自我介绍

-通过技术认证：MTCNA，MTCWE，MTCRE，MTCTCE，MTCUME，MTCINE。

-中国大陆地区首个通过MTCINE认证的技术顾问。

-独立编写多个ROS相关应用程序，集中WINBOX管理器、内网穿透管理，批量云管理运维等项目。

-当前运维中的项目包含为移动省级机房旁路游戏分流，LPL国际游戏战队网络优化，尼日利亚电信CN2机房维护，企业宽带SDWAN到公网固定IP。

配置WIFI近场认证

MUM 2019 深圳

演讲者：熊茂祥　博客：ROS6.COM

目录

01 什么是近场认证

近场认证的场景

APPLE PAY

支付

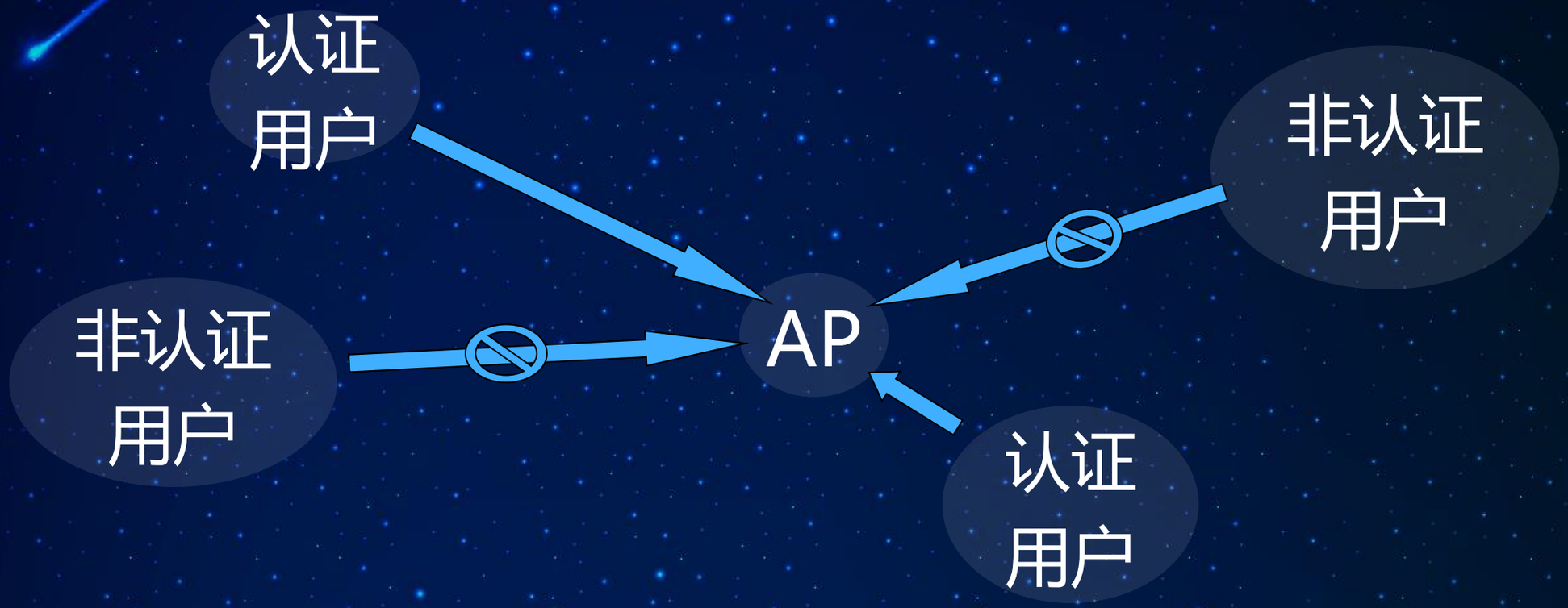
门禁卡

安全

