Mesh Wireless Router

Quick Start Guide

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. V1.0.0

Foreword

General

This manual introduces the connection, configuration and networking of the mesh wireless router (hereinafter referred to as "the device"). Read carefully before using the device, and keep the manual safe for future reference.

Safety Instructions

The following signal words might appear in the manual.

Signal Words	Meaning
DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, reductions in performance, or unpredictable results.
TIPS	Provides methods to help you solve a problem or save time.
NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	April 2023

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.

- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

This section introduces content covering the proper handling of the device, hazard prevention, and prevention of property damage. Read carefully before using the device, comply with the guidelines when using it, and keep the manual safe for future reference.

Transportation Requirements

Transport the device under allowed humidity and temperature conditions.

Storage Requirements

Store the device under allowed humidity and temperature conditions.

Installation Requirements

- Do not connect the power adapter to the device while the adapter is powered on.
- Strictly comply with the local electric safety standards.
- Personnel working at heights must take all necessary measures to ensure personal safety including wearing a helmet and safety belts.
- Do not leave outdoor models of the device hanging in the air or facing outwards when installing onto poles that are on top of buildings.

- Do not place the device in a place exposed to sunlight or near heat sources.
- Place the device in a well-ventilated place, and do not block its ventilation.
- Use an adapter or chassis power supply from the manufacturer.
- Do not connect the device to two or more kinds of power supplies, to avoid damage to the device.
- The device is a class I electrical appliance. Make sure that the power supply of the device is connected to a power socket with protective earthing.
- The device must be grounded by a copper wire with a cross-sectional area of 2.5 mm^2 and a ground resistance no more than 4 Ω.
- Voltage stabilizer and lightning surge protector are optional depending on the actual power supply on site and the ambient environment.
- To ensure heat dissipation, the gap between the device and the surrounding area should not be less than 10 cm on the sides and 10 cm on top of the device.
- When installing the device, make sure that the power plug and appliance coupler can be easily reached to cut off power.
- Outdoor models of the device must be securely installed on poles or brackets that are perpendicular to the ground. Make sure the entire surface of the device and all its related

components are covered with anti-oxidation coating (such as rust preventive paint), and that the installation site and height of the device meet the requirements of the plan.

- Install outdoor models of the device on top of buildings where there is little to no direct sunlight to avoid the device becoming overheated. Make sure to take all necessary measures to protect the device.
- Face the side with the Ethernet port downwards, and arrange the wires in a downward direction when installing outdoor models of the device.

Operation Requirements

- Do not disassemble the device without professional instruction.
- Operate the device within the rated range of power input and output.
- Make sure that the power supply is correct before running the device.
- When removing the cable device first to avoid personal injury.
- Do not unplug the power cord on the side of the device when the adapter is powered on.

- Use the device under allowed humidity and temperature conditions.
- Operating temperature: –10 °C to +55 °C (+14 °F to +131 °F).
- This is a class B product. In a domestic environment this may cause radio interference in which case you may be required to take adequate measures.

Maintenance Requirements

- Do not disassemble it unless necessary.
- Power off the device before maintenance.
- Mark key components on the maintenance circuit diagram with warning signs.

