

## Huawei MiniFTTO Solution

# User Guide

**Issue**                    04  
**Date**                     2023-12-07



**Copyright © Huawei Technologies Co., Ltd. 2023. All rights reserved.**

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

## **Trademarks and Permissions**



HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

## **Notice**

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

## **Huawei Technologies Co., Ltd.**

Address: Huawei Industrial Base  
Bantian, Longgang  
Shenzhen 518129  
People's Republic of China

Website: <https://ekit.huawei.com>

---

# Contents

---

<b>1 About This Document.....</b>	<b>1</b>
<b>2 Before You Start.....</b>	<b>3</b>
<b>3 Solution Overview.....</b>	<b>5</b>
3.1 Requirements and Challenges.....	5
3.2 Solution Introduction.....	7
<b>4 Network Components.....</b>	<b>10</b>
4.1 Optical Gateway, ONU, and optical AP.....	10
4.2 ODN.....	12
4.3 HUAWEI eKit App.....	13
<b>5 Typical Networking.....</b>	<b>14</b>
5.1 Typical Networking: F1001-AC+8*Optical APs+16*ONU.....	14
5.2 Typical Networking: F1001-AC+24*Optical APs.....	15
<b>6 Network Design Guide.....</b>	<b>17</b>
6.1 Device Naming Rules.....	17
6.2 IP Address Planning.....	17
6.3 Bandwidth Planning.....	18
6.4 Wi-Fi Planning.....	18
6.4.1 Wi-Fi Planning and Design Principles.....	18
6.4.2 Wi-Fi Coverage Design Principles.....	20
6.4.3 Principles for Deploying Optical APs.....	22
6.4.4 Channel Design Principles.....	23
<b>7 Installation and Deployment Guide.....</b>	<b>25</b>
7.1 Precautions for Installation and Deployment.....	25
7.2 Construction tools and instruments.....	30
7.3 Construction Process.....	32
7.4 Device Installation Guide.....	32
7.5 Laying out Cables.....	33
7.5.1 Video Guide for Laying out Cables.....	34
7.5.2 Laying the advanced fiber with power (AFWP).....	35
7.5.2.1 Deploying cables on cable trays.....	35
7.5.2.2 Deployment in the Ceiling Scenario.....	36

7.5.3 Laying the flexible optical cable.....	38
7.6 Construction Acceptance.....	40
7.6.1 Acceptance of electrical performance of advanced fiber with power.....	41
7.6.2 Acceptance of optical power of advanced fiber with power.....	43
7.6.3 Acceptance Label.....	45
7.6.4 Other Acceptance Contents.....	47
<b>8 Configuration Guide.....</b>	<b>48</b>
8.1 Before You Start.....	48
8.2 Deployment by Scanning Codes (Using the HUAWEI eKit App).....	49
8.3 Quick Deployment Configuration Scenario (WebUI).....	51
8.4 Customized Scenarios Configured on Demand (WebUI).....	56
8.4.1 Usage Scenarios and Data Planning.....	56
8.4.2 Configuring the Local Login Web UI.....	58
8.4.3 Configuring the Internet Service.....	60
8.4.4 Configuring the Wi-Fi Service.....	63
8.4.5 Configuring the Video Backhaul Service.....	69
8.4.6 Configuring the IPTV Service.....	71
8.4.7 Configuring Multi-LAN/WAN Upstream Transmission.....	76
8.4.8 Configuring Portal Authentication.....	84
8.5 Service Acceptance.....	87
8.5.1 Service Acceptance Guide.....	87
8.5.2 Internet Service Acceptance.....	88
8.5.3 Camera Service Acceptance.....	88
8.5.4 Wi-Fi Speed Acceptance.....	88
8.5.5 Wi-Fi Coverage Acceptance.....	90
8.5.6 Wi-Fi Roaming Acceptance.....	91
<b>9 Troubleshooting Guide.....</b>	<b>92</b>
9.1 Troubleshooting Precautions.....	92
9.2 Frequently Used Methods for Troubleshooting.....	93
9.3 Optical Power Exception Handling.....	95
9.3.1 Analyze Optical Power.....	95
9.3.1.1 Use an Optical Power Meter to Measure the Optical Power.....	97
9.3.1.2 Querying the Optical Power Through the WebUI.....	98
9.3.2 Cleaning the Connector of an Optical Fiber.....	99
9.3.3 Checking Whether the Optical Fiber Is Damaged Using the Red Pointer.....	103
9.4 Troubleshooting Common Service Faults.....	104
9.4.1 Internet Access Failure.....	104
9.4.2 Slow Internet Access.....	104
9.4.3 Wi-Fi Service Troubleshooting.....	106
9.4.4 ONUs Fail to Go Online Due to Incorrect Fiber Connector Type.....	109
9.4.5 Artifacts Occur on the Camera Due to Insufficient Bandwidth.....	110

<b>10 FAQs</b>	<b>112</b>
10.1 Where can I download the HUAWEI eKit app?	113
10.2 Why does the deployment fail by scanning codes using the eKit app?	113
10.3 Do I need to pay for using the HUAWEI eKit app to manage products and projects?	114
10.4 What is the default user name and password of the F1001-AC?	115
10.5 How many ONU can be connected to the F1001-AC?	115
10.6 Does the MiniFTTO solution support Wi-Fi roaming?	116
10.7 Can the F1001-AC be connected to the optical splitter?	116
10.8 Can the optical gateway F1001-AC connect to APs of other brands?	117
10.9 How do I log in to the web interface of the connected ONU through the primary gateway?	117
10.10 How do I restart the ONU?	117
10.11 How to Identify the Connector Type of Huawei Equipment?	118
10.12 Does the MiniFTTO networking require AP authorization?	119
10.13 Can the MiniFTTO be connected to other ONUs?	119
10.14 Can PoF cable be purchased from other companies?	119
10.15 What is the ambient operating temperature of the F1001-AC?	120
10.16 The password attached to the F1001-AC cannot be used to log in to the F1001-AC.	120
10.17 Can P series ONUs be connected to the F1001-AC optical gateway?	120
10.18 How many users can the F1001-AC support?	120
10.19 Does the MiniFTTO need to install the local NMS?	120
10.20 How many users can the F1001-AC support?	120
10.21 Is the F1001-AC input connected through optical fiber?	121
10.22 Why cannot I log in to the F1001-AC using the default password on the nameplate?	121
10.23 Does the PoF cable power supply in the MiniFTTO solution adopt the PoE power supply mode?..	121

# 1 About This Document

## Purpose

This document describes the application scenarios, planning and design, implementation, service commissioning and configuration, and troubleshooting of the Huawei MiniFTTO solution.





## Intended Audience


The intended audience of this product description are as follows:

- Network planning engineer
- Installation and deployment engineer
- Data configuration engineer
- Fault maintenance engineer

## Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
 <b>DANGER</b>	Indicates a hazard with a high level of risk which, if not avoided, will result in death or serious injury.
 <b>WARNING</b>	Indicates a hazard with a medium level of risk which, if not avoided, could result in death or serious injury.
 <b>CAUTION</b>	Indicates a hazard with a low level of risk which, if not avoided, could result in minor or moderate injury.
 <b>NOTICE</b>	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.

Symbol	Description
 NOTE	Supplements the important information in the main text. NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration.

## Change History

Issue	Date	Description
04	2023-12-07	Add: <a href="#">Deployment by Scanning Codes (Using the HUAWEI eKit App)</a>
03	2023-08-18	Add: <ul style="list-style-type: none"><li>• <a href="#">FAQ</a></li></ul>
02	2023-06-20	Add: <ul style="list-style-type: none"><li>• <a href="#">Typical Networking</a></li><li>• <a href="#">FAQ</a></li></ul>
01	2023-03-20	This is officially released for the first time.

# 2 Before You Start

---

This section describes the instructions for using this document. Read this section carefully before using this document to avoid possible misunderstandings.

## Version Support for Components

- This document describes all the device models supported in a version. To obtain accurate subscription information, visit the Huawei website or contact Huawei local sales offices. You also need to pay attention to the product change notices (PCNs) and lifecycle management bulletins on the website.
  - Huawei enterprise website: <https://e.huawei.com>
- Huawei may update this document anytime. Obtain the latest document in a timely manner to view the latest version support information.

## Supported Board Versions

- For the version mapping of boards, see the specific board description page.
- Matching version: Indicates that the R version and its patch versions support the board.
- Compatible version: Indicates that the R version and its patch versions can support the board through reverse loading.
- To check whether a board is available, visit the Huawei website or contact the local Huawei sales offices. You also need to pay attention to the PCNs and lifecycle management bulletins on the website.

## Optical and Electrical Modules

You are advised to use the optical and electrical modules matching the device. The optical modules of other Huawei devices or third-party vendors are not tested to match the device. As a result, such optical modules may not work properly.

## Device Dimensions

All device dimensions described in this document are designed dimensions and do not include dimension tolerances. In the process of component manufacturing, the actual size may deviate due to factors such as processing or measurement errors.



## Device Figures

The figures in this document are for reference only. The actual appearances of devices, components, and modules prevail.

## Configuration Examples

The networking diagrams, data planning, and operation procedures in this document are typical configuration examples designed for customers to understand and use the products. They cannot be used as templates. Before configuring services, plan data and configure services based on actual service requirements.

## IP Address and MAC Address Usage

IP addresses and MAC addresses are used in the product documentation to describe features and configuration examples. Unless otherwise specified, IP addresses and MAC addresses are examples only, and do not refer to any actual device.

## User Interfaces

This document serves only as a usage guide. The user interface (UI) content (such as CLI command format, command output, web UI, and NMS UI) is compiled based on lab devices. This document provides general guidance, but may not cover all application scenarios of all product models and versions. Due to reasons such as version upgrade, device model difference, and configuration file difference, the content provided in this document may be different with the actual UIs. This document does not elaborate on the differences in the preceding situations. The actual UIs prevail.

# 3 Solution Overview

## 3.1 Requirements and Challenges

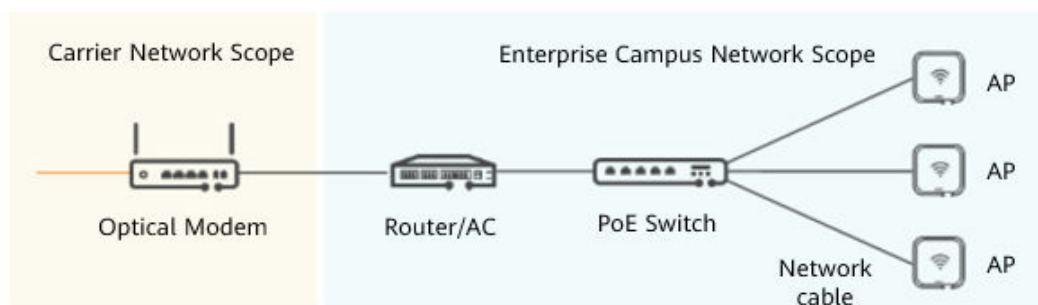
### 3.2 Solution Introduction

## 3.1 Requirements and Challenges

### Network Challenges for Small and Micro Enterprises

Currently, the mainstream intranet solution for small and micro enterprises is the traditional enterprise networking mode. Carriers provide a broadband or private line entry for enterprises. Enterprises purchase network devices such as gateways, ACs, PoE switches, and APs for internal networking.

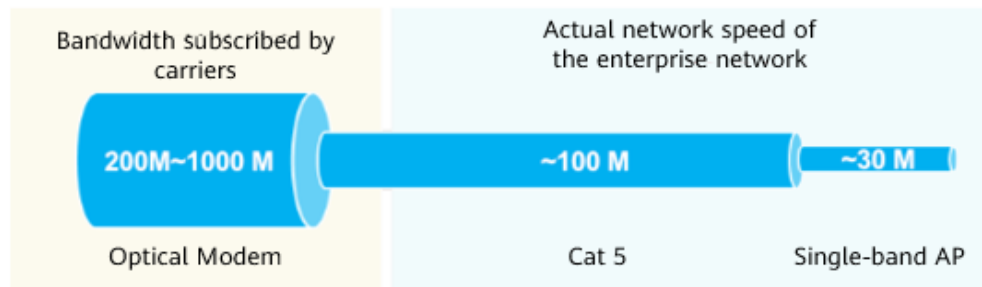
Traditional Networking Mode of Small and Micro Enterprises



Currently, the traditional networking mode has seriously hindered the development of small and micro enterprises' networks. The specific problems are as follows:

- Network bottlenecks cause low rates. Many small and micro enterprise networks form multiple bottlenecks in the network due to Cat5 network cables and Wi-Fi5 AP single frequency. As a result, the low rates cannot reach

the required bandwidth.



- The traditional network architecture is complex and difficult to maintain. The traditional P2P network architecture has three to four layers of active devices stacked. The connections between devices are complex, occupying a large amount of equipment room and cable trough space, and a large amount of repeated cabling workload.
- Smooth evolution is difficult. As an infrastructure, network cables have a service life of about 10 years. During network upgrade, high-specification network cables need to be replaced and integrated cabling is performed, which is costly.
- The transmission distance is limited. The maximum transmission distance of the network cable is 100 m.

## Network Requirements of Small and Micro Enterprises

The following table lists common application scenarios and network requirements of small and micro enterprises.

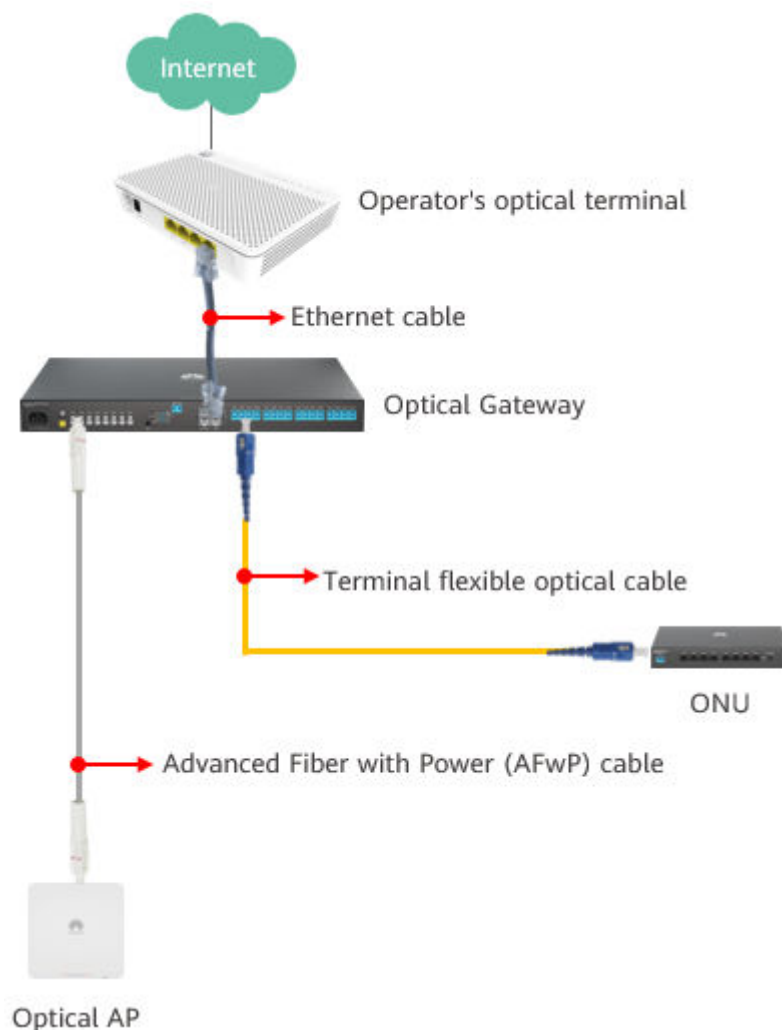
Application Scenario	Network Requirements
Office service	<ul style="list-style-type: none"> <li>• Wide coverage: Wi-Fi signals in office areas are fully covered, and mobile office services are not disconnected.</li> <li>• Large concurrency: A large number of terminals (such as PCs, tablets, mobile phones, and smart screens) are online at the same time in the office area and conference room, requiring stable network operation.</li> <li>• Large bandwidth: Multiple services, such as Internet access, cloud access, and video conferencing, are deployed. The actual rate can reach the committed rate.</li> <li>• High security: Requirements for multi-service isolation, user access security, firewall, and attack defense are reduced, and requirements for professional skills or security services are provided.</li> </ul>
Cloud services such as video creation, cloud rendering, and cloud design	Services such as video and rendering involve uploading and downloading of material files. Generally, stable uplink bandwidth and differentiated real-time stable services are required.

Application Scenario	Network Requirements
Catering, entertainment, and live broadcast industries	A large number of access users and terminals require high-quality and large-concurrency Wi-Fi 6 access.
Video backhaul	<ul style="list-style-type: none"><li>• Large bandwidth: The uplink bandwidth is greater than the downlink bandwidth, and multiple 4K/8K video streams are transmitted back.</li><li>• High security: Isolate from wireless and wired office networks.</li></ul>

## 3.2 Solution Introduction

### Network architecture

The huawei MiniFTTO solution features simple networking, deployment, and O&M. It is an ideal solution for small and micro campus networks, such as soho.



Component Name	Network layout
Optical Gateway	<p>The network is located at the network egress and connects to the carrier egress network to provide gigabit access for enterprises.</p> <p>The optical gateway has a built-in Advanced Fiber with Power (AFwP) power adapter and connection interface to provide optical connection and power supply for remote optical APs. In addition, passive optical ports are supported to provide passive optical connections for the ONU.</p>

Component Name	Network layout
Optical AP	<p>The optical AP provides Wi-Fi 6 wireless access and gigabit wired access for enterprise users, meeting the gigabit broadband access requirements of various terminals.</p> <p>The optical AP support multiple types to meet the requirements of small and micro enterprises in various application scenarios, such as:</p> <ul style="list-style-type: none"><li>• The ceiling-mounted optical AP is installed on the ceiling and Wi-Fi coverage is provided from the top to the bottom.</li><li>• The desktop optical AP support horizontal deployment of desktops and optical fibers to desks.</li></ul>
ONU	<p>The ONU provides PoE and non-PoE gigabit wired access for enterprise users, meets the remote power supply and gigabit access requirements of various PoE terminals, and supports wired office and camera backhaul.</p>
HUAWEI eKit App	<p>HUAWEI eKit App is a digital distribution platform that integrates marketing, transaction, service, enablement, and partner operations for numerous distribution partners and enterprise-level users in the enterprise market.</p>

# 4 Network Components


This section describes the products used in Huawei MiniFTTO solution.





[4.1 Optical Gateway, ONU, and optical AP](#)

[4.2 ODN](#)



[4.3 HUAWEI eKit App](#)

## 4.1 Optical Gateway, ONU, and optical AP


Product Type	Specifications
Optical Gateway	<p>F1001-AC</p>  <p>Network Interface: 4 x GE (WAN/LAN multiplexing) / 1 x XG-PON</p> <p>User Interface: 4 x GE (WAN/LAN multiplexing) +8*GPON (XC/UPC, PoF) +16*GPON (SC/UPC)</p> <p>Performance: 128K NAT session forwarding capability, maximum of 300 devices connected</p> <p>For more information, please click on <a href="#">F1001-AC Datasheet</a></p>


Product Type	Specifications
Box-shaped ONU	<p>F100D-4G</p>  <p>Network Interface: GPON</p> <p>User Interface: 4 x GE</p> <p>For more information, please click on <a href="#">F100D-4G Datasheet</a></p>
Box-shaped ONU	<p>F200D-8G</p>  <p>Network Interface: GPON</p> <p>User Interface: 8 x GE</p> <p>For more information, please click on <a href="#">F200D-8G Datasheet</a></p>
	<p>F200D-8P</p>  <p>Network Interface: GPON</p> <p>User Interface: 8 x GE, PoE/PoE+</p> <p>For more information, please click on <a href="#">F200D-8P Datasheet</a></p>
Panel type ONU	<p>F100P-2G</p>  <p>Network Interface: GPON</p> <p>User Interface: 2 x GE</p> <p>For more information, please click on <a href="#">F100P-2G Datasheet</a></p>



Product Type	Specifications
Ceiling-mounted Optical AP	<p>F600C-30-1GH</p>  <p>Network Interface: GPON</p> <p>User Interface: 1 x GE + 2.4 GHz&amp;5 GHz Wi-Fi 6</p> <p>For more information, please click on <a href="#">F600C-30-1GH Datasheet</a></p>
Desktop Optical AP	<p>F600D-30-4G1V</p>  <p>Network Interface: GPON</p> <p>User Interface: 4*GE+1*POTS+ 1*USB+2.4GHz&amp;5GHz Wi-Fi6</p> <p>For more information, please click on <a href="#">F600D-30-4G1V Datasheet</a></p>

## 4.2 ODN

Product Type	Specifications
<p>Advanced Fiber with Power(AFWP)</p> 	<p>Color: White</p> <p>Minimum bending radius: static 24 mm, dynamic 48 mm</p> <p>Length: 20/30/50/60/80 m</p> <p>Connector type: XC/UPC</p>

Product Type	Specifications
<p data-bbox="391 297 606 331">Connecting tube</p> 	<p data-bbox="754 297 1257 331">Dimensions: 55 mm x 14 mm x 14 mm</p> <p data-bbox="754 342 1066 376">Connector type: XC/UPC</p> <p data-bbox="754 387 1085 421">Insertion loss (dB): ≤ 0.25</p> <p data-bbox="754 432 1043 465">Protection rating: IP54</p> <p data-bbox="754 477 1417 577">Application scenario: The length is insufficient for connection. Two optical-electrical composite cables are plug-and-play for connection</p>

### 4.3 HUAWEI eKit App

HUAWEI eKit App is a digital distribution platform that integrates marketing, transaction, service, enablement, and partner operations for numerous distribution partners and enterprise-level users in the enterprise market.

Download HUAWEI eKit App

- For Huawei phones, search for **Huawei eKit** in Huawei AppGallery and download it.
- For non-Huawei Android phones, visit <https://app.huawei.com/eplus/soho/front/index.html#/download> in the address box of the browser to download the app.
- Scan the QR code to download.



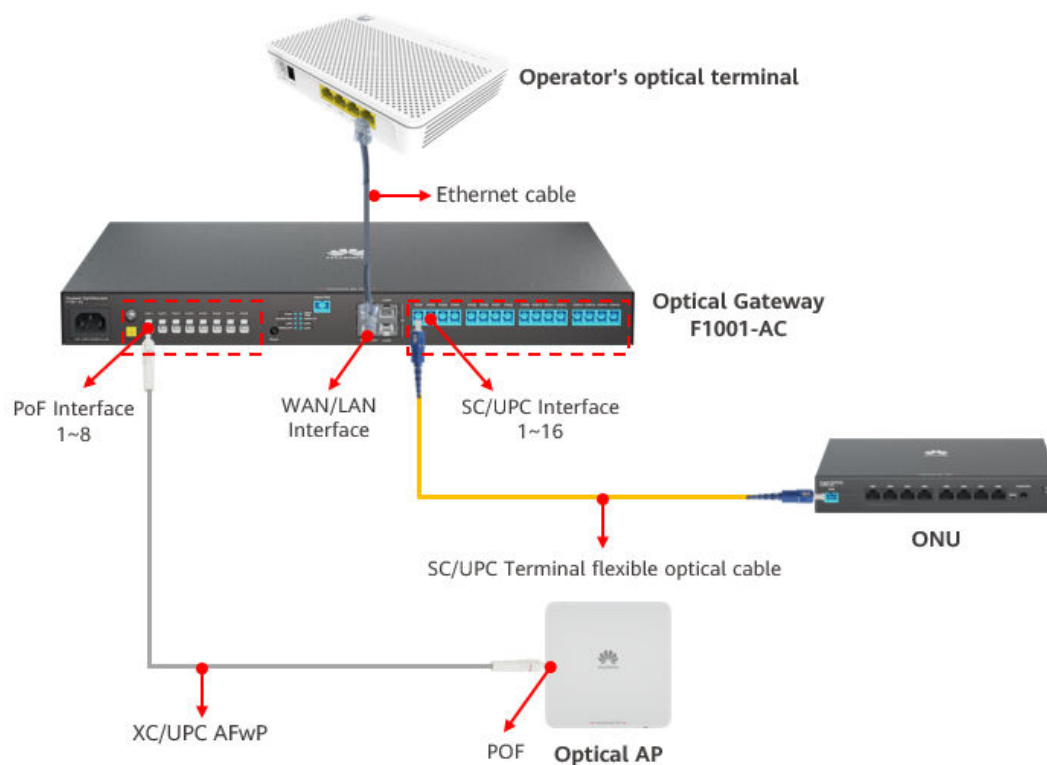
# 5 Typical Networking

The MiniFTTO solution focuses on small and micro campus scenarios with less than 100 information points, optical gateways, optical APs, and optical terminals can be flexibly networked to meet actual requirements.

[5.1 Typical Networking: F1001-AC+8\\*Optical APs+16\\*ONU](#)

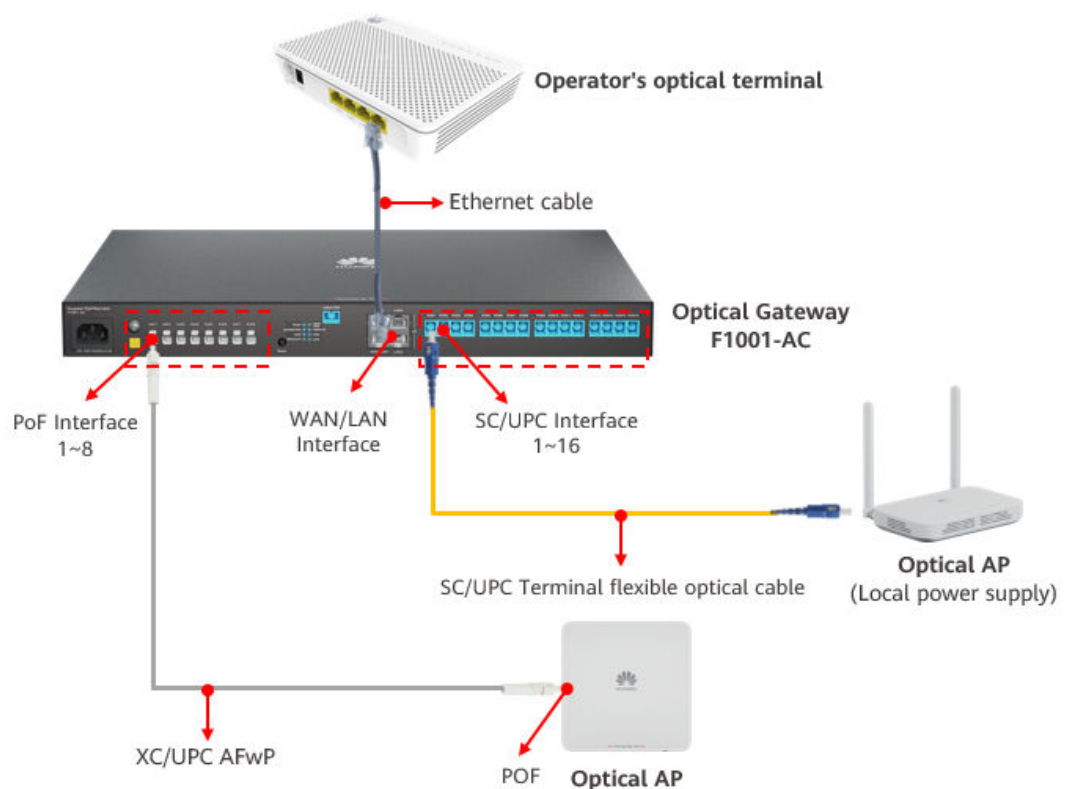
[5.2 Typical Networking: F1001-AC+24\\*Optical APs](#)

## 5.1 Typical Networking: F1001-AC+8\*Optical APs +16\*ONU



Component Type	Quantity	Description
Optical Gateway F1001-AC	1	AC power supply
SC/UPC Terminal flexible optical cable	1~16	The length depends on the actual situation
XC/UPC AFwP	1~8	The length depends on the actual situation
Optical AP (AFwP power supply)	1~8	AFwP cable power supply device
ONU	1~16	Select as required

## 5.2 Typical Networking: F1001-AC+24\*Optical APs



Component Type	Quantity	Description
Optical Gateway F1001-AC	1	AC power supply
SC/UPC Terminal flexible optical cable	1~16	The length depends on the actual situation
XC/UPC AFwP	1~8	The length depends on the actual situation

<b>Component Type</b>	<b>Quantity</b>	<b>Description</b>
Optical AP (AFwP power supply)	1~8	AFwP cable power supply device
Optical AP (Local power supply)	1~16	Local power supply device

# 6 Network Design Guide

---

[6.1 Device Naming Rules](#)

[6.2 IP Address Planning](#)

[6.3 Bandwidth Planning](#)

[6.4 Wi-Fi Planning](#)

## 6.1 Device Naming Rules

Device name planning aims to ensure accurate and efficient O&M fault handling.

The device components involved in the name planning include the optical gateway, optical AP, and optical terminal. For details, see the following suggestions.

Optical gateway name: <Enterprise name+Installation location+Uplink interface>.

Optical AP/optical terminal name: <In-enterprise installation location alias + auxiliary remarks > Auxiliary information can be a combination of the management IP address, MAC address, and rate limit.

## 6.2 IP Address Planning

The purpose of IP address planning is as follows:

- The subsequent network expansion is considered to make the network more flexible.
- The route aggregation capability is improved and the number of entries in the routing table is reduced.
- Network maintenance is considered to facilitate memory and management and improve network maintenance efficiency.
- The access list facilitates data configuration.
- In principle, capacity, security, maintainability, and service scalability must be considered.