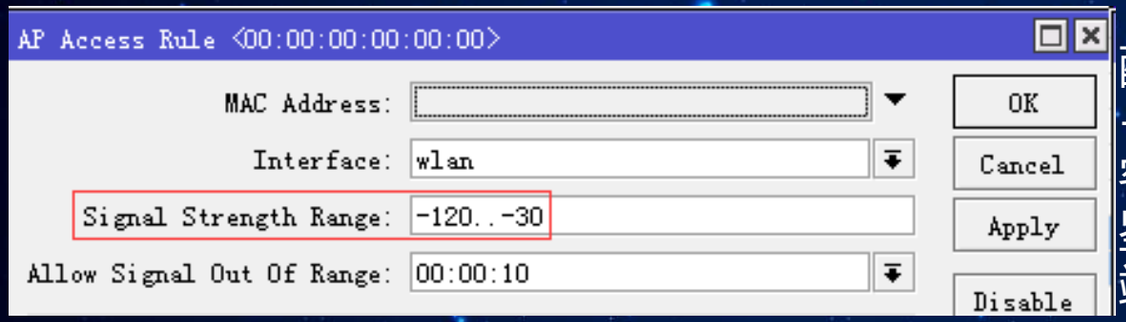
网络

WIFI

如何区分合法用户



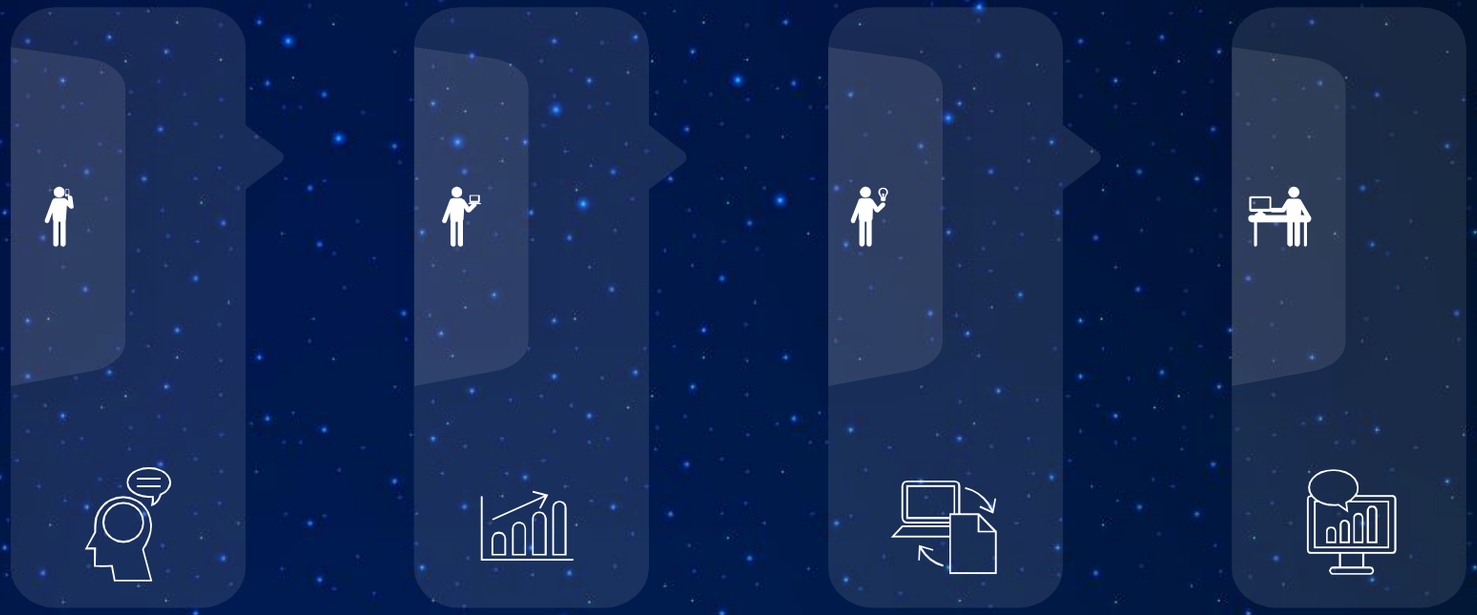
合法用户必须进入有效认证距离，否则将拒绝认证。而认证过后的合法用户再次远离AP也不受影响，依然可以正常认证。
非法用户由于无法足够靠近AP，会持续拒绝认证。



配置参数在/int wir acc栏目里，-120..-30表示，当无线客户端信号小于-30时，将拒绝联入请求。大于-30时则默认放行联入请求。只有当无线客户端距离AP足够近的时候才能达到-30以上信号，如此就完成了近场鉴权。近场鉴权推荐信号范围为-30到-60之间，这个和AP还有无线客户端天线和功率都有关系，并非固定值。