Contents

1 Connecting the Router

Figure 1-1 Connect the router

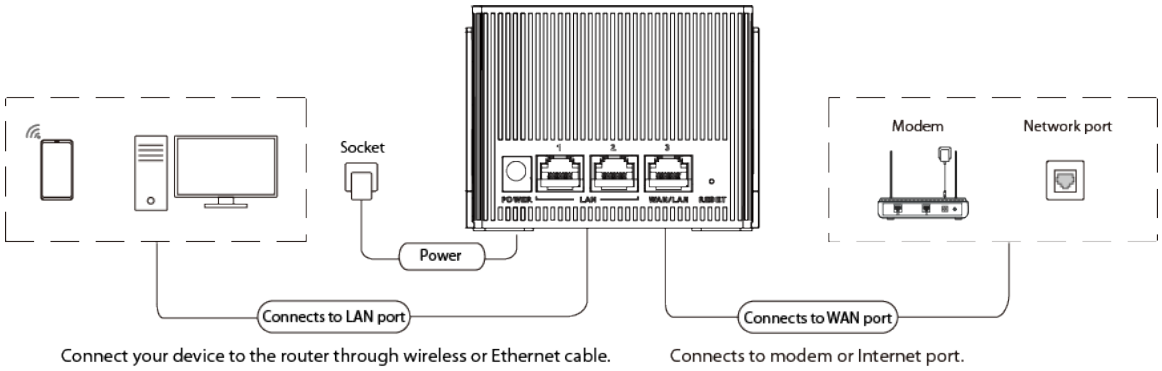


Figure 1-2 Front panel

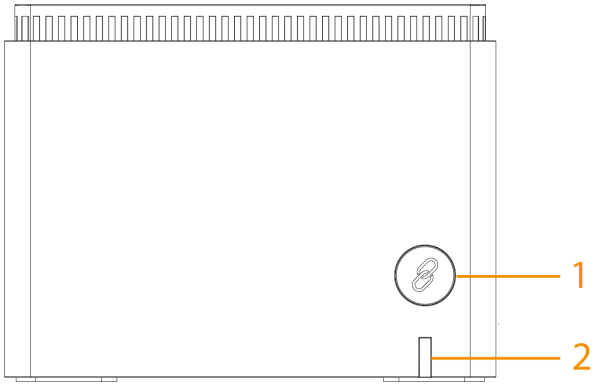


Table 1-1 Indicator and button descriptions

No.	Indicator/button	Description
1	Pairing button	Press and hold the button for more than 5 seconds to start mesh networking. Mesh networking is enabled by default. You need to log in to the webpage or the WiLynk app to disable the function.
2	Indicator status	• Red light is solid on: The router is turned on but not connected to the network. • Green light is solid on:The router is turned on and connected to the network. • Green and red light flash: Mesh networking. • Green light of the sub router is solid on for 5 seconds and then off: Pairing was successful. • The light is off: The router is turned off and set as off. The lights of the sub router are off: Mesh networking and repeater networking was successful.

Figure 1-3 Rear panel

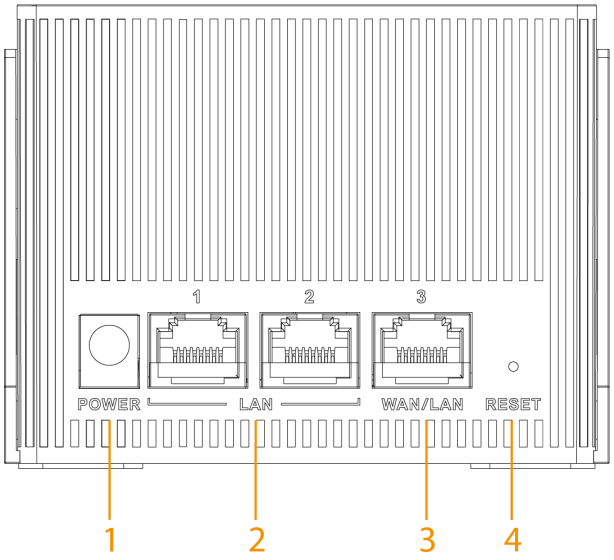


Table 1-2 Rear panel description

No.	Description
1	Power port. Connects to the power supply.
2	LAN port. Connects to wired devices such as computers and set top boxes. You can switch between the WAN port and LAN port.
3	WAN port. Connects to the modem or Ethernet port. You can switch between the WAN port and LAN port.
4	Reset button. Press and hold the button for more than 5 seconds, and then the router will restore its factory defaults.

2 Configuring the Router

You can initialize the device and log in to it through the device webpage and WiLynk app.

2.1 App Configuration

You can initialize the device and log in to the app to configure the device.

- For the first time use or after the device is restored to its factory defaults, you need to initialize the device.
- To protect your device, keep the admin login password safe after initialization, and change the password regularly.
- For more details on app configuration, go to **Me** > **User Manual** on WiLynk.

2.1.1 Downloading App

Scan the QR code to download the WiLynk app.

