (Athero...	1500	0 bps	
	;;; managed by CAPsMAN				
	;;; channel: 5300/20-eeCe/ac(20dBm), SSID: CAP-5G, local forwarding				
RS	wlan2	Wireless (Athero...	1500	4.8 kbps	

CAP全局配置



禁用/启用CAP功能

指定要被管理的无线接口

指定二层发现接口

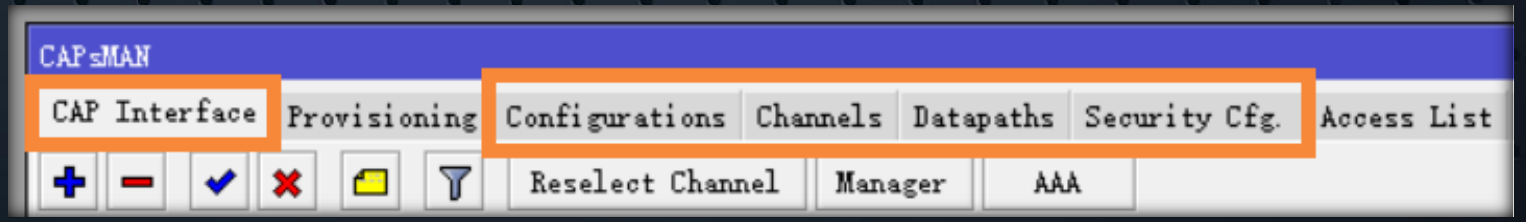
指定CAPsMAN IP地址
（用于跨三层连接）

将被成功管理的接口添加到指定桥接口（仅用于本地转发模式）

将VAP接口转换为静态（仅用于本地转发模式）

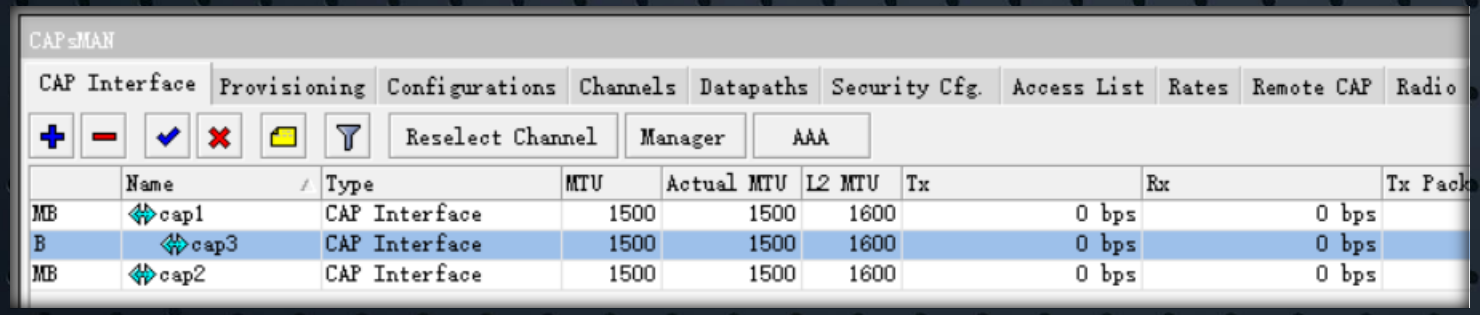
CAPsMAN配置概念

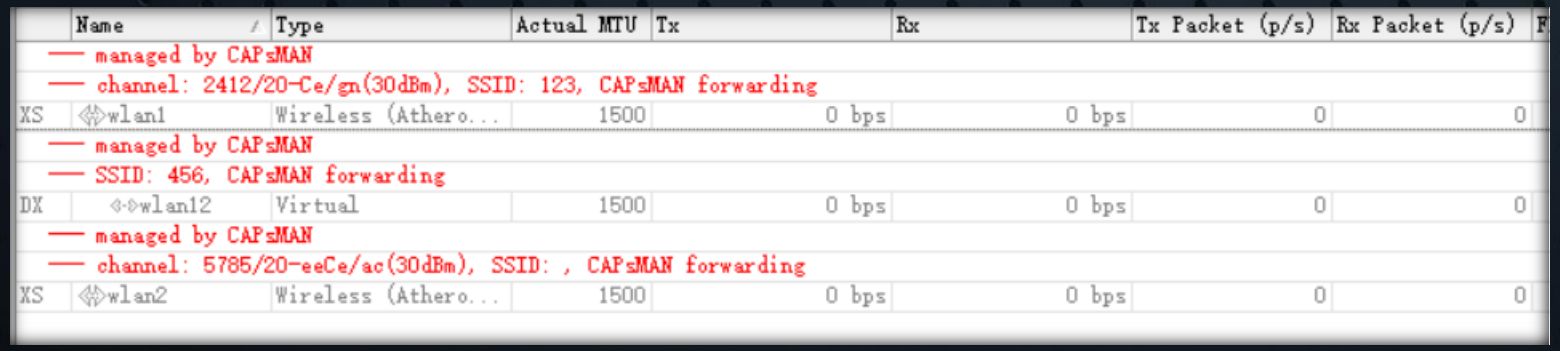
- 在CAPsMAN控制下，CAP上的每个无线接口显示为CAPsMAN上的虚拟接口。这为使用常规的RouterOS功能(如路由、桥接、防火墙等)的数据转发控制提供了最大的灵活性。
- 无线接口设置能够被组合成配置组，从而简化了配置的重用。当前有以下配置组：
  - channel（频段） - 频段相关设置，例如频率和宽度
  - datapath （数据路径） - 数据转发相关设置，例如将特定接口自动添加为网桥端口
  - security（安全性） - 与安全性相关的设置，例如允许的身份验证类型或密码
  - configuration（配置） - 包含所有配置条目相关，可以调用上述三种配置组。 此外，可以在配置文件中直接覆盖调用组的任何设置。
- Interface（接口）菜单：将所有配置组绑定在一起，还可以在接口设置中直接重写任何设置。
- 配置路径的优先级：
  - 高：Interface（接口）
  - 中：configuration（配置）
  - 低：channel（频段）/datapath （数据路径）/security（安全性）



主从接口与全局配置

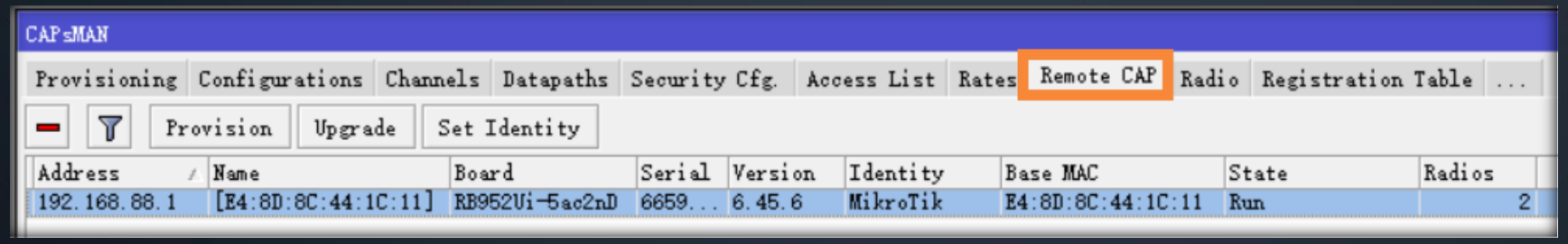
- CAPsMAN上有两种类型的接口 - “master”和“slave”。主接口保存实际无线接口（radio）的配置，而从接口链接到主接口，用于保存Virtual-AP的配置（多SSID支持）。
- 有些设置仅对主接口有意义，即主要是与硬件设置相关的参数，例如无线信道设置。只有在启用主接口的情况下，从接口才能运行。
- CAPsMAN上的接口可以是静态的，也可以是动态的。静态接口存储在RouterOS配置中，并将在重新引导后保留。仅当特定CAP连接到CAPsMAN时，才存在动态接口。



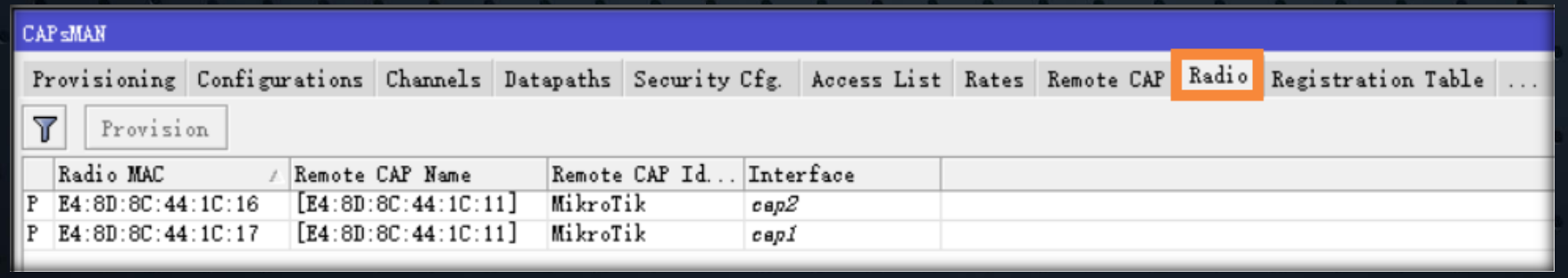


无线电Provisioning（供应）相关

- CAPsMAN基于标识符区分CAP。 标识符基于以下规则生成：
  - 如果CAP提供了证书，则将标识符设置为证书中的“Common Name”字段，否则，标识符基于CAP提供的Base-MAC，形式为：'[XX：XX：XX：XX：XX：XX]'。
- 当前连接的CAPs列在/caps-man remote-cap菜单中：

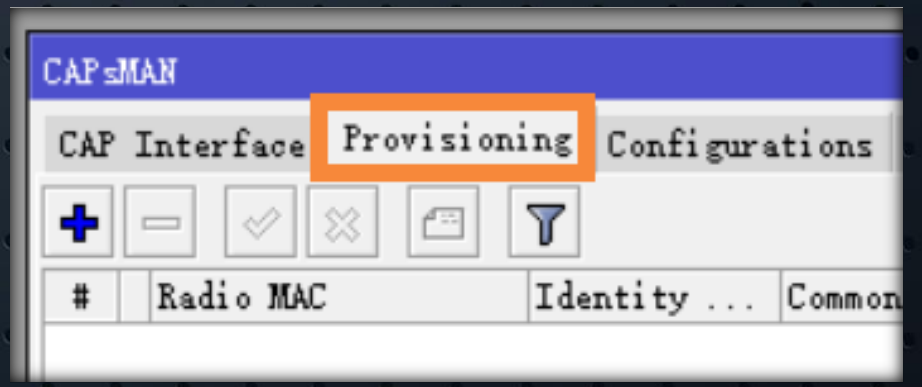


- CAPsMAN基于其内置MAC地址（radio-mac）区分实际无线接口（radios）。 即在一个CAPsMAN上管理的无线接口不会有相同的MAC地址。 由CAPsMAN管理的无线电（由连接的CAP提供）列在/caps-man radio菜单中：