02 为什么需要近场认证

为什么需要近场认证



信息安全　　网络效率　　快速鉴权　　个性化

有效防止非法入侵。不用消耗资源在非法用户上，也不需要加密，传输效率更高。无感知认证让生活更美好。

03 如何实现近场认证

如何实现近场认证

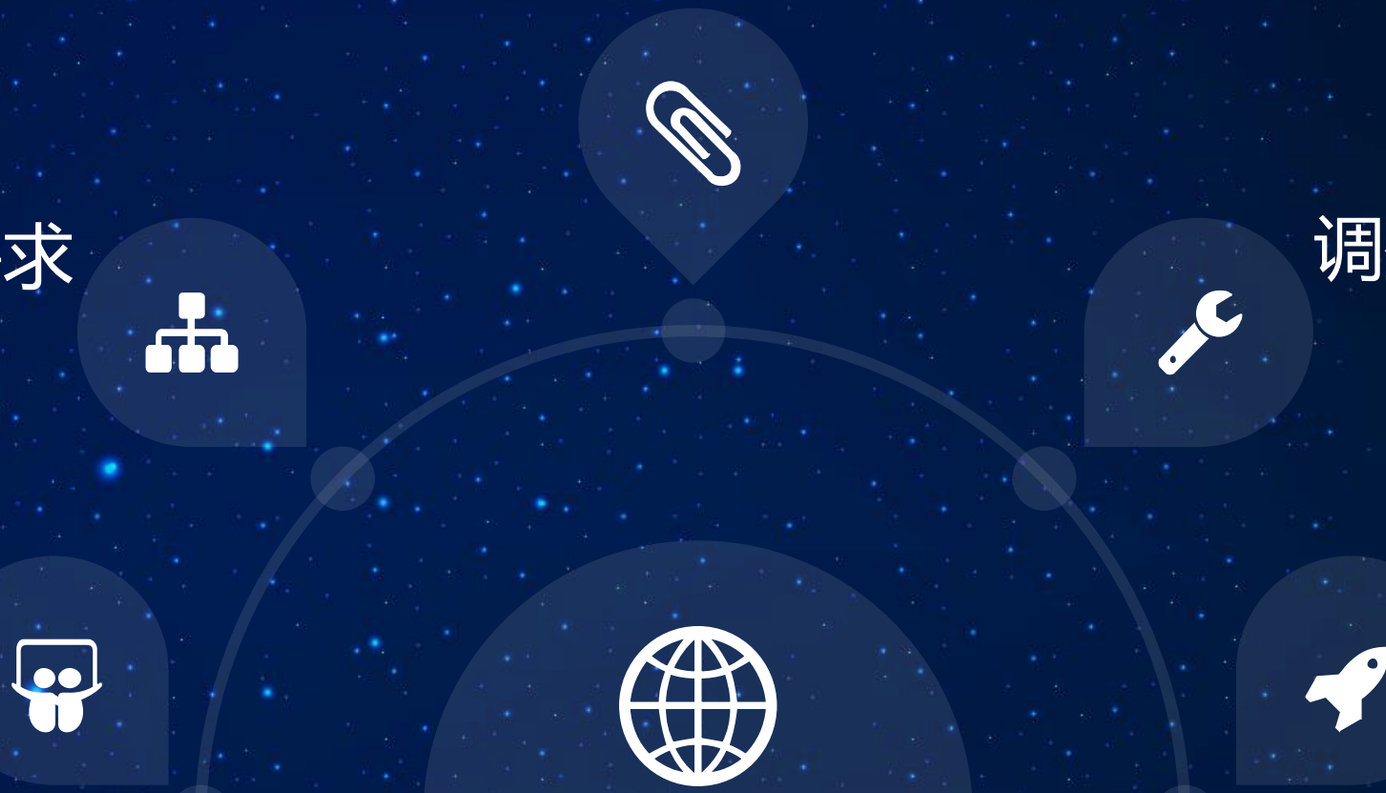
导入近场认证脚本

配置网络需求

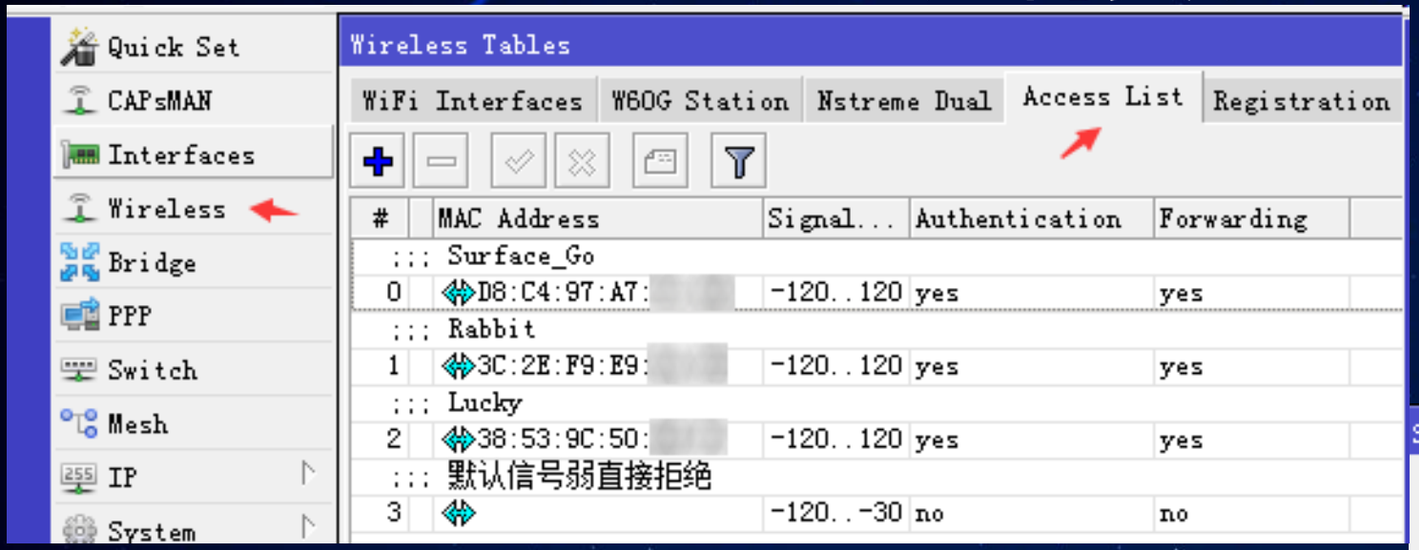
调整近场认证参数

配置白名单

畅快享用网络



如何实现近场认证

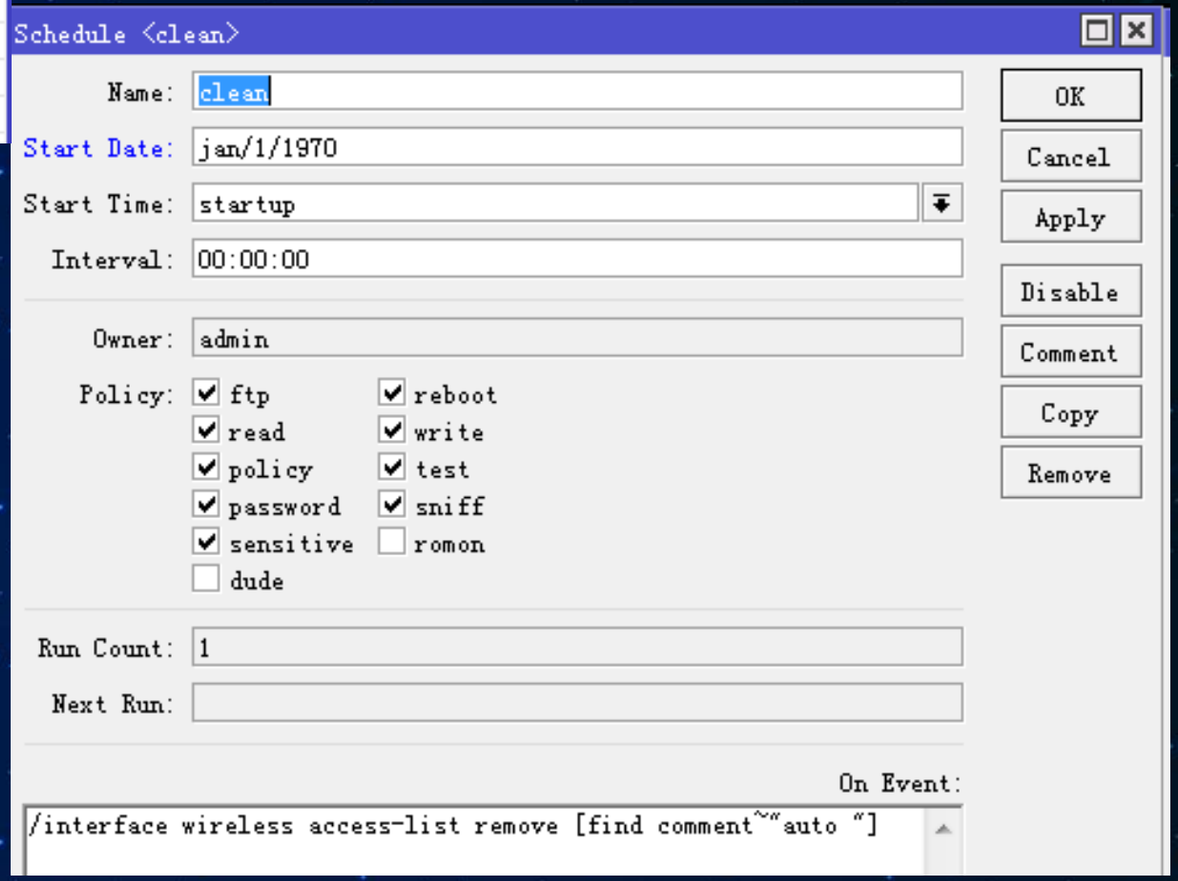


首先我们配置白名单用户，如左图

然后我们自己的设备加入手工白名单，这样重启后也不需要再认证。如右图

右图的脚本会在每次重启的时候清空白名单以外的近场认证名单。

重启后所有之前近场认证的用户都需要重新再进行认证。适合公共上网环境，比如咖啡厅，餐厅，这样用户隔天再来，必须靠近AP认证一下才能上网。家庭用户可以不使用这个脚本。



如何实现近场认证

脚本介绍：

每5秒自动寻找所有已在线且不在白名单的无线客户端，当这些客户端信号值大于-30的时候加入到白名单完成近场认证。

并在完成近场认证的时候AP的CAP-LED灯将点亮2秒，来区分是否认证成功。

这个脚本是针对mAP lite设计，其他设备需自行调整脚本内容。