Figure 2-1 QR code

You can also search for WiLynk at the app store, and then download it.

2.1.2 Registering Accounts

Procedure

Step 1 Open WiLynk, tap **Register** , and then enter the **Register** page.

Step 2 Select the country or region, enter the email address or phone number, enter the password, and then confirm it.

Phone number is only supported in select countries.

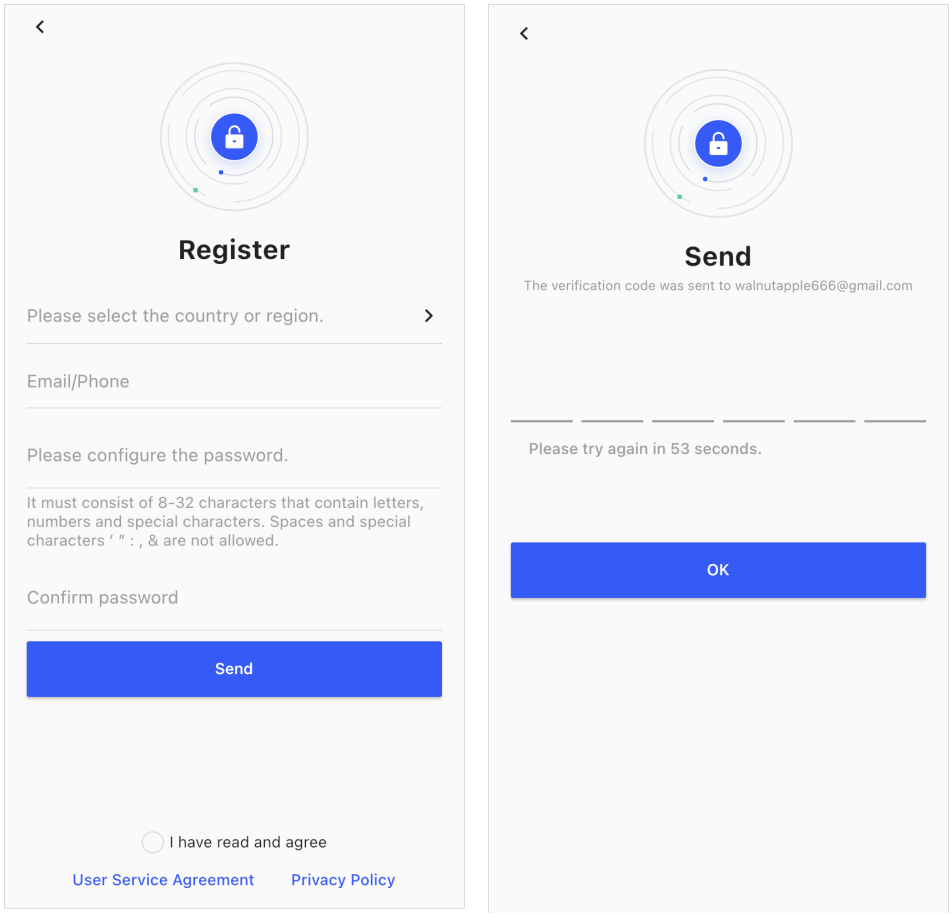
Step 3 Click the **I have read and agree** checkbox.

You can click to view the user service agreement and privacy policy.

Step 4 Click **Send**.

Step 5 Enter the verification code, and then click **OK**.