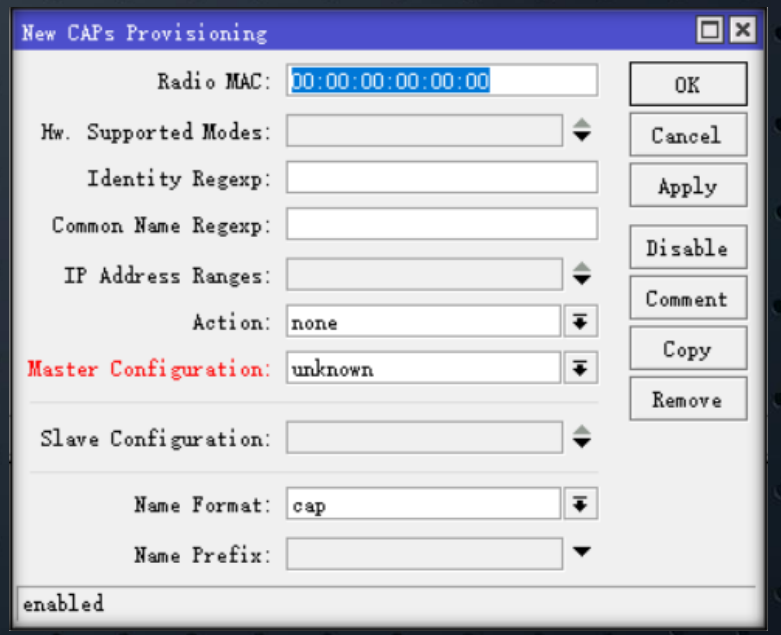
Provisioning（供应）菜单

- 当CAP连接时，CAPsMAN首先尝试将每个CAP无线接口绑定到基于Radio-Mac的CAPsMAN接口。
- 如果找到合适的接口（已存在静态接口），则使用接口配置和引用特定主接口的从接口的配置来设置无线电。
- 如果没有找到匹配的无线电主接口，CAPsMAN将执行“供应规则”。供应规则是有序规则列表，其中包含指定要匹配哪个无线电的设置和指定在无线电匹配时要采取的操作的设置。
- 应用方式：匹配条件项，则执行动作项
- 常用的条件项：
  - radio-mac：要匹配的无线电的MAC地址，空MAC(00:00:00:00:00:00) 表示匹配所有MAC地址
  - hw-supported-modes：通过支持的无线协议来匹配无线网卡
  - ip-address-ranges ：将CAP与配置的地址范围内的IP匹配
- Action动作项：
  - create-disabled：创建禁用的静态接口。
  - create-enabled：创建启用的静态接口。
  - create-dynamic-enabled：创建启用的动态接口。



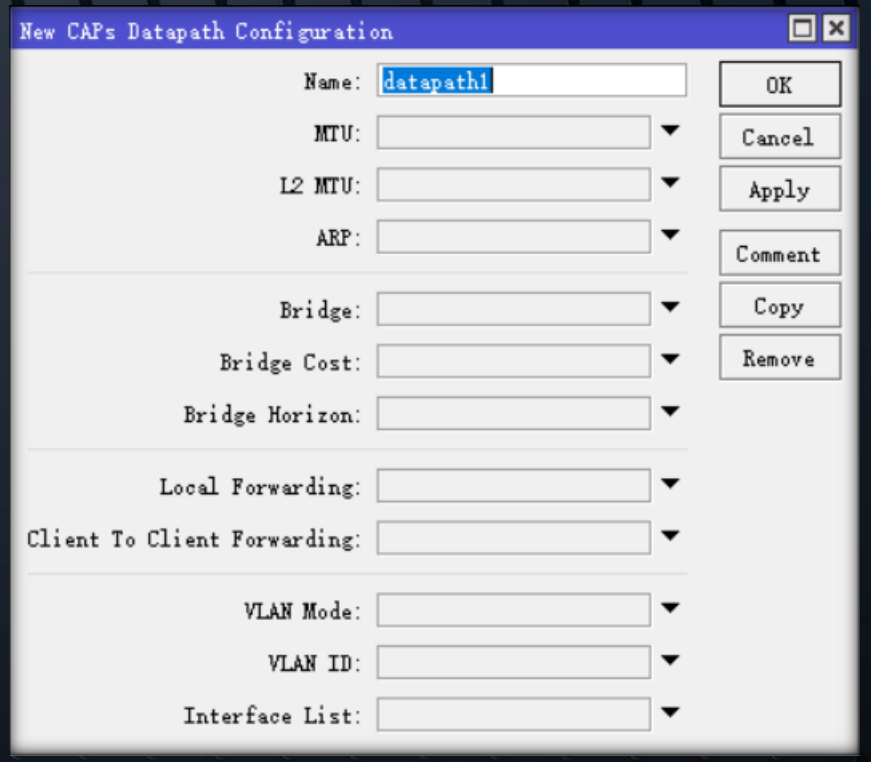
Provisioning（供应）菜单

- 其他项：
  - master-configuration：如果action指定创建接口，则将创建一个新的主接口，其配置设置为此配置文件
  - slave-configurations：如果action指定创建接口，则会创建一个新的从接口，其配置设置为此配置文件
  - name-format：指定CAP接口名称创建的格式
    - cap - 默认名称
    - identity - CAP板系统身份名称
    - prefix - 以指定名称前缀命名
    - prefix-identity - 以名称前缀值和CAP板系统标识名称
  - name-prefix：名称前缀，可以在名称格式中用于创建CAP接口名称
  - 手动执行供应规则：
    - Remote AP菜单的Provision按钮——对指定CAP的所有wlan供应
    - Radio菜单的Provision按钮——对某个wlan供应

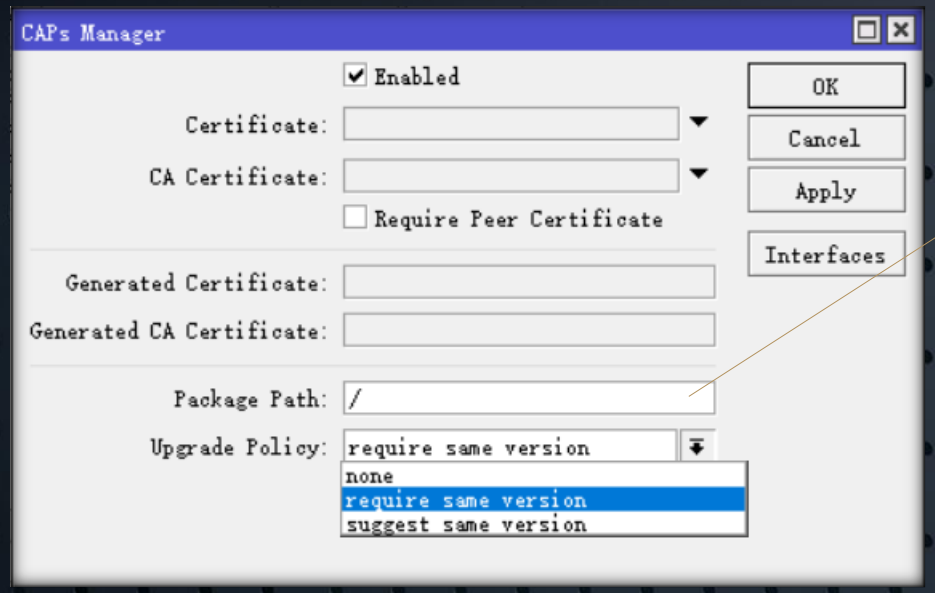


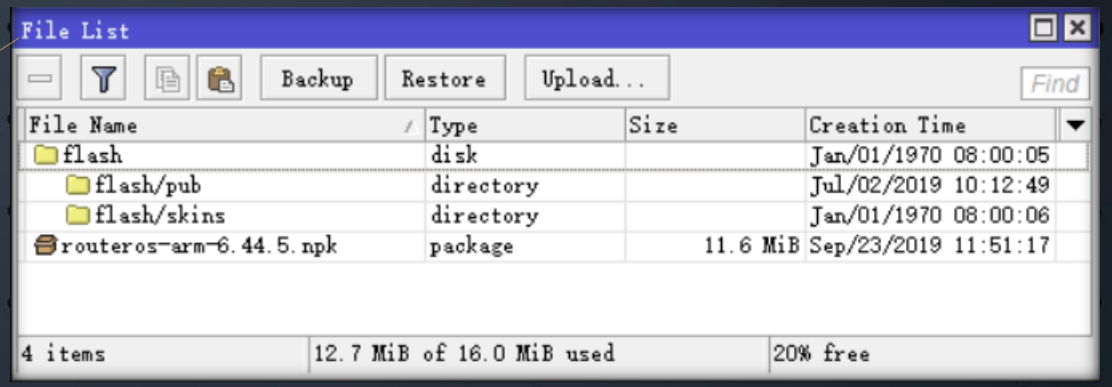
Datapaths（数据路径）相关

- 主要功能：控制数据转发相关。如设置管理（集中）转发和本地转发。该菜单大多数设置项仅在管理转发模式下使用，因为在本地转发模式中，CAPsMAN没有对数据转发的控制。
- 举例：CAPsMAN管理了CAP的wlan1口，生成cap1接口。cap1口添加于CAPsMAN端的bridge1，wlan1口添加于CAP端的bridge1。针对接入WIFI的CPE设备IP进行限速：
  - 管理转发模式下：限速规则应在CAPsMAN端创建，且控制客户端之间的转发
  - 本地转发模式下：限速规则应在CAP端创建
- 同理，针对不同模式下接口策略也应该对应模式选择cap1口或者wlan1口