Schedule <wire_access_auto>

Name: wire_access_auto

Start Date: Jan/01/1970

Start Time: 00:00:00

Interval: 00:00:05

Owner: admin

Policy: ftp, reboot, read, write, policy, test, password, sniff, sensitive, romon, dude

Run Count: 29947

Next Run: May/12/2019 07:28:50

On Event

```
:foreach wirc in=[/interface wireless registration-table find interface="wlan"] do={
:if ($wirc!="") do={
:global wirmac [/interface wireless registration-table get $wirc mac-address]
:if ([/interface wireless access-list find mac-address=$wirmac]="") do={
:if (([/interface wireless registration-table get $wirc signal-strength-ch0] > -30) || ([/interface wireless registration-table get $wirc signal-
strength-ch1] > -30)) do={
:put ($wirmac." alllow into access.")
/interface wireless access-list pr
/interface wireless access-list add place-before=0 interface="wlan" mac-address=$wirmac comment=("auto ".[/system clock get date]." ".[/system clock get
time])
:if ([/system leds get [find leds="cap-led"] type]="off") do={/system leds set [find leds="cap-led"] type=on}
} else={:put ($wirmac." deny into access.")}
}}}
:if ([/system leds get [find leds="cap-led"] type]="on") do={:delay 2s;/system leds set [find leds="cap-led"] type=off}
```

