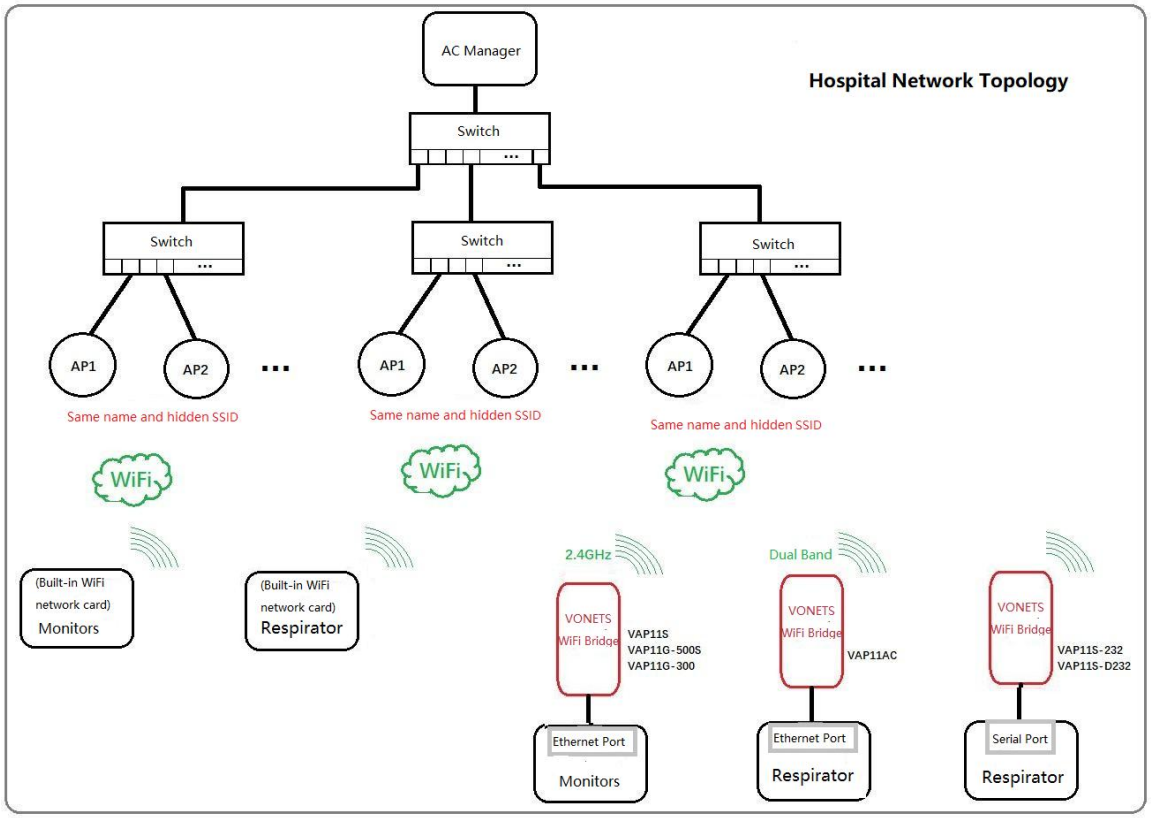
VONETS WiFi bridge is applied to the solution of the hospital network being denied access



