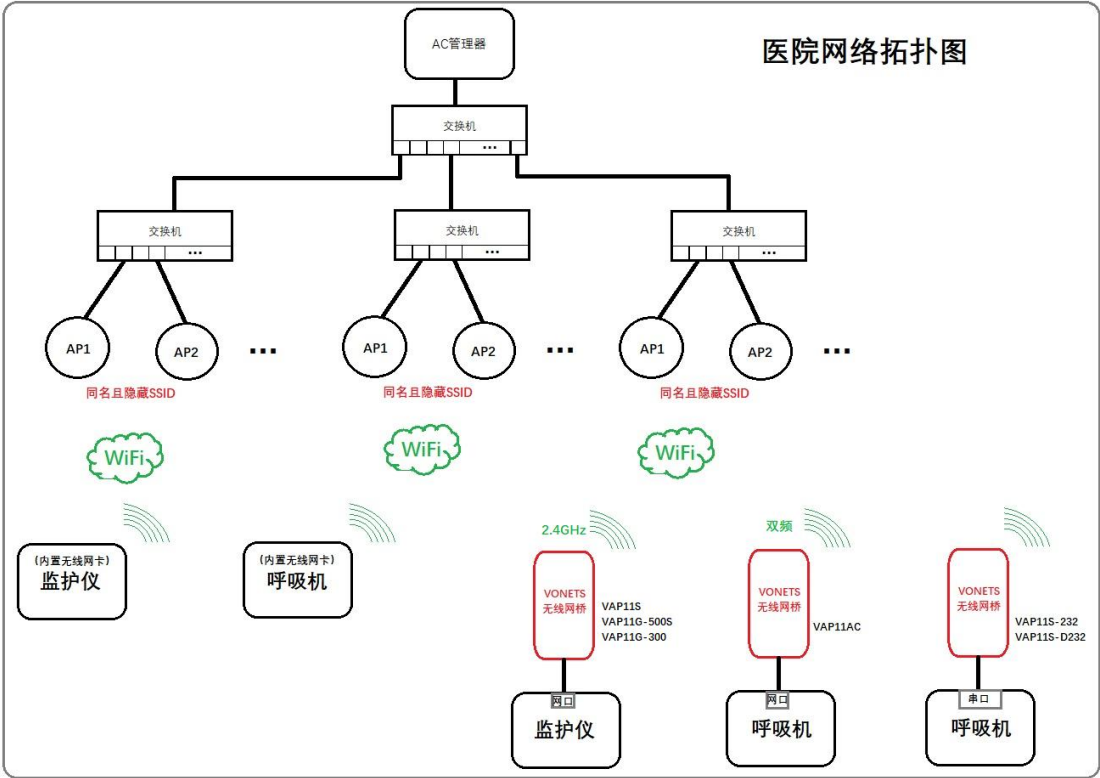


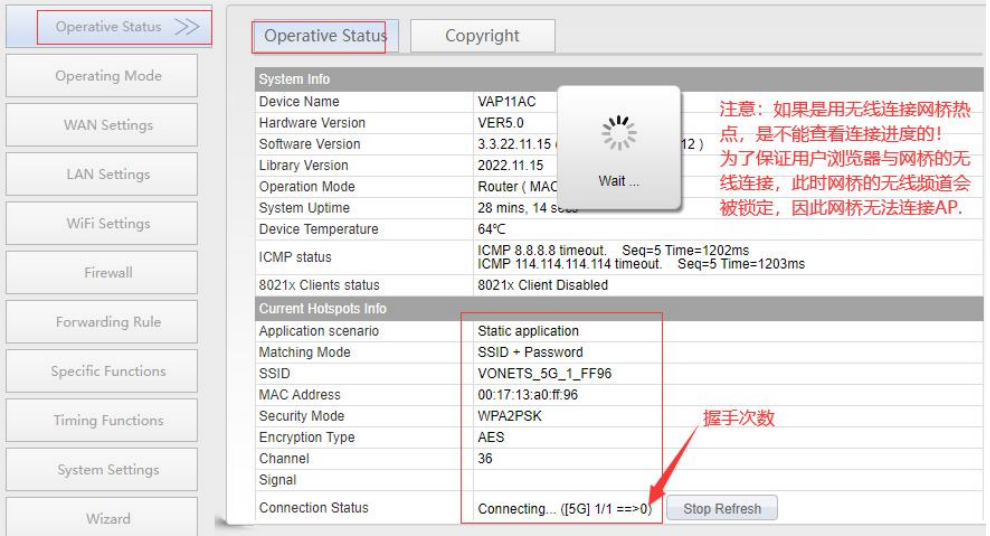
VONETS 无线网桥应用于医院网络被拒绝接入的解决办法



现象 1：网桥配置并重启后，无线连接指示灯快闪几秒后马上又变为慢闪，此时登录状态页则显示网桥正在循环切换不同的热点连接中，热点信号很强，但始终连接不上，或连接上后过几秒又马上断开。