如何实现近场认证

如何设置合适的近场认证信号参数呢：

1.将手机放到离AP想要认证的距离。

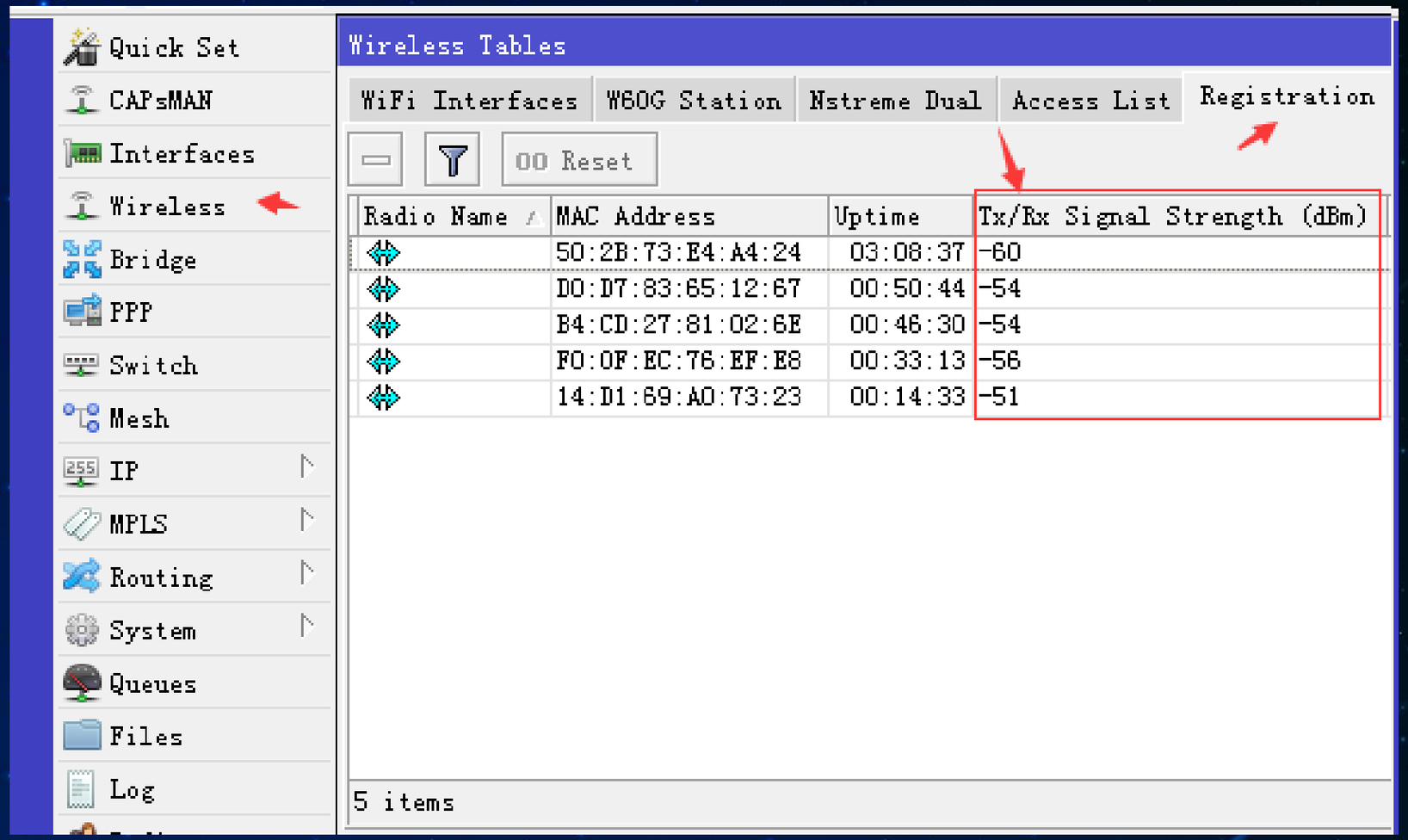
2.在AP里查看当前设备信号强度。

3.将脚本和白名单里的信号强度调整为理想值。

4.清除自动添加的认证白名单后测试近场认证。

5.建议将AP看到认证的距离信号强度值减5。

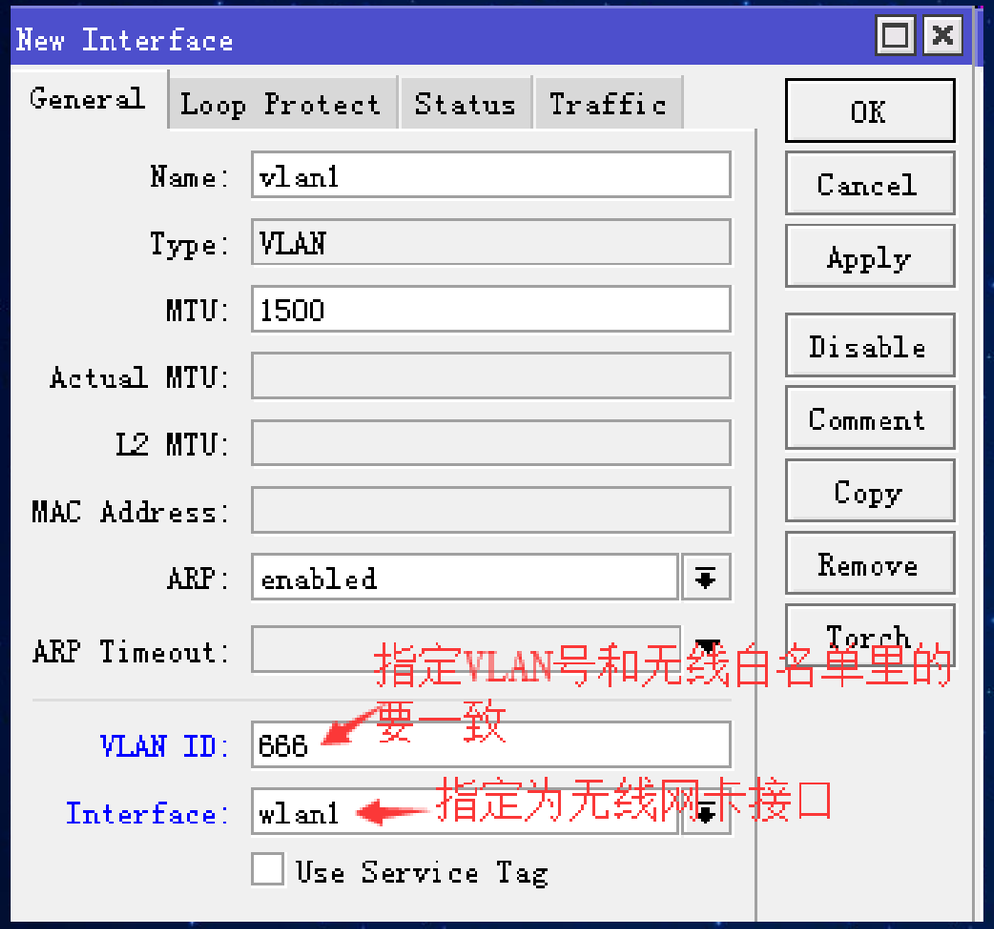
一共有2个地方需要调整。
1./int wir acc里的最后一条（默认允许的认证信号范围）
2.wire_access_auto脚本内容的信号参数