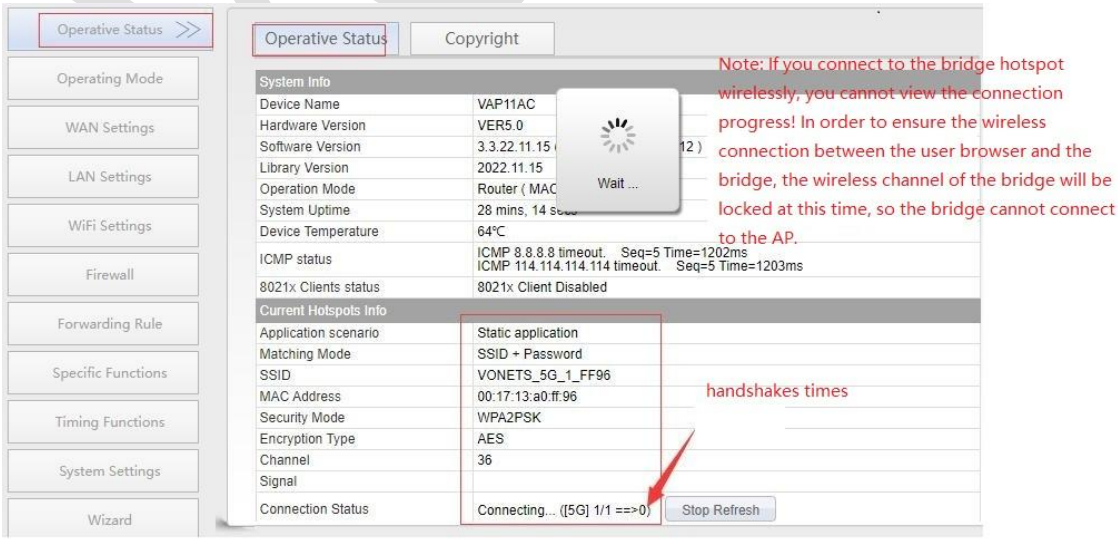
Phenomenon 1：

After the bridge is configured and restarted, the wireless connection indicator flashes quickly for a few seconds and then flashes slowly again. At this time, the login status page shows that the bridge is cyclically switching between different hotspot connections. The hotspot signal is strong, but it is still not connected, or disconnected after a few seconds.

Phenomenon 2:

After the bridge is configured and restarted, the wireless connection indicator is always flashing slowly. At this time, the login status page shows that the bridge is switching between different hotspot connections in a cycle. The hotspot signal is strong, but it still cannot connect.

Phenomenon 2 is not just a manifestation of being denied access, but may also be caused by other reasons. Here we only analyze the solutions to access denial.

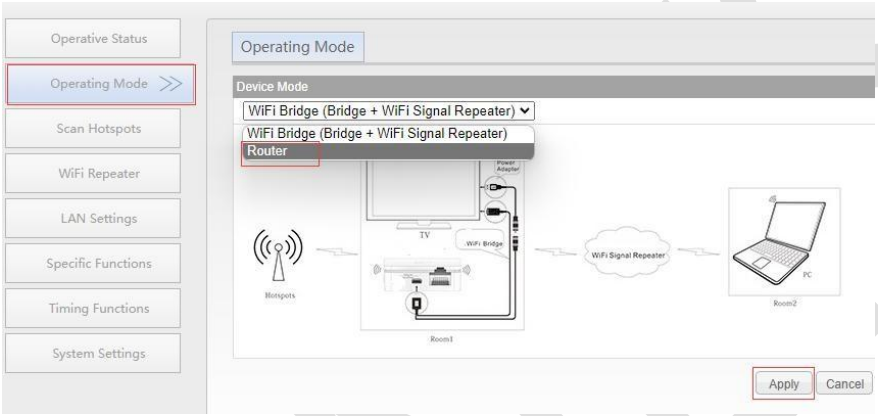


Reason:

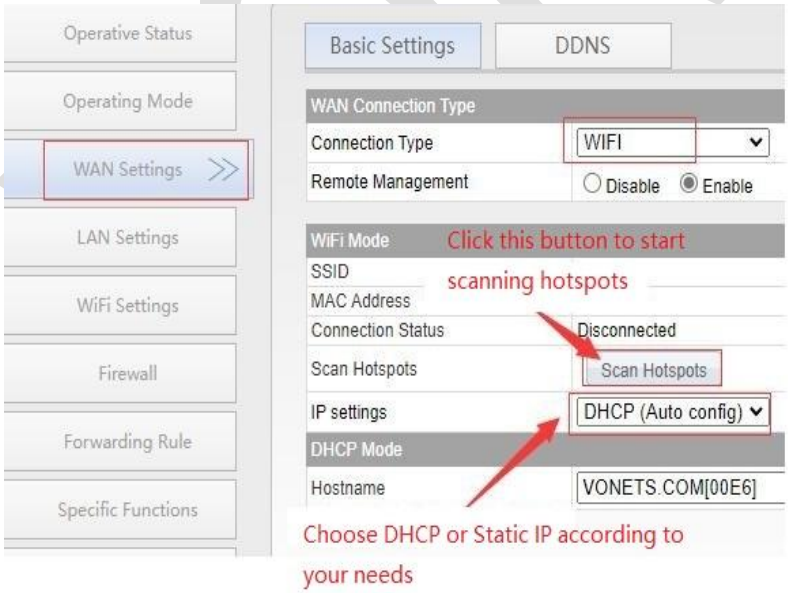
The medical equipment directly uses its own wireless connection to the hospital AP and connects to the AP through a wireless bridge. There is no problem based on the analysis of the wireless transmission protocol. However, some brands of AP or AC management strategies will restrict medical devices from accessing the network through wireless bridges due to security or commercial monopoly considerations. The AP will compare and judge from the WiFi protocol layer and the IP data transmission layer to know Whether the medical device is connected to the network through a wireless bridge.

