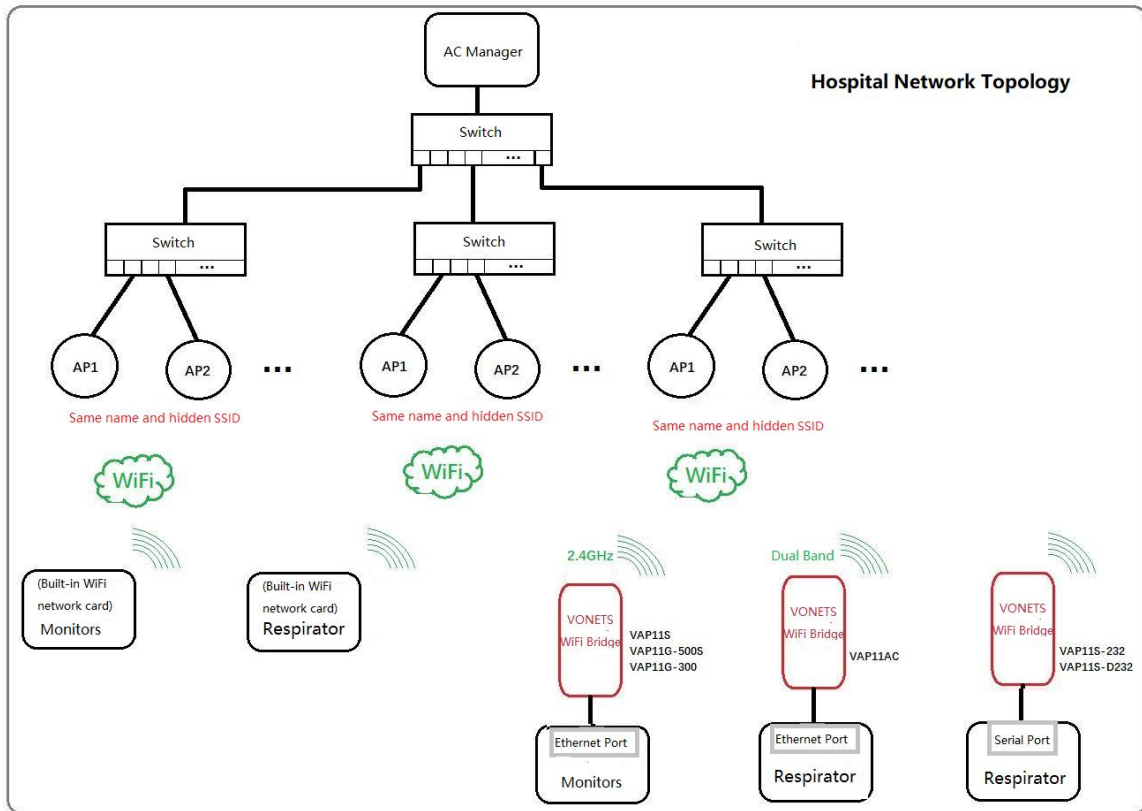


## VONETS WiFi bridge is applied to the solution of the hospital network being denied access



### 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.

The screenshot shows the management interface of a VONETS WiFi bridge. On the left is a sidebar with menu items: Operative Status, Operating Mode, WAN Settings, LAN Settings, WiFi Settings, Firewall, Forwarding Rule, Specific Functions, Timing Functions, System Settings, and Wizard. The main area is titled 'Operative Status' and contains a 'Copyright' tab. A 'Wait ...' dialog box is overlaid on the system info section. Below the system info is the 'Current Hotspots Info' section, which is highlighted with a red box. A red arrow points to the 'Connection Status' field in this section, which shows 'Connecting... ([5G] 1/1 ==>0)'. A 'Stop Refresh' button is located to the right of this field. A red note is overlaid on the right side of the interface, and the text 'handshakes times' is written in red near the connection status.

Note: If you connect to the bridge hotspot wirelessly, you cannot view the connection progress! In order to ensure the wireless connection between the user browser and the bridge, the wireless channel of the bridge will be locked at this time, so the bridge cannot connect to the AP.

handshakes times

System Info	
Device Name	VAP11AC
Hardware Version	VER5.0
Software Version	3.3.22.11.15 (12)
Library Version	2022.11.15
Operation Mode	Router (MAC)
System Uptime	28 mins, 14 s
Device Temperature	64°C
ICMP status	ICMP 8.8.8.8 timeout. Seq=5 Time=1202ms ICMP 114.114.114.114 timeout. Seq=5 Time=1203ms
8021x Clients status	8021x Client Disabled