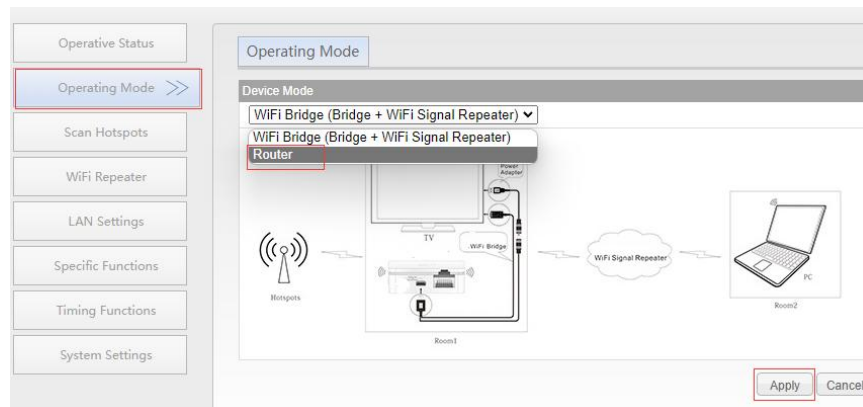
现象 2：网桥配置并重启后，无线连接指示灯始终为慢闪，此时登录状态页则显示网桥正在循环切换不同的热点连接中，热点信号很强，但始终连接不上。

现象 2 不只是被拒绝接入的表现，也可有其他原因造成，这里只分析拒绝接入的解决办法。

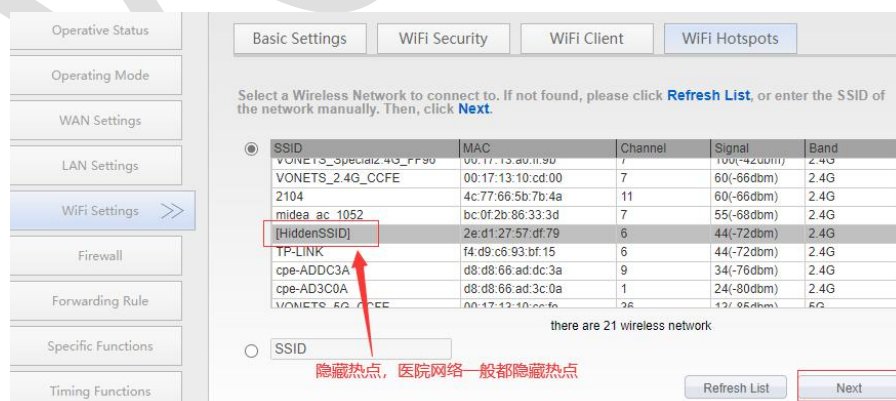
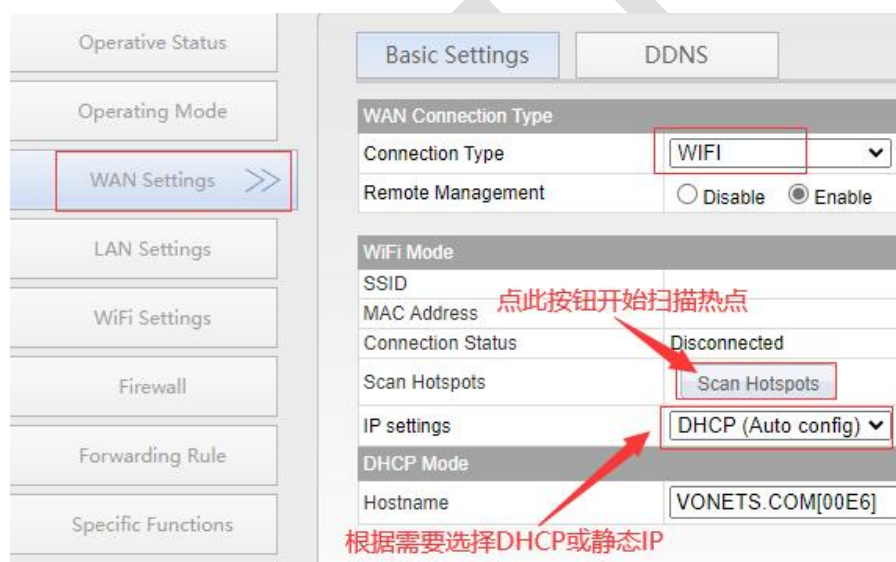