- The enterprise intranet IP address planning is to evaluate the IP capacity based on the number of terminals or users that need to access the network, and to plan IP address segments for different services.
- When planning internal IP addresses, avoid the management IP addresses of optical APs to avoid IP address conflicts.
- If the number of access users exceeds 253, plan a pre-warning for the problem by expanding the address pool of the optical gateway or expanding the IP address resources of VLANs or sub-interfaces on the user side.
- When VLANs are divided for different services or departments on the enterprise intranet and subnet segments are divided, you can configure a subnet segment with a mask of at least 24 bits based on the VLAN.
- Internal networks have service mutual access requirements, such as inter-department collaboration and public resource access. Configure access policies for intra-VLAN or cross-VLAN Layer 3 communication based on the service mutual access control granularity, or configure access policies based on refined IP network segments or routes.
- The WAN-side IP address of the optical gateway generally provides the management WAN address and data channel WAN address (DHCP address and static IP address).

## 6.3 Bandwidth Planning

Bandwidth planning is designed from the following aspects:

- Bandwidth between the optical AP/optical terminal and STA.
- Bandwidth between the optical gateway and the optical AP/optical terminal.

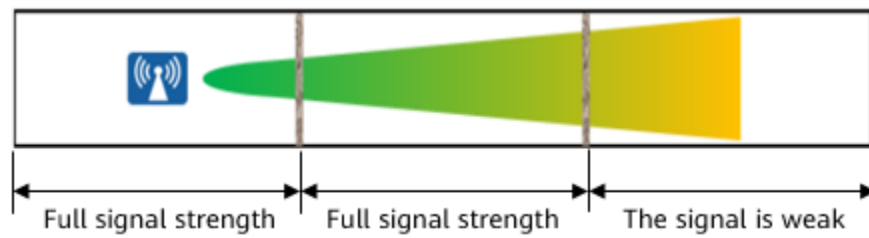
The overall bandwidth convergence ratio needs to be considered.

- The bandwidth between the optical AP and STA is 5 Mbit/s for each terminal user to guarantee basic service experience (such as Internet access, email, and video conferencing). A single optical AP can access 64 users on the basis of guaranteed user bandwidth. The actual bandwidth convergence ratio of a single optical AP is designed based on the bandwidth convergence ratio of the full link.
- Physical bandwidth between the optical gateway and optical APs/optical terminals = (optical terminal access bandwidth/Total number of optical terminals) x Bandwidth convergence ratio. To ensure enterprise intranet service experience, the bandwidth convergence ratio is generally 1:1 in general scenarios and 1:1 in high-density access scenarios.

## 6.4 Wi-Fi Planning

### 6.4.1 Wi-Fi Planning and Design Principles

- In the wall-through scenario, only one wall (such as brick wall or concrete) has the best signal.

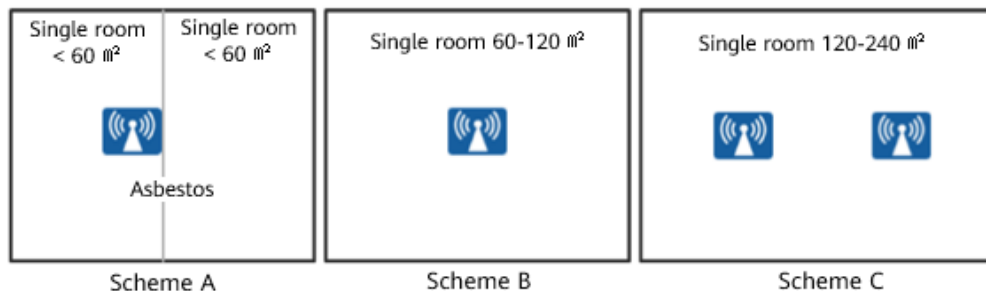


Typical barrier penetration loss is shown in the following table.

obstacle	Thickness (mm)	2.4 GHz Signal Attenuation (dB)	5 GHz Signal Attenuation (dB)
Ordinary brick wall	120	10	20
Thickened brick wall	240	15	25
Concrete	240	25	30
Asbestos	8	3	4
Foam board	8	3	4
Hollow wood	20	2	3
Ordinary wooden door	40	3	4
Solid wood door	40	10	15
Ordinary glass	8	4	7
Thickened glass	12	8	10
Bulletproof glass	30	25	35
Bearing column	500	25	30
Rolling shutter door	10	15	20
Steel plate	80	30	35
Elevators	80	30	35

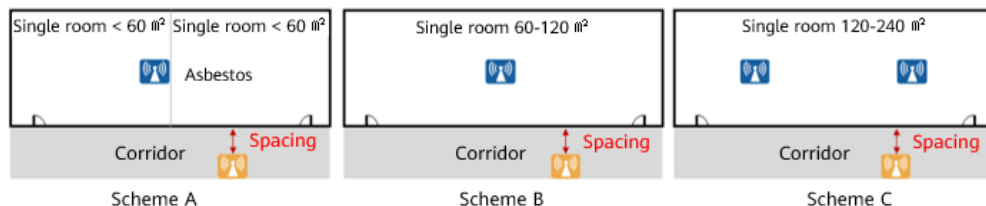
- The coverage of a single device is about 100 square meters (large open room, no heavy partition).



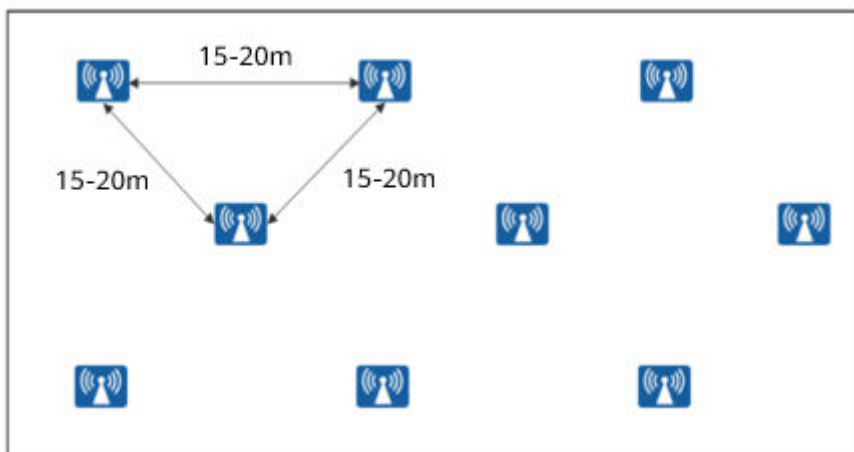


- If the area of a single room is less than 60 square meters and the walls between the rooms are asbestos, deploy one optical AP in each two rooms by referring to solution A.
- If the area of a single room ranges from 60  $\text{m}^2$  to 120  $\text{m}^2$ , deploy one optical AP in each room by referring to solution B.
- If the area of a single room exceeds 120  $\text{m}^2$  to 240  $\text{m}^2$ , deploy two optical APs in each room according to solution C.

Light APs in the room are evenly installed far from the doorway. For details, see the blue light APs in the preceding figure. The optical APs outside the room must be placed at a certain distance from the conference room. If the external wall of the room is a solid wall (brick wall or concrete wall), the distance between the optical AP and the wall must be greater than 3 m. If the external wall of the room is a non-solid wall (asbestos or glass), the distance between the optical AP and the wall must be greater than 6 m.



- In the open area, the equilateral triangle is deployed with the minimum interference (the distance between optical APs is 15 m to 20 m).

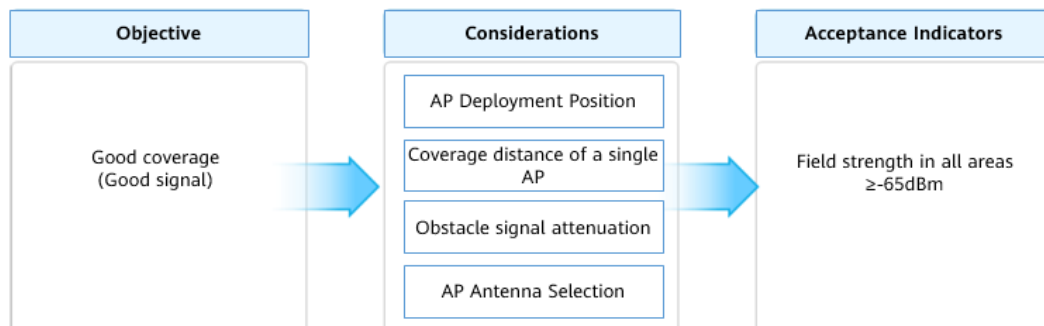


## 6.4.2 Wi-Fi Coverage Design Principles

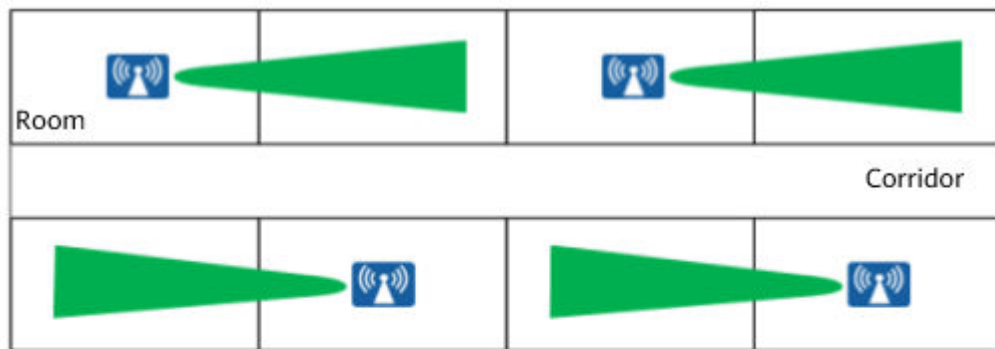
The coverage is simply the number of Wi-Fi signal bars on the mobile phone.

To ensure good signal coverage, consider the following items:

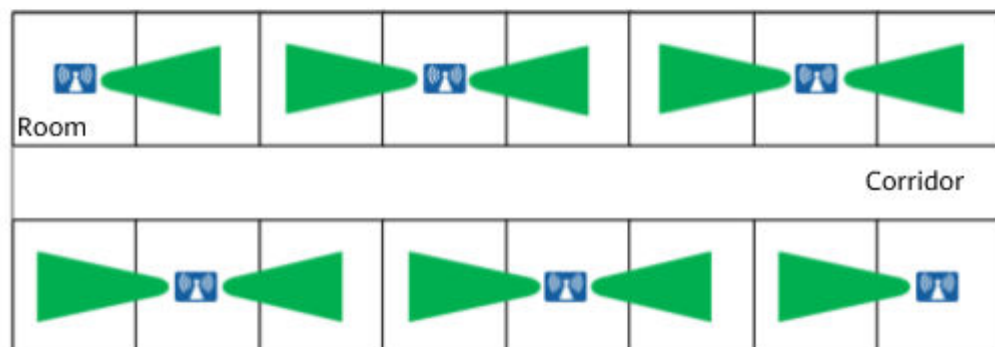
The field strength is greater than or equal to -65 dBm and the signal coverage is good. This is an empirical value obtained in engineering practice. However, different projects may have special requirements. Generally, the signal strength is less than or equal to -75 dBm and less than -65 dBm. The signal coverage quality is medium.



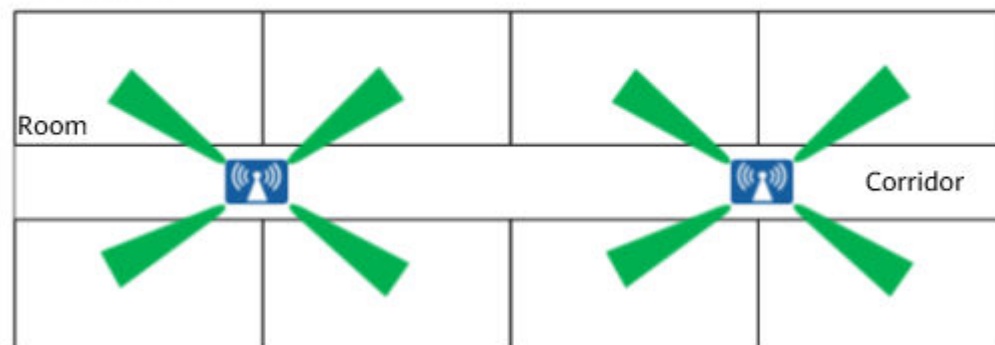
The Classic 3 model is the most stable quality.



**Preferred: APs cover two rooms, high cost, and excellent effect**



**Second choice: APs cover three rooms. The cost is medium and the effect is excellent**



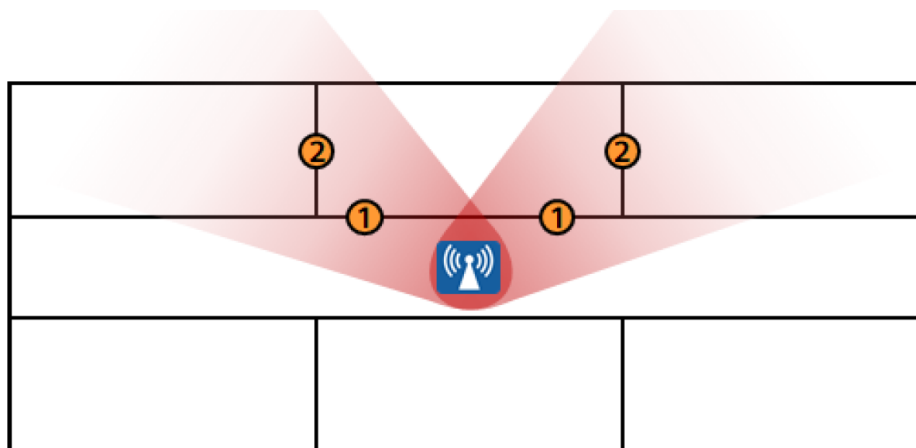
**Alternative: APs cover four rooms, with low costs and excellent effects**

### 6.4.3 Principles for Deploying Optical APs

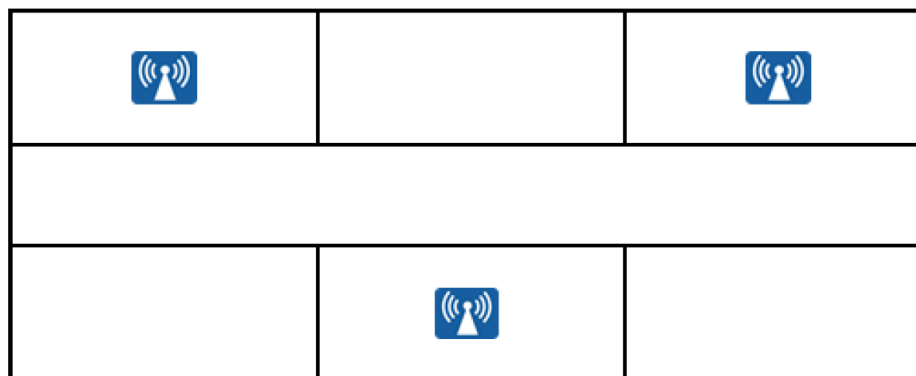
#### General Principles for Deploying Optical APs

- Optical APs are deployed indoors in key areas to ensure user experience.
- Minimize the number of obstacles that signals pass through.
- Optical APs are deployed at intersections or corners to ensure signal coverage continuity and roaming experience.
- Optical APs can be installed on the ceiling (with the top height of no more than 5 m) or on the wall (with the height of about 3 m).

As shown in the following figure, the optical AP is improperly deployed and signals traverse multiple walls.



As shown in the following figure, the optical AP is located properly and signals traverse the single-layer wall.

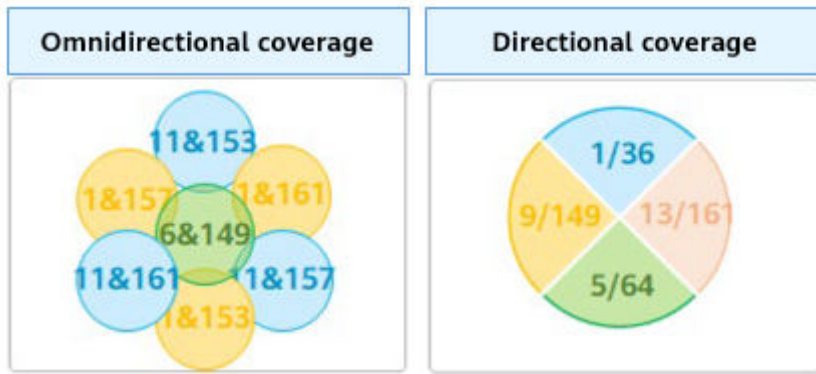


## 6.4.4 Channel Design Principles

Confirm the available local channels: For example, 40 MHz channels 36, 44, 52, 60, 149, and 157 can be used for indoor 5 GHz frequency bands. In common scenarios, 40 MHz networking is recommended by default.

The available channels vary according to countries or regions. Some channels may be reserved in some regions. Therefore, you need to confirm the channel planning before the planning.

Avoiding co-channel interference: Ensure the reuse distance of co-channels. In addition, consider the staggered channels of the surrounding and upper and lower floors. If the channels cannot be staggered, the power is usually reduced to reduce the overlap area.



# 7 Installation and Deployment Guide

---

[7.1 Precautions for Installation and Deployment](#)

[7.2 Construction tools and instruments](#)

[7.3 Construction Process](#)

[7.4 Device Installation Guide](#)

[7.5 Laying out Cables](#)

[7.6 Construction Acceptance](#)

## 7.1 Precautions for Installation and Deployment

### Precautions for Equipment Installation

The installation of the equipment shall take into consideration the subsequent maintenance and equipment operation requirements.

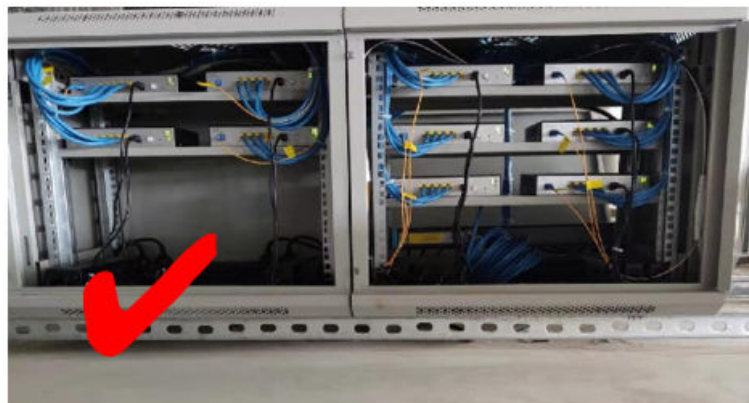
- The ONU installation and deployment have no safety risks, such as heat dissipation, waterproof, dustproof, and electromagnetic protection. The ONU installation complies with the safety and protection specifications. The ONU is fixed to prevent damage to life and property caused by falling.

 CAUTION

[Wrong case] The installation environment has security risks (a large amount of dust blocks the heat dissipation holes), which leads to device faults.



[Correct case] The ONU installation space is reserved properly to facilitate heat dissipation. The ONU is fixed on a tray to prevent falling.



- The ONU installation space is reserved for future expansion or upgrade.
- Easy maintenance must be considered during device installation. If a device is faulty, it can be replaced quickly. Easy maintenance ensures quick and convenient subsequent maintenance.

 CAUTION

[Wrong case] The installation position is improper, which makes maintenance difficult. The ONU is installed on the ceiling keel. As a result, the ceiling buckle must be removed during each maintenance.

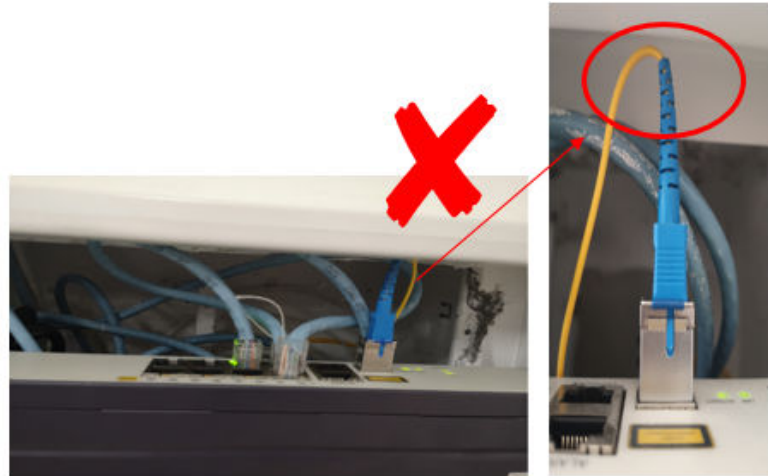


- After the ONU or ONU network box is deployed, try to match the environment to meet customer requirements.
- The ONU installation position, height, and network box style must be the same in the campus.
- In the network box installation scenario, select a proper network box based on the device size and reserve sufficient cabling space for easy operation.



**⚠ CAUTION**

[Wrong case] The size of the network box is improper. As a result, the cabling space is insufficient. The fiber is bent.



[Correct case] The network box is properly laid out, and the cabling is orderly, which is easy to deploy and maintain.



## Precautions for Routing Optical Cables

The cable construction personnel must be trained and comply with the operation regulations.

Do not perform operations on the optical cable distribution system if you are not trained.

During the installation, the construction safety regulations and safety regulations must be observed.

Optical cables must be deployed in strict compliance with related requirements to minimize the probability of fiber damage and prevent the increase of splicing loss caused by fiber core damage.

During optical cable construction, pay attention to the following points:

- Before routing optical cables, attach labels to both ends of each optical cable to facilitate management and maintenance.
- When laying out optical cables, protect them from being pulled, twisted, or damaged.

---

 **CAUTION**

[Wrong case] The bending radius of the optical cable is too small. As a result, the attenuation is too large.



- 
- Strong-current and weak-current cables are routed separately and far away from strong-current or other heat sources.
  - In the case of mice, it is recommended that you use PVC tubes to protect the cables to prevent the mice from tearing the cables.
  - Optical fibers must be routed neatly and do not affect unused space, facilitating capacity expansion and maintenance.
  - When optical cables are routed and secured, straighten the optical cables every 5 m and ensure that the bending radius of the optical cables meets the requirements.
  - Pay attention to the protection of the optical fiber connector and do not hit the connector abnormally.
  - Cover unused fiber connectors with jackets to avoid contamination.

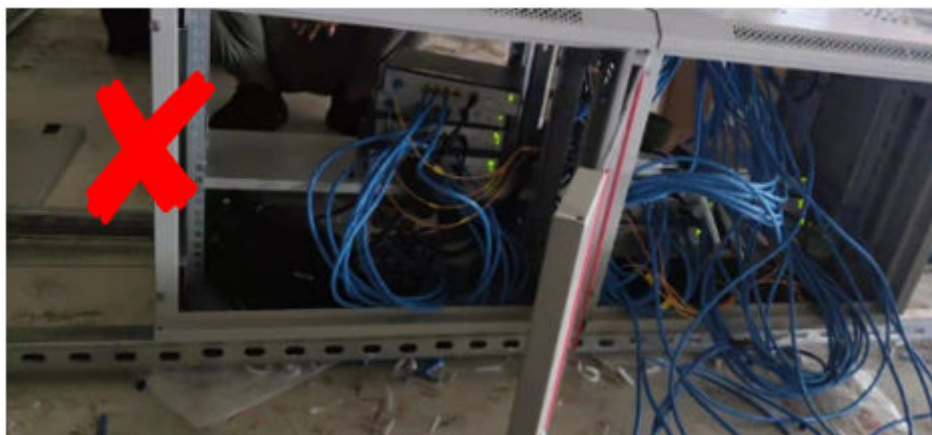
## Precautions for Routing Network Cables

- Install a protective ring or round corner on the cable hole in advance to remove burrs (not sharp if you touch the cable hole with your bare hands) and cut the cable.
- Sufficient slack must be reserved at the cable connection points to facilitate insertion and removal.
- Bind and arrange the cables with proper force. Obvious deformation on the cable surface is not allowed. Otherwise, the signal quality is affected.
- Prevent rotating components, such as doors, from squeezing or pulling cables.
- Ethernet cables and power cables do not interfere with each other.
- If a cable is not long enough, replace the cable instead of adding connectors or soldering points to the middle of the cable.
- Redundant network cables must be coiled neatly for easy search.

---

**CAUTION**

[Wrong case] Cables are laid out disorderly. As a result, the faulty cable port cannot be quickly located during maintenance.



## 7.2 Construction tools and instruments

### Construction tools

Prepare suitable construction tools to ensure normal construction. See the following table for common construction tools.

**Table 7-1** List of Common Tools

Tool Name	Description
Tape measure	Used to measure length
Marker pen	Used for marking when marking lines

Tool Name	Description
Leveling instrument	Used to verify that the equipment is installed horizontally
Percussion drill	Used for mounting holes
Vacuum cleaner	Used to absorb dust and drilling debris during drilling
Flat-head screwdriver	Used to tighten small screws and bolts. The head of the screwdriver is one word.
Phillips screwdriver	Used to tighten small screws and bolts. The head of the screwdriver is cross.
Diagonal pliers	Used for shearing, but also can be used instead of scissors to shear insulation sleeve, cable tie and so on.
Ladder	For ascending operations
Rubber hammer	Can be used to install expansion bolts
Paper cutter	Used to strip the jacket when making cables onsite.
Wire stripper	Used to strip the insulation layer and sheath of the small-section communication cable
Crystal tip wire crimping pliers	Used for crimping the connector of the telephone cable and the RJ45 connector of the network cable.
ESD gloves	Used for antistatic

## Meter

See the following table for common construction instruments.

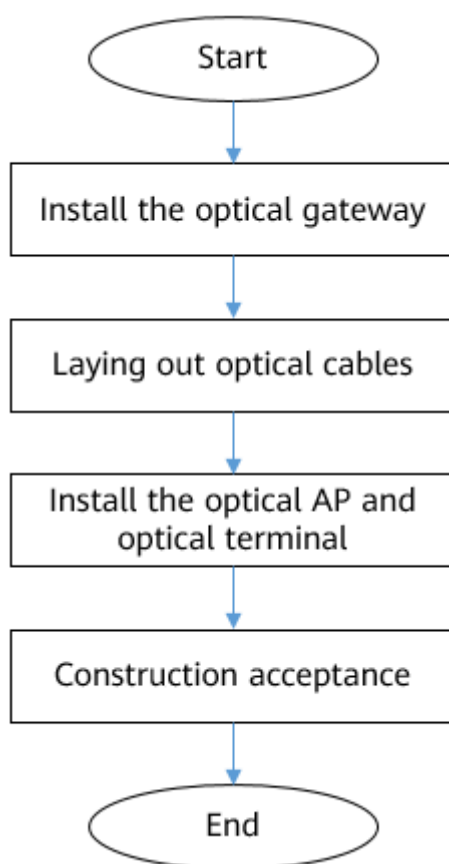
**Table 7-2** List of Common Instruments

Tool Name	Description
Network cable tester	Used to test the connection and disconnection of network cables.
Optical power meter	Used to test the optical power.
Multimeter	Used for cabinet insulation, cable connection and disconnection, and electrical performance indexes of equipment, including voltage, current, and resistance.
Red Light Pen	The red light pen is also called visual fault locator and visual fault detector. Check whether the optical fiber leaks by emitting red light to locate the damaged optical fiber.

Tool Name	Description
Optical fiber cutting knife	Used for cutting optical fibers to ensure smooth end surfaces.
Optical fiber fusion splicing machine	The two optical fibers are spliced together by hot melting.


## 7.3 Construction Process

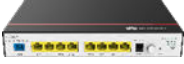




The overall construction flow chart is as follows:



## 7.4 Device Installation Guide

This section describes how to install the optical gateway, optical AP, and ONU.

Product Type	Installation Guide
F1001-AC 	<a href="https://support.huawei.com/enterprise/en/doc/EDOC1100294162">https://support.huawei.com/enterprise/en/doc/EDOC1100294162</a> (Video) <a href="https://support.huawei.com/enterprise/en/doc/EDOC1100317216">https://support.huawei.com/enterprise/en/doc/EDOC1100317216</a>




Product Type	Installation Guide
F200D-8G 	<a href="https://support.huawei.com/enterprise/en/doc/EDOC1100292228">https://support.huawei.com/enterprise/en/doc/EDOC1100292228</a>
F200D-8P 	<a href="https://support.huawei.com/enterprise/en/doc/EDOC1100292227">https://support.huawei.com/enterprise/en/doc/EDOC1100292227</a>
F100P-2G 	<a href="https://support.huawei.com/enterprise/en/doc/EDOC1100294159">https://support.huawei.com/enterprise/en/doc/EDOC1100294159</a>
F600C-30-1GH 	<a href="https://support.huawei.com/enterprise/en/doc/EDOC1100294163">https://support.huawei.com/enterprise/en/doc/EDOC1100294163</a> (Video) <a href="https://support.huawei.com/enterprise/en/doc/EDOC1100299747">https://support.huawei.com/enterprise/en/doc/EDOC1100299747</a>
F600D-30-4G1V 	<a href="https://support.huawei.com/enterprise/en/doc/EDOC1100292226">https://support.huawei.com/enterprise/en/doc/EDOC1100292226</a>

## 7.5 Laying out Cables

This section describes the methods and precautions for routing advanced fiber with power and flexible optical cable.