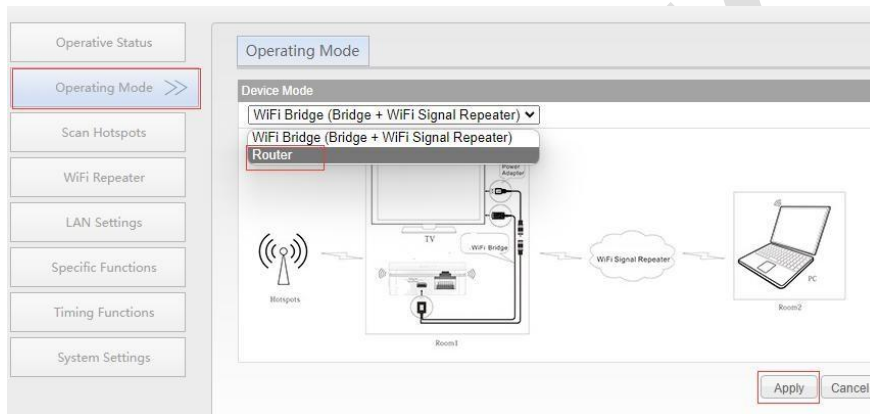
Current Hotspots Info	
Application scenario	Static application
Matching Mode	SSID + Password
SSID	VONETS_5G_1_FF96
MAC Address	00:17:13:a0:f:96
Security Mode	WPA2PSK
Encryption Type	AES
Channel	36
Signal	
Connection Status	Connecting... ([5G] 1/1 ==>0)

Reason:

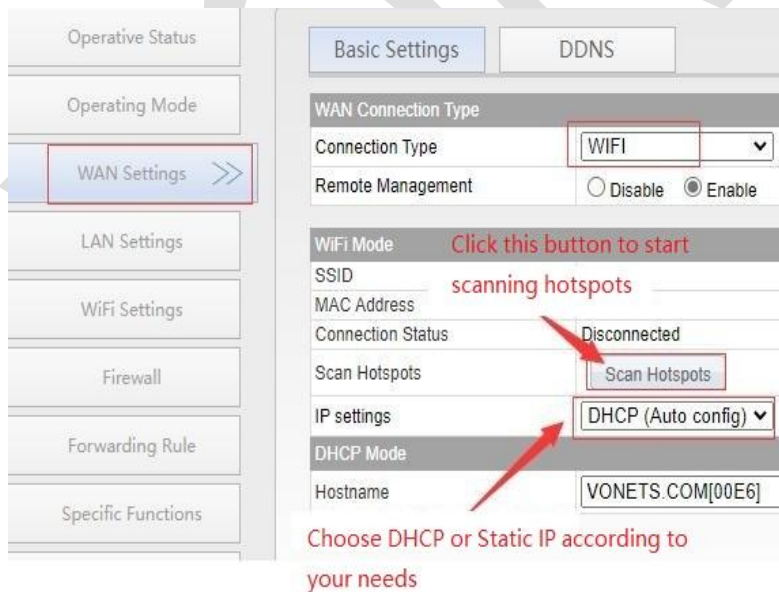
The medical equipment directly uses its own wireless connection to the hospital AP and connects to the AP through a wireless bridge. There is no problem based on the analysis of the wireless transmission protocol. However, some brands of AP or AC management strategies will restrict medical devices from 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_Specializ_4G_FF90	00:17:13:40:11:90	7	100(-42dbm)	2.4G
VONETS_2.4G_CCFE	00:17:13:40:11:90	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
VONETS_5G_CCFE	00:17:13:40:11:90	26	12(-86dbm)	5G

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)

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)

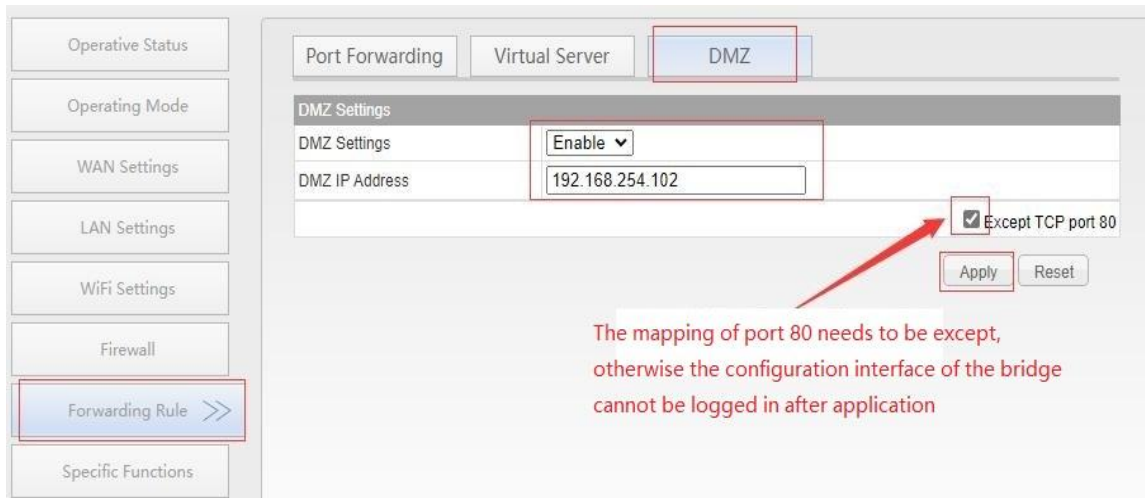
Maximum number of authentication handshakes  15 (1~20)

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.