CAPsMAN集中升级与远端CAP操作示例



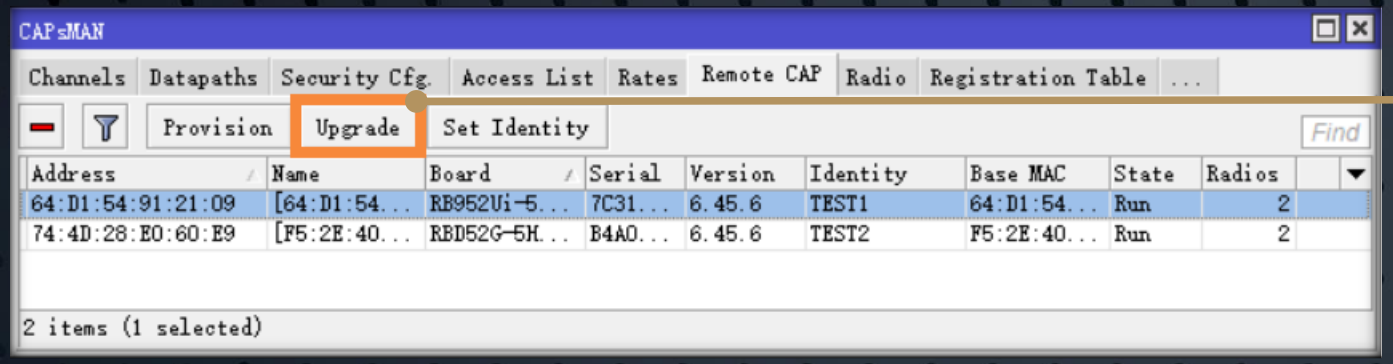


Package-path：RouterOS包的文件夹位置。空字符则使用自身ROS软件包。

upgrade-policy：升级策略选项

- none - 不执行升级
- require-same-version - CAPsMAN建议升级CAP RouterOS版本，如果失败则不提供CAP配置
- suggest-same-version - CAPsMAN建议升级CAP RouterOS版本，如果失败，它仍然会被配置