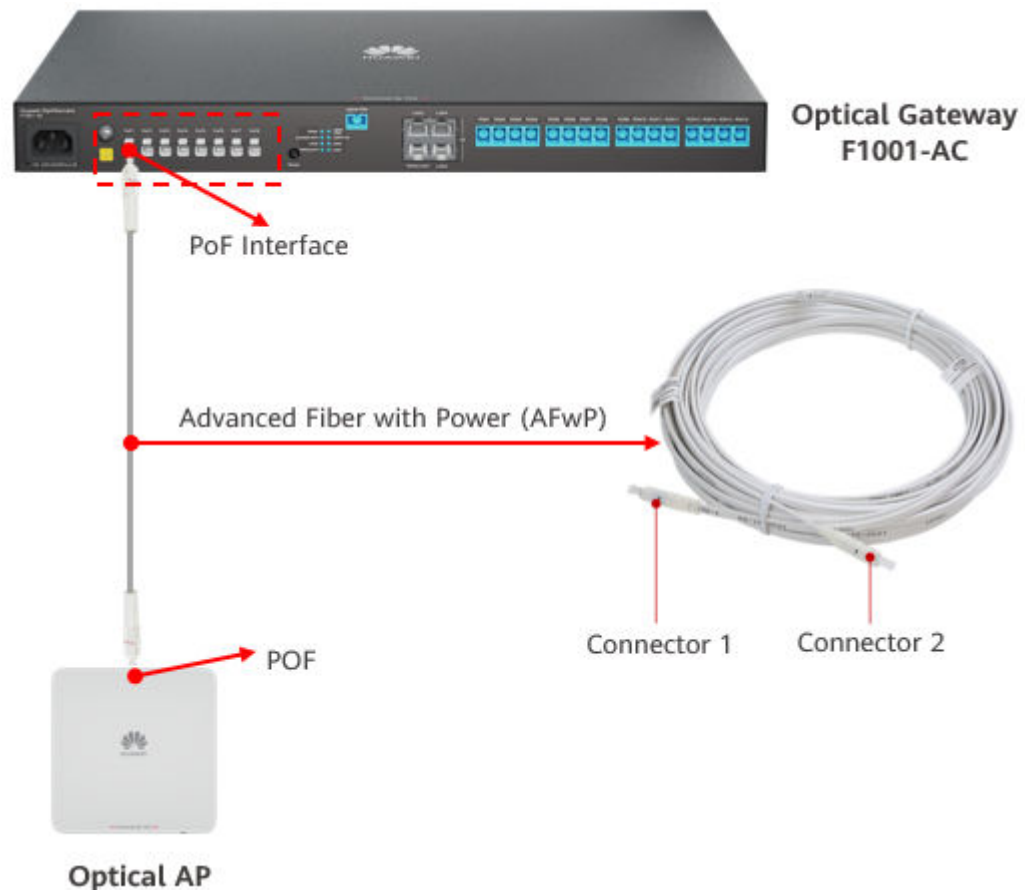
## 7.5.1 Video Guide for Laying out Cables

**Table 7-3** Video Guide for Laying out Cables

Video Guide	Link
<p>Connect two AFwP cables using photoelectric adapter</p>	<p><a href="https://support.huawei.com/enterprise/en/doc/EDOC1100257165">https://support.huawei.com/enterprise/en/doc/EDOC1100257165</a></p> 
<p>AFwP cable connection 01-Low temperature tin-welded waterproof heat-shrinking tube connection</p>	<p><a href="https://support.huawei.com/enterprise/en/doc/EDOC1100297784?section=o003">https://support.huawei.com/enterprise/en/doc/EDOC1100297784?section=o003</a></p> 
<p>Optical/electrical performance acceptance of AFwP cables</p>	<p><a href="https://support.huawei.com/enterprise/en/doc/EDOC1100297183">https://support.huawei.com/enterprise/en/doc/EDOC1100297183</a></p> 

## 7.5.2 Laying the advanced fiber with power (AFwP)

Advanced fiber with power are used to connect the PoF port of the optical gateway to an optical terminal.



### 7.5.2.1 Deploying cables on cable trays

- Step 1** Determine the optimal cabling route based on the onsite environment layout.
- Step 2** Mark the optical gateway interface and optical AP positions on both ends of the advanced fiber with power.

**NOTE**

Before routing cables, mark the labels on both ends of the advanced fiber with power for future identification, management, and maintenance.



From: PoF 1  
To: A01-AP1



**Step 3** Lay the advanced fiber with power along the weak-current cable tray.



**Step 4** When the advanced fiber with power is routed out of the cable tray, protect the cable from being exposed and damage. Use PVC hoses to protect the end of the advanced fiber with power.



**Step 5** Connect the connectors of the advanced fiber with power to the optical gateway and optical AP according to the labels on both ends of the advanced fiber with power.

**Step 6** Prepare and attach labels according to the label specifications to facilitate subsequent maintenance.

----End

### 7.5.2.2 Deployment in the Ceiling Scenario

It is recommended that the advanced fiber with power be protected by PVC rigid pipes on the top of the ceiling.

**Step 1** Determine the optimal cabling route based on the onsite environment layout.

- Step 2** Mark the optical gateway interface and optical AP positions on both ends of the advanced fiber with power.

 **NOTE**

Before routing cables, mark the labels on both ends of the advanced fiber with power for future identification, management, and maintenance.



From: PoF 2  
To: A02-AP2

- Step 3** Open two ceiling maintenance windows about 5 m apart for pipe-through and wiring construction. Straighten the optical cable every 5 m to avoid twisting or winding.

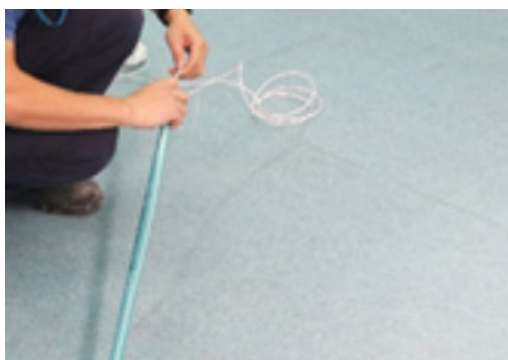
---

 **CAUTION**

Pay attention to the high-altitude construction, please wear safety helmet.

---

- Step 4** Wrap the head end of the advanced fiber with power with adhesive tape for protection. Route the optical/electrical composite cable through the PVC pipe to the optical AP. It is recommended that one PVC pipe be routed through one advanced fiber with power.



- Step 5** Coil the redundant advanced fiber with power and place them inside the ceiling. Route one end of the advanced fiber with power through a hole in the ceiling and insert it into the ceiling-mounted optical AP. Connect the other end of the advanced fiber with power to the optical gateway.



**Step 6** Prepare and attach labels according to the label specifications to facilitate subsequent maintenance.

----End

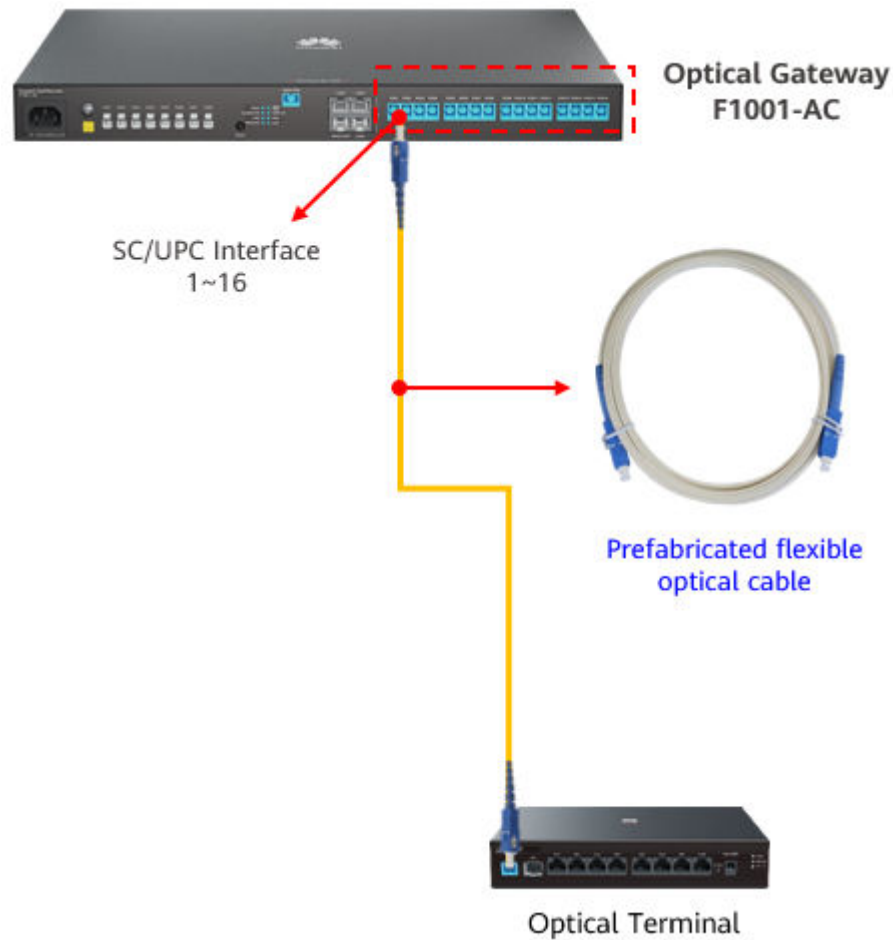
### 7.5.3 Laying the flexible optical cable

The flexible optical cable includes prefabricated flexible optical cable and non-prefabricated flexible optical cable.

- Both ends of the prefabricated flexible optical cable are prefabricated with connectors. After the cable is routed, insert the connectors into the optical port of the device.
- There are no prefabricated connectors at both ends of the non-prefabricated flexible optical cable. You need to make connectors onsite after the cable is routed. You can use hot melt splicing pigtails or make FMC cold connectors onsite.

The routing of the flexible optical cable is the same as that of the advanced fiber with power. The difference is that the flexible optical cable does not have prefabricated ports. Therefore, the head end of the flexible optical cable needs to be prepared on site after the routing is complete.

## Laying the prefabricated flexible optical cable



### Step 1 Lay out cables.

The routing of prefabricated flexible optical cable is the same as that of advanced fiber with power. For details, see the routing process of advanced fiber with power.

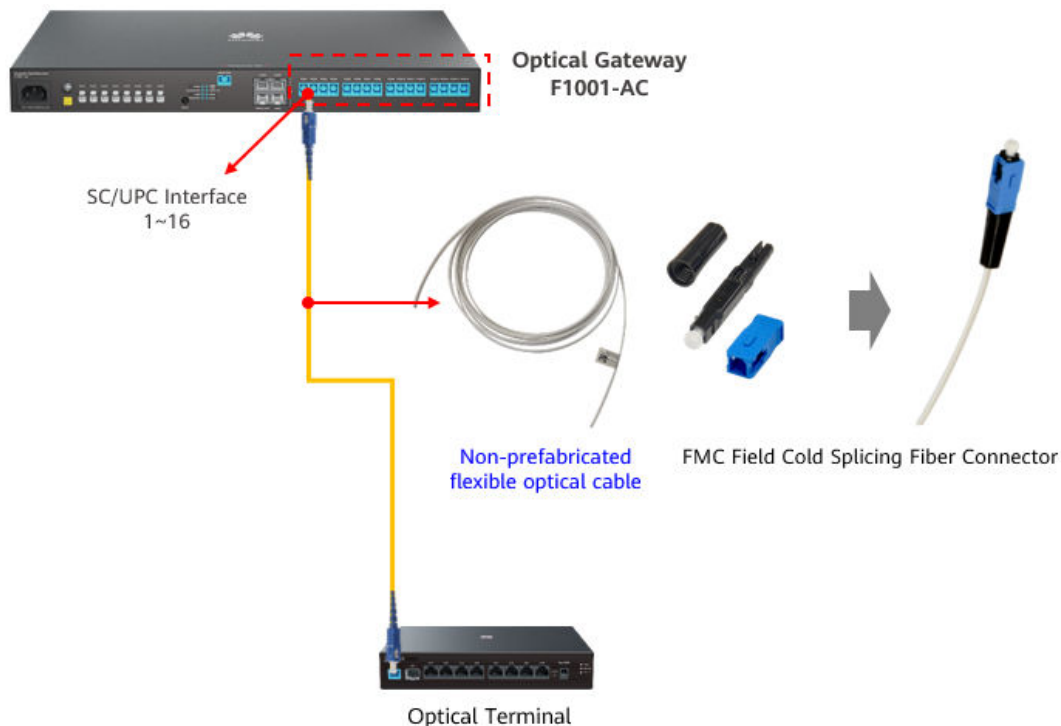
- [7.5.2.1 Deploying cables on cable trays](#)
- [7.5.2.2 Deployment in the Ceiling Scenario](#)

**Step 2** After the routing is complete, insert one end of the flexible optical cable into the optical terminal, and insert the other end of the flexible optical cable into the optical gateway.

**Step 3** Prepare and attach labels according to the label specifications to facilitate subsequent maintenance.

----End

## Laying the non-prefabricated flexible optical cable



### Step 1 Lay out cables.

The routing of non-prefabricated flexible optical cable is the same as that of advanced fiber with power. For details, see the routing process of advanced fiber with power.

- [7.5.2.1 Deploying cables on cable trays](#)
- [7.5.2.2 Deployment in the Ceiling Scenario](#)

### Step 2 Preparing an FMC Connector.

The method of making the FMC connector depends on the actual material.

This section describes how to make Huawei FMC 21 series products. For details, see <https://support.huawei.com/enterprise/en/optical-access/odn-fmc21-pid-250584311>.

**Step 3** After routing the cables and preparing the FMC connectors, insert one end of the flexible cable into the optical terminal and the other end into the optical gateway.

**Step 4** Prepare and attach labels according to the label specifications to facilitate subsequent maintenance.

----End

## 7.6 Construction Acceptance

## 7.6.1 Acceptance of electrical performance of advanced fiber with power

The advanced fiber with power may be broken during cable layout. The following methods can be used to verify the result.

Materials and tools: 1 piece of copper wire of about 50 mm length, 2 XC adapters, 1 multimeter.

### NOTE

The XC adapter is used to connect the XC connector of the advanced fiber with power to the SC connector. It can be used with multimeter to judge the circuit conduction and optical performance of advanced fiber with power.

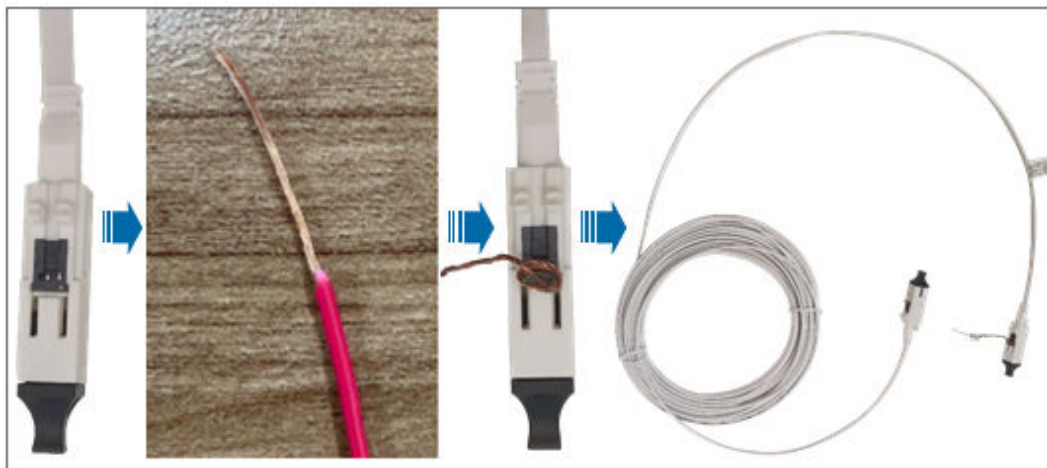
Click here to view the video guide for optical/electrical performance acceptance of AFwP cables.

<https://support.huawei.com/enterprise/en/doc/EDOC1100297183>



### Operation Procedure

**Step 1** After the advanced fiber with power is laid, connect the XC adapter to one end of the connector and bind the two electrodes together with copper wires.



- Step 2** Connect the connector at the other end of the advanced fiber with power to the XC adapter, set the multimeter to the diode/buzzer gear, and connect the two probes to the two electrodes on the XC adapter. If the multimeter dial displays 0, At the same time, there is a "drip-drip" sound, indicating that a loop is formed between the two electrodes of the advanced fiber with power, indicating that there is no open circuit under the whole section of the advanced fiber with power, and the advanced fiber with power is in good condition.



- Step 3** If the preceding situation does not occur, the advanced fiber with power is disconnected. Remove and replace the advanced fiber with power with a new one.

**NOTE**

If the end-to-end device has been installed and meets the power-on conditions, power on the device for acceptance. Check the electrical performance of the advanced fiber with power based on the device indicators.

----End

## 7.6.2 Acceptance of optical power of advanced fiber with power


During the routing of advanced fiber with power, optical cables may be broken or bent. As a result, the optical power is too high. The following method can be used to verify the results.

Materials and tools: one XC adapter, one optical power meter, and pigtail.

 **NOTE**

The XC adapter is used to connect the XC connector of the advanced fiber with power to the SC connector. It can be used with multimeter to judge the circuit conduction and optical performance of advanced fiber with power.

**Table 7-4** advanced fiber with power

Acceptance Item	requirements
Cable bending	<p>The bending radius of the advanced fiber with power shall not be less than 24 mm.</p> <p><b>NOTE</b> If the bending radius is too small, the attenuation is too large.</p> 



Acceptance Item	requirements
Acceptance of Optical Path Attenuation	<p><b>NOTE</b> The optical power must be greater than or equal to -23 dBm.</p> <p>The optical attenuation meets the requirements, that is, the optical power to the ONU meets the requirements of the ONU.</p> <ul style="list-style-type: none"> <li>• If the attenuation of the optical path is too small, the optical power of the ONU is too large. As a result, the optical power received by the ONU exceeds the overload optical power, which may cause damage to the ONU.</li> <li>• If the attenuation of the optical path is too large, the optical power of the ONU is too small. As a result, the optical power received by the ONU cannot reach the receiver sensitivity. As a result, faults such as the ONU cannot go online may occur.</li> </ul>

## Operation Procedure

### Step 1 Measure the optical power.

- Method 1: Query the optical power.

Query the information on the web page of the optical gateway. Choose **System Information > Optical**. In the right pane, you can view the Tx optical power and Rx optical power of the optical module.

The screenshot shows the web interface for device F1001-AC. The left sidebar contains navigation options: Device, WAN, Optical, Service Provisioning..., Eth Port, WAN-side statistics..., PoE, User Device Information..., Network Info, VLAN packet statistics..., Link Tracking Statistics..., and Tunnel Status. The main content area is titled 'Optical Information' and includes a note: 'On this page, you can query the status of the optical gateway.' Below this are two tables: 'ONT Information' and 'OLT Information'. A callout box points to the 'Reference Value' column in the ONT table with the text: 'Compare the queried value with the reference value to determine whether the optical power is abnormal.'

	Current Value	Reference Value
Optical Signal Sending Status:	--	Auto
TX Optical Power:	-- dBm	2 to 7 dBm
RX Optical Power:	-- dBm	-28 to -8 dBm
Working Voltage:	3280 mV	3100 to 3500 mV
Bias Current:	0 mA	0 to 90 mA
Working Temperature:	36 °C	-10 to +85 °C

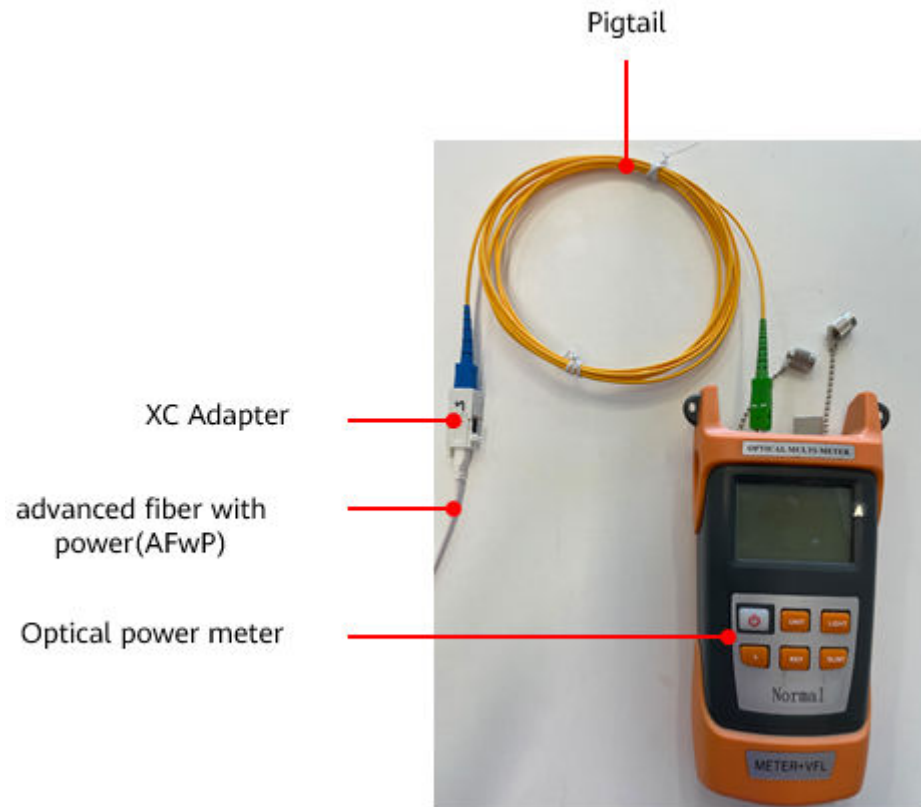
  

	Current Value	Reference Value
Optical module type:	--	--
Transmit optical power:	-- dBm	--
PON port identifier:	--	--

- Method 2: Measure the optical power.

After routing the advanced fiber with power, power on the optical cable, remove the optical cable connected to the ONU, connect the optical power

meter with the XC adapter and pigtail, and measure the optical power using the optical power meter.



**Step 2** After the inspection, insert the optical cable into the ONU if the requirements are met.

**Step 3** If the requirements are not met, clean the end surface and repeat the test. Check the cable routing path (especially the corner area) on site. Adjust the cable routing path if the requirements are not met. If the requirements are still not met, remove the optical cable and replace it with a new one.

----End

### 7.6.3 Acceptance Label

Correct labels facilitate future management and maintenance. All cables must be labeled.

There are two ways to fill the label: one is to print the label, the other is to use the oil pen to write manually. In consideration of efficiency and aesthetics, it is recommended to use the printer printing mode.

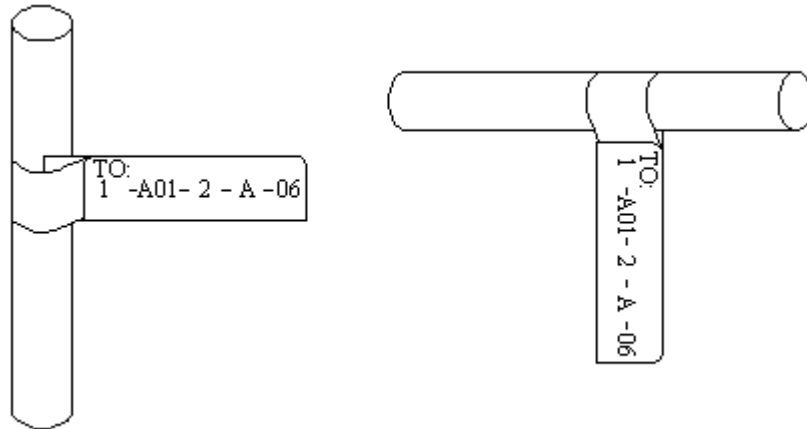
#### Signal cable label

By default, the label is attached 2 cm away from the plug. Special handling can be performed in special cases. For example, the label should be placed away from the bending of the cable or other positions that affect the installation of the cable.

Labels must be attached to both ends of the cable. After the label is attached to the cable, the long strip text area must face the right side or lower side. That is, at

the position where the label is attached, the label faces right when the cable is laid out vertically. When the cable is horizontally laid, the label faces downwards, As shown in the following figure.

**Figure 7-1** Attaching the label to the signal cable at a proper position



## Power cable label

Remove the label paper from the whole label material and attach it to the label plate of the wire buckle (only one side is attached).

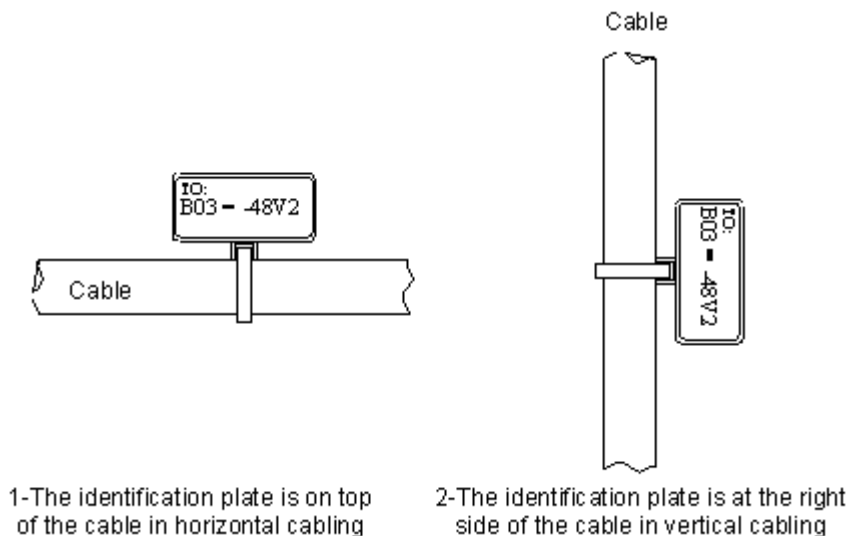
When pasting, stick it in the square groove of the signboard. (The side on which to paste is not specified. The onsite personnel can determine the side according to the operation habits. However, in the same equipment room, ensure that the side on which to paste is consistent.)

By default, the cable tie is 2 cm away from the plug. Special handling can be performed in special cases.

Cable ties should be bound at both ends of the cable. After the cable ties are bound on the cable, the label should be oriented to the right or upper side: that is, when the cable is laid vertically, the label should be oriented to the right. When the cable is laid horizontally, the label should face upwards and the side of the label should face outwards, as shown in the figure.

The following figure shows the binding effect of the power cable label.

**Figure 7-2** Appearance of the label attached to the power cable



## 7.6.4 Other Acceptance Contents

After the equipment is powered on, check the indicator status of each equipment to determine the circuit status.

Check the records item by item according to [Table 7-5](#).

**Table 7-5** Checking After Installation

Acceptance Item	Acceptance Criteria
Equipment Installation Acceptance	<ul style="list-style-type: none"> <li>• The equipment is installed in a proper position.</li> <li>• Installation Specifications of Mechanical Parts</li> <li>• The device heat dissipation is good.</li> </ul>
Circuit acceptance	<ul style="list-style-type: none"> <li>• The device is powered on normally.</li> <li>• Check the power switch.</li> <li>• The network box and equipment must be grounded.</li> </ul>
Acceptance of construction cabling	<ul style="list-style-type: none"> <li>• Ensure that cables are not crossed or bent.</li> <li>• The optical cables are routed neatly and the bending radius of the optical fibers meets the requirements.</li> <li>• In addition to neat and beautiful cabling, the unused space should not be affected for expansion and maintenance.</li> <li>• All cables must be labeled for easy management and maintenance.</li> </ul>

# 8 Configuration Guide

---

- [8.1 Before You Start](#)
- [8.2 Deployment by Scanning Codes \(Using the HUAWEI eKit App\)](#)
- [8.3 Quick Deployment Configuration Scenario \(WebUI\)](#)
- [8.4 Customized Scenarios Configured on Demand \(WebUI\)](#)
- [8.5 Service Acceptance](#)

## 8.1 Before You Start

This section describes the instructions for using this document. Read this section carefully before using this document to avoid possible misunderstandings.

### Configuration Examples

The networking diagrams, data planning, and operation procedures in this document are typical configuration examples designed for customers to understand and use the products. They cannot be used as templates. Before configuring services, plan data and configure services based on actual service requirements.

### IP Address and MAC Address Usage

IP addresses and MAC addresses are used in the product documentation to describe features and configuration examples. Unless otherwise specified, IP addresses and MAC addresses are examples only, and do not refer to any actual device.

### User Interfaces

This document serves only as a usage guide. The user interface (UI) content (such as CLI command format, command output, web UI, and NMS UI) is compiled based on lab devices. This document provides general guidance, but may not cover all application scenarios of all product models and versions. Due to reasons such as version upgrade, device model difference, and configuration file difference, the content provided in this document may be different with the actual UIs. This

document does not elaborate on the differences in the preceding situations. The actual UIs prevail.

#### NOTE

The operation steps and data in the configuration example are designed for easy understanding and reference, and cannot be used as templates. Before configuring services, plan data based on the actual networking scenario and service requirements.

The screenshots in this section use the login page of the F1001-AC user (Epadmin) as an example. The screenshots may vary with software versions. The actual screenshots prevail.

## 8.2 Deployment by Scanning Codes (Using the HUAWEI eKit App)

This section describes how to use the HUAWEI eKit app to perform deployment by scanning codes.

### Prerequisites

- Devices have been installed and deployed, and the optical gateway, optical AP, and ONU have been correctly connected.
- The device has been powered on and is running properly.
- You have downloaded and installed the Huawei eKit app.