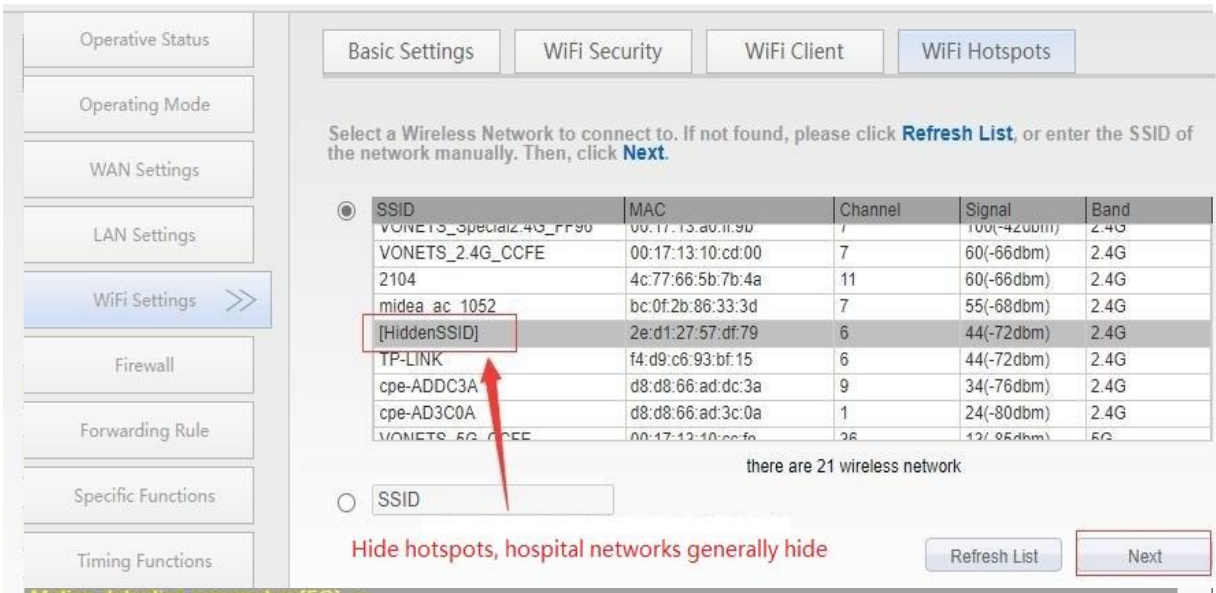
Solution: 1.1

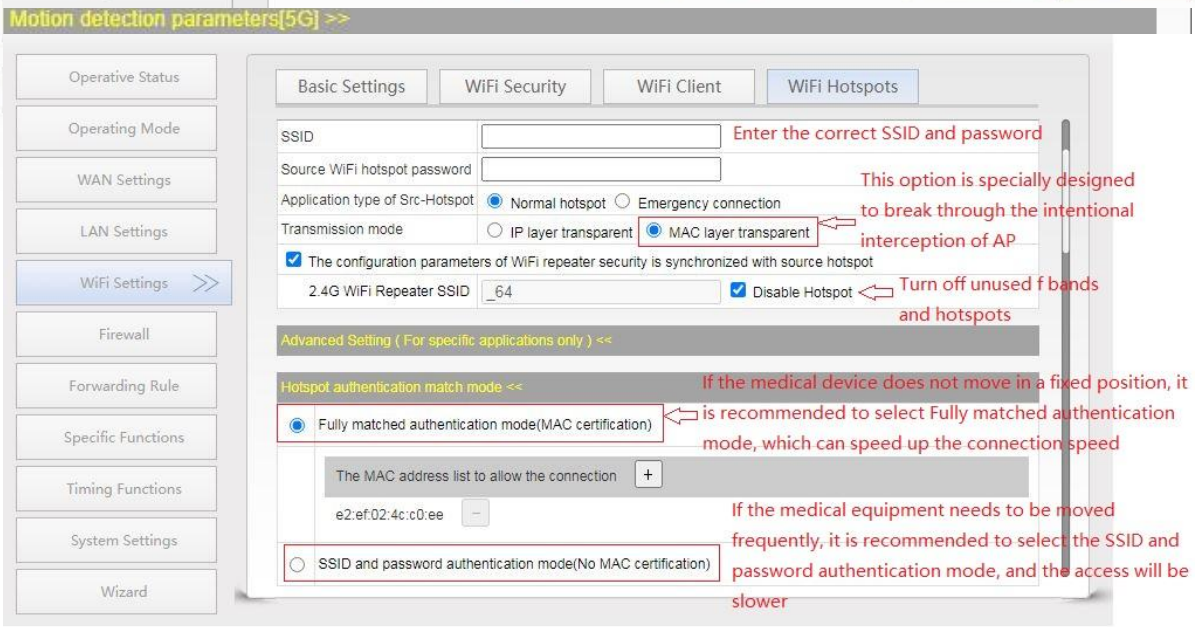
Use a computer to connect to the bridge to log in to the bridge configuration page, switch the bridge mode to router mode, and then restart the bridge;