Figure 2-2 Registration

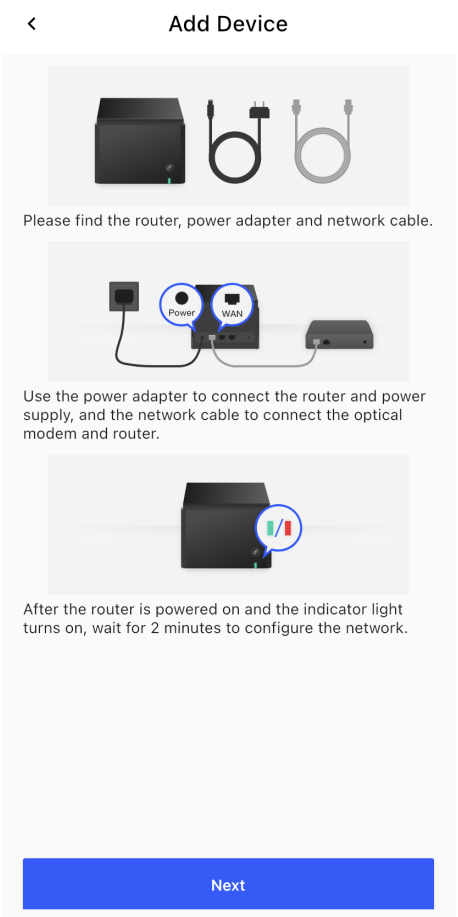


2.1.3 Adding Devices

Prerequisites

Make sure that the device is connected with power and modem. After the device is powered on, wait for 2 minutes, and then add devices.

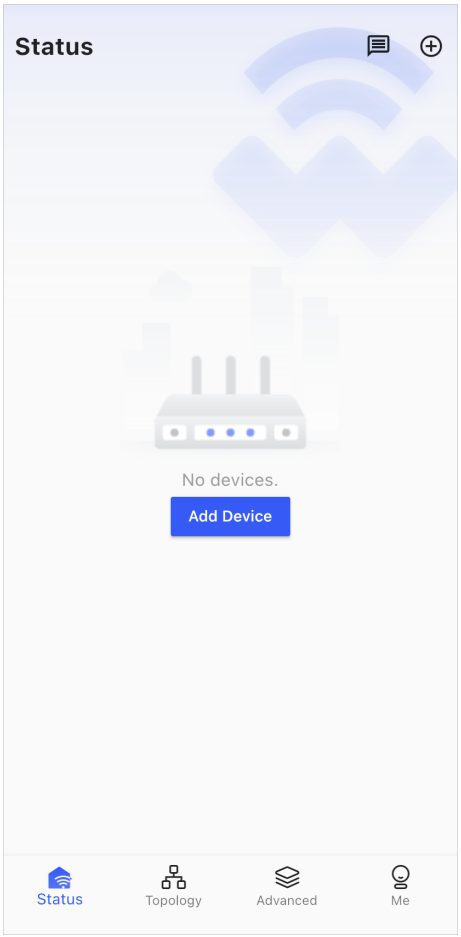
Figure 2-3 Preparations for adding device



Procedure

Step 1 On the **Status** page, tap **Add Device** or ⊕ on the right-upper corner.

Figure 2-4 Add devices



Step 2 Scan the QR code on the device, or tap **Select Type** of the device, and then enter the SN.

Step 3 Go to the Wi-Fi settings on your system settings, connect the router SSID, and then tap **Next**.

Step 4 Configure the login password of the device, and then tap **Next**.

Step 5 Configure the networking method of the device, and then tap **Next**.