#### NOTE

HUAWEI eKit App is a digital distribution platform that integrates marketing, transaction, service, enablement, and partner operations for numerous distribution partners and enterprise-level users in the enterprise market.

Download HUAWEI eKit App

- For Huawei phones, search for **Huawei eKit** in Huawei AppGallery and download it.
- For non-Huawei Android phones, visit <https://app.huawei.com/eplus/soho/front/index.html#/download> in the address box of the browser to download the app.
- Scan the QR code to download.



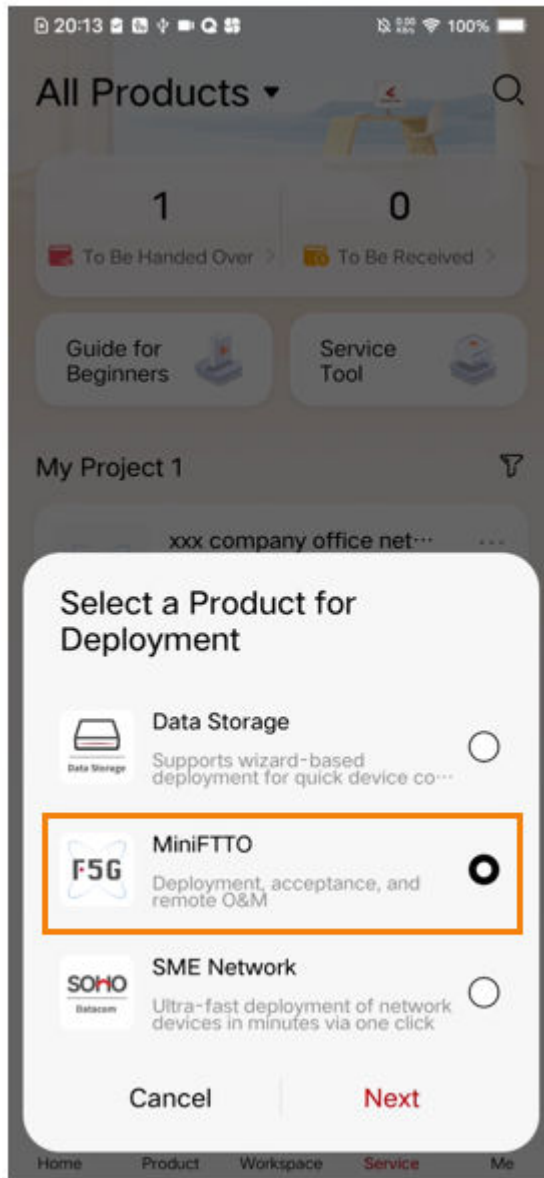
- The mobile phone must support carrier networks or be connected to a Wi-Fi network that can access the Internet.
- The version of the optical gateway at the sites is V500R023C00 or later.

#### NOTE

In addition, to use the latest functions, you are advised to upgrade the optical gateway, ONU, and optical AP to the latest versions.

## Procedure

On the Service tab page, tap +, select MiniFTTO, and select Deployment by Scanning Codes to deploy the project.



For details, see the document: [Huawei eKit APP \(MiniFTTO\) Product Overview](#)

## Configuration Video Guide

Configuration Item	Video Link
How to Quickly Scan the QR Code for Deployment	<a href="https://support.huawei.com/enterprise/en/optical-access/optixstar-f1001-pid-255462555?category=configuration-commissioning">https://support.huawei.com/enterprise/en/optical-access/optixstar-f1001-pid-255462555?category=configuration-commissioning</a>
One-stop Configuration Wizard	<a href="https://support.huawei.com/enterprise/en/optical-access/optixstar-f1001-pid-255462555?category=configuration-commissioning">https://support.huawei.com/enterprise/en/optical-access/optixstar-f1001-pid-255462555?category=configuration-commissioning</a>

Configuration Item	Video Link
How to Perform One-Click Acceptance and Manage Acceptance Reports	
How to Perform Deployment, Configurations, Upgrade and Delivery	
How to Deploy Pured Wired Networking	
Experience Deployment and O&M Scenarios	

## 8.3 Quick Deployment Configuration Scenario (WebUI)

In the quick deployment configuration scenario, the default template parameters are used for service configuration. You only need to connect the optical gateway to the physical lines of optical terminals to implement wired and wireless access for Internet services.

For details about the default template parameters, see Table 1-1. If the default template parameters meet the service deployment requirements, you can use the quick deployment mode. [Table 8-1](#)

**Table 8-1** Default system parameters

Configuration Item	Default Parameter
WAN	System default WAN connection: <ul style="list-style-type: none"><li>• Connection name: 1_INTERNET_R_VID</li><li>• Encapsulation type: IPoE</li><li>• Protocol type: IPv4</li><li>• WAN type: routed WAN</li><li>• IP address obtaining mode: DHCP</li><li>• Enable VLAN: VLAN is disabled and services are not isolated.</li></ul>
DHCP Server Configuration	Default primary address pool <ul style="list-style-type: none"><li>• Enable the DHCP master server: Enable</li><li>• LAN host IP address: 192.168. 10.1</li><li>• Subnet mask: 255.255. 254.0</li><li>• Start IP address: 192.168. 10.2</li><li>• End IP address: 192.168. 11.254</li><li>• Lease time: 6 hours</li></ul>

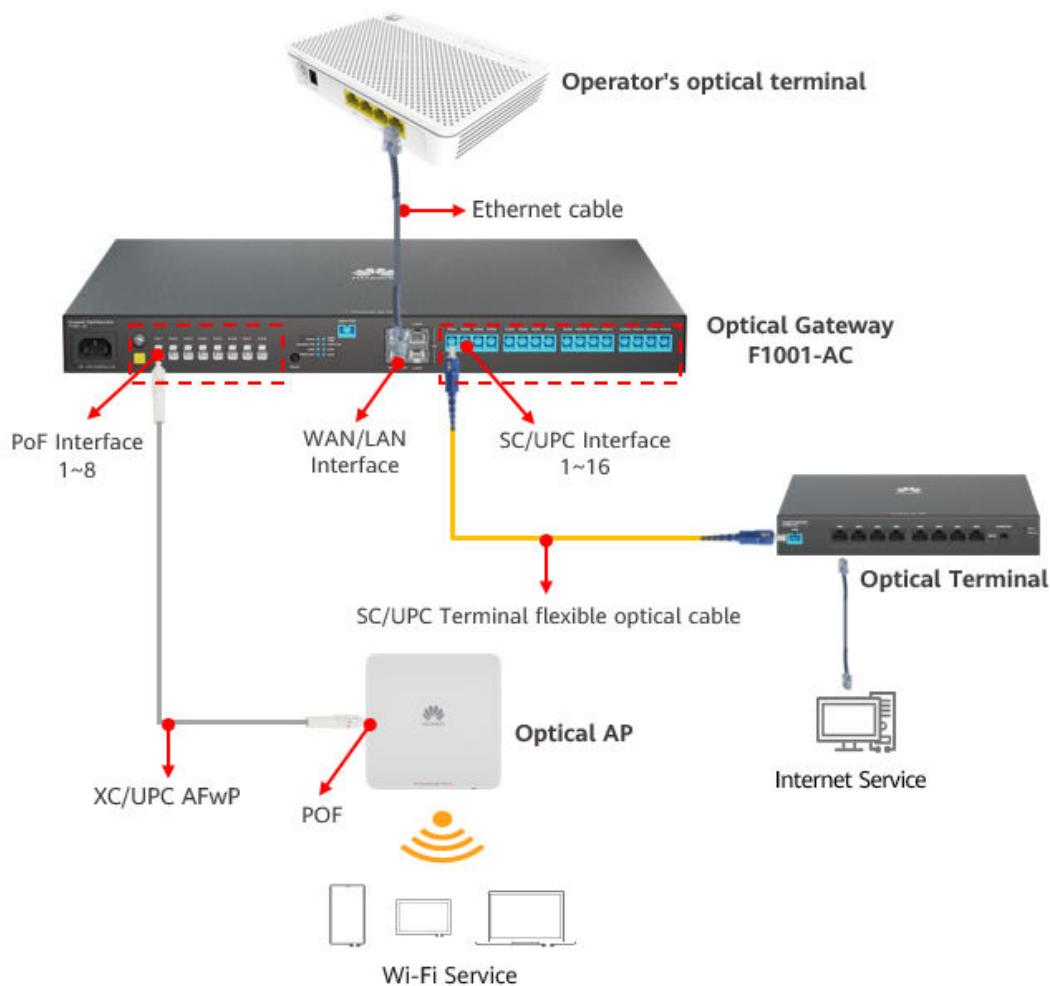


Configuration Item	Default Parameter
Wi-Fi	<p>By default, the system creates 7 SSIDs:</p> <ul style="list-style-type: none"> <li>• Number of 2.4G SSIDs: 4</li> <li>• Number of 5G SSIDs: 3</li> </ul> <p><b>NOTICE</b> To ensure security, if you use the default SSID, change the password as required.</p>

## Application Scenarios

The typical application scenarios are as follows:

- The optical gateway uses LAN upstream transmission and connects to the optical modem of the carrier through Ethernet cables.
- The optical gateway connects to optical APs and optical terminals and provides wired and wireless Wi-Fi access modes.
- Wi-Fi networks can be distinguished by SSIDs that cannot be configured.
- Different services are not isolated from each other.



## Configuration Process

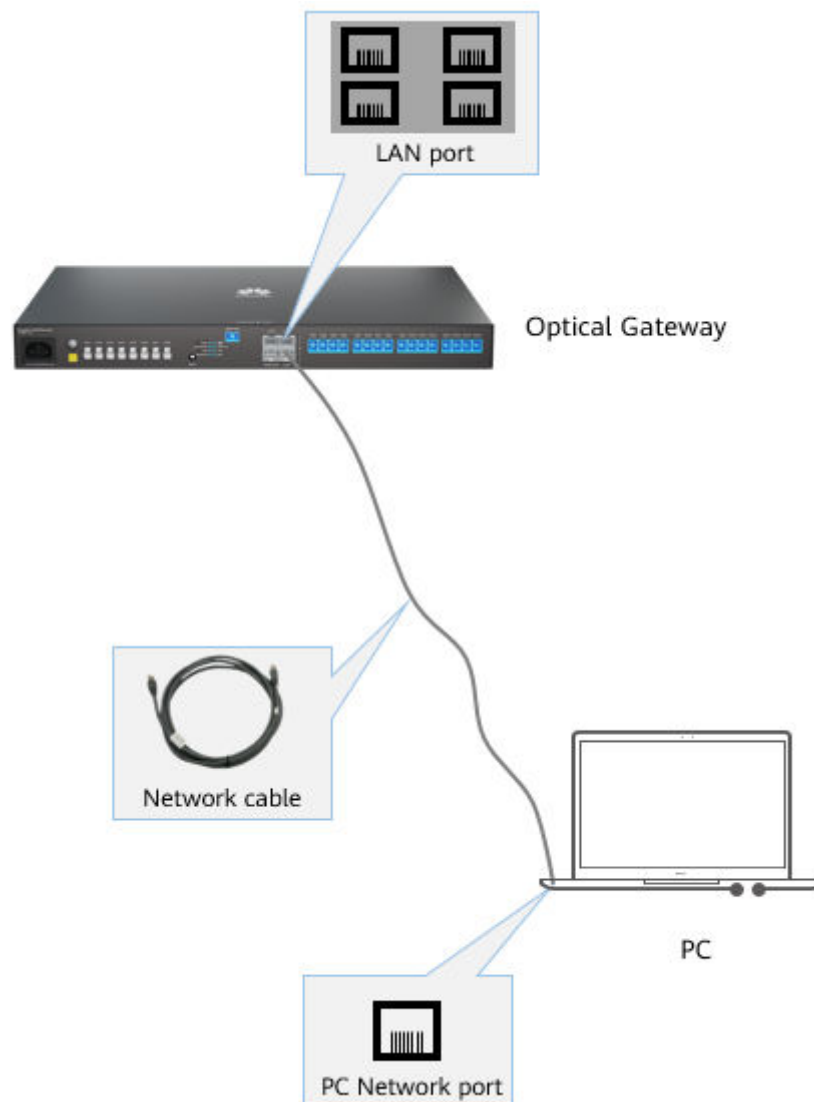
**Table 8-2** Configuration process in the default configuration scenario

No.	Configuration Item	Description
Step 1	Configuring WAN Connections	Use the default values of the system parameters.
Step 2	Configuring the Internet Service	Use the default values of the system parameters.
Step 3	Configuring the Video Backhaul Service	Use the default values of the system parameters.
Step 4	Configuring the Wi-Fi Service	The system provides seven SSIDs by default: <ul style="list-style-type: none"><li>• If the default SSID is used, you do not need to set this parameter.</li><li>• If the default SSID is not used, you need to configure the SSID parameters.</li></ul>

## Configuration Procedure

**Step 1** Configure local login to the web UI.

1. Use a network cable to connect the LAN port (not the LAN upstream port) of the optical gateway to the network port of the PC.



2. Set the IP address of the computer to be in the same network segment as the management IP address of the optical gateway.

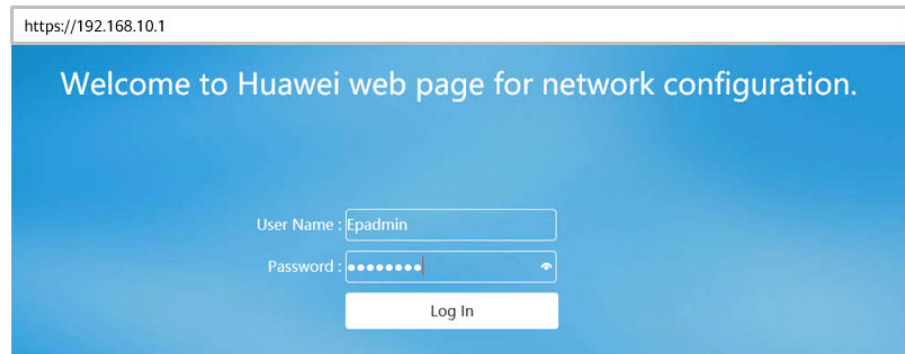
**NOTE**

The default management IP address and subnet mask of the optical gateway F1001 are as follows:

- IP Address: 192.168. 10.1
- Subnet mask: 255.255. 254.0

You can also obtain the default management IP address and subnet mask of the optical gateway F1001 from the nameplate at the bottom of the product.

3. Log in to the web UI.
  - a. Enter `http://192.168.10.1` in the address box of the browser. (192.168.10.1 is the default management IP address of the F1001.) and press Enter to switch to the login page. As shown in the following figure.
  - b. Enter the user name and password in the login window. (For the initial user name and password, see the product nameplate.) After the account is verified, you can access the web configuration page.



---

#### NOTICE

To ensure account security, change the initial password of the administrator account in time after logging in to the WebUI using the initial user name and password.

---

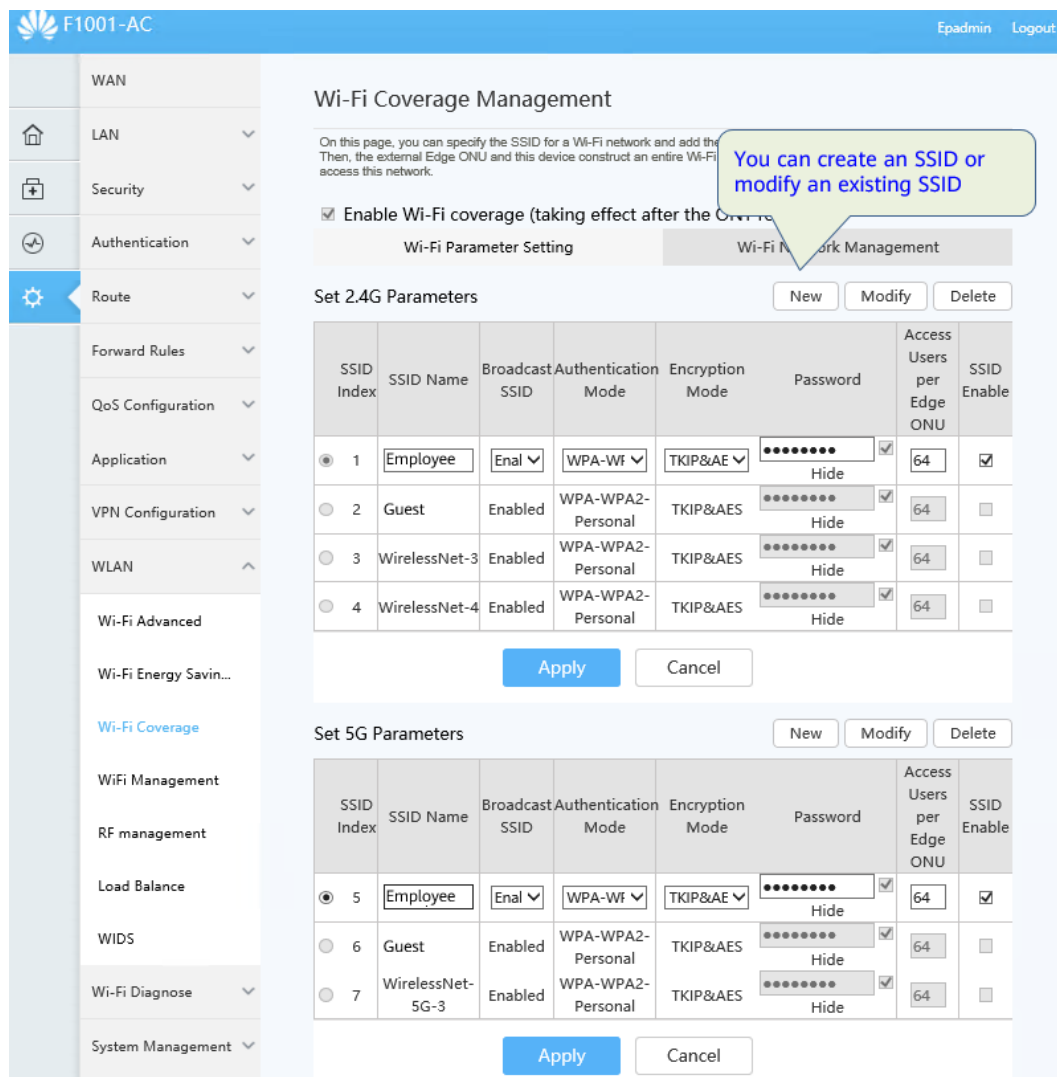
#### Step 2 Configure the SSID.

Choose **Advanced > WLAN > Wi-Fi Coverage**. On the **Wi-Fi Parameter Setting** tab page, configure the SSID.

Select SSIDs 1 and 5, click **Modify**, change the SSID name to **Employee**, and set the employee Wi-Fi password.

Select SSIDs 2 and 6, click **Modify**, change the SSID name to **Guest**, and set the employee Wi-Fi password.

After the configuration is complete, click **Apply**.



**Step 3** After the configuration is complete, both the wired and wireless networks can access the Internet.

----End

## 8.4 Customized Scenarios Configured on Demand (WebUI)

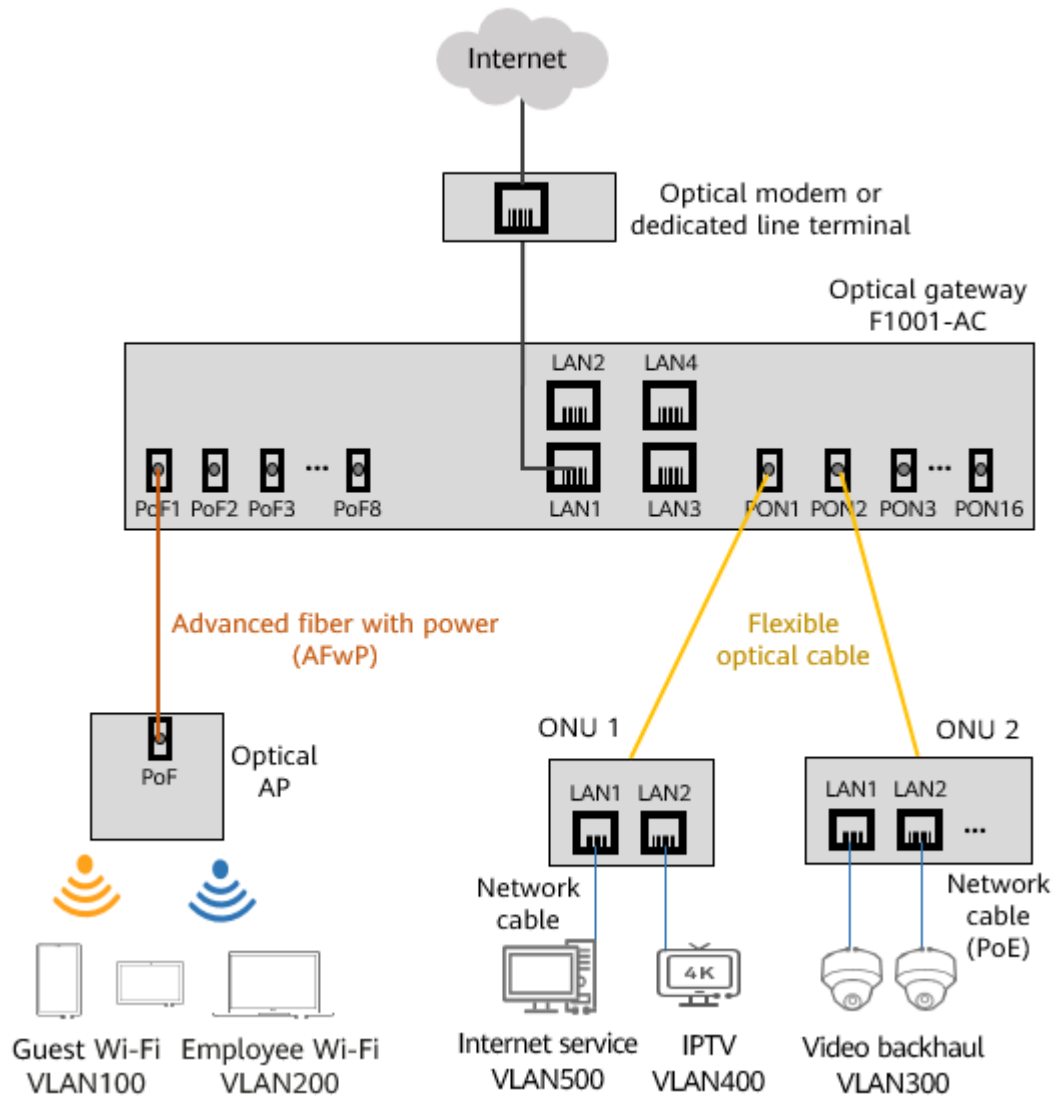
### 8.4.1 Usage Scenarios and Data Planning

#### Networking Scenario

Typical usage scenarios are as follows:

- The optical gateway uses the LAN upstream mode.
- The optical gateway connects to optical APs and optical terminals and provides wired and wireless Wi-Fi access modes.

- Wi-Fi is divided into employee Wi-Fi and guest Wi-Fi, and employee Wi-Fi and guest Wi-Fi are isolated from each other.
- Different services are isolated by VLANs.



## Data Planning

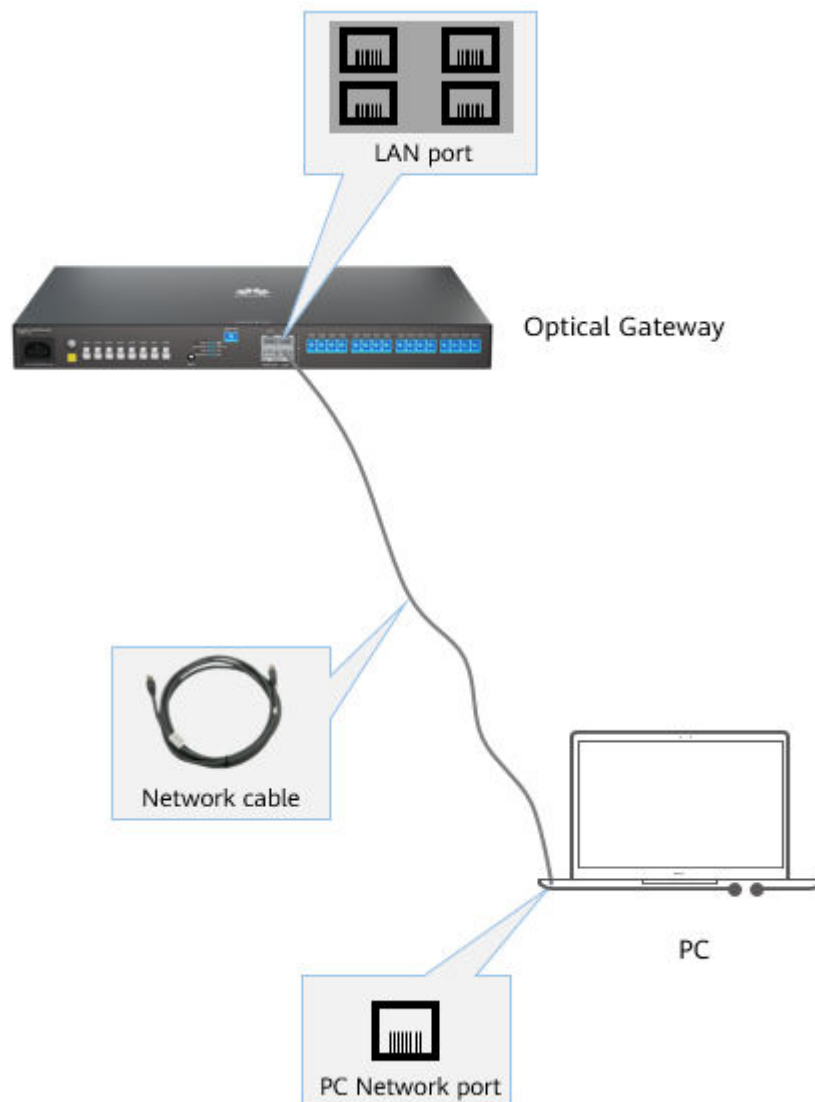
**Table 8-3** Service Data Planning

Service Type	Service VLAN	WAN connection	Network port and SSID
Internet service	500	Create an Internet. <ul style="list-style-type: none"> <li>Encapsulation type: IPoE</li> <li>Protocol type: IPv4</li> <li>WAN type: Routed WAN</li> <li>Service type: Internet</li> <li>IP address obtaining mode: DHCP</li> </ul>	ONU: ONU 1 Network port: LAN 1
Wi-Fi service	Employee: 200 Guest: 100		Employee Wi-Fi <ul style="list-style-type: none"> <li>SSID Name: Employee</li> <li>2.4 GHz SSID index: 1</li> <li>5G SSID index: 5</li> </ul> Guest Wi-Fi: <ul style="list-style-type: none"> <li>SSID Name: Guest</li> <li>2.4 GHz SSID index: 2</li> <li>5G SSID index: 6</li> </ul>
Camera service	300	<ul style="list-style-type: none"> <li>Other parameters: default values</li> </ul>	ONU: ONU 2 Network port: LAN 1 and LAN 2
IPTV service	400	Create an IPTV service. <ul style="list-style-type: none"> <li>Encapsulation type: IPoE</li> <li>Protocol type: IPv4</li> <li>WAN Type: Bridging WAN</li> <li>Service type: IPTV</li> <li>Multicast VLAN: 400</li> <li>Other parameters: default values</li> </ul>	ONU: ONU 1 Network port: LAN 2

### 8.4.2 Configuring the Local Login Web UI

#### Configuration Procedure

- Step 1** Use a network cable to connect the LAN port (not the LAN upstream port) of the optical gateway to the network port of the PC.



**Step 2** Set the IP address of the computer to be in the same network segment as the management IP address of the optical gateway.

**NOTE**

The default management IP address and subnet mask of the optical gateway F1001 are as follows:

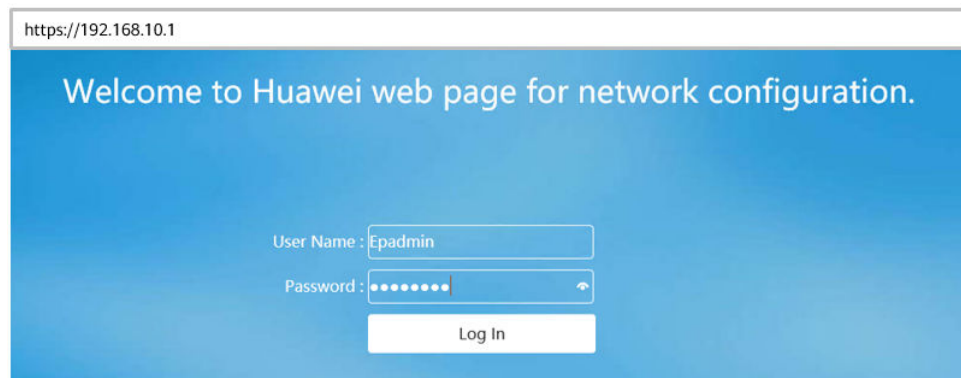
- IP Address: 192.168. 10.1
- Subnet mask: 255.255. 254.0

You can also obtain the default management IP address and subnet mask of the optical gateway F1001 from the nameplate at the bottom of the product.

**Step 3** Log in to the web configuration page.

1. Enter `http://192.168.10.1` in the address box of the browser. (192.168. 10.1 is the default management IP address of the F1001.) and press Enter to switch to the login page. As shown in the following figure.
2. Enter the user name and password in the login window. (For the initial user name and password, see the product nameplate.) After the account is verified, you can access the web configuration page.