原因：医疗设备直接使用自身的无线连接医院 AP 与经过无线网桥连接 AP, 基于无线传输协议分析是没有任何问题的。但某些品牌的 AP 或 AC 管理策略出于安全或商业垄断的考量，会限制医疗设备通过无线网桥接入网络，AP 会从 WiFi 协议层和 IP 数据传输层作比对判断，从而得知医疗设备是否是经过无线网桥接入网络。

解决办法：1.1 用电脑**有线连接**网桥登录网桥配置页，切换网桥模式为路由模式，然后重启网桥；



1.2 再次用网桥的 LAN IP(默认为 192.168.254.254)有线登录网桥，配置 WAN 为 WiFi 接入；



SSID		输入正确的SSID和密码
Source WiFi hotspot password		
Application type of Src-Hotspot	☒ Normal hotspot ☐ Emergency connection	
Transmission mode	☐ IP layer transparent ☒ MAC layer transparent	此项是专为突破AP的故意拦截行为而设
☒ The configuration parameters of WiFi repeater security is synchronized with source hotspot		
2.4G WiFi Repeater SSID	_2.4G_E6	☒ Disable Hotspot ☒ Disable WiFi Hardware
5G WiFi Repeater SSID	_5G_E6	☒ Disable Hotspot

Advanced Setting (For specific applications only) <<

Hotspot authentication match mode <<

☒ Fully matched authentication mode(MAC certification) 若医疗设备是在固定位置不动的建议选完全匹配模式，可以加快连接速度

The MAC address list to allow the connection +

00:17:13:a0:ff:98 -

☐ SSID and password authentication mode(No MAC certification) 若医疗设备是需要经常移动的，建议用SSID和密码匹配即可，接入会稍慢

Basic Settings WiFi Security WiFi Client WiFi Hotspots

☐ Enable dynamic whitelist ☐ Enable dynamic blacklist

BSSID of hotspots allowed to be connected: First bit Last bit (0,2,4...)

The MAC address list to ignore the connection +

ICMP query for internet connection >>

802.1x authentication client configuration >>

Signal strength and connection parameters[5G] <<

Minimum signal strength of hotspots allowed to be connected dbm (-100 ~ 0)

Maximum number of authentication handshakes (1~20)

Automatic scan interval Sec(1~600)

有较强同频干扰时，网桥与热点需要经过多次的反复握手才能连接成功，适当调高此阈值，有利于类似环境下的连接速度

Motion detection parameters[5G] >>

Temperature compensation parameters[5G] >>

Basic Settings WiFi Security WiFi Client WiFi Hotspots

☐ SSID and password authentication mode(No MAC certification)

☐ Enable dynamic whitelist ☐ Enable dynamic blacklist

BSSID of hotspots allowed to be connected: First bit Last bit (0,2,4...)

The MAC address list to ignore the connection +

ICMP query for internet connection >>

802.1x authentication client configuration >>

Signal strength and connection parameters[5G] >>

Motion detection parameters[5G] >>

Temperature compensation parameters[5G] >>

Apply Back

- 1.3 把医疗设备设为静态 IP (网桥的 LAN 网段), 并把此 IP 映射 (DMZ) 到 VONETS 网桥的 WAN 口, 便于网络内相关设备的主动访问, 若数据只是从医疗单向向上汇报, 则无需做此映射操作;



- 1.4 重启设备。

经过以上操作, 医疗设备和无线网桥在 MAC 层和 IP 头部合并为无线网桥的无线上行网卡的 IP 和 MAC, 对于 AP 来说两者已合为一体, 视两者为一个独立的网络设备, 所以不会再拒绝其接入。其他网络设备若要访问医疗设备, 直接访问网桥的 WAN 口 IP 即可;

- 1.5 在 AC 管理器中添加通行 MAC.

对于有 MAC 通行限制的医院网络, 还需要把网桥的上行网卡 MAC 添加到 AC 管理器的白名单中, 以便放行所有从无线网桥发出的数据包。