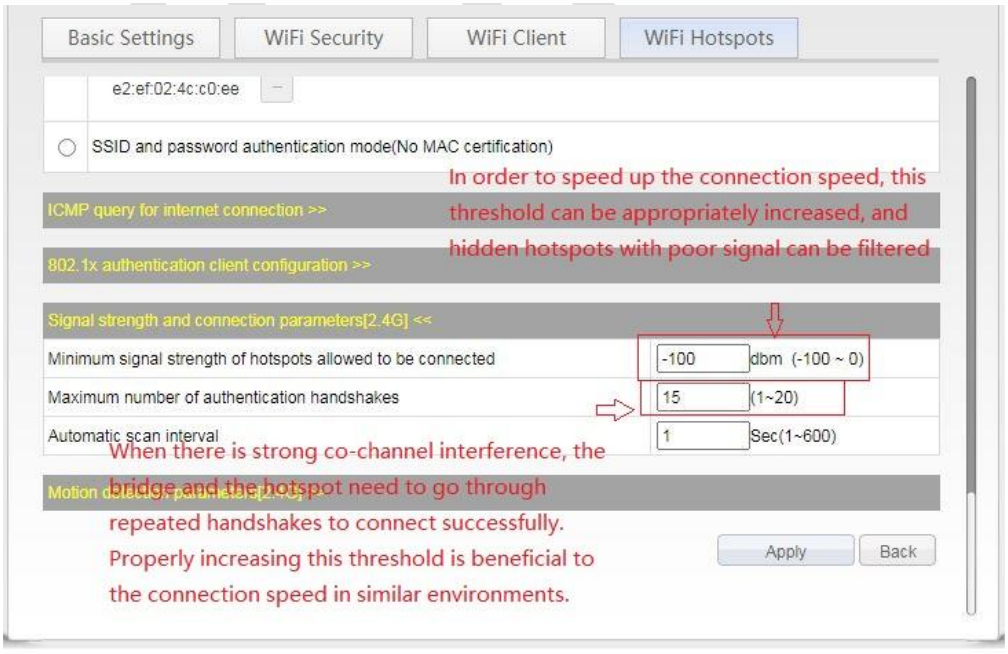


1.2 Use the LAN IP of the bridge (192.168.254.254 by default) to log in to the bridge wiredly again, and configure WAN Settings ---Connection Type to “WiFi” access;