### NOTICE

To ensure account security, change the initial password of the administrator account after logging in to the WebUI using the initial user name and password.

----End

## 8.4.3 Configuring the Internet Service

### Configuration Process

**Table 8-4** Flowchart for configuring the Internet service

Step No.	Configuration Item	Description
Step 1	Configuring WAN	WAN Service Type: INTERNET
Step 2	Configuring Port VLAN	<ul style="list-style-type: none"> <li>• Enable port VLAN isolation</li> <li>• Setting Layer 3 Interfaces</li> <li>• Enable DHCP Server</li> </ul>
Step 3	Configuring the NATIVE VLAN for Ethernet port LAN 1 connecting ONU1 to the PC	Each network port can be configured with only one native VLAN

### Configuration Procedure

#### Step 1 Configure WAN.

In the navigation tree on the left, choose **Advanced** > **WAN**. In the pane on the right, click **New**. In the dialog box that is displayed, set parameters based on the data plan.

- Encapsulation Mode: IPoE

- Protocol Type: IPv4
- WAN Mode: routed WAN
- Service Type: INTERNET
- Upstream Port: LAN1(Default)
- IP address obtaining mode: DHCP
- Other parameters: default values

After the configuration is complete, click **Apply**.

The screenshot displays the 'WAN Configuration' page in the Huawei MiniFTTO management interface. The left sidebar shows the navigation menu with 'Route' highlighted. The main content area contains a table of WAN connections and a configuration form. The table lists a connection named '1\_INTERNET\_R\_VID\_' with VLAN/Priority '-/-' and Protocol Type 'IPv4'. The configuration form includes sections for 'Basic Information' and 'IPv4 Information'. Callouts highlight specific settings: 'Encapsulation Mode' is set to IPoE, 'WAN Mode' is 'Route WAN', 'Service Type' is 'INTERNET', 'Upstream Port' is 'Default', and 'IP Acquisition Mode' is 'DHCP'. Other visible settings include 'Enable WAN' checked, 'MTU' at 1800, and 'Enable NAT' checked.

## Step 2 Configure the Port VLAN.

Choose **Advanced > LAN > Port VLAN Configuration**. In the right pane, perform the following operations:

- Select **Enable Port VLAN isolation**.
- Click **New** to create an Internet service VLAN. Set **VLAN Name** to Internet Service and **VLAN ID** to 500. Select the downstream PON port in **Port List**.

- Select the Internet service VLAN, click **Layer 3 Interface Settings**, and set the IP address and subnet mask of the Layer 3 interface of VLAN500.
- Select **Enable DHCP server** and configure the DHCP address pool used by Internet access services.

After the configuration is complete, click **Apply**.

The screenshot displays the configuration interface for a Huawei MiniFTTO device. The left sidebar shows the navigation menu with 'Port VLAN Configur...' selected. The main area is titled 'Port VLAN Configuration' and contains the following elements:

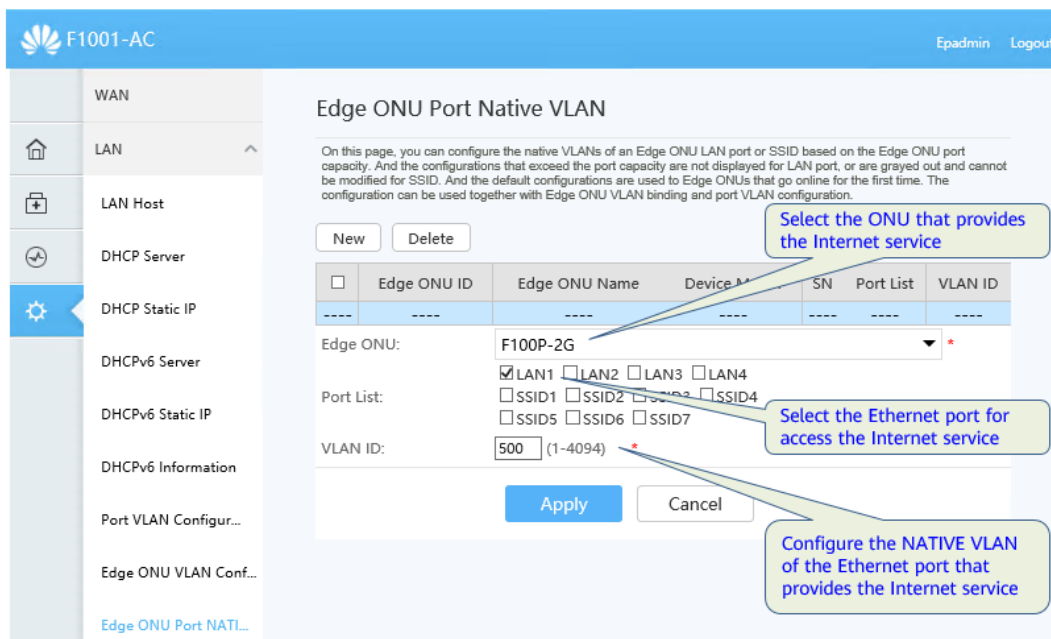
- Enable Port VLAN isolate:** A checkbox that is checked. A callout box points to it with the text 'Select this option'.
- Buttons:** 'New' and 'Delete' buttons.
- Table:** A table with columns 'VLAN Name', 'VLAN ID', and 'Port List'. It contains one entry: 'Internet' with VLAN ID '500' and Port List 'Downlink PON'.
- Form Fields:**
  - VLAN name: 'Internet'
  - VLAN ID: '500' (with a note '( 1-4094 )')
  - Port list: Radio buttons for 'LAN1', 'LAN2', 'LAN3', 'LAN4', and a checked radio button for 'Downlink PON'. A callout box points to the 'Downlink PON' option with the text 'Select this option'.
  - Disabling WAN-side Access: An unchecked checkbox.
- Layer 3 interface settings:** A section with a callout box pointing to it with the text 'Configure Layer 3 interface'. It contains:
  - Interface name: 'VLAN500'
  - IP address: '10.10.10.1'
  - Subnet mask: '255.255.255.0'
  - DHCP server: Radio buttons for 'Enable' (selected) and 'Disable'. A callout box points to the 'Enable' option with the text 'Select Enable'.
  - Starting IP address: '10.10.10.2' (with a note '(The IP address and the IP of the Layer 3 interface are on the same subnet)')
  - End IP address: '10.10.10.254'
  - Address pool mask: '255.255.255.0'
  - Gateway address: '10.10.10.1'
  - Lease time: '6' (with a dropdown menu set to 'Hour')
- Buttons:** 'Apply' and 'Cancel' buttons.

**Step 3** Configure the native VLAN for LAN 1 that connects ONU1 to the PC.

Choose **Advanced > LAN > Edge ONU Port NATIVE VLAN Configuration**. In the right pane, perform the following operations:

- Click **New** and select Edge ONU from the drop-down list box, that is, the ONU used to access Internet services.
- Select LAN 1 in the **Port List** area, that is, the network port used to access the Internet service terminal.
- Enter the VLAN ID, that is, VLAN 500 planned for the Internet service.

After the configuration is complete, click **Apply**.



**Step 4** The configuration is complete.

----End

## 8.4.4 Configuring the Wi-Fi Service

### Configuration Process

**Table 8-5** Wi-Fi Service Configuration Process

Step No.	Configuration Item	Description
Step 1	Configuring WAN	WAN Service Type: INTERNET
Step 2	Configuring Port VLAN	<ul style="list-style-type: none"> <li>• Enable Port VLAN isolation</li> <li>• Setting Layer 3 Interfaces</li> <li>• Enable DHCP Server</li> </ul>
Step 3	Configuring the SSID	Configure employee SSIDs and guest SSIDs
Step 4	Configuring Roaming Handover	Turn on the roaming handover switch
Step 5	Configuring Native-VLAN for Ports of Optical AP	Configuring a Native-VLAN based on the SSID
Step 6	Configure the port rate limit	Set this parameter based on the actual service requirements

## Configuration Procedure

### NOTE

The following uses employee Wi-Fi configuration as an example. The method of configuring guest Wi-Fi is the same as that of configuring employee Wi-Fi.

### Step 1 Configure the WAN.

#### NOTE

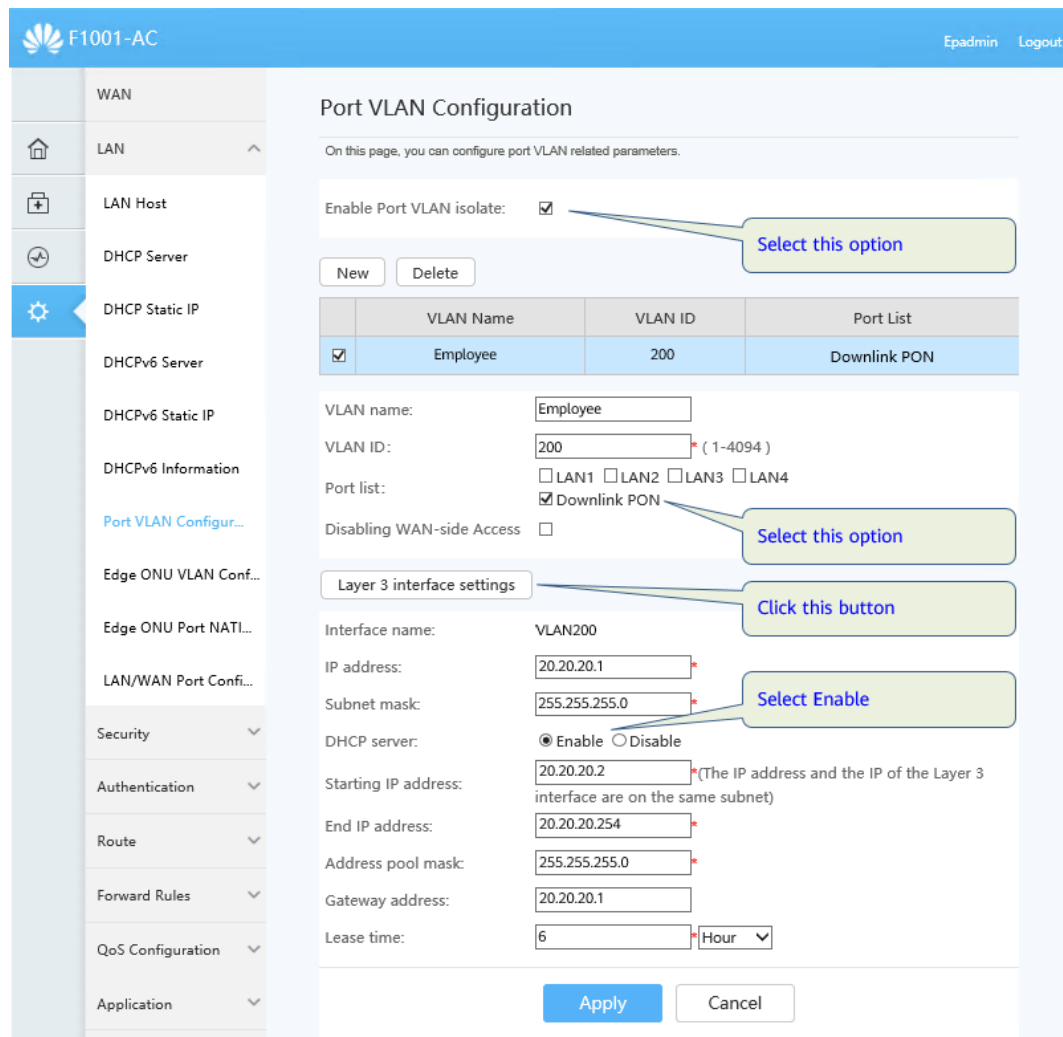
The Wi-Fi service and Internet service use the same WAN. If the WAN has been configured for the Internet service, you do not need to configure the WAN again.

### Step 2 Configure the Port VLAN.

Choose **Advanced > LAN > Port VLAN Configuration**. In the right pane, perform the following operations:

- Select **Enable Port VLAN isolation**.
- Click **New** to create an employee Wi-Fi service VLAN. Set **VLAN Name** to Employee, **VLAN ID** to 200, and **Port list** to select the downstream PON port.
- Select VLAN for employee Wi-Fi service, click Layer 3 Interface Settings, and set the IP address and subnet mask of VLAN 200.
- Select **Enable DHCP Server** and configure the DHCP address pool used by employee Wi-Fi services.

After the configuration is complete, click **Apply**.



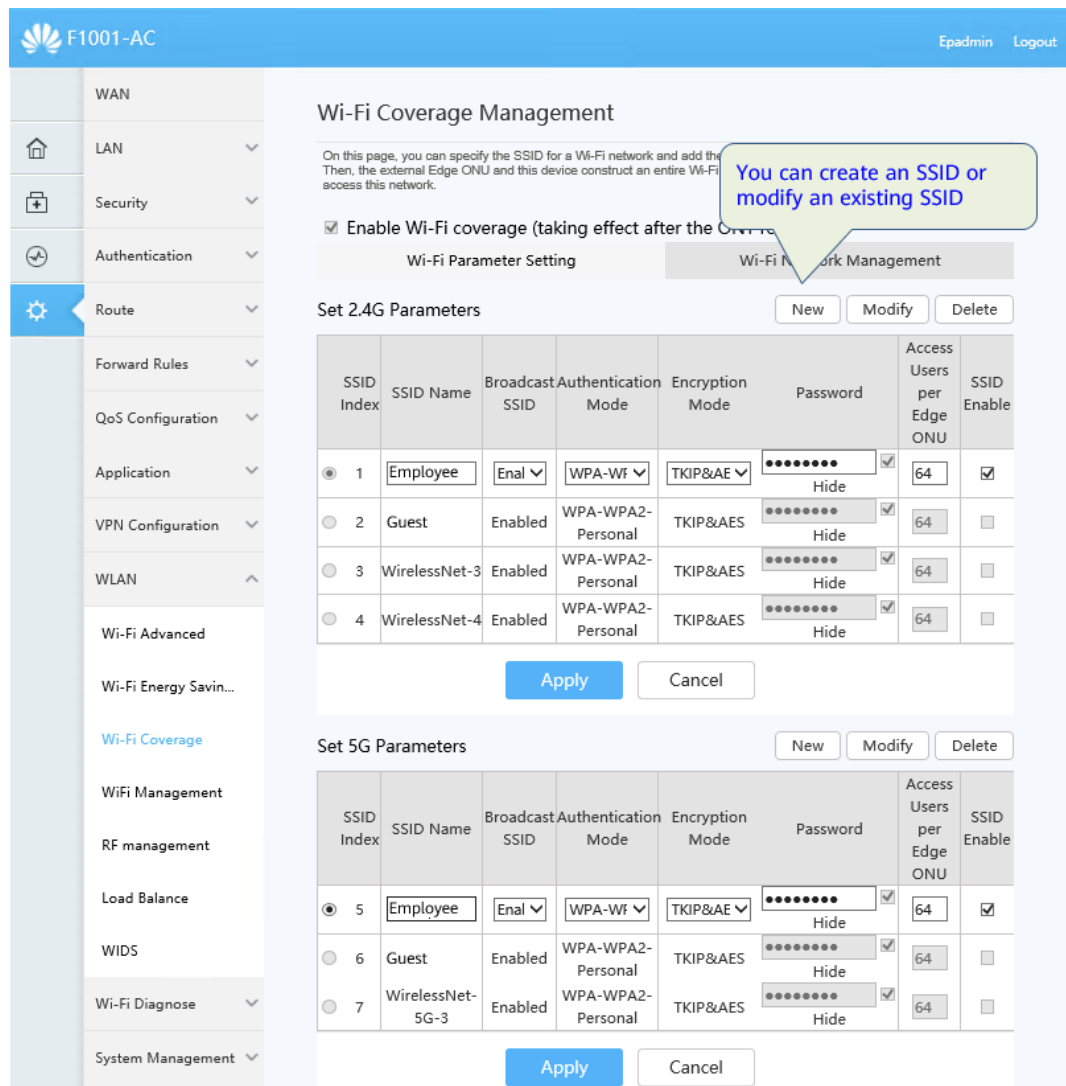
**Step 3** Configure the SSID.

Choose **Advanced > WLAN > Wi-Fi Coverage**. On the **Wi-Fi Parameter Setting** tab page, configure the SSID.

Select SSIDs 1 and 5, click **Modify**, change the SSID name to **Employee**, and set the employee Wi-Fi password.

Select SSIDs 2 and 6, click **Modify**, change the SSID name to **Guest**, and set the employee Wi-Fi password.

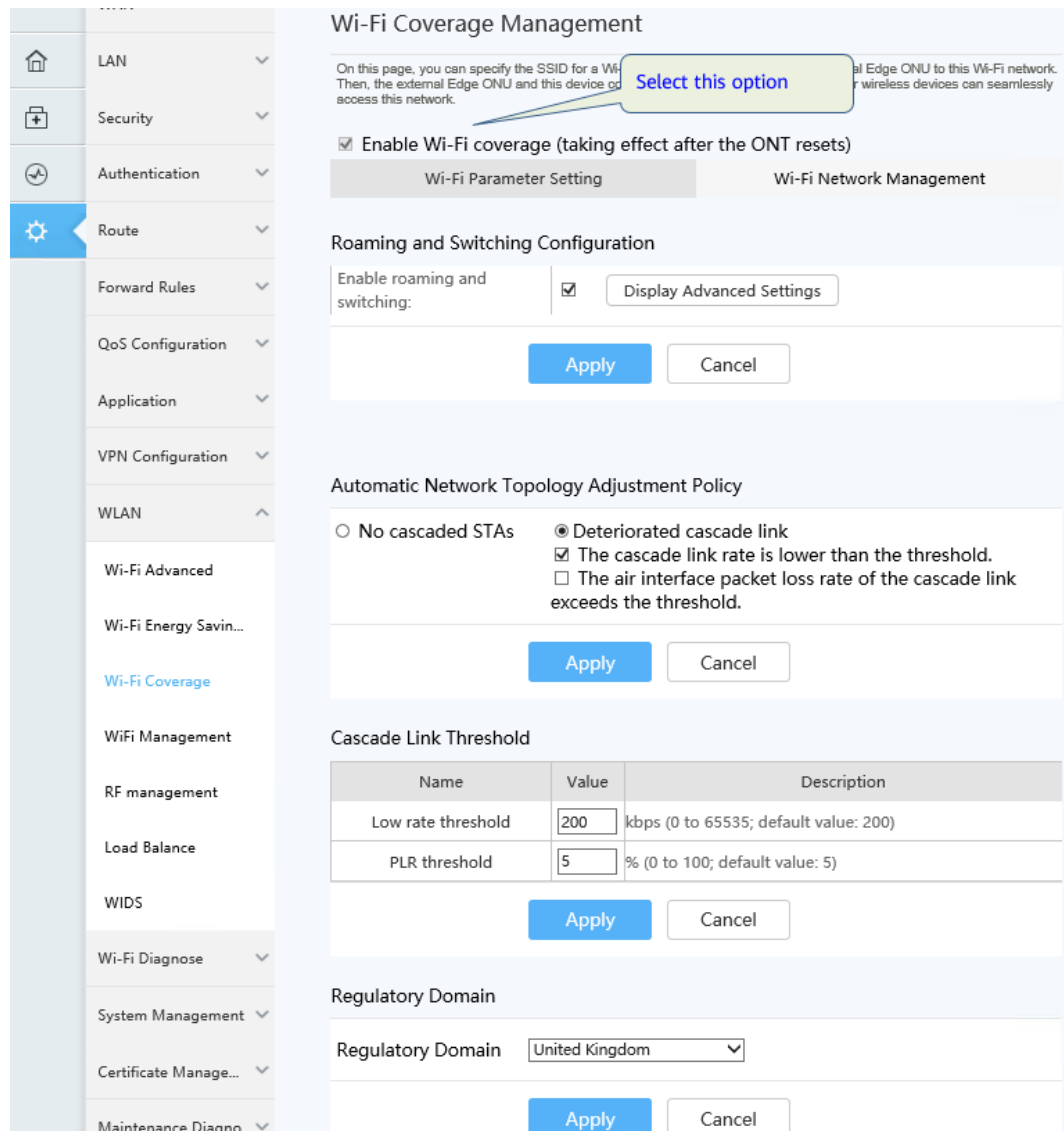
After the configuration is complete, click **Apply**.



**Step 4** Enable roaming switchover.

Choose **Advanced > WLAN > Wi-Fi Coverage**. Click the **Wi-Fi Network Management** tab and enable roaming switching.

After the configuration is complete, click **Apply**.



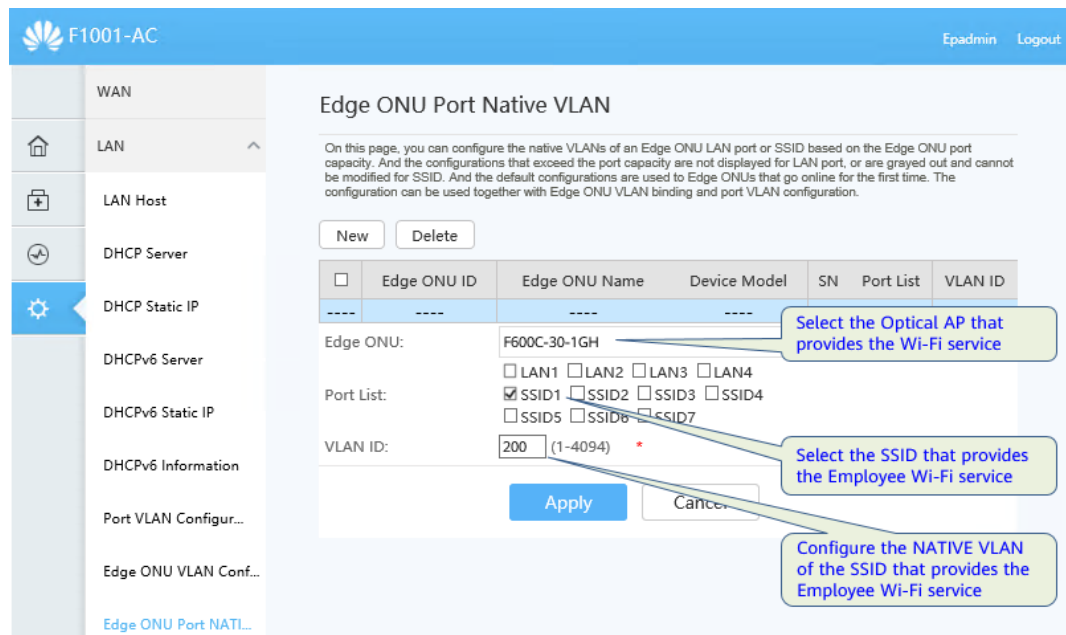
**Step 5** Configure the NATIVE-VLAN for the SSID of the employee Wi-Fi network.

Choose **Advanced > LAN > Edge ONU Port NATIVE VLAN Configuration**. In the right pane, perform the following operations:

- Select the optical AP that is used to access the employee's Wi-Fi service from the drop-down list box.
- Select SSID 1 for employee Wi-Fi in the port list.
- Enter employee Wi-Fi service VLAN 200.

After the configuration is complete, click **Apply**.

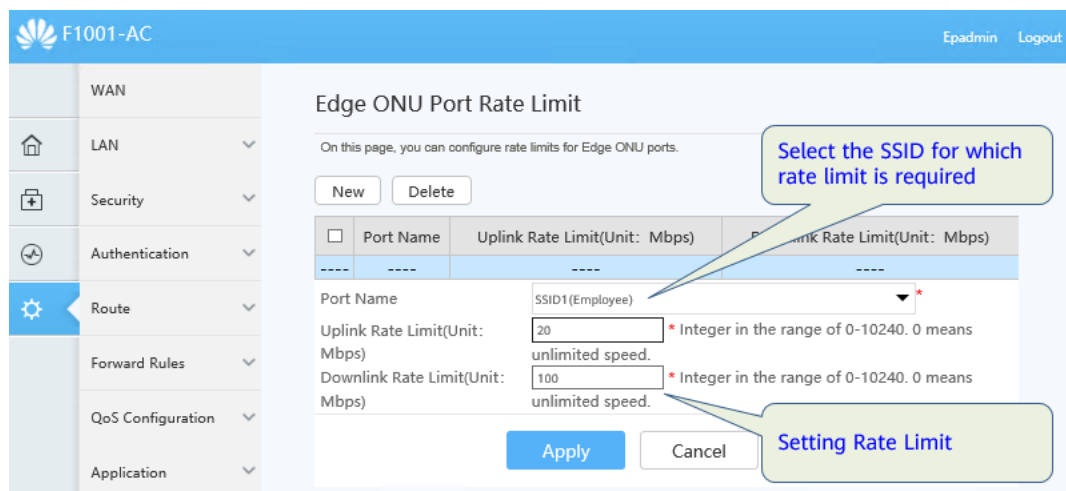




**Step 6** Configure the port rate limit.

Choose **Advanced > Rate Limit Management > Edge ONU Port Rate Limit**. In the right pane, click **New** or **Modify** to create or modify the selected rate limit information.

After the configuration is complete, click **Apply**.



**Step 7** The configuration is complete.

----End

## 8.4.5 Configuring the Video Backhaul Service

### Configuration Process

**Table 8-6** Flowchart for configuring the video backhaul service

Step No.	Configuration Item	Description
Step 1	Configuring WAN	Set the WAN service type to INTERNET
Step 2	Configuring Port VLAN	<ul style="list-style-type: none"><li>• Enable Port VLAN isolation</li><li>• Setting Layer 3 Interfaces</li><li>• Enable DHCP Server</li></ul>
Step 3	Configuring the NATIVE VLAN for Ethernet ports 1 and 2 of ONU2 that are connected to cameras.	Each Ethernet port can be configured with only one NATIVE VLAN

### Configuration Procedure

#### Step 1 Configure the WAN.

##### NOTE

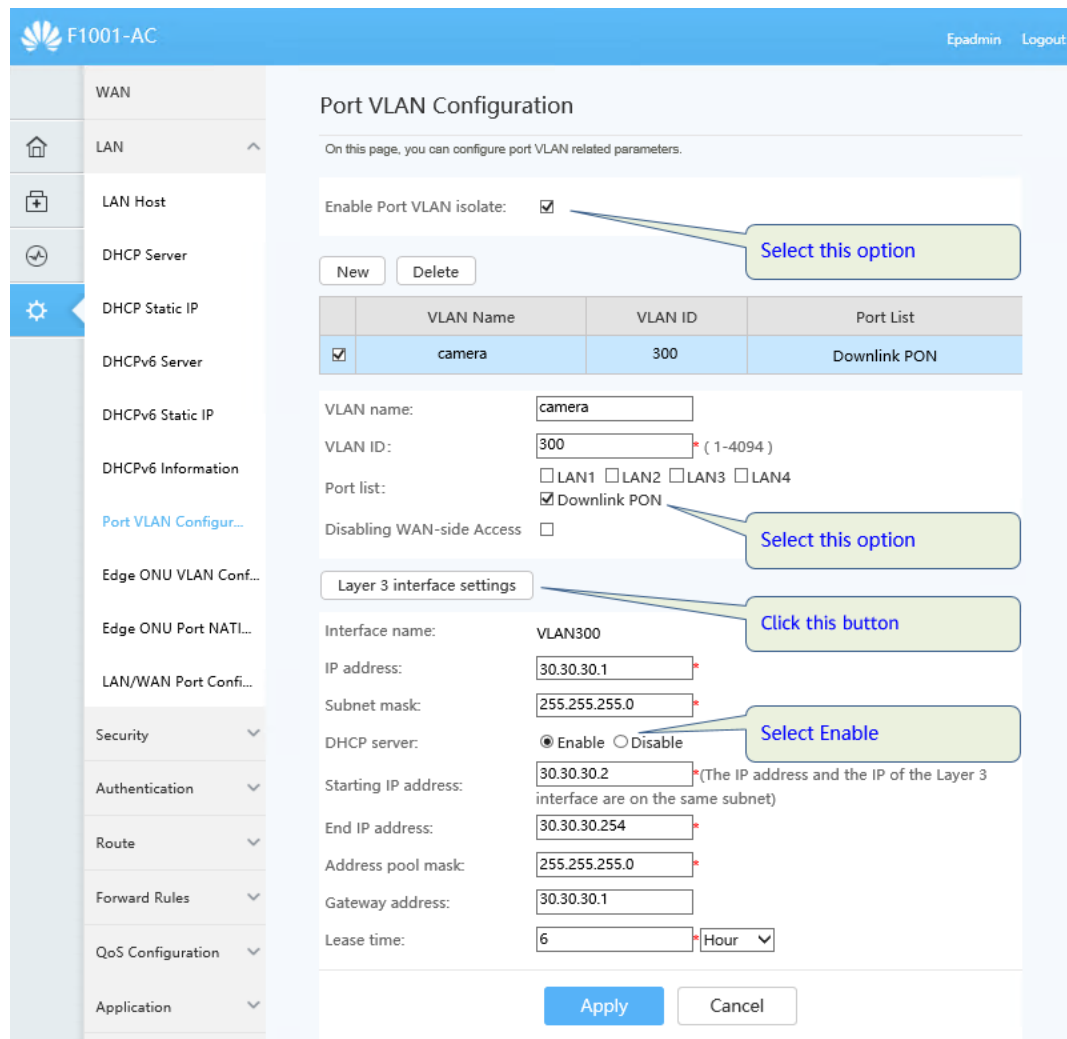
The video backhaul service and Internet service use the same WAN port. If the WAN port has been configured when the Internet service is configured, you do not need to configure the WAN port again.