如何实现近场认证

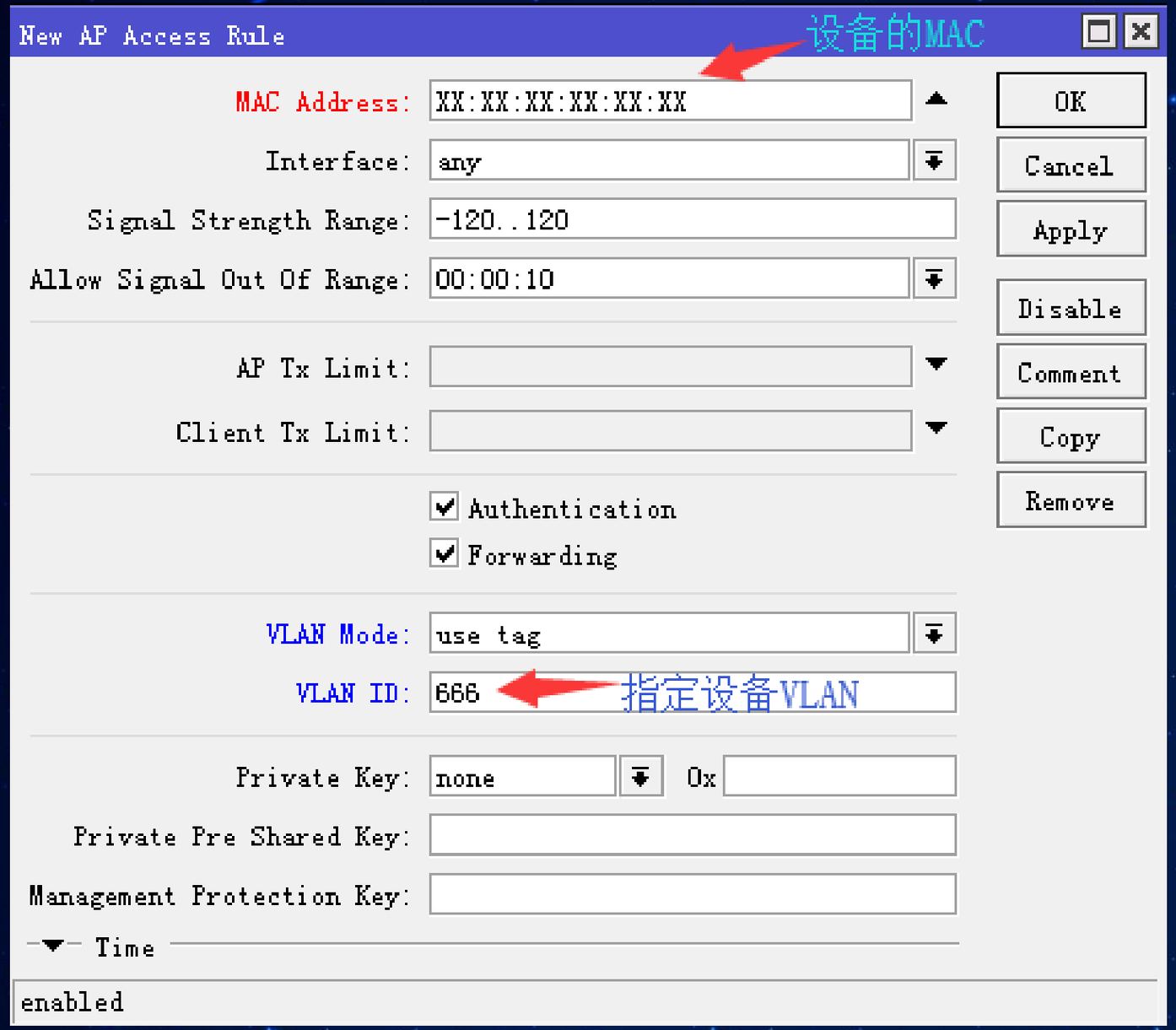
由于商业环境里会有一些内部网络不允许普通用户访问，这个时候需要用到VLAN来隔离，但是这并不影响普通用户使用近场认证。