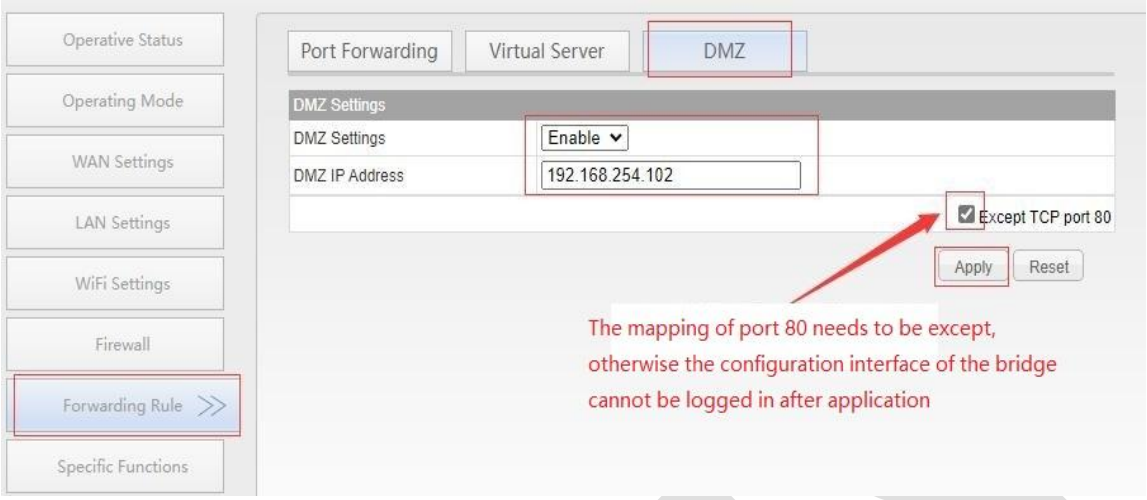



Operative Status
Operating Mode
WAN Settings
LAN Settings
WiFi Settings
Firewall
Forwarding Rule
Specific Functions
Timing Functions
Basic Settings
WiFi Security
WiFi Client
WiFi Hotspots
Select a Wireless Network to connect to. If not found, please click Refresh List, or enter the SSID of the network manually. Then, click Next.
SSID
MAC
Channel
Signal
Band
VONETS_2.4G_CCFE 00:17:13:10:cd:00 7 60(-66dbm) 2.4G
2104 4c:77:66:5b:7b:4a 11 60(-66dbm) 2.4G
midea_ac_1052 bc:0f:2b:86:33:3d 7 55(-68dbm) 2.4G
[HiddenSSID] 2e:d1:27:57:df:79 6 44(-72dbm) 2.4G
TP-LINK f4:d9:c6:93:bf:15 6 44(-72dbm) 2.4G
cpe-ADDC3A d8:d8:66:ad:dc:3a 9 34(-76dbm) 2.4G
cpe-AD3C0A d8:d8:66:ad:3c:0a 1 24(-80dbm) 2.4G
there are 21 wireless network
SSID
Hide hotspots, hospital networks generally hide
Refresh List
Next


Motion detection parameters[5G] >>
Operative Status
Operating Mode
WAN Settings
LAN Settings
WiFi Settings
Firewall
Forwarding Rule
Specific Functions
Timing Functions
System Settings
Wizard
Basic Settings
WiFi Security
WiFi Client
WiFi Hotspots
SSID
Enter the correct SSID and password
Source WiFi hotspot password
Application type of Src-Hotspot
Normal hotspot
Emergency connection
Transmission mode
IP layer transparent
MAC layer transparent
This option is specially designed to break through the intentional interception of AP
The configuration parameters of WiFi repeater security is synchronized with source hotspot
2.4G WiFi Repeater SSID
_64
Disable Hotspot
Turn off unused f bands and hotspots
Advanced Setting (For specific applications only) <<
Hotspot authentication match mode <<
Fully matched authentication mode(MAC certification)
If the medical device does not move in a fixed position, it is recommended to select Fully matched authentication mode, which can speed up the connection speed
The MAC address list to allow the connection
e2:ef:02:4c:c0:ee
SSID and password authentication mode(No MAC certification)
If the medical equipment needs to be moved frequently, it is recommended to select the SSID and password authentication mode, and the access will be slower


Basic Settings
WiFi Security
WiFi Client
WiFi Hotspots
e2:ef:02:4c:c0:ee
SSID and password authentication mode(No MAC certification)
In order to speed up the connection speed, this threshold can be appropriately increased, and hidden hotspots with poor signal can be filtered
ICMP query for internet connection >>
802.1x authentication client configuration >>
Signal strength and connection parameters[2.4G] <<
Minimum signal strength of hotspots allowed to be connected
-100
dbm (-100 ~ 0)
Maximum number of authentication handshakes
15
(1~20)
Automatic scan interval
1
Sec(1~600)
When there is strong co-channel interference, the bridge and the hotspot need to go through repeated handshakes to connect successfully. Properly increasing this threshold is beneficial to the connection speed in similar environments.
Apply
Back

1.3 Set the medical device to a static IP (the LAN network segment of the bridge), and map this IP (DMZ) to the WAN port of the VONETS bridge to facilitate active access to related devices in the network. If the data is only from the medical one-way up report, there is no need to do this mapping operation;



1.4 Restart device.

After the above operations, the medical equipment and the wireless bridge are merged into the IP and MAC of the wireless uplink network card of the wireless bridge at the MAC layer and the IP header. For the AP, the two have been integrated and regarded as an independent network device, so it is no longer denied access. If other network devices want to access medical devices, they can directly access the WAN port IP of the bridge;

1.5 Add pass MAC in AC manager.
For hospital networks with MAC access restrictions, it is also necessary to add the MAC of the uplink network card of the bridge to the white list of the AC manager, so as to allow all data packets sent from the wireless bridge.

2022.11.15 VONETS