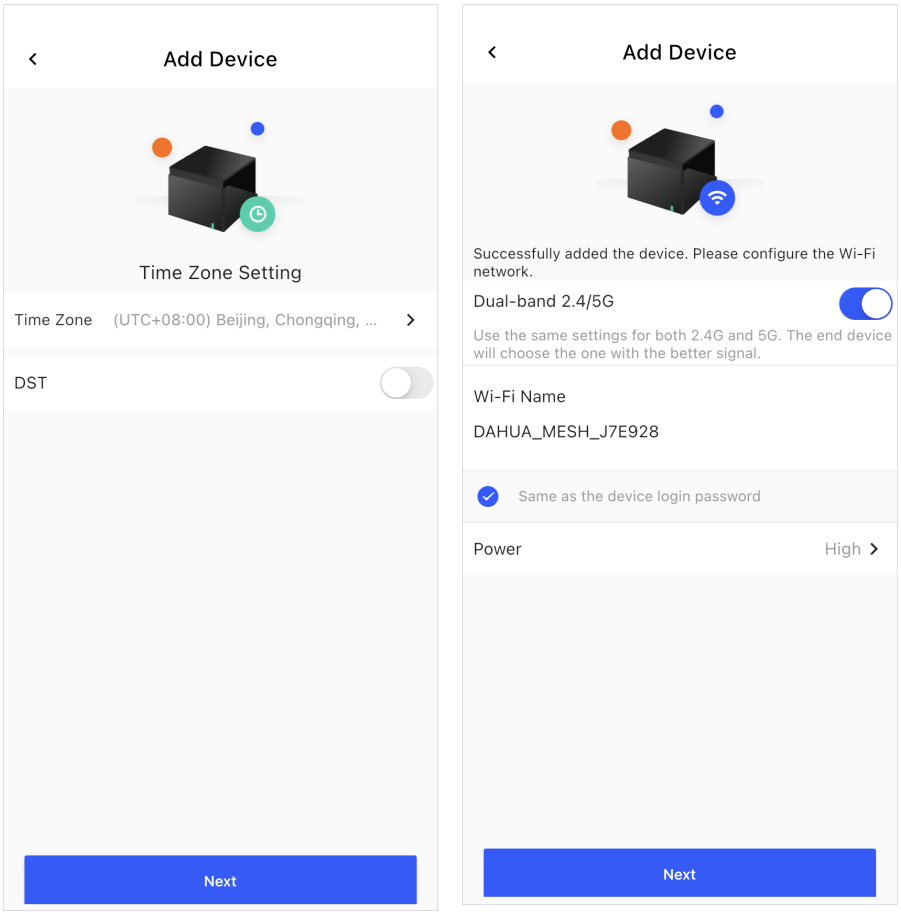
Step 6 Wait until the screen prompts **Connect to Internet** , and then tap **Next**.

Step 7 Configure the time zone and DST of the device, configure the device SSID, and then tap **Next** to finish the configuration.

Step 8 You can start Mesh networking.

For details on Mesh networking, see “3 Mesh Networking”.

Figure 2-5 Configure time zone and Wi-Fi network



2.2 Web Configuration

You can initialize the device and log in to it through the device webpage.

- For first-time use or after the device is restored to its factory defaults, you need to initialize the device.
- To protect your device, keep the admin login password safe after initialization, and change the password regularly.
- Make sure that the local computer and the device are on the same network segment. The default IP address is 192.168.1.110.

2.2.1 Initializing Devices

Procedure

Step 1 Open web browser, enter dahuawifi.com or the default IP address of the device in the address bar, and then press the Enter key.

Step 2 Click **OK**.

Step 3 Select the **I have read and agree to the terms of the Software License Agreement and Privacy Policy** checkbox, and then click **OK**.

Step 4 Set your password and an associated email address.

If you forget the username or password, you can find them back from the email address.

Step 5 Click **Next**.

2.2.2 Logging in to Webpage

Procedure

Step 1 Open web browser, enter the IP address of the device in the address bar, and then press Enter.

Step 2 Enter the password, and then click **Login**.

Log in to the webpage, and then click **Forgot password?** to reset the password.