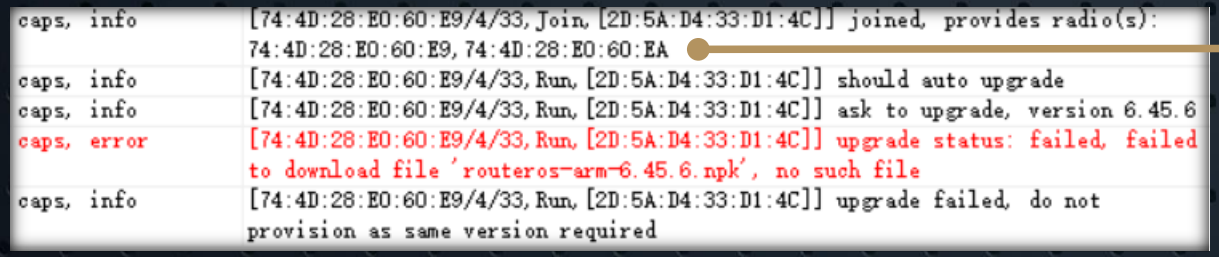
CAPsMAN升级管理与远端CAP操作示例



Upgrade：执行手动升级

Provision：指定重供应同步

Set Identity：指定系统标识名



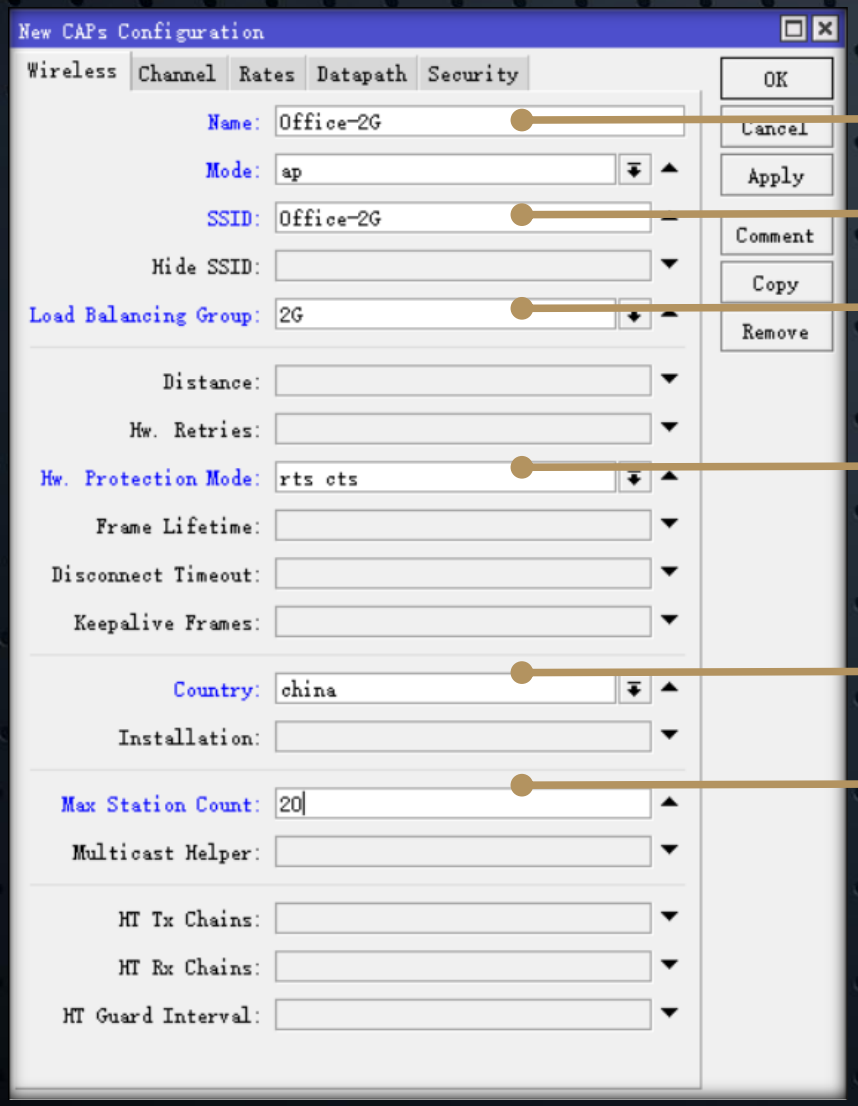
CAP采用升级日志示例

升级策略供应正常如前三行所示

升级策略供应错误出现红色错误提示

简单的CAPsMAN集中管理配置示例

- 步骤一：创建Configuration（配置）文件——Wireless相关



配置文件名称

无线WIFI名称

负载均衡组标识

（同一负载均衡组下的AP会均衡客户接入数量）

帧保护模式

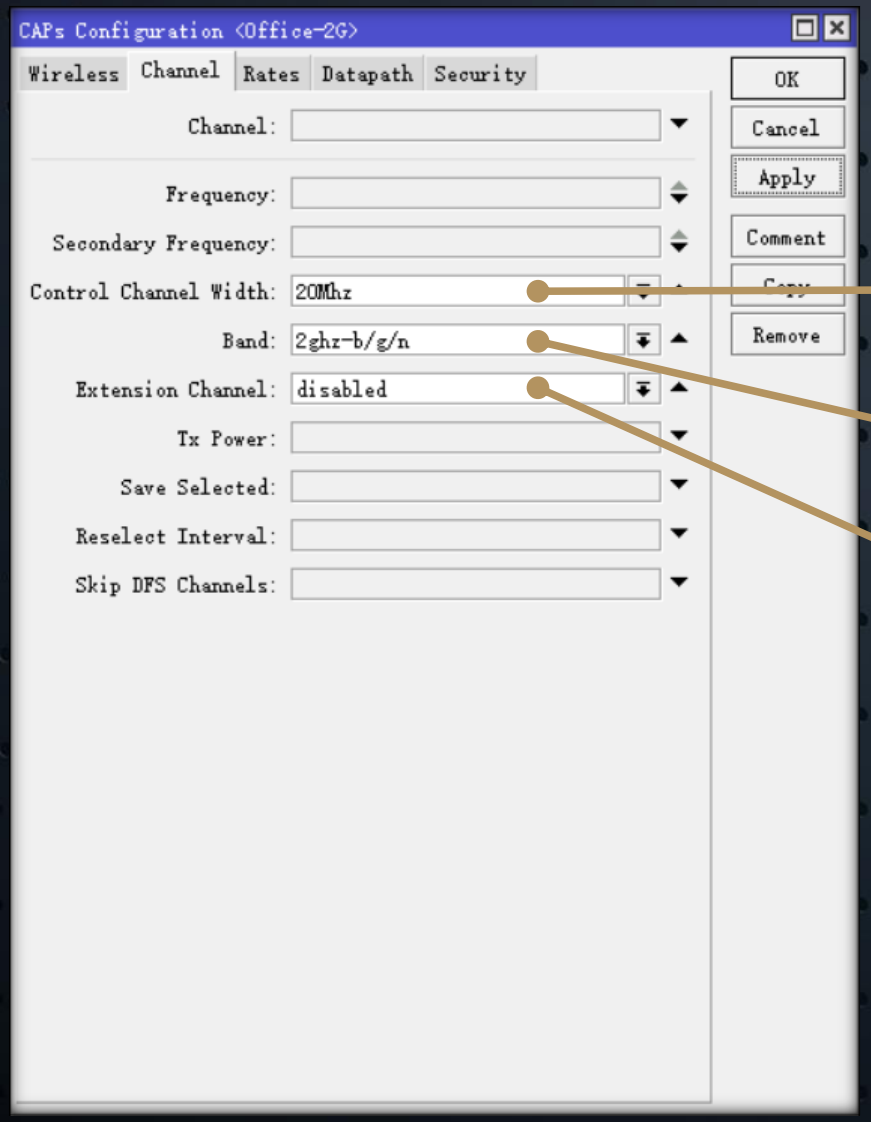
（有助于解决“隐藏节点”问题）

国家代码（限制可以用的信道、频宽和发射功率）

每个无线接口的最大接入客户端数量

简单的CAPsMAN集中管理配置示例

- 步骤二：创建Configuration（配置）文件——Channel相关



控制信道宽度

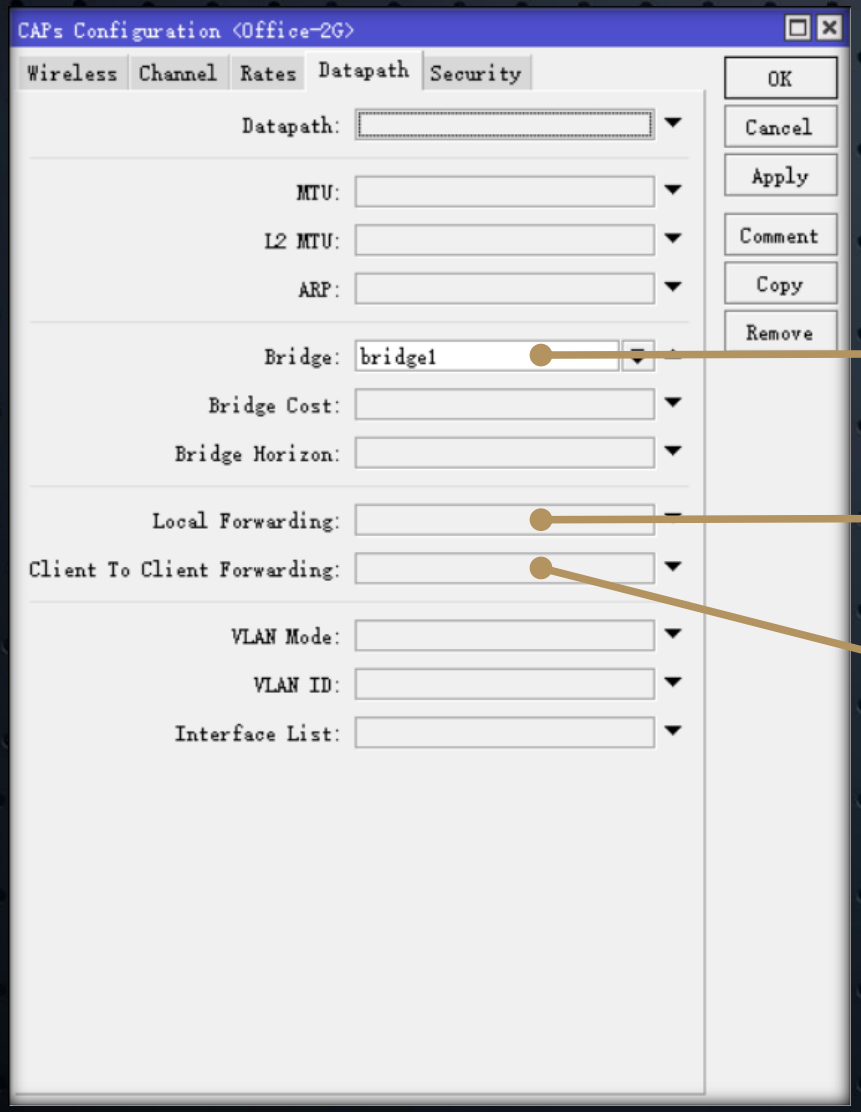
无线频段标准

扩展信道选项

（由于2G频谱资源拥挤，故禁用扩展信道，即20M频宽）

简单的CAPsMAN集中管理配置示例

- 步骤三：创建Configuration（配置）文件——Datapath相关



生成的CAP接口添加到指定桥

（通过桥建立不同的IP子网，进一步实现网络隔离）

是否使用本地转发

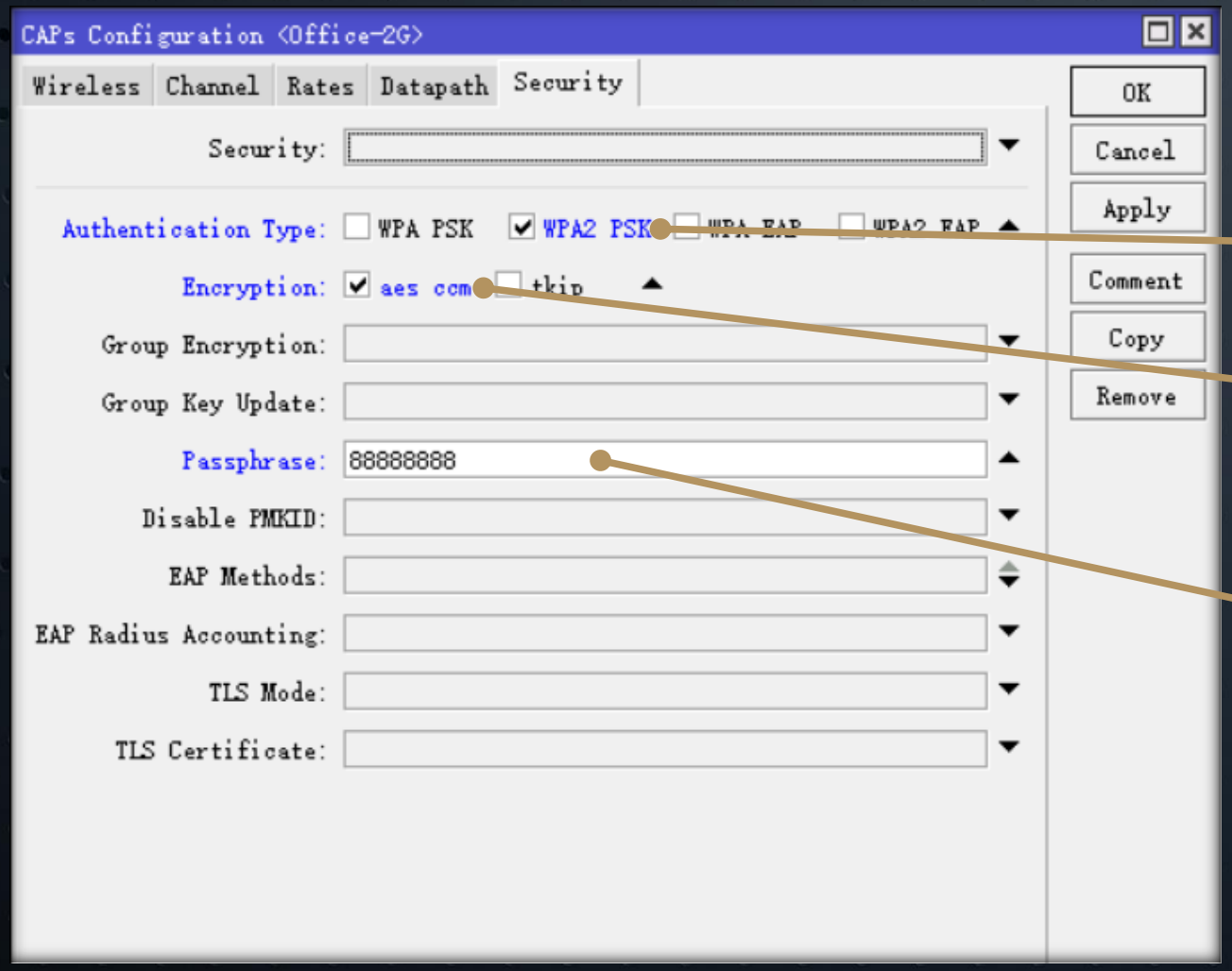
（根据流量控制需求按需选择，集中控制则不勾选）

是否允许客户端之间的数据转发

（集中管理时客户端互访操作，默认拒绝，按需选择）

简单的CAPsMAN集中管理配置示例

- 步骤四：创建Configuration（配置）文件——Security相关



配置认证类型

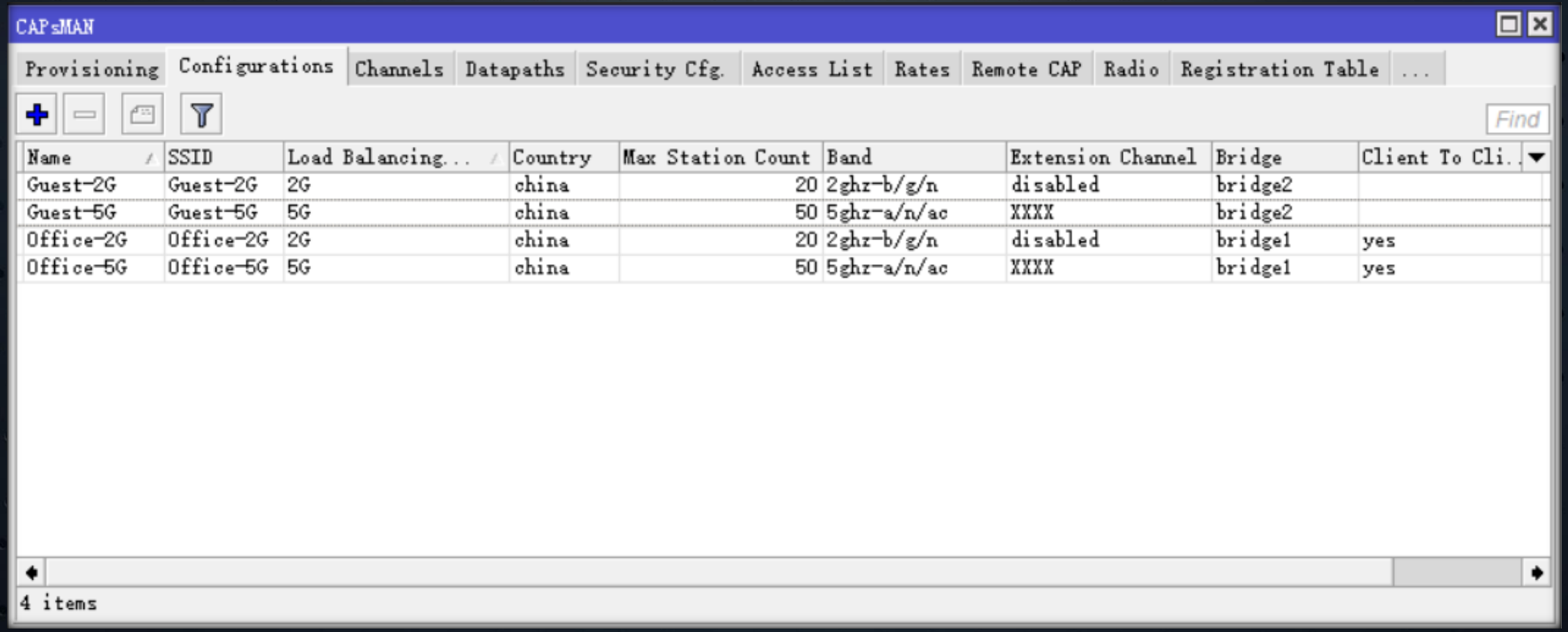
配置加密模式

配置至少8个字符的密码

（建议由3种字符组成，如字母、符号和数字）

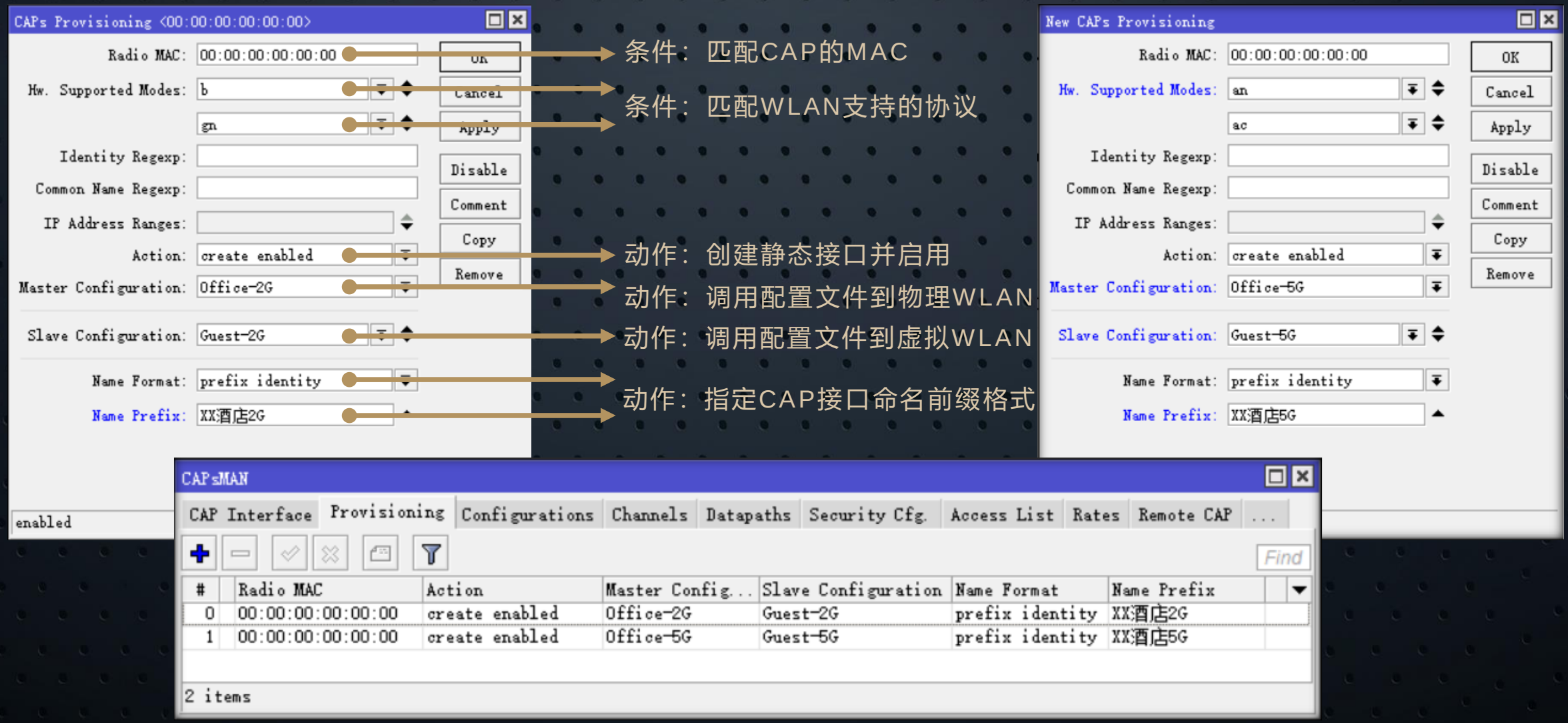
简单的CAPsMAN集中管理配置示例

- 本例建立4个配置文件，用于分频广播和内外部网络隔离，完成如下图所示（建议不同SSID分别指定一个均衡标识）



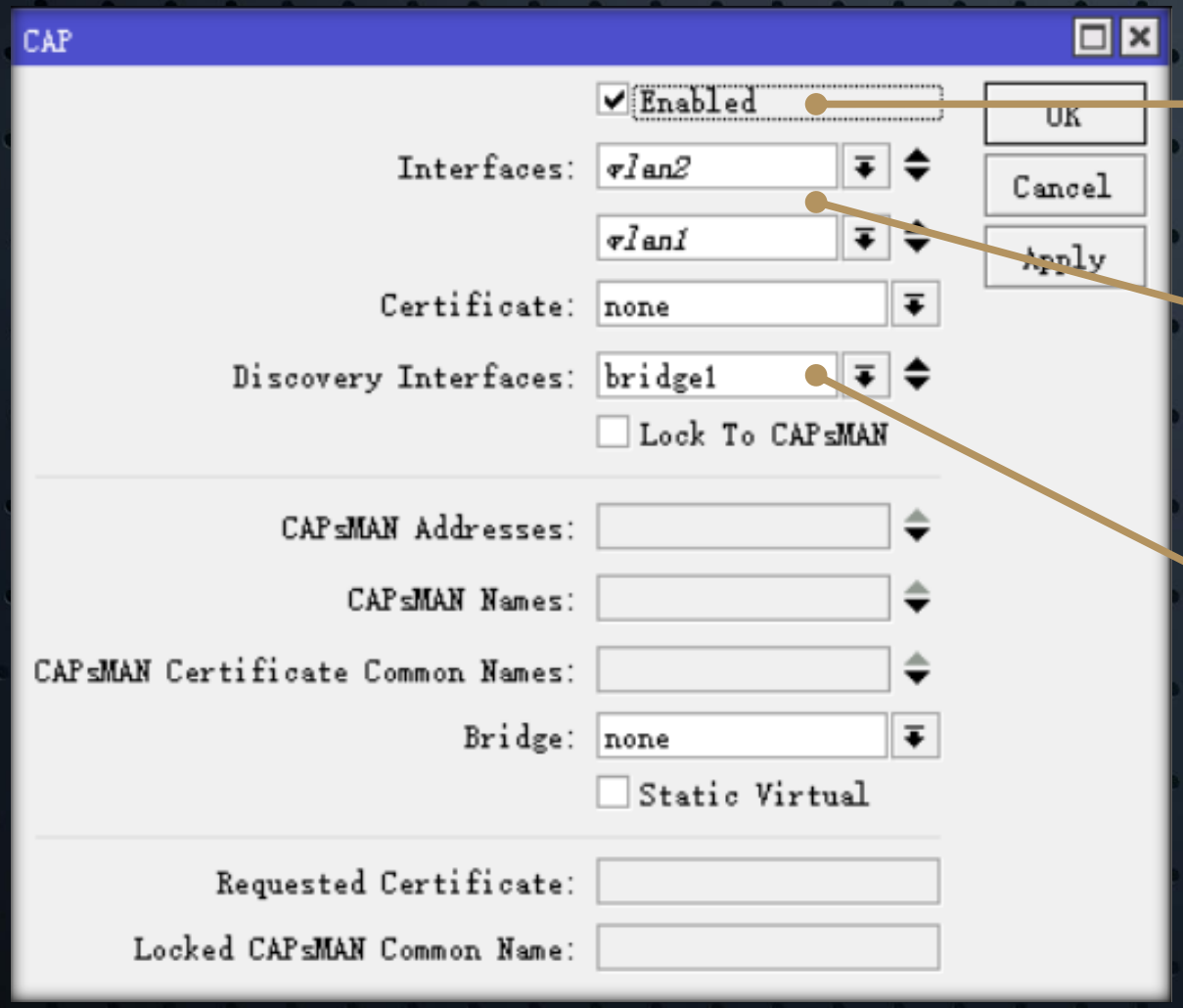
简单的CAPsMAN集中管理配置示例