我们可以将内部用户白名单放在一个特定VLAN，将内部服务器也分配到这个VLAN里即可。这里讲解一下如何将白名单用户放到特定VLAN。



首先我们需要新建个VLAN到无线接口上，比如左图这样。然后将这个VLAN口和内网服务器的口桥接。并在桥上面设置IP和DHCP。这样就隔离了普通用户和内部网络的广播域。防火墙里再加上IP策略，彻底完成互访隔离。

如何实现近场认证



按左图所示，将特定用户无线设备放入到内部VLAN里。这样该无线设备在联入后将被分配到666这个VLAN里，由于该VLAN桥接到了内部网络里，所以可以和内部网络互通，也在同一个广播域。

到此已经完成整个商业环境的近场认证。

既照顾了商业环境的安全需求，又照顾了用户的便捷快速认证的需求。

同样的思路也可以用CAPSMAN来实现，大家可以研究更多方式来让近场认证做得更美好。

如何实现近场认证

脚本介绍：

每5秒自动寻找所有已在线且不在白名单的无线客户端，当这些客户端信号值大于-30的时候加入到白名单完成近场认证。

并在完成近场认证的时候AP的CAP-LED灯将点亮2秒，来区分是否认证成功。

这个脚本是针对mAP lite设计，其他设备需自行调整脚本内容。

Schedule <wire_access_auto>

Name: wire_access_auto
Start Date: Jan/01/1970
Start Time: 00:00:00
Interval: 00:00:05
Owner: admin
Policy: ftp, reboot, read, write, policy, test, password, sniff, sensitive, romon, dude
Run Count: 29947
Next Run: May/12/2019 07:28:50

On Event

```
:foreach wirc in=[/interface wireless registration-table find interface="wlan"] do={
:if ($wirc!="") do={
:global wirmac [/interface wireless registration-table get $wirc mac-address]
:if ([/interface wireless access-list find mac-address=$wirmac]="") do={
:if (([/interface wireless registration-table get $wirc signal-strength-ch0] > -30) || ([/interface wireless registration-table get $wirc signal-
strength-ch1] > -30)) do={
:put ($wirmac." alllow into access.")
/interface wireless access-list pr
/interface wireless access-list add place-before=0 interface="wlan" mac-address=$wirmac comment=("auto ".[/system clock get date]." ".[/system clock get
time])
:if ([/system leds get [find leds="cap-led"] type]="off") do={/system leds set [find leds="cap-led"] type=on}
} else={:put ($wirmac." deny into access.")}
}}}
:if ([/system leds get [find leds="cap-led"] type]="on") do={:delay 2s;/system leds set [find leds="cap-led"] type=off}
```

04 其他近场认证设备

其他近场认证设备

Keewifi kisslink
Hello WiFi

只需将手机平板等设备靠近路由器，轻轻一吻，轻松连接

即插即用，无需密码

05 演示近场认证WIFI

演示近场认证WIFI

现在使用MAP LITE演示近场认证，让大家体验近场认证的魅力。

大家搜索一下信号名为MUM_Xiong的信号，你会发现它不需要密码，但是你无法连接，因为没有达到有效认证距离。

连接上后即使断开WIFI再重新连接也依然可以正常通过认证。

欢迎大家参与现场测试

熊茂祥

湖北 武汉

扫一扫上面的二维码图案，加我微信

感谢观看

邮箱：9939781@gmail.com
博客：ROS6.COM