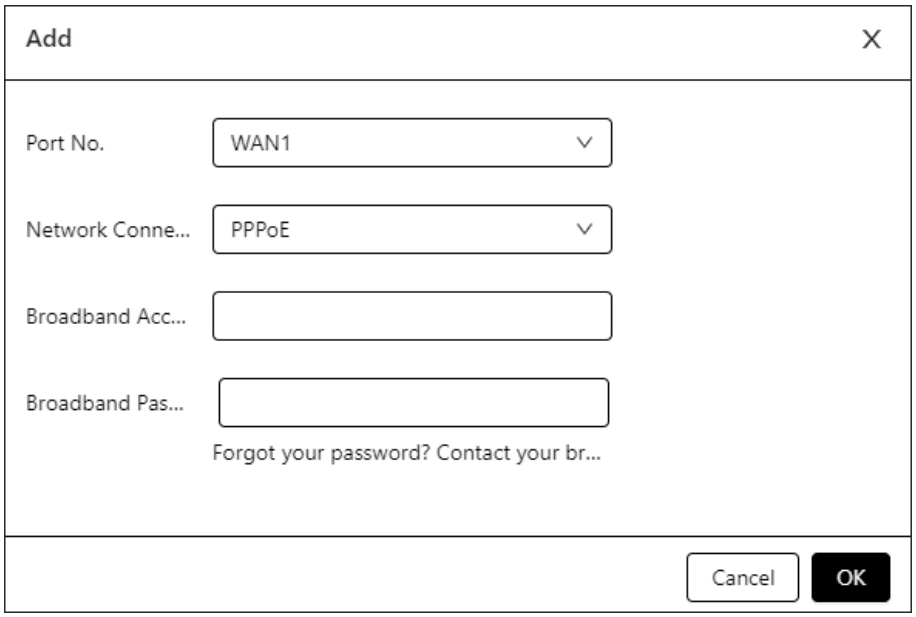
2.2.3 Configuration Guide

Procedure

Step 1 Click on the upper-right corner of the home page.

Step 2 Click **Add** to configure the network parameters, and then click **OK**.

Figure 2-6 Network settings



Step 3 Configure WLAN parameters, and then click **Next**.

Figure 2-7 WLAN connection settings

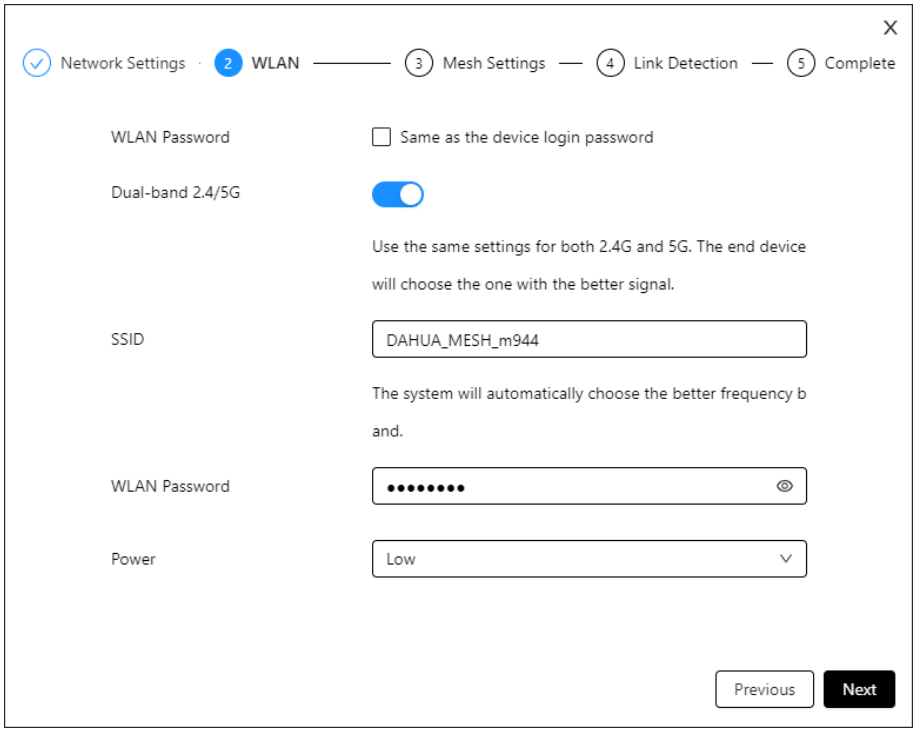


Table 2-1 Descriptions of WLAN parameters

Parameter	Description
WLAN Password	Select **Same as the device login password**, and then the password of WLAN will be the same as the login password of the device.
Dual-band 2.4/5G	Enable **Dual-band 2.4/5G** by default, and then strongest Wi-Fi signal will be automatically selected. Only when **Dual-band 2.4/5G** is enabled, the name of 2.4 GHz and 5 GHz will be the same. You will automatically connect to the fastest network.
SSID	
Power	Select from **Low** , **Middle** and **High**. The higher the power is, the larger the area the signal will cover.

Step 4 Configure mesh settings, and then click **Next**.