- 步骤五：创建Provisioning（供应）条目



简单的CAPsMAN集中管理配置示例

- 步骤六：开启AP设备的CAP选项



启用CAP模式

选择受控WLAN

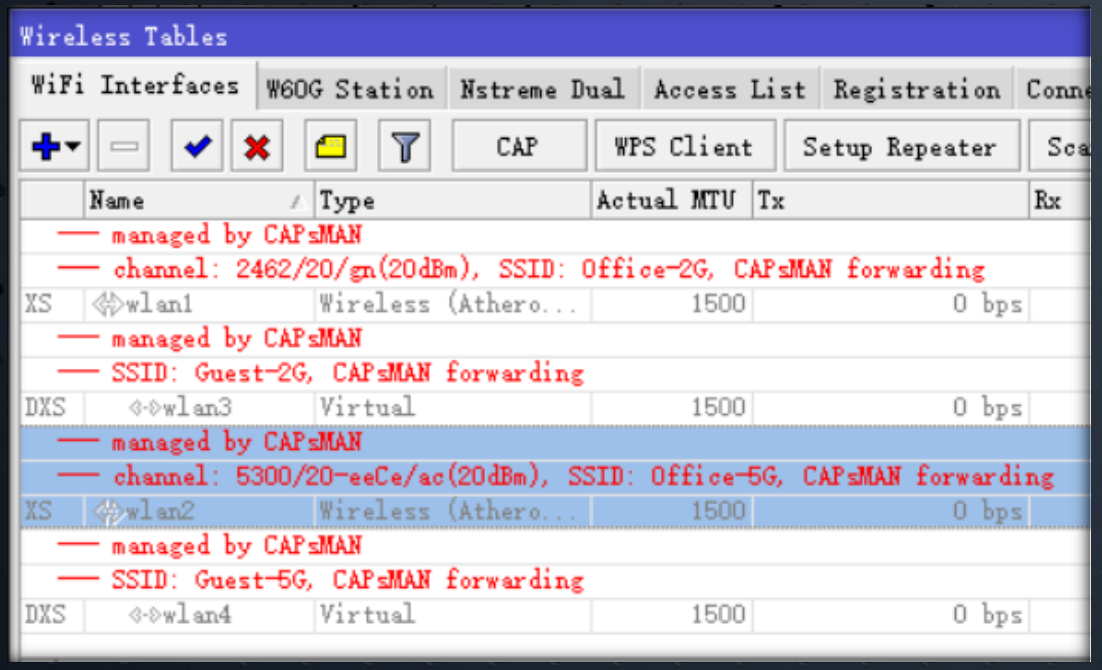
（wlan1为2G，wlan2为5G）

指定二层发现接口

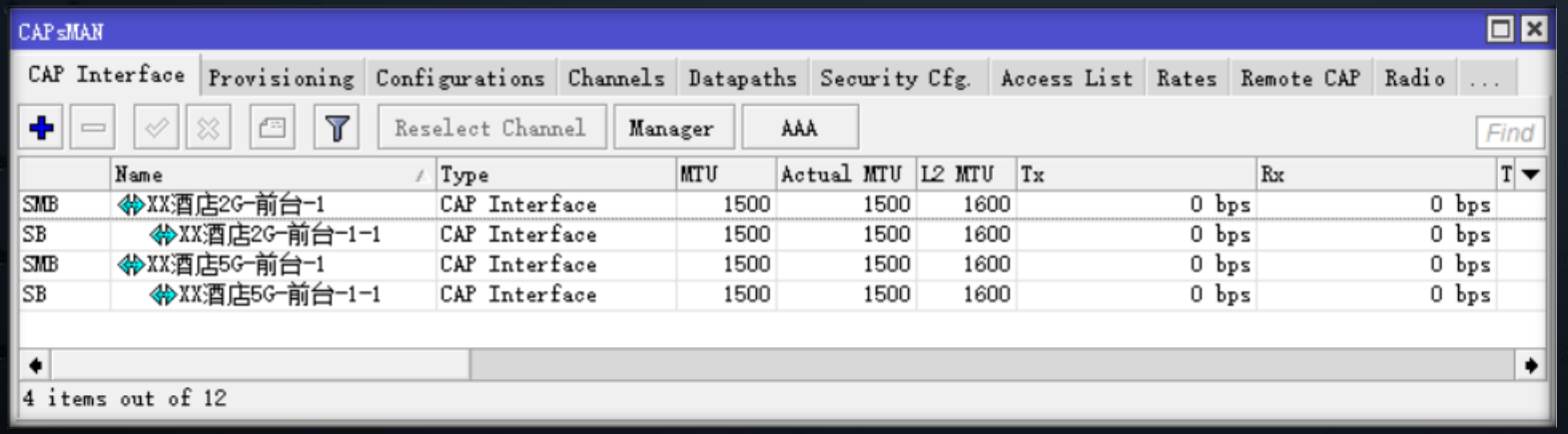
（根据情况可选择其他发现方式）

简单的CAPsMAN集中管理配置示例

- 完成界面预览



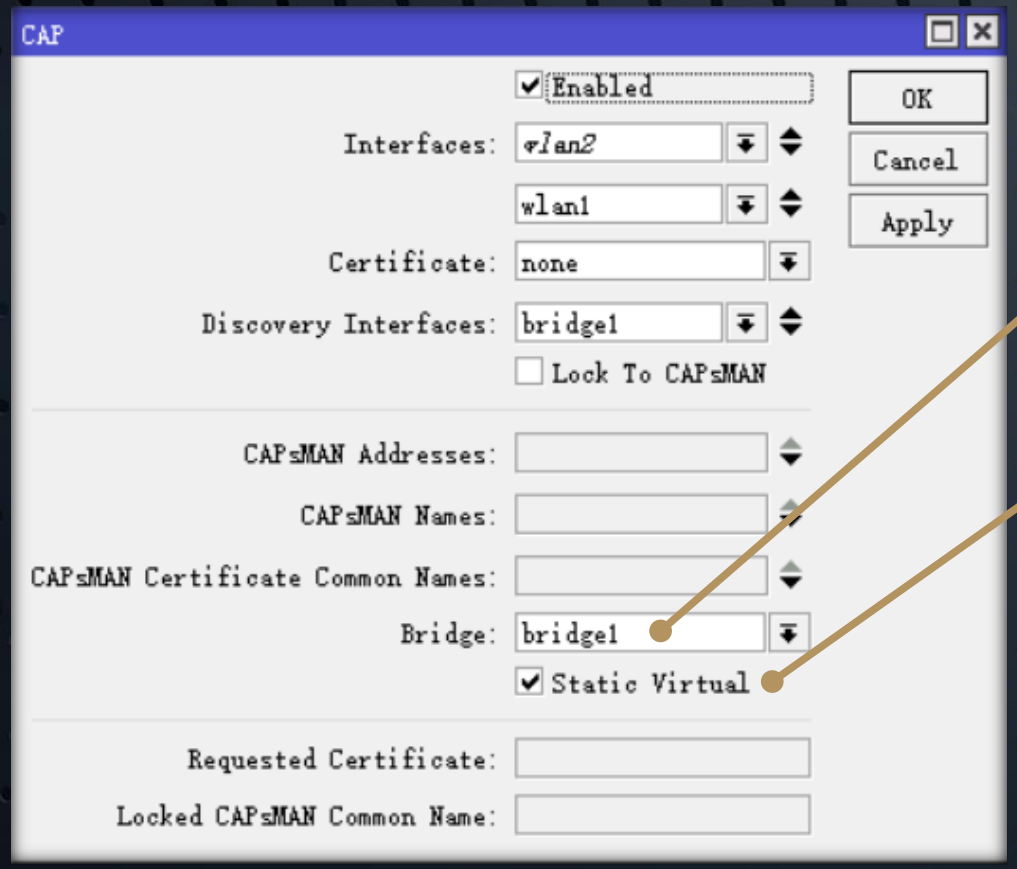
CAP端接口显示



CAPsMAN端接口显示

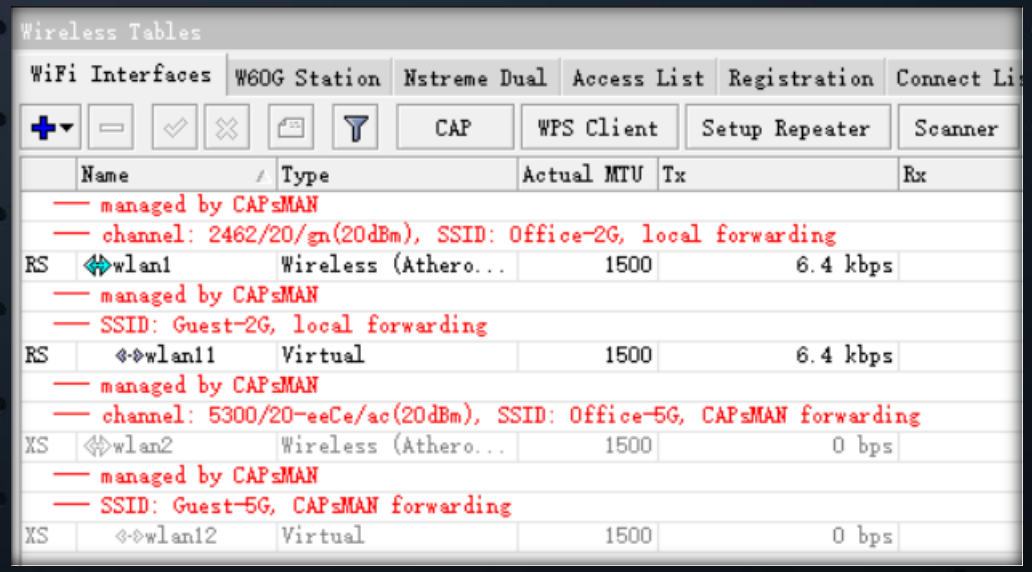
CAPsMAN本地转发管理配置示例

- 通过勾选CAPsMAN系统配置里本地转发修改模式，并进行以下操作



指定WLAN接口被CAPsMAN管理后加入的本地桥

专用于本地转发模式的虚拟接口使其可以静态编辑，如用于独立IP配置



CAPsMAN系统的漫游性问题

- 官方针对CAPsMAN功能的描述是统一管理，没有相关无缝漫游的描述
- 实测验证结果：部署规划合理则可以达到不丢包无缝漫游效果

```
caps, info          38:BA:F8:15:F6:D5@cap8 connected, signal strength -35
dhcp, info          dhcp1 assigned 192.168.179.249 to 38:BA:F8:15:F6:D5
interface, info     ether5 link down
system, info, a...  user admin logged out from 00:0E:C6:C1:C6:DD via winbox
system, info, a...  user admin logged in from 192.168.179.249 via winbox
caps, info          38:BA:F8:15:F6:D5@cap10 connected, signal strength -22
caps, info          38:BA:F8:15:F6:D5@cap8 disconnected, registered to other interface
caps, info          38:BA:F8:15:F6:D5@cap8 connected, signal strength -57