#### Step 2 Configure the Port VLAN.

Choose **Advanced > LAN > Port VLAN Configuration**. In the right pane, perform the following operations:

- Select **Enable Port VLAN isolation**.
- Click **Create** to create a video backhaul service VLAN. Set **VLAN name** to the camera. Set **VLAN ID** to 300. Select the downstream PON port in the **Port List** area.
- Select the video backhaul service VLAN, click **Layer 3 interface settings**, and set the IP address and subnet mask of the L3 interface of VLAN 300.
- Select **Enable DHCP Server** and configure the DHCP address pool for video backhaul.

After the configuration is complete, click **Apply**.

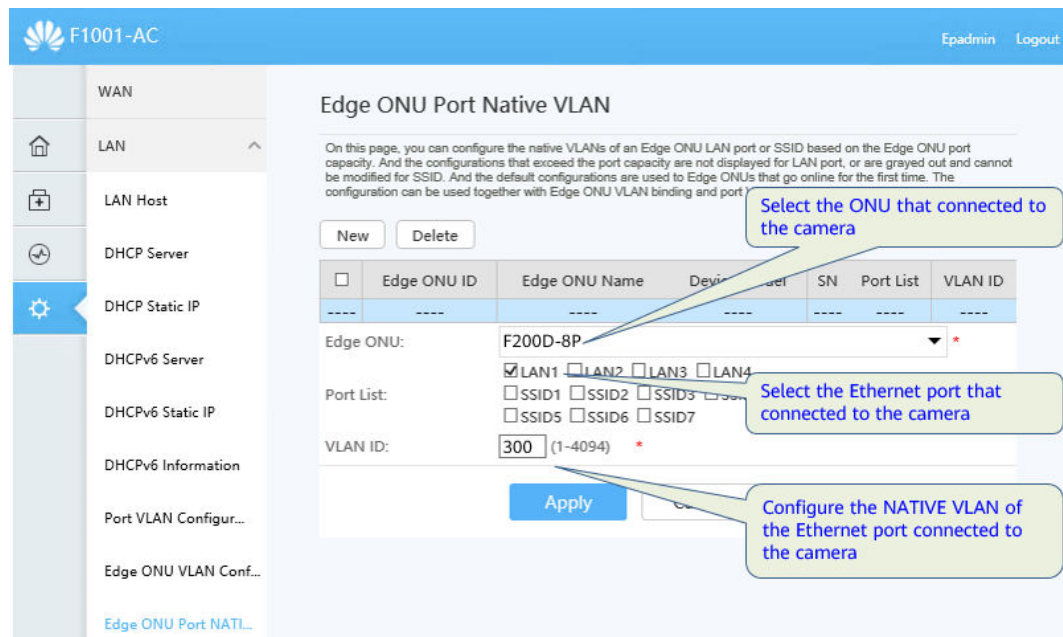


**Step 3** Configure the NATIVE VLAN for Ethernet ports 1 and 2 of ONU2 that are connected to cameras.

Choose **Advanced > LAN > Edge ONU Port NATIVE VLAN Configuration**. In the right pane, perform the following operations:

- Select Edge ONU from the drop-down list box, that is, ONU2 for accessing video backhaul services.
- Select Ethernet port 1 and Ethernet port 2 in the **Port List** area, that is, the Ethernet port used to access the camera.
- Enter the VLAN ID, that is, VLAN 300 planned for the video surveillance service.

After the configuration is complete, click **Apply**.



**Step 4** The configuration is complete.

----End

## 8.4.6 Configuring the IPTV Service

### Configuration Process

**Table 8-7** Process of configuring the IPTV service

Step No.	Configuration Item	Description
Step 1	Configuring WAN	An independent WAN is required for IPTV services to connect to the IPTV server
Step 2	Configuring Multicast Parameters	-
Step 3	Configuring the ONU VLAN binding	-
Step 4	Configuring the NATIVE VLAN of the Ethernet port connecting the ONU to the TV	-

### Configuration Procedure

**Step 1** Configure the WAN.

Choose **Advanced** > **WAN**. In the navigation tree on the left, choose **WAN Configuration**. In the right pane, click **New**. In the displayed dialog box, set parameters based on the data plan.

- Encapsulation type: IPoE
- Protocol type: IPv4
- WAN Type: Bridge WAN
- Service type: IPTV
- Enable VLAN: Enabled
- VLAN ID:400
- Multicast VLAN: 400

After the configuration is complete, click **Apply**.

### WAN Configuration

On this page, you can set WAN port parameters. A gateway communicates with an upper-layer device using the WAN port. During the communication, WAN port parameters must be consistent with upper-layer device parameters.

	Connection Name	VLAN/Priority	Protocol Type
<input type="checkbox"/>	1_INTERNET_R_VID_	-/-	IPv4
----	----	----	----

#### Basic Information

Enable WAN:

Encapsulation Mode:  IPoE  PPPoE

Protocol Type:

WAN Mode:  Select Bridged WAN

Service Type:  Select IPTV

Enable VLAN:

VLAN ID:  \*(1-4094)

802.1p Policy:

802.1p:

Binding Options:  LAN1  LAN2  LAN3  LAN4

Downlink PON Binding:

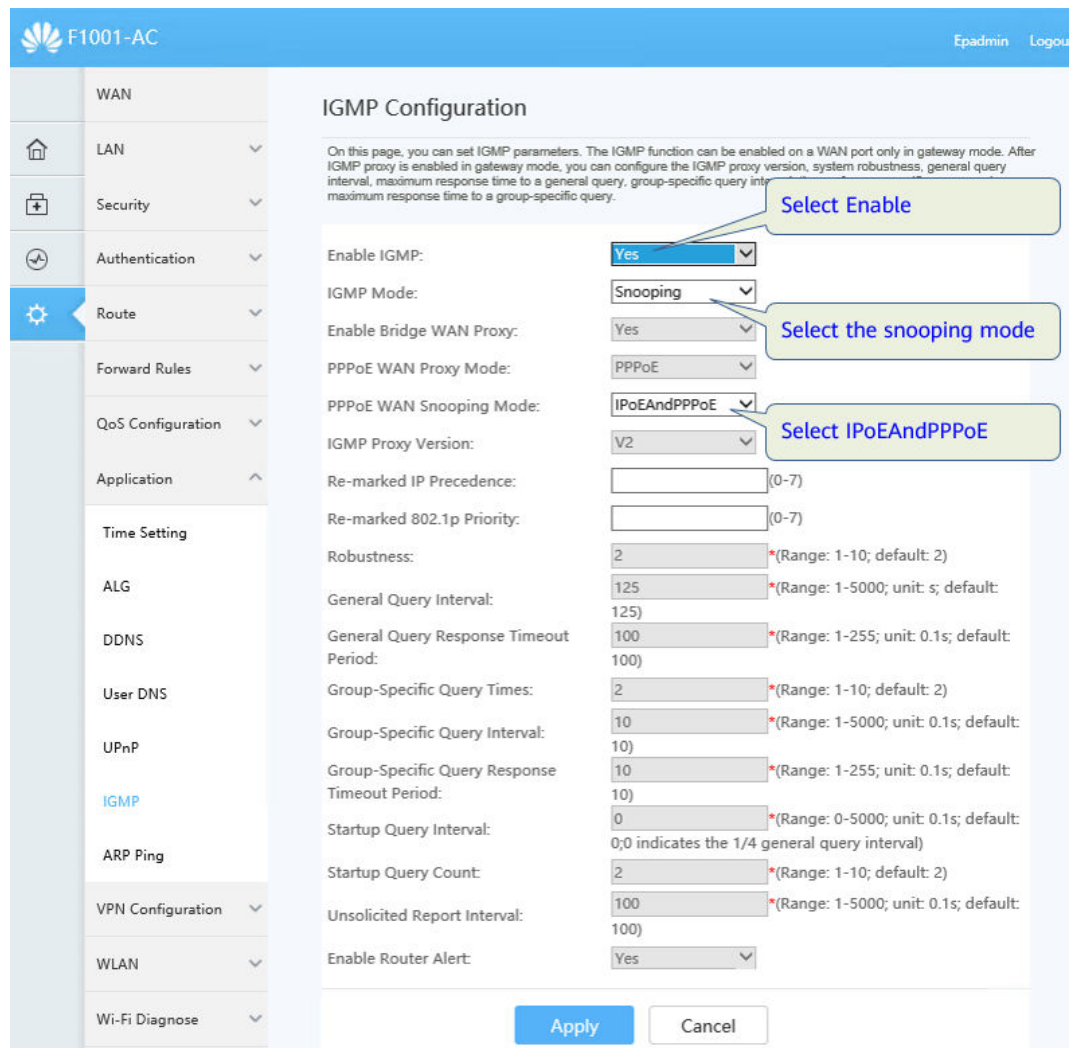
#### IPv4 Information

Multicast VLAN ID:  (0-4094; 0 indicates untagged VLAN.) Configuring a Multicast VLAN

**Step 2** Configure multicast parameters.

Choose **Advanced > Application > IGMP**. In the right pane, perform the following operations:

- Enable IGMP: **Enable**
- IGMP Mode: **snooping**
- After the configuration is complete, click **Apply**.



**Step 3** Configure the ONU VLAN binding.

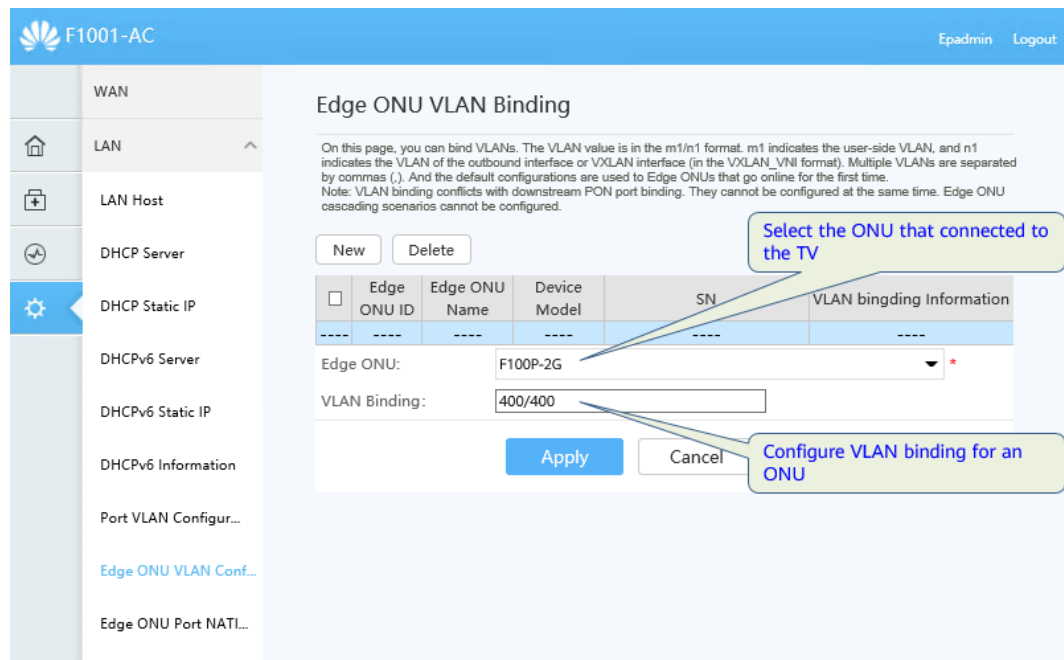
Choose **Advanced > LAN > Edge ONU VLAN Configuration**. In the right pane, perform the following operations:

Click **New**. Configure VLAN binding according to the data plan.

Select the ONU that connected to the TV.

Configure VLAN binding for the ONU.

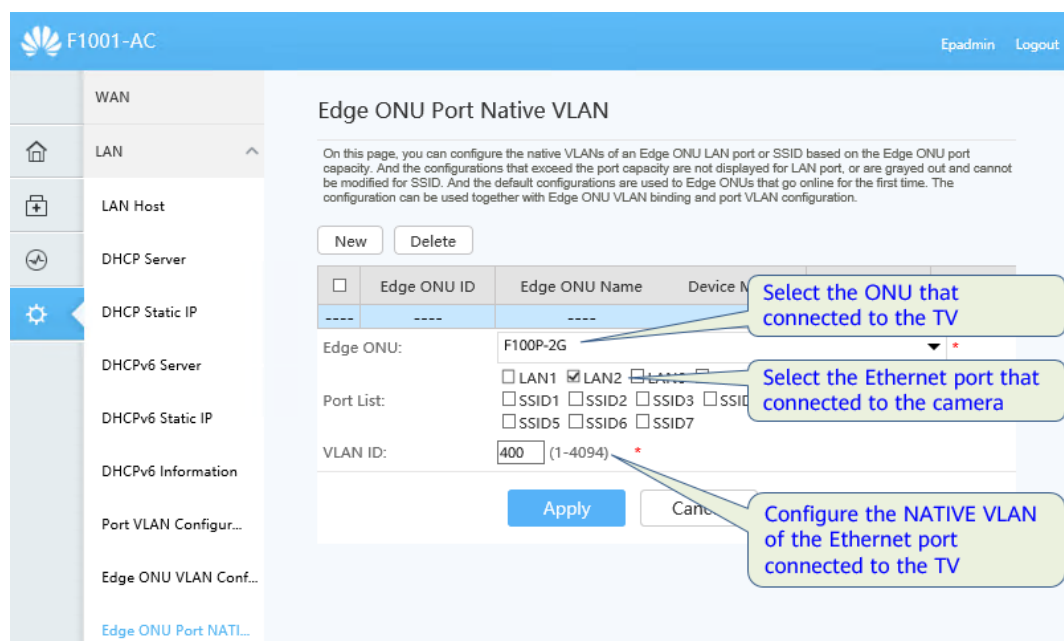
After the configuration is complete, click **Apply**.



**Step 4** Configure the NATIVE VLAN of the Ethernet port connecting the ONU to the TV.

Choose **Advanced > LAN > Edge ONU Port NATIVE VLAN Configuration**. In the right pane, perform the following operations:

- Select **Edge ONU** from the drop-down list box, that is, ONU1 used to access IPTV services.
- Select Ethernet port 2 in the **Port List** area, that is, the network port used to access the IPTV.
- Enter the **VLAN ID**, that is, VLAN 400 planned for the IPTV service.
- After the configuration is complete, click **Apply**.





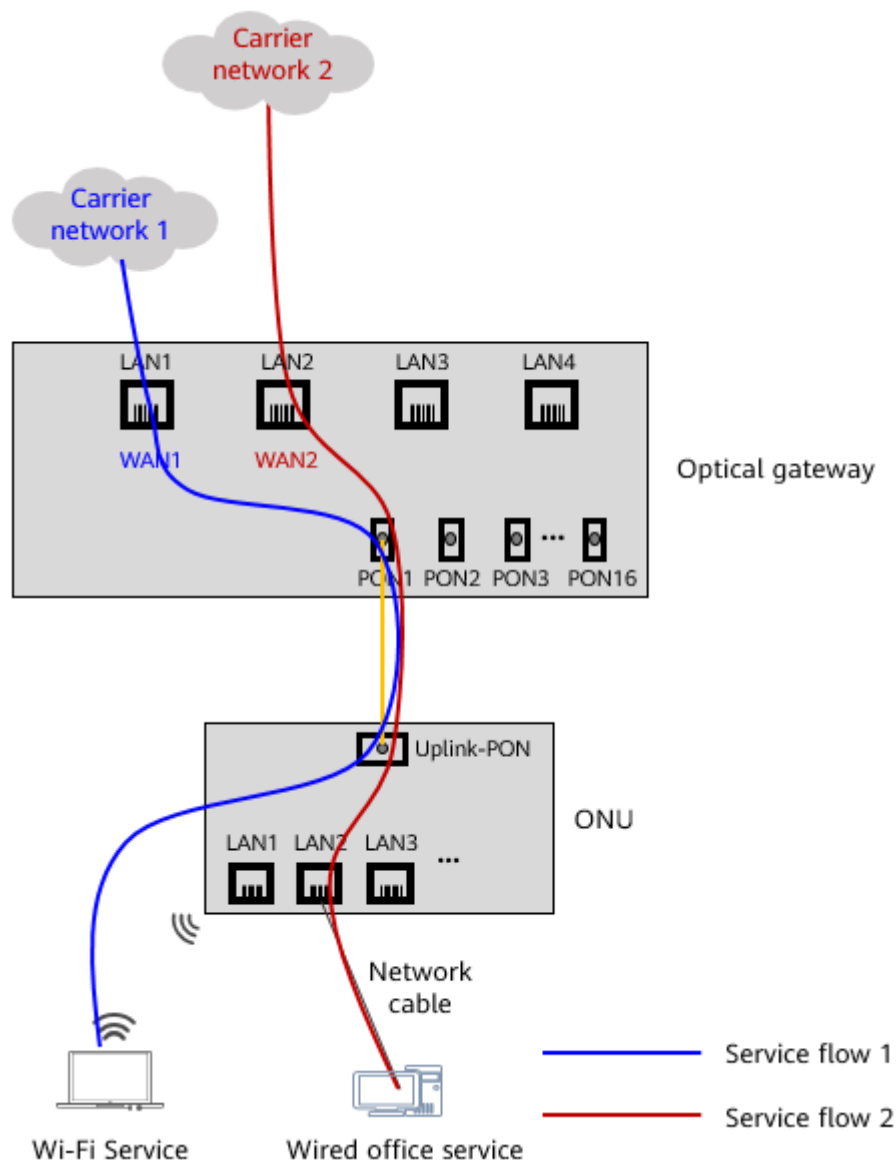
**Step 5** The configuration is complete.

----End

## 8.4.7 Configuring Multi-LAN/WAN Upstream Transmission

### What Is Multi-LAN/WAN Upstream Transmission?

To connect to different networks through different LAN ports and use different WAN ports for upstream transmission, use the multi-LAN/WAN upstream transmission function. Multiple LAN/WAN uplinks can carry different services through different upstream ports, fully utilizing the network bandwidth.



## Data Planning

**Table 8-8** Example of multi-LAN/WAN upstream data planning

Service	Upstream port	WAN	Network
Wi-Fi Service	LAN1 <b>NOTE</b> The default upstream port is LAN1.	WAN1: No configuration is required. By default, the WAN port meets the requirements and can be used directly. <ul style="list-style-type: none"><li>• Encapsulation type: IPoE</li><li>• Protocol type: IPv4</li><li>• WAN type: route WAN</li><li>• Service type: INTERNET</li><li>• IP address obtaining mode: DHCP</li></ul>	Network 1: carrier 1
Wired office Service	LAN2	WAN2: Need to create <ul style="list-style-type: none"><li>• Encapsulation type: IPoE</li><li>• Protocol type: IPv4</li><li>• WAN type: route WAN</li><li>• Service type: INTERNET</li><li>• IP address obtaining mode: DHCP</li></ul>	Network 2: carrier 2

## Configuration Process

**Table 8-9** Process of configuring the multi-LAN/WAN upstream service

Step No.	Configuration Item	Description
Step 1	Configuring LAN upstream port	Configure LAN1 and LAN2 as upstream ports according to the data plan
Step 2	Configuring WAN	Configure WAN1 and WAN2 according to the data plan
Step 3	(Optional) Configure the route load balancing	Determine whether to configure it based on service requirements
Step 4	(Optional) Configure the policy-based routing	Determine whether to configure it based on service requirements

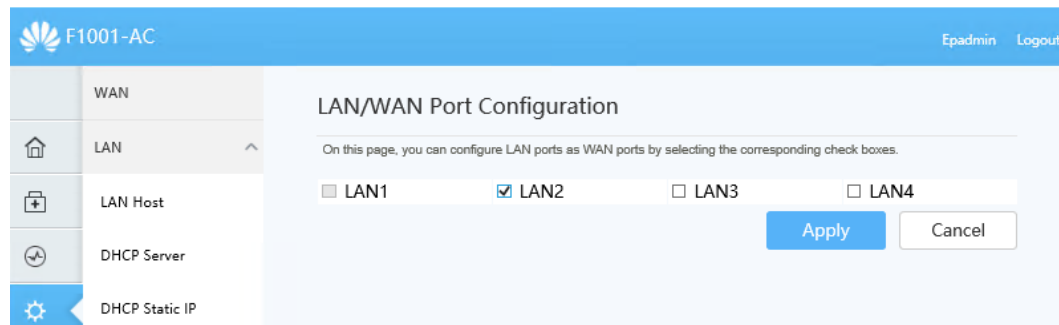
## Configuration Procedure

**Step 1** Configuring LAN upstream port.

Choose **Advanced > LAN > LAN/WAN Port Configuration**. In the pane on the right, configure the LAN port as the upstream port.

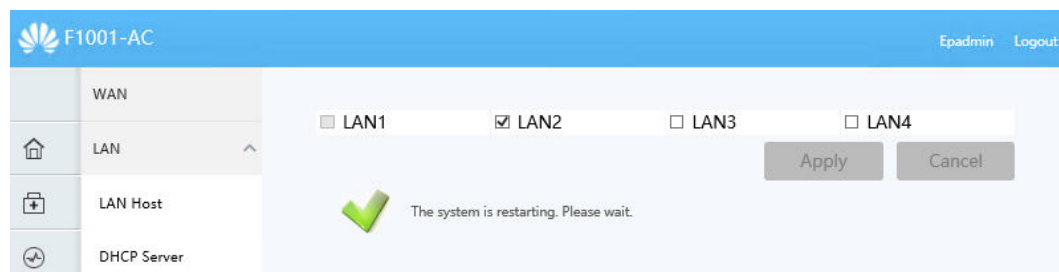
LAN1 is the default upstream port. You do not need to select LAN1. You only need to select LAN2.

After the configuration is complete, click **Apply**.



### CAUTION

- Select the LAN/WAN upstream port and click Apply. The system will restart, which will interrupt services. Exercise caution when performing this operation.
- After the system is restarted, LAN1 and LAN2 become uplink ports. The WAN-side HTTPS access control function is disabled by default. Therefore, the web interface cannot be accessed locally through LAN1 and LAN2, and the web interface that has been connected will be interrupted.



## Step 2 Configure the WAN.

Configure WAN1 and WAN2 according to the data plan.

1. Configure the WAN1.

### NOTE

No configuration is required. By default, the WAN port meets the requirements and can be used directly.

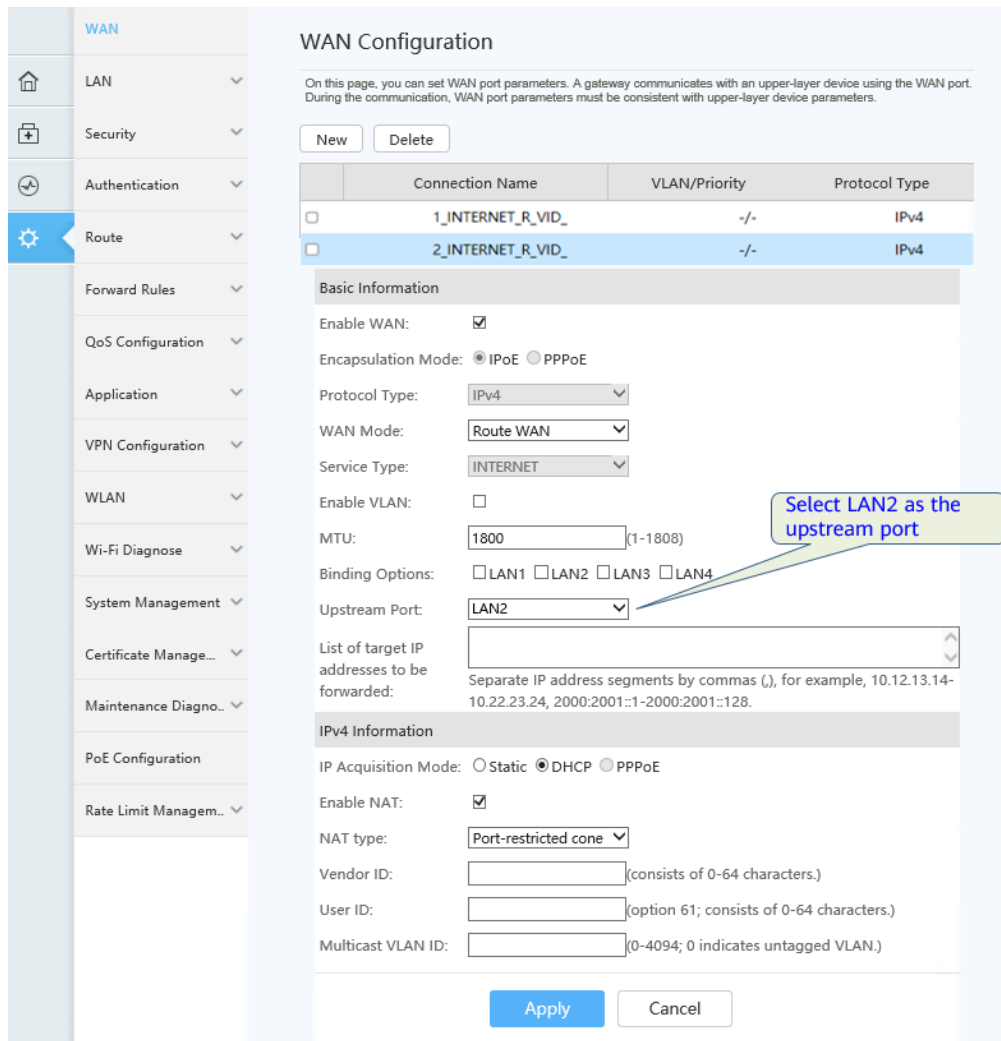
2. Configure the WAN2.

Choose **Advanced > WAN**. In the right pane, click **New**. In the displayed dialog box, set parameters based on the data plan.

- Service Type: INTERNET
- WAN Mode: Route WAN

– Upstream Port: LAN2

After the configuration is complete, click **Apply**.



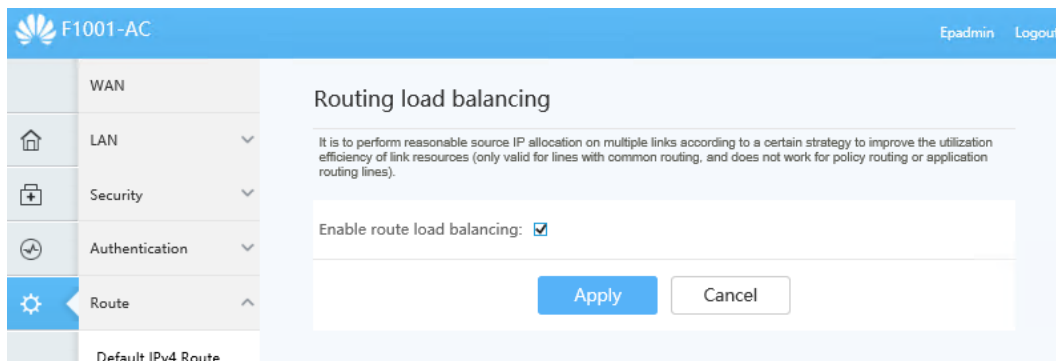
**Step 3** (Optional) Configure the route load balancing.

**NOTE**

Route load balancing can be configured only when the following conditions are met:

- The WAN service type is **INTERNET**.
- The WAN type is **Route WAN**.

Choose **Advanced > Route > Routing Load Sharing**. In the pane on the right, set to enable route load balancing.



After the configuration is complete, click **Apply**.

**Step 4** (Optional) Configure the policy-based routing.

Choose **Advanced > Route > IPv4 Policy-based Routing**. In the pane on the right, select "IP", click New. In the dialog box that is displayed, set policy-based routing parameters.

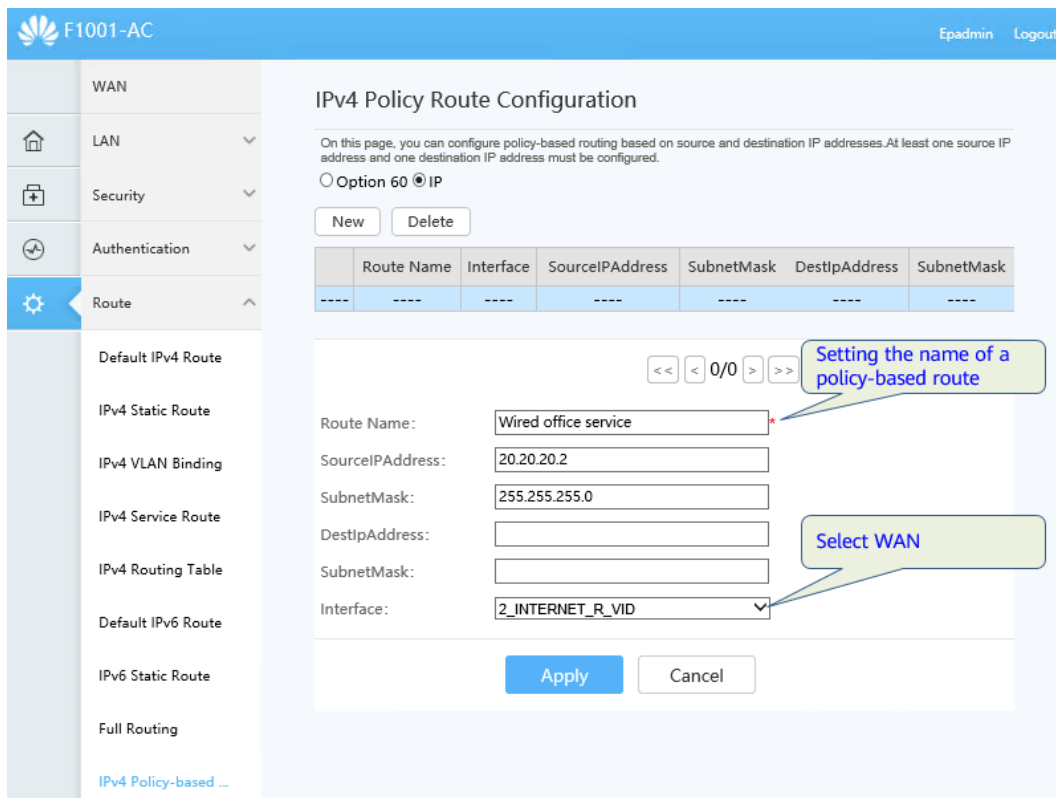
**NOTE**

Policy-based routing can be configured only when the following conditions are met:

- The WAN service type is **INTERNET**.
- The WAN type is **Route WAN**.