Figure 2-8 Mesh settings

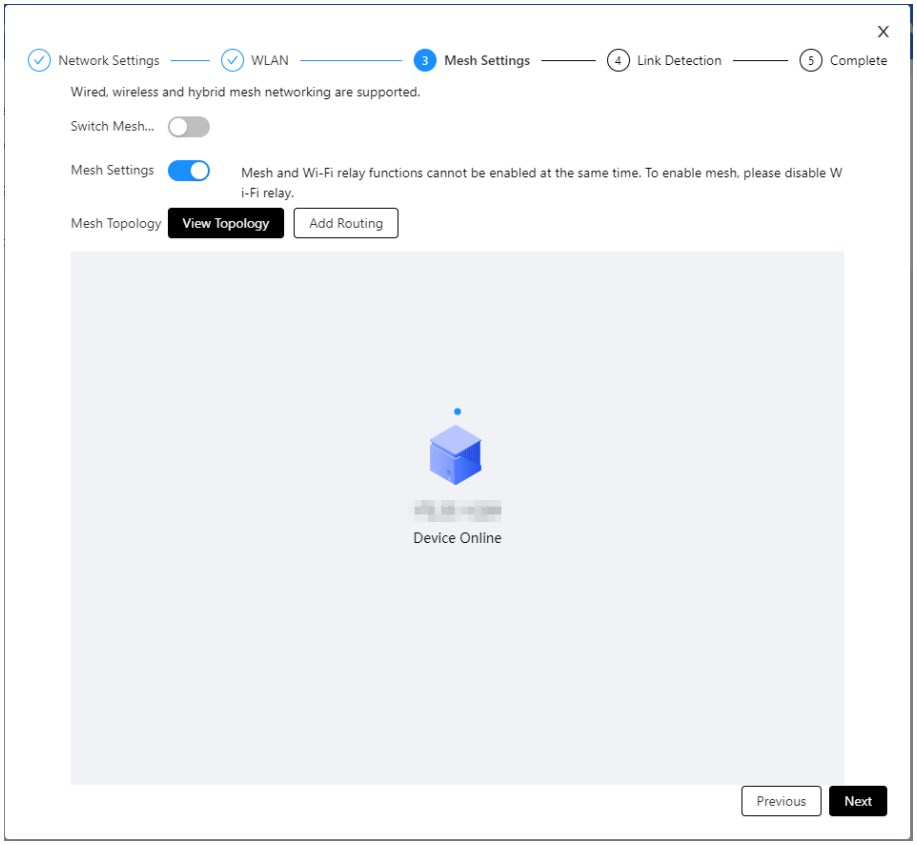


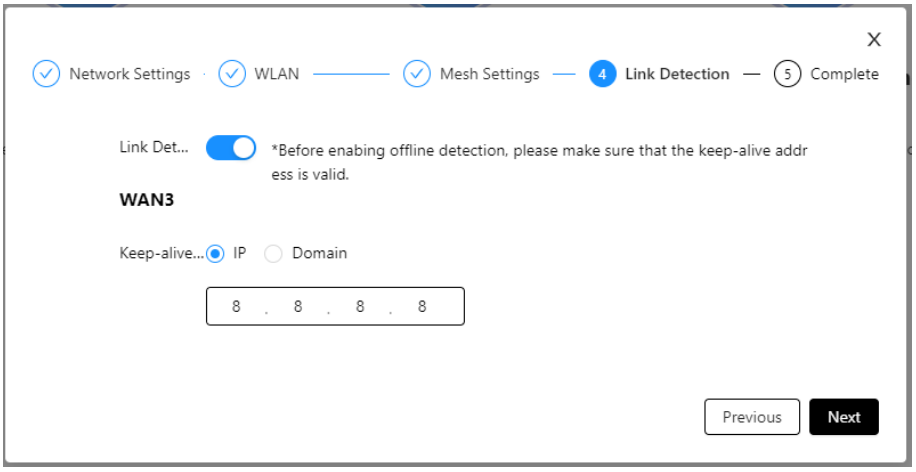
Table 2-2 Descriptions of mesh settings

Parameter	Description
Switch Mesh	Click to enable **Mesh Switch**, and then you can switch meshing when the main router is disconnected to the network and the sub router is properly connected.
Mesh Settings	**Dual-band 2.4/5G** is enabled by default.
Mesh Topology	• Wired, wireless and combined Mesh networking are supported. • For details on Mesh networking, see “3 Mesh Networking”. • Mesh and Wi-Fi repeater cannot be enabled at the same time. To enable Mesh networking, you need to disable Wi-Fi repeater.