caps, info          38:BA:F8:15:F6:D5@cap10 disconnected, registered to other interface
dhcp, info          dhcp1 deassigned 192.168.179.254 from 00:0E:C6:C1:C6:DD
caps, info          38:BA:F8:15:F6:D5@cap10 connected, signal strength -41
caps, info          38:BA:F8:15:F6:D5@cap8 disconnected, registered to other interface
caps, info          38:BA:F8:15:F6:D5@cap8 connected, signal strength -59
caps, info          38:BA:F8:15:F6:D5@cap10 disconnected, registered to other interface
```

首次接入：客户端连接至cap8（信号-35）

第一次漫游：cap8漫游至cap10（信号-22）

第二次漫游：cap10漫游至cap8（信号-57）

第三次漫游：cap8漫游至cap10（信号-41）

第四次漫游：cap10漫游至cap8（信号-59）

第一次漫游过程Ping包情况

```
192.168.179.1 的 Ping 统计信息:
    数据包: 已发送 = 264，已接收 = 264，丢失 = 0 (0% 丢失)，
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms，最长 = 576ms，平均 = 17ms
```

第二次漫游过程Ping包情况

```
192.168.179.1 的 Ping 统计信息:
    数据包: 已发送 = 101，已接收 = 100，丢失 = 1 (0% 丢失)，
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms，最长 = 91ms，平均 = 3ms
```

第三次漫游过程Ping包情况

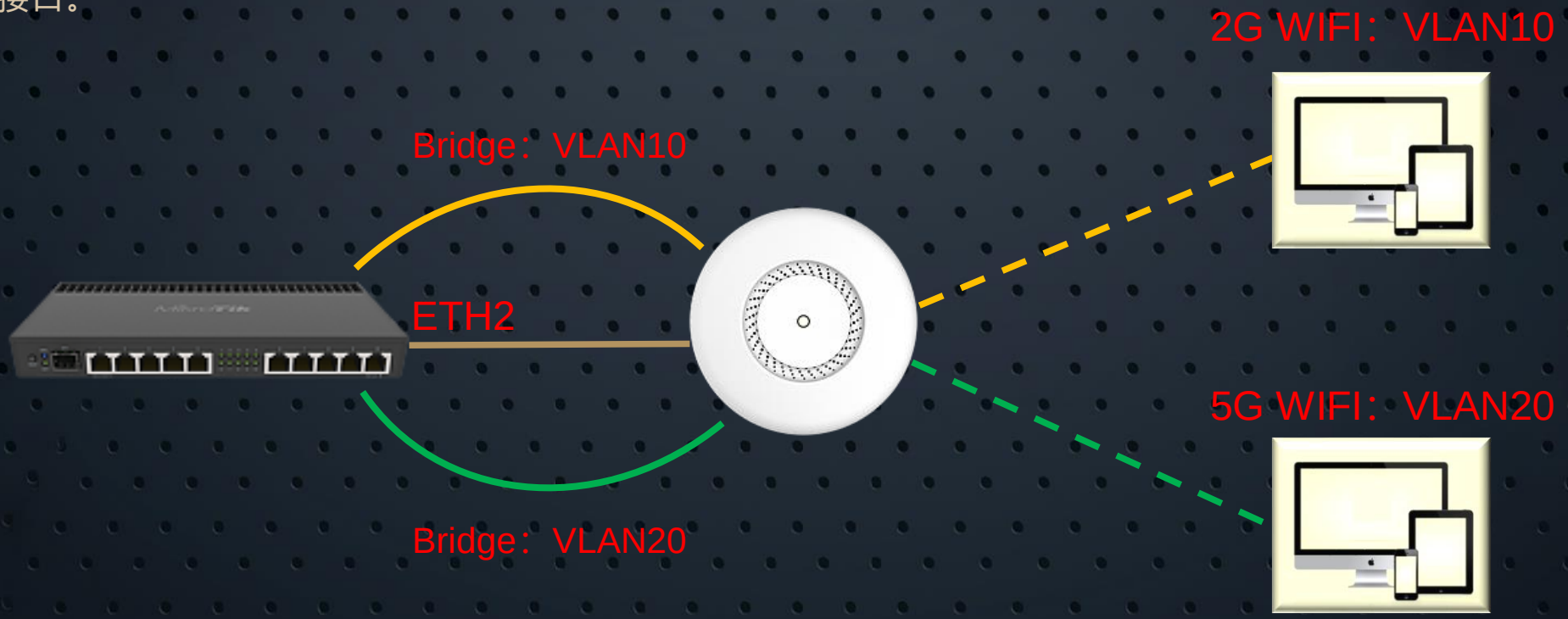
```
192.168.179.1 的 Ping 统计信息:
    数据包: 已发送 = 101，已接收 = 101，丢失 = 0 (0% 丢失)，
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms，最长 = 192ms，平均 = 13ms
```