For example, configure a policy-based route to enable wired office services to be transmitted upstream through WAN2.

- Route name: Wired office service
- Wired office service IP address segment: 20.20.20.2-20.20.20.254
- WAN2 Name: 2\_INTERNET\_R\_VID



After the configuration is complete, click **Apply**.

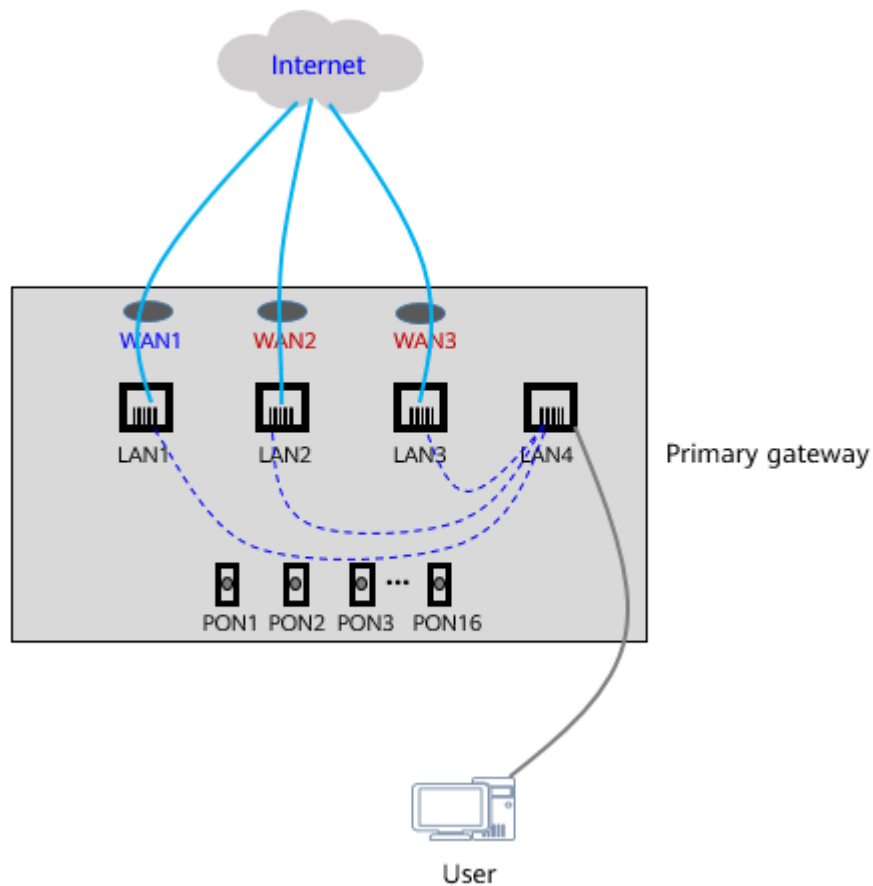
**Step 5** The configuration is complete.

----End

## Multi-WAN, Route load balancing and Policy-based routing

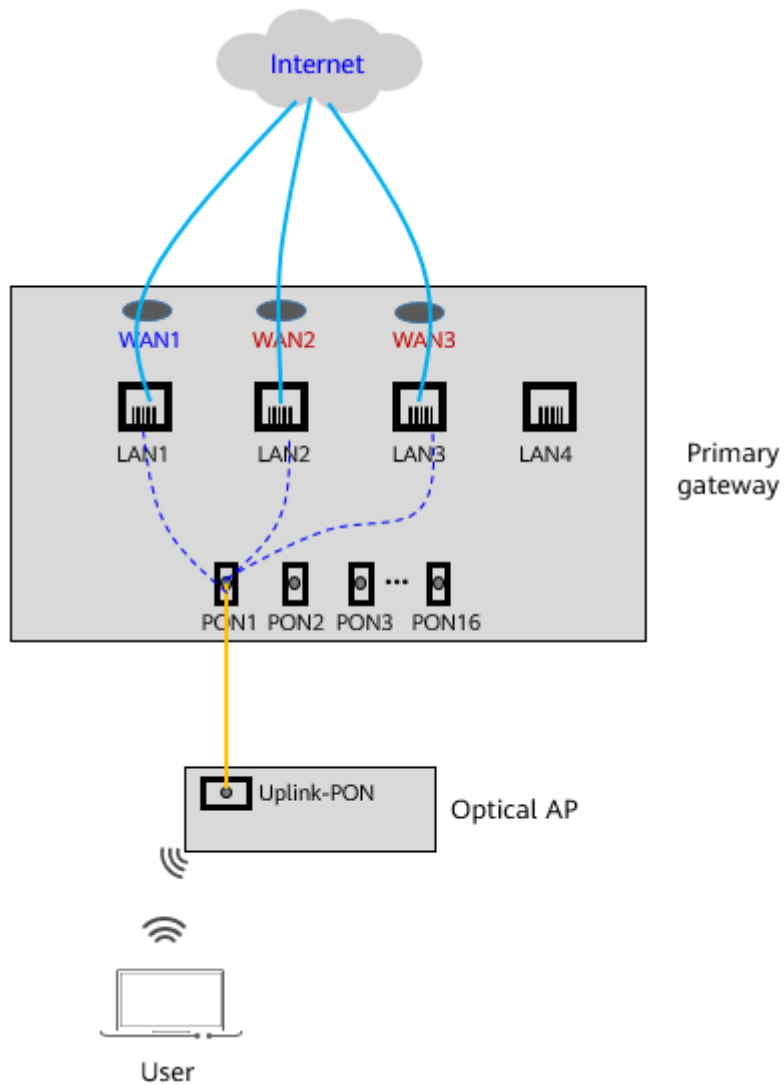
Assume that WAN1 upstream ports LAN1, WAN2 upstream ports LAN2, WAN3 upstream ports LAN3, and LAN4 are user-side ports. The impact on services is as follows:

**Scenario 1: Users access the network through LAN4.**



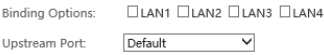
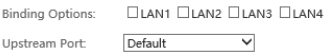
Route load balancing	Policy-based routing	WAN Configuration	Service Impact
Enable	Not configured	<ul style="list-style-type: none"> <li>● Binding Options: LAN4</li> <li>● Upstream Port: LAN1</li> </ul> <p>Binding Options: <input type="checkbox"/> LAN1 <input type="checkbox"/> LAN2 <input type="checkbox"/> LAN3 <input checked="" type="checkbox"/> LAN4</p> <p>Upstream Port: <input type="text" value="Default"/></p>	<p>When the upstream port LAN1 is faulty, the system cannot perform WAN switchover through route load balancing because the binding option LAN4 is selected. As a result, services are interrupted.</p>
Enable	Not configured	<ul style="list-style-type: none"> <li>● Binding Options: None</li> <li>● Upstream Port: LAN1</li> </ul> <p>Binding Options: <input type="checkbox"/> LAN1 <input type="checkbox"/> LAN2 <input type="checkbox"/> LAN3 <input type="checkbox"/> LAN4</p> <p>Upstream Port: <input type="text" value="Default"/></p>	<p>When the upstream port LAN1 is faulty, route load balancing is enabled. Services are switched from WAN1 to WAN2/WAN3 through route load balancing. After the switchover, services are normal.</p>

**Scenario 2: Users access the network through Wi-Fi.**



Route load balancing	Policy-based routing	WAN Configuration	Service Impact
Enable	Not configured	<ul style="list-style-type: none"> <li>Binding Options: None</li> <li>Upstream Port: LAN1</li> </ul> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;">                     Binding Options: <input type="checkbox"/> LAN1 <input type="checkbox"/> LAN2 <input type="checkbox"/> LAN3 <input type="checkbox"/> LAN4                      Upstream Port: <input type="text" value="Default"/> </div>	When the upstream port LAN1 is faulty, route load balancing is enabled. Services are switched from WAN1 to WAN2/WAN3 through route load balancing. After the switchover, services are normal.



Route load balancing	Policy-based routing	WAN Configuration	Service Impact
Enable	Configured Select WAN1 as the outbound interface of the policy-based route.	<ul style="list-style-type: none"> <li>● Binding Options: None</li> <li>● Upstream Port: LAN1</li> </ul> 	<p>The priority of policy-based routing is higher than that of route load, and the outbound interface of policy-based routing is WAN1.</p> <p>Therefore, when the upstream port LAN1 is faulty, the route load balancing function is disabled, the services are interrupted.</p>
Disable	Configured Select WAN1 as the outbound interface of the policy-based route.	<ul style="list-style-type: none"> <li>● Binding Options: None</li> <li>● Upstream Port: LAN1</li> </ul> 	<p>Because load balancing is disabled and the outbound interface of the policy-based route is WAN1. Therefore, services are interrupted when the upstream port LAN1 is faulty.</p>

## 8.4.8 Configuring Portal Authentication

### Configuration Process

**Table 8-10** Portal authentication configuration process

Step No.	Configuration Item	Description
Step 1	Configure a QoS profile	The QoS profile is the traffic profile bound to portal authentication.
Step 2	Customizing the Portal Authentication Page	Customize a personalized authentication page.
Step 3	Configuring the Portal Authentication Mode and Parameters	-

## Configuration Procedure

### Step 1 Configure a QoS profile.

The QoS profile can be used to set the upstream rate limit and downstream rate limit, which are invoked during Portal authentication.

In the navigation tree on the left, choose **Advanced > Authentication > User QoS**. In the pane on the right, click **New**. In the dialog box that is displayed, you can configure the QoS template.

After the configuration is complete, click **Apply**.

QoS Template

On this page, you can configure user QoS rate limit templates.

[Configure QoS parameters](#)

<input type="checkbox"/>	Template Name	Uplink Rate Limit (Unit: Mbps)	Downlink Rate Limit (Unit: Mbps)
--	--	--	--

Template Name:  \*

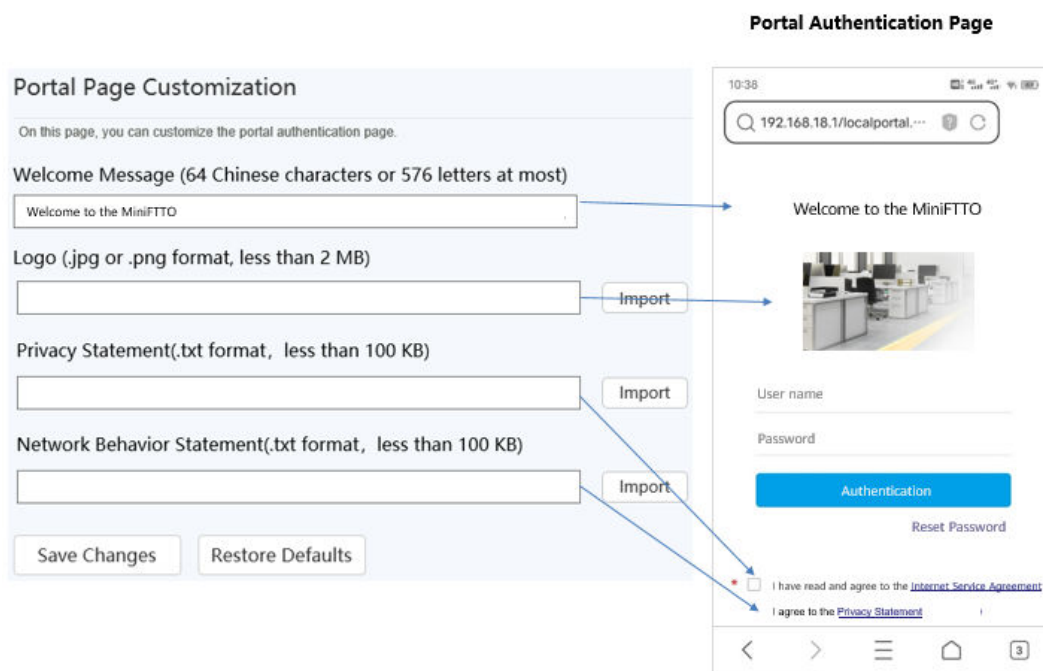
1. Length: 1-64; 2. Special characters (, "\=--+@) are not allowed.

Uplink Rate Limit:  \* (Unit: Mbps)

Downlink Rate Limit:  \* (Unit: Mbps)

### Step 2 Customizing the Portal Authentication Page.

In the navigation tree on the left, choose **Advanced > Authentication > Portal Page Customization**. In the pane on the right, click **New**. In the dialog box that is displayed, you can customize the portal authentication page.



**Step 3** Configuring the Portal Authentication Mode and Parameters.

In the navigation tree on the left, choose **Advanced > Authentication > PORTAL Authentication**. In the pane on the right, click **New**. In the dialog box that is displayed, you can configure the portal authentication function.

After the configuration is complete, click **Apply**.

### PORTAL Authentication

On this page, you can configure portal authentication. When a user accesses the portal, a specified authentication page is displayed.

Redirection URL Address:

Save/Apply

### Local Authentication Parameters Configuration

You can import local authentication parameters in batches or export all the parameters to files in strict accordance with the Import Template Format.

User Name:	<input style="width: 90%;" type="text"/> * <small>1. Length: 1-32; 2. Special characters ( , \ = - + @ ) are not allowed.</small>
Password:	<input style="width: 90%;" type="password"/> * <small>1. Length: 8-64; 2. Cannot be the same as the user name; 3. Contains at least two types of the following characters: lowercase letters, uppercase letters, digits, and special characters. ( ~ ! @ # \$ % ^ &amp; * 0 - _ = + [ { } ; : " &lt; . &gt; / ? and space )</small>
Account Type:	<div style="border: 1px solid #ccc; padding: 2px;">Public ▼</div> * <small>Public accounts do not allow individuals to reset their passwords on the authentication page.</small>
Maximum Users:	<input style="width: 90%;" type="text"/> * (1-1000)
Authentication Validation Period:	<input style="width: 90%;" type="text"/> <small>1. Unit: day; 2. Indicates the validity period of authentication-free login. 3. The default value is 7.</small>
Authentication Duration:	<input style="width: 90%;" type="text"/> <small>1. Unit: hour; 2. Indicates the allowed online duration in a day. 3. The default value is 24.</small>
QoS Template:	<div style="border: 1px solid #ccc; padding: 2px;">▼</div>

Apply
Cancel

**Step 4** The configuration is complete.

----End

## 8.5 Service Acceptance

### 8.5.1 Service Acceptance Guide

#### Acceptance Point Selection

Select acceptance sites based on typical application areas, such as conference rooms, office areas, and manager's rooms with high network requirements in office scenarios.

## Wi-Fi test terminal selection

To test the Wi-Fi, use a Wi-Fi 6 terminal. To test the Gbit/s rate, use a Wi-Fi 6 160 MHz terminal.

## 8.5.2 Internet Service Acceptance

### Acceptance Method

- Step 1** Use the speed test app to test the download and upload rates.
- Step 2** Perform the following operations in sequence: browsing web pages, watching videos, playing games online, and downloading or uploading large files.

----End

### Acceptance Criterion

Acceptance Item	Acceptance Criterion
Internet Service	The Internet service is smooth and free of frame freezing. Files can be uploaded and downloaded at a high speed.

## 8.5.3 Camera Service Acceptance

### Acceptance Method

- Step 1** Observe the real-time image of the camera to check whether the image is clear and smooth.

----End

### Acceptance Criterion

Acceptance Item	Acceptance Criterion
Camera Service	The service image of the camera is clear without artifacts or black screen.

## 8.5.4 Wi-Fi Speed Acceptance

### Acceptance Method

- Step 1** Open the speed test app on the mobile phone within 3 to 5 meters away from the AP without obstacles.

**Figure 8-1** Test position diagram

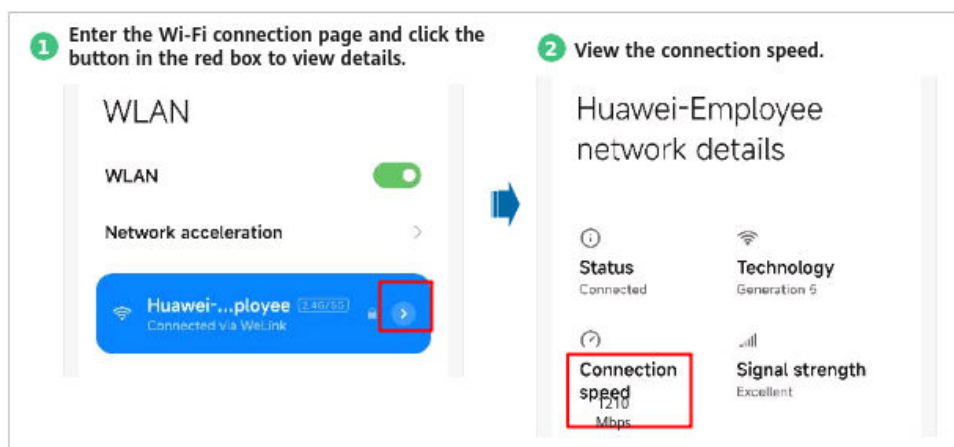


**Step 2** View and record the Wi-Fi download speed, upload speed, latency, and signal strength.

**NOTICE**

1. The following conditions must be met during the speed test:
  - Terminals that support Wi-Fi 6 must be used in the test.
  - During the speed test, the mobile phone must be connected to the 5G Wi-Fi SSID.
  - To verify the gigabit speed, use a terminal that supports Wi-Fi 6 160 MHz. In addition, the negotiated speed (connection speed shown in **Figure2 Checking the negotiated speed**) must be greater than 1201 Mbit/s, which can be viewed in the Wi-Fi details on the mobile phone.

**Figure 8-2** Checking the negotiated speed



- During the speed test, the Wi-Fi signal bars are full.
  - The frequency bandwidth of the optical AP is set to 160 MHz.
2. During the test, ensure that no other terminal is connected to the Wi-Fi network to run services.

----End

### Acceptance Criterion

Acceptance Item	Acceptance Criterion
Wi-Fi Speed	Tested Wi-Fi download and upload rates reach 95% of the expected rates.

## 8.5.5 Wi-Fi Coverage Acceptance

### Acceptance Method

- Step 1** Select an acceptance site (such as a conference room, office area, or manager's room) based on the typical application area, open the test app, and record the signal strength data at the current location.

**Step 2** Repeat **Step 1** for all other points.

----End

### Acceptance Criterion

Acceptance Item	Acceptance Criterion
Wi-Fi Coverage	Wi-Fi coverage has no blind spots and good signal strength.

## 8.5.6 Wi-Fi Roaming Acceptance

### Acceptance Method

- Step 1** Start the roaming test using the test app. Move the test terminal between different optical APs. Record the test data after the test.
- Step 2** When watching a short video or live broadcast, making a WeChat video call, or enabling a game, walk among multiple optical APs and check whether frame freezing affects service experience.

---

**NOTICE**

1. The test must be performed in the network of the same optical gateway.
  2. Ensure that the performance of the phone is stable. Otherwise, the test result is affected by performance problems.
- 

----End

### Acceptance Criterion

Acceptance Item	Acceptance Criterion
Wi-Fi Roaming	When roaming occurs, services such as short video, live broadcast, video call, and game run smoothly without obvious frame freezing.



# 9 Troubleshooting Guide

---

[9.1 Troubleshooting Precautions](#)

[9.2 Frequently Used Methods for Troubleshooting](#)

[9.3 Optical Power Exception Handling](#)

[9.4 Troubleshooting Common Service Faults](#)

## 9.1 Troubleshooting Precautions

Before locating and rectifying faults, read and comply with the following precautions:

- Strictly follow the regulations on operations and industry safety to prevent personal injury and equipment damage.
- When replacing and maintaining parts of equipment, take antistatic measures (for example, wear the ESD wrist strap).
- When any problem occurs during the troubleshooting, record the original information in detail.
- Make a record when performing significant operations (for example, restarting the device or erasing the database). Before such significant operations are performed by qualified engineers, check whether these operations are feasible and at the same time carry out the backup and work out contingency and security measures.
- To improve troubleshooting efficiency, make the following preparations before a fault occurs on the device:
  - Get ready the information about physical connections of the on-site devices.
  - Make a table containing information (including VLAN, IP address, interconnected port ID, and firewall configurations) about the communications, interconnection, and rights of parts and devices.
  - Make on-site part/device archives where the software and hardware configurations, the software and hardware versions, and the change information are recorded.
  - Periodically maintain the backup device to ensure that its hardware configuration, software version, and parameters are the same as the

working device running over the existing network. In this way, when the working device is faulty in an emergency, the faulty device can be replaced with the backup device quickly.

## 9.2 Frequently Used Methods for Troubleshooting

There are various of methods for fault location. In fault location, different methods are used together. Therefore, mastering and using these methods are important for improving the efficiency of troubleshooting.

To improve fault location efficiency, follow the principles of from external to internal and from large to small. Specifically, check whether the connection of external cables is reliable and whether the indicators are normal, check the running status of the system through the console, and check the running status of each module.

Table 1 lists the frequently used methods for locating a fault.

**Table 9-1** Troubleshooting procedure

Troubleshooting Procedure	Frequently Used Methods	Other Methods
Troubleshoot an external device fault	<ul style="list-style-type: none"><li>• Comparison analysis</li><li>• Interchange analysis</li><li>• Meter test</li><li>• Protocol analysis</li></ul>	<ul style="list-style-type: none"><li>• Alarm analysis</li><li>• Performance analysis</li></ul>
Locate a fault to a specified device	<ul style="list-style-type: none"><li>• Exclusive method</li><li>• Configuration data analysis</li></ul>	<ul style="list-style-type: none"><li>• Alarm analysis</li><li>• Performance analysis</li></ul>
Locate a fault to a board	<ul style="list-style-type: none"><li>• Exclusive method</li><li>• Interchange analysis</li><li>• Meter test</li></ul>	Protocol analysis

### Configuration Data Analysis

Incorrect re-configurations and expansion configurations, and outstanding problems of existing configurations are possible causes of a fault. Therefore, when locating and troubleshooting a fault, analyze the configuration data. Maintenance engineers need to master configuration methods and implementation principles of different services and functions to check the configuration data for different faults and to improve troubleshooting efficiency.

### Alarm Analysis

Causes of certain faults can be found by analyzing alarms, or a fault can be located using alarm analysis together with other methods.

An alarm is an important message when a fault or an event occurs. The alarm information includes the detailed description and the possible cause of a fault or

an abnormality, and the troubleshooting advice. The information also involves aspects such as the hardware, link, service, and CPU usage. The volume of the alarm information is large and complete, which is the important basis for fault analysis and location.

When a fault occurs in the system, check whether an alarm is generated in the system. If an alarm is generated, analyze the alarm associated with the fault, and clear the alarm to rectify the fault by referring to Alarm Reference.

### Comparison Analysis

Comparison analysis compares the faulty components or symptoms with the normal components or symptoms, and find out differences, to locate the fault. For example, compare line parameters of faulty services with line parameters of normal services, or compare devices at the same network layer. Comparison analysis applies to faults that are caused by a single factor.

### Interchange Analysis

When a fault cannot be located after the faulty parts are replaced, maintenance engineers can locate and troubleshoot the fault using the interchange analysis.

Interchange is to interchange the parts that may be faulty with normal parts (such as boards and cables), and compare the running conditions to locate the faults.

Before interchange parts, ensure that the versions of the parts are the same or compatible. It is recommended that you interchange the parts of the same type and version.

#### NOTE

The interchange operation is risky to certain extent. For example, when users install the short-circuited board in a normal running subrack, the subrack is damaged. Therefore, to prevent another fault from occurring, exercise caution when using the interchange analysis.

### Exclusive Method

When a fault is complicated and involves multiple stages, maintenance engineers can locate the fault using the exclusive method to exclude the normal stages.

To use the exclusive method, maintenance engineers must know stages where the fault may occur, and use applicable methods (such as loopback and configuration data analysis) to locate the fault. Therefore, maintenance engineers must be familiar with the following information:

- System structure and working principles of the device
- Stages where the fault may occur
- Fault diagnosis operations, such as loopback and configuration data analysis
- Usage of testers

#### NOTE

The exclusive method involves all the stages on the entire network. It is recommended that maintenance engineers exclude normal stages in the following principle: remote end first and local end, major cause first and the minor cause, simpleness first and then complication. This reduces troubleshooting cost and improves troubleshooting efficiency.

### Protocol Analysis

Protocol analysis locates and troubleshoots a fault when the device is improperly interconnected with the upper layer device.

Protocol analysis indicates the method for analyzing a fault by tracing the signaling and capturing the packets. To use the protocol analysis method, maintenance engineers must be familiar with the related protocols and the exchange process for packets so that they can locate the fault based on the obtained packets.

For example, a user fails to order multicast programs. After the packets are captured and analyzed, it is found that the BRAS discards the Internet Group Management Protocol (IGMP) packets sent from the user.

### **Meter Test**

Meter test method locates and troubleshoots a fault by comparing the actual values of performance parameters tested by various instruments and meters with the correct values. Instruments and meters directly indicate the running status of the device through visual and quantitative data.

The following instruments and meters are frequently used for troubleshooting:

- Multimeter
- Line tester
- Optical power meter
- Optical attenuator

### **Performance Analysis**

Performance analysis uses the performance statistics provided by the device to analyze the performance indexes of the faulty service to locate the fault.

Maintenance engineers must query different performance statistics to locate different faults and therefore they must be familiar with the following information:

- System structure and operation mechanism
- Statistics provided by the system
- Method of querying and analyzing the statistics

## **9.3 Optical Power Exception Handling**

Checking the optical power is one of the most common methods for troubleshooting optical fiber networks. By checking and analyzing the upstream and downstream optical power, you can determine whether the fiber link quality is normal.

### **9.3.1 Analyze Optical Power**

In optical power analysis, the actual optical attenuation is compared with the theoretical value to determine the quality of the optical line and locate the abnormal attenuation point in the optical line.

In normal cases, the actual optical attenuation is close to the theoretical value. If the actual attenuation is much greater than the theoretical attenuation, there are abnormal attenuation points on the fiber link.

The theoretical values of optical attenuation are shown in Table 3-1. [Table 9-2](#)

**Table 9-2** Theoretical optical attenuation

Name	Type	Average Loss (dB)
Connection Point	fusion	≤ 0.1
	Active connector (flanged plate)	≤ 0.3
	Cold/Quick Coupler	≤ 0.5
Optical fiber	1490nm/1577nm (1 km)	≤ 0.23
	1310nm / 1270nm (1 km)	≤ 0.35
Advanced fiber with power	04053088 & 04053162 Indoor Double-End Flat advanced fiber with power	Insertion loss of connector: <ul style="list-style-type: none"> <li>• Insertion loss ≤ 0.50</li> <li>• Return loss ≥ 50</li> </ul> Insertion loss of cable (optical fiber): <ul style="list-style-type: none"> <li>• 1310 nm: 0.35 dB / km</li> <li>• 1550 nm: 0.21 dB / km</li> </ul> Overall insertion loss of the advanced fiber with power = Insertion loss of the connector + Insertion loss of the cable.

Table 3-2 lists the possible fault points and possible causes when the actual optical attenuation value is greater than the theoretical value. [Table 9-3](#)

**Table 9-3** Fault Type

Fault point	Possible Causes
Connection points (cold connection, fusion connection, movable connector, quick connector, etc.)	<ul style="list-style-type: none"> <li>• The fiber cores at both ends of the fiber at the cold or fusion point are not aligned.</li> <li>• Bubbles exist at the fusion point.</li> <li>• The active connector, quick coupler is faulty, or the interface is dirty.</li> </ul>
optical fiber	<ul style="list-style-type: none"> <li>• The end surface of the optical fiber connector is dirty, scratched, or dented.</li> <li>• The optical fiber connector is too tight or loose.</li> <li>• Different types of fiber connectors are interconnected.</li> <li>• The optical fiber is bent.</li> <li>• The optical fiber is damaged.</li> <li>• Multimode fiber is used.</li> </ul>

### 9.3.1.1 Use an Optical Power Meter to Measure the Optical Power

This topic describes how to use an optical power meter to measure the optical power.

#### Prerequisites

- The device has been powered on.
- The laser on the optical port is turned on.

#### Tools, Instruments and Materials

- The length of the fiber jumper is less than 1 m. It is recommended that new fiber jumpers be used.
- Optical power meter.

#### Impact on the System

When the optical power meter is used to measure the downstream optical power, the services carried on the link are interrupted.