Step 5 Enable **Link Detection** , and then click **Next**.

- After enabling the link detection function, the network status of the WAN port will be automatically detected to ensure the network connection remains stable.
- When you enable the link detection function, make sure that the address can be accessed.

Figure 2-9 Limk detection



Step 6 Click **OK**.

3 Mesh Networking

Procedure

Step 1 Turn on the routers.

Make sure that the distance between every 2 routers is less than 3 meters.

Step 2 Press the pairing button on the main router. If the indicator flashes, it indicates that the main router activates pairing mode.

Step 3 Press the pairing button on the sub router within 2 minutes for it to connect.

- If the indicator of the sub router flashes red and green alternatively, it indicates that the router has activated pairing mode. The pairing fails if it times out.
- If the indicator of the sub router displays green for 5 seconds and then goes off, it indicates that the router was successfully connected to network.

- When multiple routers are ready to be networked, you need to repeat Step 2 to Step 3 until mesh networking of all the routers is complete.
- A mesh domain can include up to 4 routers.
- Before mesh networking, you need to initialize the main router on the webpage. Sub routers cannot be initialized, otherwise, mesh networking will fail.
- Once mesh networking succeeds, you can differentiate between the main and sub router by their indicators. If the indicator is solid on, it is the main router. If the indicator is off, it is the sub router.

Appendix 1 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations from Dahua on how to create a more secured security system.

Mandatory actions to be taken for basic device network security:

1. **Use Strong Passwords**

   Please refer to the following suggestions to set passwords:

   - The length should not be less than 8 characters.
   - Include at least two types of characters; character types include upper and lower case letters, numbers and symbols.
   - Do not contain the account name or the account name in reverse order.
   - Do not use continuous characters, such as 123, abc, etc.
   - Do not use overlapped characters, such as 111, aaa, etc.

2. **Update Firmware and Client Software in Time**

   - According to the standard procedure in Tech-industry, we recommend to keep your device (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the device is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
   - We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your device network security:

1. **Physical Protection**

   We suggest that you perform physical protection to device, especially storage devices. For example, place the device in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable device (such as USB flash disk, serial port), etc.

2. **Change Passwords Regularly**

   We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. **Set and Update Passwords Reset Information Timely**

   The device supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. **Enable Account Lock**

   The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

5. **Change Default HTTP and Other Service Ports**

   We suggest you to change default HTTP and other service ports into any set of numbers between 1024–65535, reducing the risk of outsiders being able to guess which ports you are using.

6. **Enable HTTPS**

   We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. **MAC Address Binding**

   We recommend you to bind the IP and MAC address of the gateway to the device, thus reducing the risk of ARP spoofing.

8. **Assign Accounts and Privileges Reasonably**

   According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

9. **Disable Unnecessary Services and Choose Secure Modes**

   If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

   If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:

   - SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
   - SMTP: Choose TLS to access mailbox server.
   - FTP: Choose SFTP, and set up strong passwords.
   - AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

10. **Audio and Video Encrypted Transmission**

    If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

    Reminder: encrypted transmission will cause some loss in transmission efficiency.

11. **Secure Auditing**

    - Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
    - Check device log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

12. **Network Log**

    Due to the limited storage capacity of the device, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

13. **Construct a Safe Network Environment**

    In order to better ensure the safety of device and reduce potential cyber risks, we recommend:

    - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
    - The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
    - Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
    - Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.

More information

Please visit Dahua official website security emergency response center for security announcements and the latest security recommendations.

ENABLING A SAFER SOCIETY AND SMARTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.
Address: No. 1399, Binxing Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053
Email: dhoverseas@dhvisiontech.com | Tel: +86-571-87688888 28933188