第四次漫游过程Ping包情况

```
192.168.179.1 的 Ping 统计信息:
    数据包: 已发送 = 109，已接收 = 109，丢失 = 0 (0% 丢失)，
来自 192.168.179.1 的回复: 往返行程的估计时间(以毫秒为单位):
    最短 = 0ms，最长 = 104ms，平均 = 5ms
```

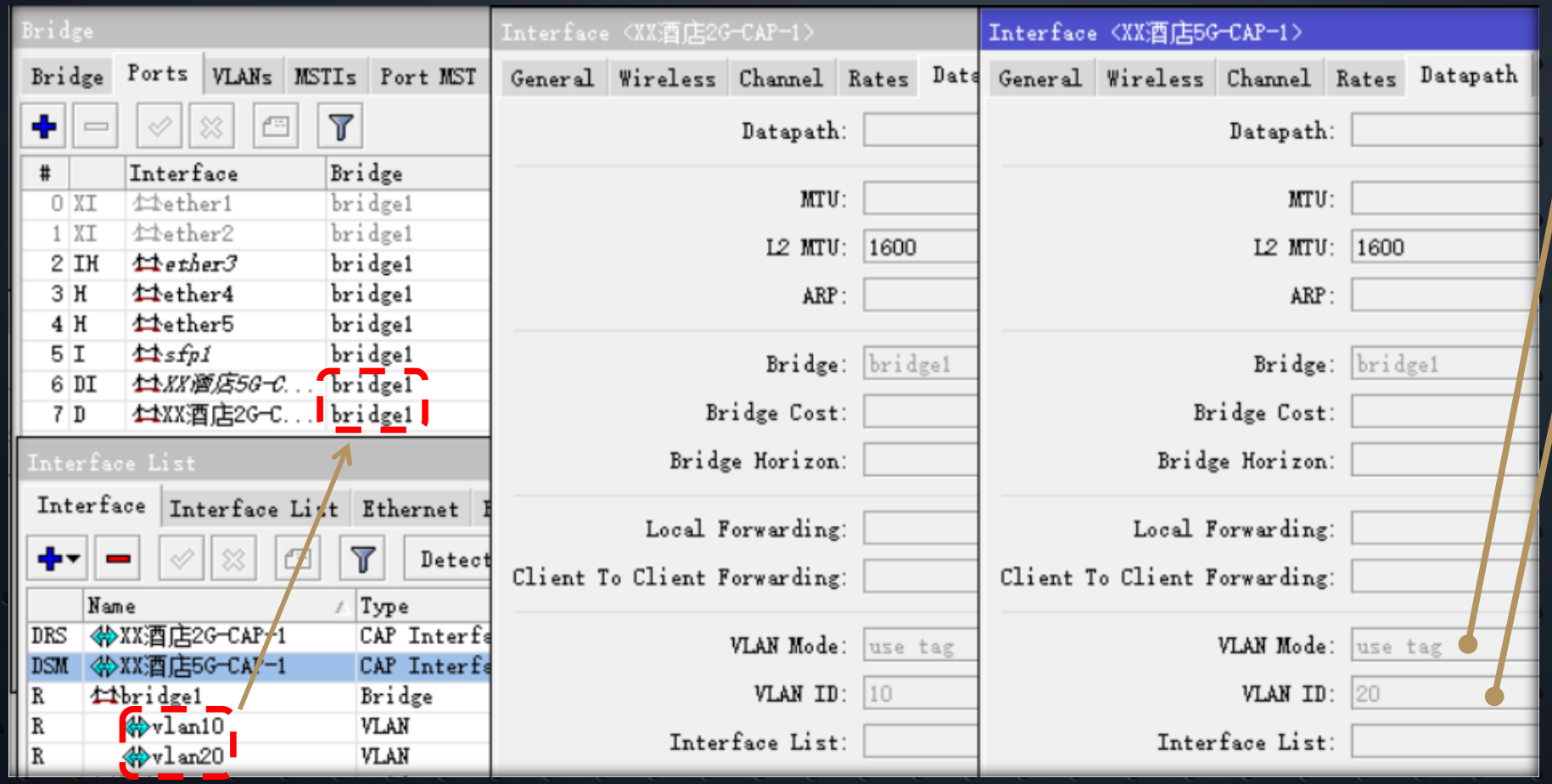
CAPsMAN的VLAN标记

- CAPsMAN集中转发时，vlan标记被特殊的CAPsMAN报头封装，由CAPsMAN设备上解封CAPsMAN报头，才能识别到vlan标记，故给CAP接口分配VLAN tag时，CAPsMAN设备的VLAN网关应该建立于CAP接口所属桥，而不是实际相连的物理接口。



ETH2与CAP接口不在相同Bridge

CAPsMAN的VLAN标记

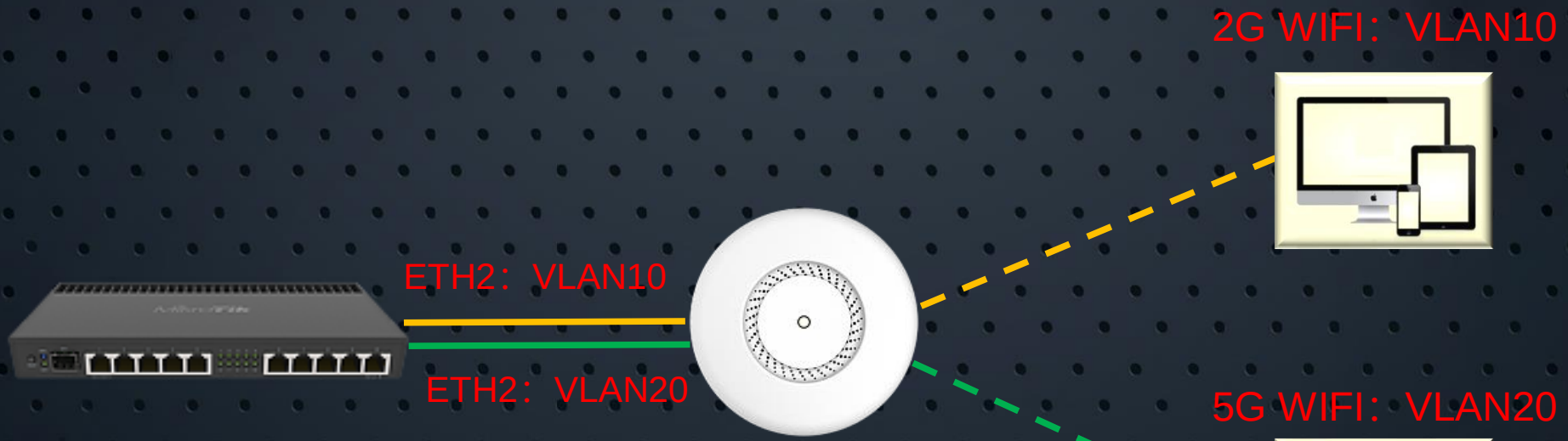


给指定CAP接口传入数据指定VLAN模式

根据VLAN tag模式指定对应VLAN ID

CAPsMAN的VLAN标记

- CAPsMAN本地转发时，没有特殊的CAPsMAN报头，vlan 标记直接可以被途中交换机识别，以便通过交换机获取更大的转发吞吐，同时也可以转发到其他非CAPsMAN设备的VLAN网关。如下图所示VLAN网关应该建立于相连物理接口上。

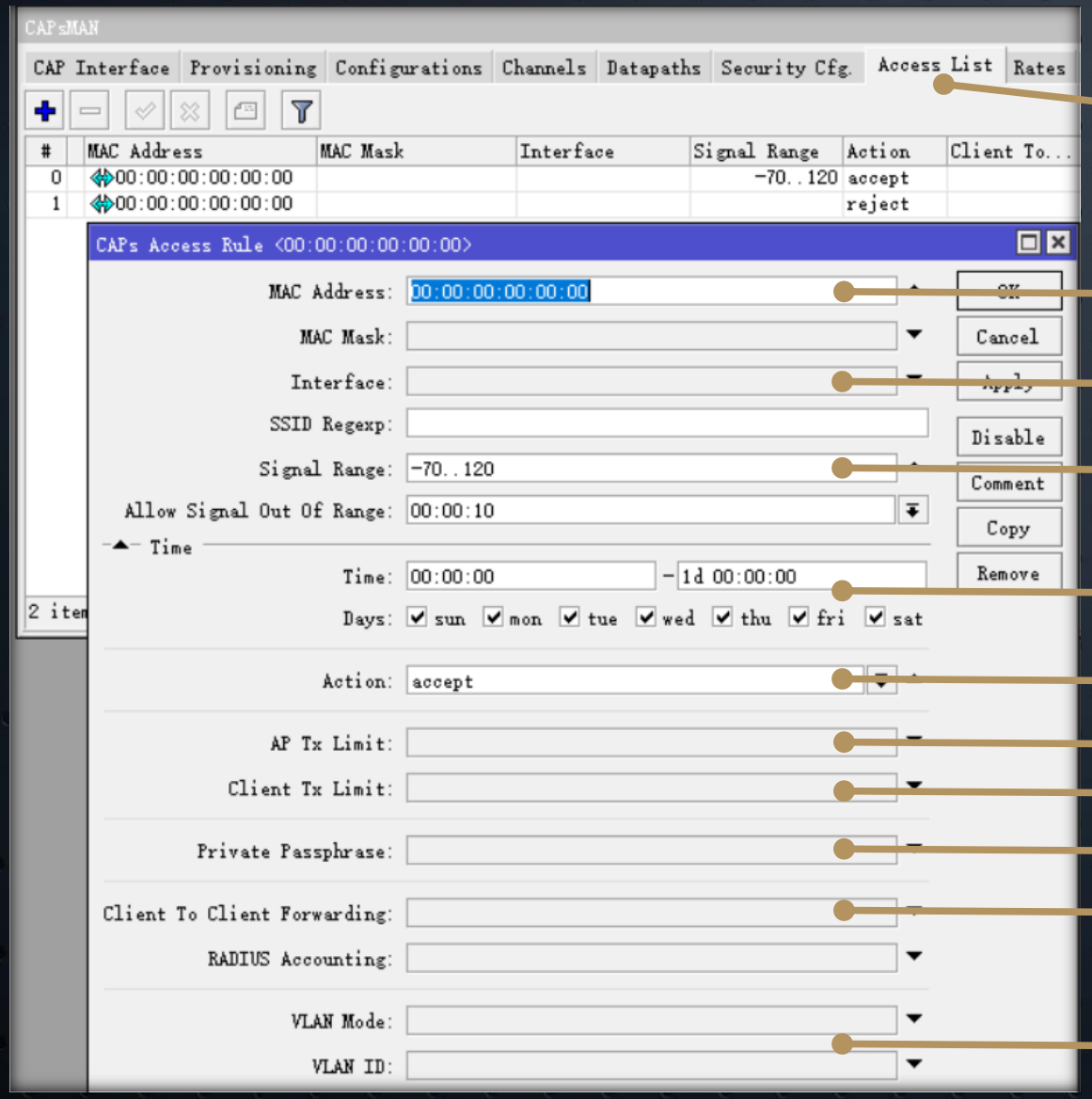


Interface List

Interface | Interface List | Ethernet | EoIP Tunnel | Detect Internet

	Name	Type	Ac
DRS	XX酒店2G-CAP-1	CAP Interface	
DSM	XX酒店5G-CAP-1	CAP Interface	
R	bridge1	Bridge	
X	bridge2	Bridge	
R	ether1	Ethernet	
R	ether2	Ethernet	
R	vlan10	VLAN	
R	vlan20	VLAN	

限制弱信号客户端接入及访问列表相关应用



Access List：控制客户端接入相关。从上到下有序处理，直到找到匹配规则为止。然后执行匹配规则中的操作。

条件项：匹配终端的MAC地址

条件项：匹配终端连接的CAP接口

条件项：匹配终端连接的信号强度

条件项：匹配终端连接的日期时间

动作项：接受或拒绝客户端

动作项：客户端下载速率限制

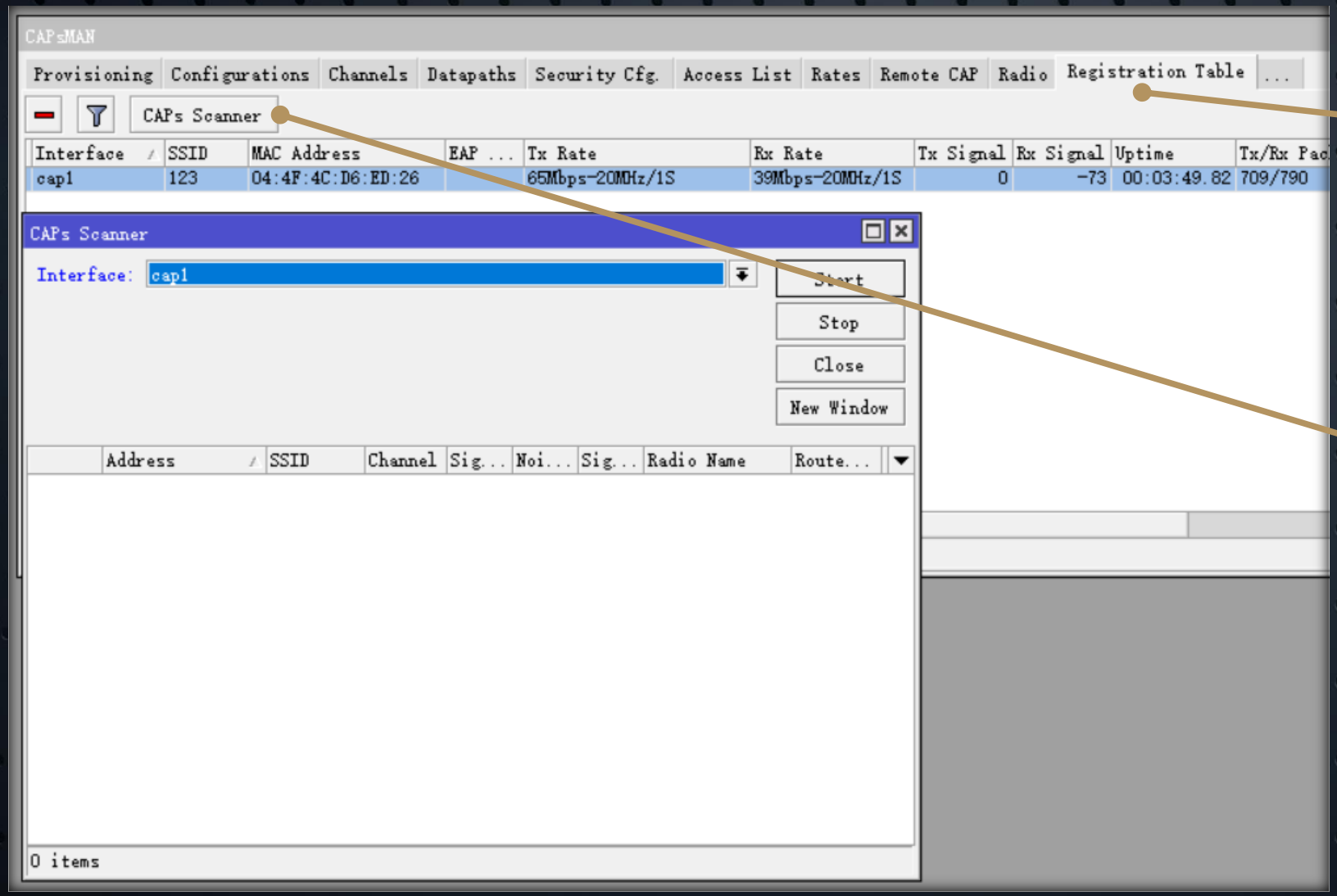
动作项：客户端上传速率限制（仅ROS客户端）

动作项：指定额外接入密钥

动作项：客户端数据转发相关

动作项：客户端传入流量VLAN相关

登记列表相关



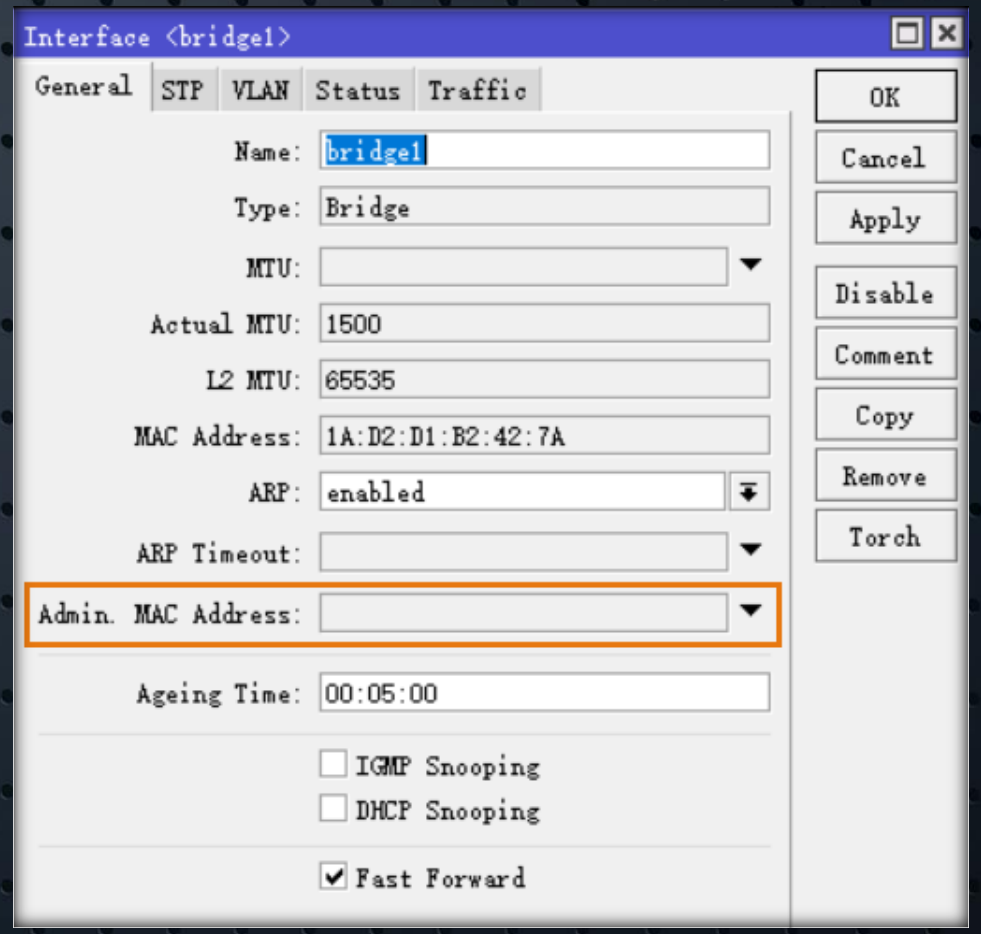
登记列表：查看当前已连接客户的关联信息

CAPs Scanner：环境扫描工具，指定CAP扫描所在环境。

自动MAC与默认防火墙可能导致的问题点等

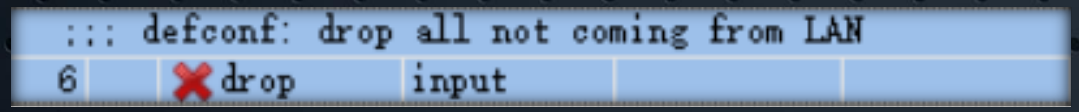
- 当用于CAPsMAN接口的桥配置了自动MAC地址（默认），可能会导致环路或其他一些故障问题，导致CAP接口反复离线。可通过指定静态桥管理MAC解决。

```
[admin@WaveKing] > interface bridge print
Flags: X - disabled, R - running
 0 R name="bridge1" mtu=auto actual-mtu=1500 l2mtu=65535 arp=enabled
     arp-timeout=auto mac-address=1A:D2:D1:B2:42:7A protocol-mode=rstp
     fast-forward=yes igmp-snooping=no auto-mac=yes ageing-time=5m
     priority=0x8000 max-message-age=20s forward-delay=15s
     transmit-hold-count=6 vlan-filtering=no dhcp-snooping=no
```

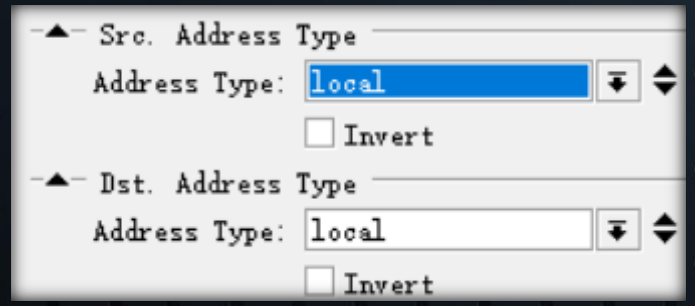


- 不支持ROS CPE以station bridge模式连接
- 当想用一台无线路由器通过CAPsMAN管理自身WLAN时，

若无法发现CAP，需注意



可通过在其上方增加input的放行规则：



谢谢观看