#### Precautions

---

**NOTICE**

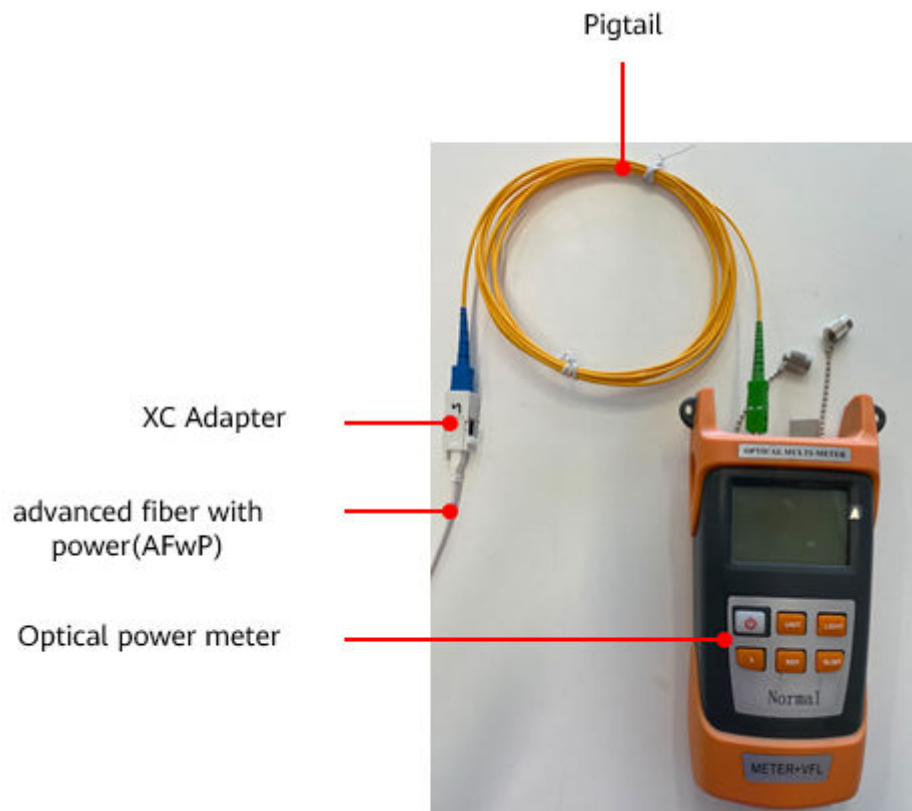
Note that the laser is not visible, which has nothing to do with wearing laser protective glasses. Do not look close to or directly into the laser transmitter port and fiber connector of the optical interface board. Otherwise, the laser can cause damage to the eyes and even lead to blindness. It is prohibited to point bright light against flammable materials.

---

Before and after measuring the optical power, clean the optical interface. If the contaminated fiber is in contact with the normal fiber end face, the normal fiber end face will be contaminated, causing abnormal attenuation and reflection, and affecting the fiber link quality.

#### Procedure

- Step 1** Set the measurement parameters of the optical power meter.
- Step 2** Remove the optical fiber connector from the ONU and connect the optical power meter to the optical fiber connector for measurement.



**NOTE**

advanced fiber with power and leather optical cables have different fiber connectors. Therefore, you need to use an adapter to connect the optical cables.

**Step 3** Check and record the reading of the optical power meter.

**NOTE**

- If the optical power meter jitters within 0.2 dBm, it is normal. In this case, take the average value.
- If the change of the optical power meter exceeds 0.2 dBm, the optical fiber may not be properly connected, the optical fiber may be bent too much, or the connector of the optical fiber may be dirty.
- Do not bend the optical fiber. Otherwise, the test result may be affected.

**Step 4** After the test is complete, remove the optical power meter and reconnect the optical fiber link.

----End

### 9.3.1.2 Querying the Optical Power Through the WebUI

This topic describes how to query the optical power on the WebUI.

#### Prerequisites

- The primary gateway and optical terminal are powered on.
- The laser on the optical port is turned on.

## Procedure

**Step 1** Log in to the device web page.

**Step 2** Queries the optical power.

Choose System Info > Optical Module Info. In the right pane, you can view the transmit optical power and receive optical power of the optical module.

The screenshot shows the 'Optical Information' page in the Huawei MiniFTTO web interface. The page title is 'F1001-AC' and the user is logged in as 'Epadmin'. The left navigation menu is expanded to 'Optical'. The main content area displays 'Optical Information' with a sub-header 'On this page, you can query the status of the optical module.' Below this, there are two tables: 'ONT Information' and 'OLT Information'. A callout box points to the 'ONT Information' table with the text: 'Compare the queried value with the reference value to determine whether the optical power is abnormal.'

	Current Value	Reference Value
Optical Signal Sending Status:	--	Auto
TX Optical Power:	-- dBm	2 to 7 dBm
RX Optical Power:	-- dBm	-28 to -8 dBm
Working Voltage:	3280 mV	3100 to 3500 mV
Bias Current:	0 mA	0 to 90 mA
Working Temperature:	36 °C	-10 to +85 °C

	Current Value	Reference Value
Optical module type:	--	--
Transmit optical power:	-- dBm	--
PON port identifier:	--	--

Compare the query value with the reference value and perform corresponding processing based on the comparison result.

----End

### 9.3.2 Cleaning the Connector of an Optical Fiber

This topic describes how to clean the connector of an optical fiber. Frequent insertion and removal or not taking dustproof treatment for a long time causes the connector to be unclean and deteriorated, which compromises the quality of the line. Therefore, you need to take measures to prevent dust and periodically clean optical fiber connectors, including the connector endface of an optical fiber, optical port of an optical module, and fiber adapter.

#### Prerequisites

Prepare the cleaning tools before cleaning, and follow the instructions in "Precautions".

#### Context

A large number of optical fiber connectors are used in optical transmission, which are easy to be contaminated in OM. The dust particles that can be seen by a microscope affect the quality of optical signals. As a result, the system



performance deteriorates and network stability is affected. For two connected optical components, dust particles may damage the surface of the optical fiber. If the cladding or edge of an optical fiber has dust particles, the cores of two connected optical fibers may not be exactly aligned. As a result, the quality of optical signals is affected.

A 1  $\mu\text{m}$  dust particle on a single-mode optical fiber blocks 1% optical signals and therefore leads to 0.05 dB attenuation loss. A 9  $\mu\text{m}$  dust particle is hard to be seen without a microscope but it completely blocks the core of an optical fiber. Therefore, even an extremely small contaminant that can only be found by an instrument such as a microscope may block the connector of an optical fiber. Besides dust particles, the following contaminants need to be cleaned away:

- Grease (usually brought by hands)
- Condensation residues
- Powder (evaporation residues of water or solvent)

Such contaminants will also damage optical components and are more difficult to clean away than dust particles. To clean optical components, you must follow the corresponding steps.

## Tools and Materials

The following lists commonly used cleaning tools and materials:

- Optical power meter: used for testing whether the laser on the connector of an optical fiber is disabled.
- Lint-free wipe: a piece of long silk cotton specially used for cleaning the connector endfaces of an optical fiber.
- Lint-free swab: used for cleaning the optical port of an optical module, and a fiber adapter. It has two specifications:  $\phi 2.5$  mm and  $\phi 1.25$  mm. You can select one according to the port type (use the lint-free swab with  $\phi 2.5$  mm for the ports of SC and FC types, and use that with  $\phi 1.25$  mm for the ports of LC and MTRJ types).
- Protective cap: used on the connector of an optical fiber, optical port of an optical module, and fiber adapter.
- Cleaning tool box: used for placing lint-free wipes and protective caps. Place lint-free wipes and protective caps separately from other tools.
- Cleaning reagent (alcohol): used for cleaning the connector of an optical fiber. It is flammable and therefore must be safely stored and kept clean.
- Optical fiber endface magnifier: a microscope (400\*) used for checking whether the connector endface of an optical fiber is clean and smooth.

## Impact on the System

An optical module must be powered off before its port is cleaned. In this case, services carried on the optical port will be interrupted.


## Precautions

---

** DANGER**

- Never look into the optical port or the connector of an optical fiber without eye protection. Never put an optical port towards the flammables.
  - Never clean an optical fiber connector when the laser is on.
  - ESD discharge damages the equipment. To remove or insert a pluggable optical module before or after cleaning, wear an ESD wrist strap or ESD gloves.
- 
- Put a protective cap into the cleaning tool box immediately after taking it off. Place unused protective caps in the cleaning tool box, or in the ESD bag for sealed storage. Clean protective caps quarterly (it is recommended to clean them by using an ultrasonic cleaner).
  - Keep your hands clean and dry before cutting a lint-free wipe, and place unused lint-free wipes in the clean ESD bag or the cleaning tool box for sealed storage.
  - After the cleaning, cover the connector of the optical fiber, optical module, and fiber adapter that will not be immediately used with protective caps.

## Procedure

- Clean the connector endface of an optical fiber.
    - a. Power off the laser of the connector before cleaning. Disconnect the optical fiber (at both ends) to be cleaned.
    - b. Use the optical power meter to test the optical power and ensure that no optical signals are sent from the connector of the optical fiber.
    - c. Clip a piece of lint-free wipe into 32 small pieces of the same size.
    - d. Use a dry lint-free wipe (two-layer) to wipe the connector endface of the optical fiber along one direction once. For a seriously contaminated connector, use a lint-free wipe (two-layer) dipped with a little cleaning reagent to wipe the connector endface of the optical fiber along one direction once, and then use a dry lint-free wipe (two-layer) to wipe it along one direction once again for ensuring that the connector endface is dry
-  **NOTE**
- A lint-free wipe can be used only once. Use the portion of the lint-free wipe that is not touched by your hands.
  - You can use the optical fiber end magnifier to check the cleaning and abrasion condition of an optical fiber connector.
- e. After the cleaning, do not touch the connector. Connect the optical fiber (at both ends) immediately. Cover the optical connectors that will not be immediately used with protective caps.
  - f. Power on the laser.
- Clean the optical port of an optical module.
    - a. Power off the laser of the optical module before cleaning. Disconnect the optical fiber (at both ends) from the optical module.

- b. Use the optical power meter to test the optical power and ensure that no optical signals are sent from the port of the optical module.
- c. Wear an ESD wrist strap or ESD gloves to remove a pluggable optical module.
- d. Select lint-free swabs with a suitable diameter according to the type of the optical port. Dip a swab with the cleaning reagent, insert the swab into the inside of the optical port, and then clean it by rotating the swab 360 degrees in one direction along the inner wall of the optical port.

 **NOTE**

The lint-free swab with  $\phi 2.5$  mm is used for the ports of SC and FC types and that with  $\phi 1.25$  mm is used for the ports of LC and MTRJ types.

- e. Insert a dry swab of the same type into the inside of the optical port and clean it by rotating the swab 360 degrees in one direction along the inner wall of the optical port.
- f. After the cleaning, connect the optical fiber (at both ends). Cover the ports of the optical modules that will not be immediately used with protective caps. Wear an ESD wrist strap or ESD gloves to insert a pluggable optical module.
- g. Power on the laser.
- Clean a fiber adapter.
  - a. Power off the laser of the optical port before cleaning. Disconnect the optical fiber (at both ends) from the fiber adapter.
  - b. Use the optical power meter to test the optical power and ensure that no optical signals are sent from the connector of the fiber adapter.
  - c. Select lint-free swabs with a suitable diameter according to the type of the fiber adapter. Dip a swab with the cleaning reagent, insert the swab into the socket inside the fiber adapter, and then clean it by rotating the swab 360 degrees in one direction along the inner wall of the fiber adapter.

 **NOTE**

The lint-free swab with  $\phi 2.5$  mm is used for the ports of SC and FC types and that with  $\phi 1.25$  mm is used for the ports of LC and MTRJ types.

- d. Insert a dry swab of the same type into the socket inside the fiber adapter and clean it by rotating the swab 360 degrees in one direction along the inner wall of the fiber adapter.

 **NOTE**

Use an ultrasonic cleaner to clean fiber adapters when there are a large quantity of them.

- e. After the cleaning, connect the optical fiber (at both ends). Cover the fiber adapters that will not be immediately used with protective caps.
- f. Power on the laser.

----End

### 9.3.3 Checking Whether the Optical Fiber Is Damaged Using the Red Pointer

The red pointer, also called visual fault locating meter or visual fault detector, sends red light to check whether the optical fiber has red light leak to locate the damage point of an optical fiber.

#### Context

You can directly see the position with red light leak by using the red pointer. For onsite observation, it can only be used for locating the damage point of an optical fiber in a short distance.

An optical fiber is generally damaged on the bare fiber, coiled fiber or fusion splicing point.

#### Precautions

---

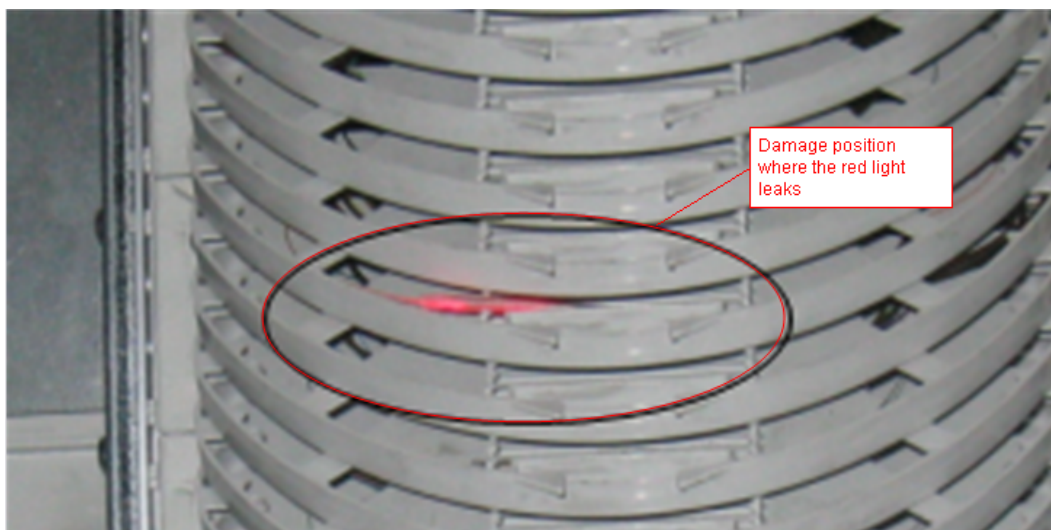
 **DANGER**

Never look directly into the optical fiber connector or the laser transmit port on the optical port board without eye protection. Never put the optical port towards the flammables.

---

#### Procedure

- Step 1** Place the red pointer on the endface of an optical fiber and send red light.
- Step 2** Check whether the optical fiber has red light leak. If the red light leaks, the fiber is damaged.



- Step 3** Replace or re-splice the optical fiber that has red light leak.
  - Replace the optical fiber if its bending is excessively large.

 **NOTE**

The bending diameter of an optical fiber must be longer than 6 cm.

- Splice the optical fiber again if air bubbles exist at the splicing point.

----End

## 9.4 Troubleshooting Common Service Faults

### 9.4.1 Internet Access Failure

Internet access failure means that Internet resources cannot be obtained, for example, web pages cannot be opened or files cannot be downloaded.

To rectify the fault, you can start from the fault scope and preliminarily determine the possible causes of the fault based on the fault scope.

**Table 9-4** Possible Causes for Internet Access Failure

Fault Symptom	Fault Scope	Possible Causes
Only one PC connected to an ONU fails to access the Internet, and other PCs connected to the same ONU can access the Internet normally	User terminal	<ul style="list-style-type: none"><li>• The PC fails to obtain an IP address.</li><li>• Virus in the user PC.</li><li>• The browser on the PC is faulty.</li><li>• The PC runs for a long time, causing slow response.</li><li>• The network adapter of the user PC is abnormal or faulty.</li></ul>
All PCs connected to the same ONU cannot access the Internet, but PCs connected to other ONUs are normal	ONU	<ul style="list-style-type: none"><li>• The WAN port of the ONU is not established.</li><li>• The SSID broadcast function of the ONU is not enabled on the ONU, and Wi-Fi terminals cannot find the SSID.</li><li>• The ONU hardware is abnormal or faulty.</li></ul>
Users connected to all ONUs of the primary gateway cannot access the Internet	Primary gateway	<ul style="list-style-type: none"><li>• The hardware of the primary gateway is abnormal or faulty.</li><li>• The upper-layer network is faulty.</li></ul>

### 9.4.2 Slow Internet Access

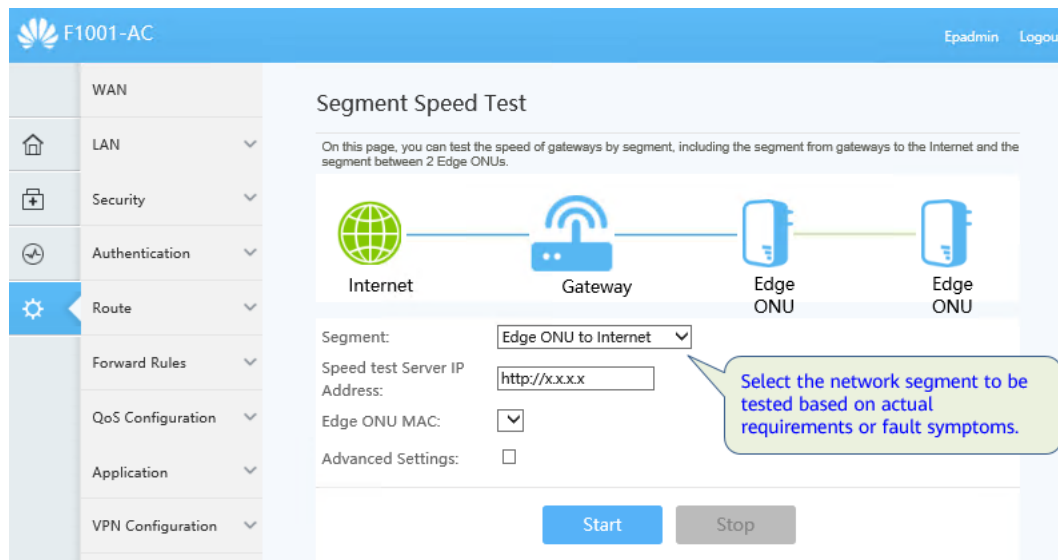
Low Internet access speed indicates that the Internet access speed of a subscriber is much lower than the subscribed Internet access speed.

When the Internet access speed is low, you can perform segment-by-segment speed test to determine the network segment that causes the slow speed.

Currently, segment-by-segment speed test scenarios are as follows:

- Gateway to Internet
- Edge ONU to gateway
- Edge ONU to Internet

Choose **Settings > Maintenance Diagnosis > Segmented Speed Test**. On the right pane, you can perform speed test based on the segmented scenario.



Determine the network segment where the fault occurs based on the segmented speed test result.

**Table 9-5** Locate the fault based on the segmented speed test result.

Network segment	Test Result	Faulty network segment	Possible Causes
Gateway to Internet	Normal	Fault scope from the user terminal to the gateway	<ul style="list-style-type: none"> <li>• The number of STAs that access the network exceeds the upper limit.</li> <li>• Poor Wi-Fi signal</li> <li>• Terminal device fault</li> <li>• The port rate is limited</li> <li>• Fiber network fault</li> </ul>
	Abnormal	The fault range is from the gateway to the Internet	<ul style="list-style-type: none"> <li>• The egress bandwidth is insufficient. A large number of STAs access the network, and congestion occurs</li> <li>• Insufficient subscribed bandwidth</li> <li>• Upper-layer network fault</li> </ul>

Network segment	Test Result	Faulty network segment	Possible Causes
Edge ONU to gateway	Normal	Faults range from the edge ONU to the user terminal and from the gateway to the Internet	<ul style="list-style-type: none"> <li>Poor Wi-Fi signal</li> <li>Terminal device fault</li> <li>The port rate is limited.</li> <li>The egress bandwidth is insufficient. A large number of STAs access the network, and congestion occurs.</li> <li>Insufficient subscribed bandwidth</li> <li>Upper-layer network fault</li> </ul>
	Abnormal	The fault range is from the edge ONU to the gateway	<ul style="list-style-type: none"> <li>Edge ONU Fault</li> <li>Gateway fault</li> <li>Fiber network fault</li> </ul>
Edge ONU to Internet	Normal	The fault range is from the edge ONU to the user terminal	<ul style="list-style-type: none"> <li>Poor Wi-Fi signal</li> <li>Terminal device fault</li> <li>The port rate is limited.</li> <li>Edge ONU Fault</li> </ul>
	Abnormal	The fault range is from the edge ONU to the Internet	<ul style="list-style-type: none"> <li>The egress bandwidth is insufficient, and a large number of STAs access the network, causing congestion</li> <li>Insufficient subscribed bandwidth</li> <li>Upper-layer network fault</li> <li>Edge ONU Fault</li> <li>Fiber network fault</li> </ul>

### 9.4.3 Wi-Fi Service Troubleshooting

The following table lists the common Wi-Fi service faults.

**Table 9-6** Common Wi-Fi Service Faults

Fault Symptom	Possible Causes	Treatment Method
No Wi-Fi signal is found	The optical AP hardware is abnormal or faulty	Check whether the operating status indicator of the optical AP is normal

Fault Symptom	Possible Causes	Treatment Method
	The Wi-Fi switch of the optical AP is not turned on	Check Wi-Fi radio management and Wi-Fi parameter settings. (The two switches must be turned on at the same time so that the corresponding SSID signal can be found.) If not, open it and try again
Unable to connect to Wi-Fi	The terminal selects an incorrect SSID	Check the SSID and connect the correct SSID
	The authentication information entered by the terminal is incorrect	Check the password and re-enter the correct password
Wi-Fi signal intermittently	There are strong interference sources around the optical AP, and Wi-Fi signals are interfered	Check whether there are microwave ovens, electric refrigerators, wireless mice, and cordless phones around the optical AP because the frequency of these appliances interferes with the frequency of Wi-Fi signals, causing performance degradation
	Too many obstacles cause severe Wi-Fi signal attenuation	Signal attenuation is mainly caused by metal objects, walls (especially load-bearing walls), and large household appliances/furniture

Common Wi-Fi signal interference of home appliances is as follows:

Wi-Fi signal transmission frequency:

- 802.11b/g/n: 2.4 GHz
- 802.11a/n/ac: 5 GHz

This frequency is the same as that of microwave ovens, refrigerators, wireless mice, or cordless phones. Co-channel interference exists, and the closer the distance, the greater the impact.

If there are multiple radio signals around, the radio signals on the same channel or adjacent channels also affect each other, resulting in low stability.

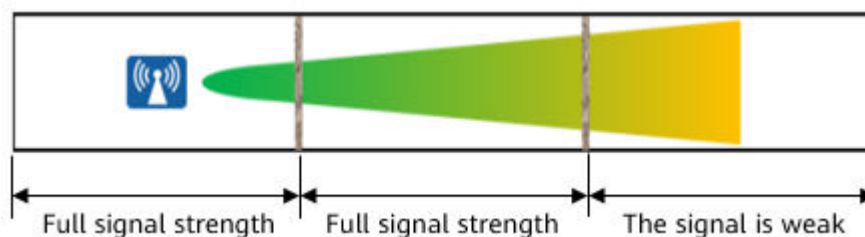
**Table 9-7** Common frequency interference

Devices	Parameter	Interference Evaluation
Microwave oven	Frequency: S (2.4-2.5 GHz) Power: > 800 W	Large interference range: The Wi-Fi rate decreases significantly when the distance is less than 4 m. The Wi-Fi network is occasionally disconnected when the distance is less than 2 m.



Devices	Parameter	Interference Evaluation
Mobile phone	Frequency: 2.4 GHz Power: 3 W	Severe short-distance interference: If the distance is less than 1 m, the Wi-Fi rate decreases significantly. If the distance is less than 0.5 m, the Wi-Fi network is disconnected.
Wireless Cameras	Frequency: 2.4 GHz Power: 0.5-1 W	The interference is relatively light and still needs to be far away from.
Bluetooth Device	Frequency: 2.4 GHz Power: 1 mW	Very little interference.

The more obstacles, the greater the attenuation of Wi-Fi signals.



Typical barrier penetration loss is shown in the following table.

**Table 9-8** Typical Barrier Penetration Loss

Obstacles	Thickness (mm)	2.4 GHz Signal Attenuation (dB)	5 GHz Signal Attenuation (dB)
Ordinary brick wall	120	10	20
Thickened brick wall	240	15	25
Concrete	240	25	30
Asbestos	8	3	4
Foam board	8	3	4
Hollow wood	20	2	3

Obstacles	Thickness (mm)	2.4 GHz Signal Attenuation (dB)	5 GHz Signal Attenuation (dB)
Ordinary wooden door	40	3	4
	40	10	15
Solid wood door	8	4	7
Ordinary glass	12	8	10
Thickened glass	30	25	35
Bulletproof glass	500	25	30
Bearing column	10	15	20
Rolling shutter door	80	30	35
Steel plate	80	30	35
Elevators			

## 9.4.4 ONUs Fail to Go Online Due to Incorrect Fiber Connector Type

### Fault symptom

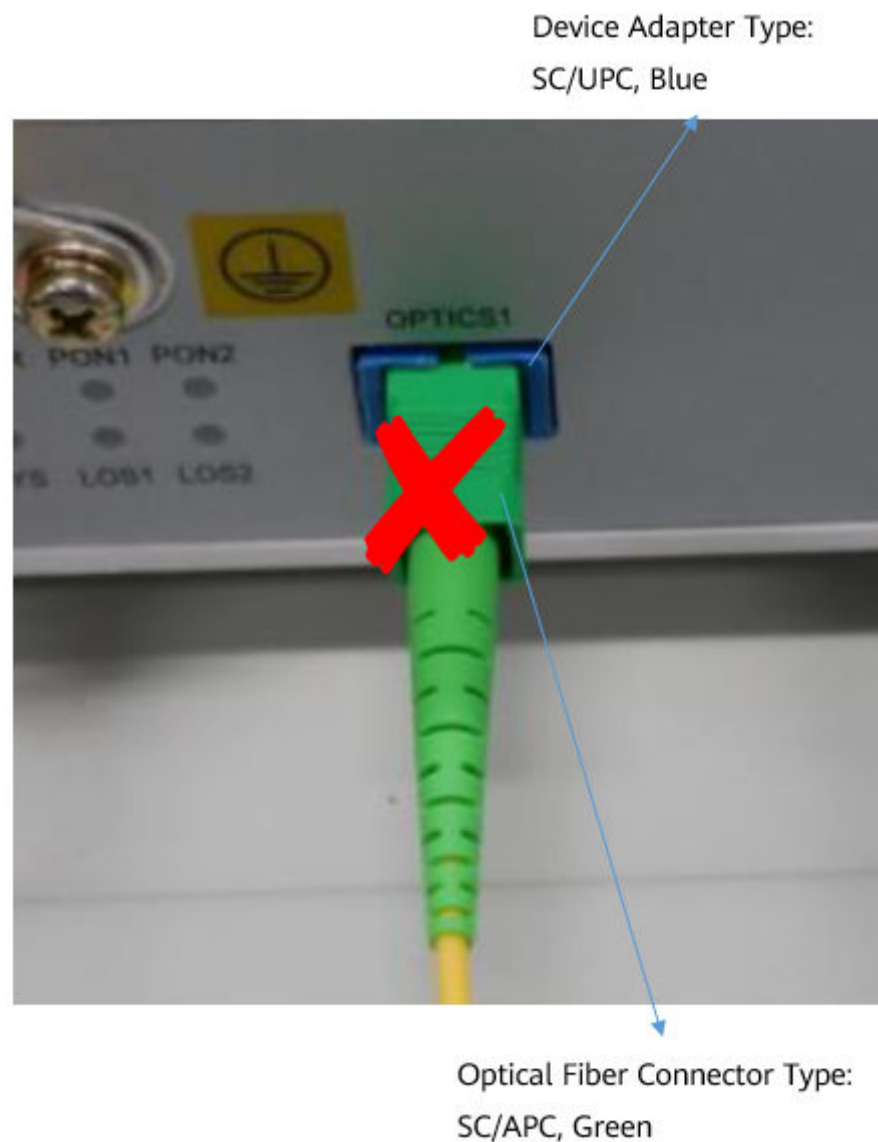
The ONU cannot go online. The optical power attenuation exceeds the range.

### Fault Cause

The fiber connector type is incorrect.

### Troubleshooting

1. Observe the ONU power indicator on site. The indicator status is normal.
2. Check the ONU optical signal indicator on site. It is found that the indicator is off, which indicates that the optical port does not receive downstream optical signals or the optical fiber is not connected to the device.
3. After the optical fiber is removed and inserted again, the indicator is still off.
4. Measure the receive optical power of the ONU. It is found that the receive optical power of the ONU in the OLT direction is less than  $-30$  dBm, which is lower than the optical power threshold ( $-27$  dBm).
5. Check the fiber. It is found that the fiber connector type is incorrect. The optical adapter of the ONU is of the SC/UPC type, but the fiber connector used on site is of the SC/APC type. After the fiber connector is replaced with the SC/UPC type, the fault is rectified.



**NOTE**

Ensure that the fiber connector type is the same as the adapter type. Otherwise, the fiber connector cannot work properly.

The SC/UPC connector is blue and the SC/APC connector is green. The fiber connector and adapter must be of the same type. That is, the blue fiber connector is connected to the blue fiber connector and the green fiber connector is connected to the green fiber connector. Otherwise, the optical power is abnormal.

## 9.4.5 Artifacts Occur on the Camera Due to Insufficient Bandwidth

### Fault symptom

Frame freezing or erratic display occurs in the video surveillance service.

## Troubleshooting

If the camera bandwidth is too low, frame loss occurs.

Check whether the bandwidth configuration of the video service meets the camera requirements.

Take a single 1080p full HD camera as an example. It is recommended that the guaranteed bandwidth be 10 Mbit/s and the maximum bandwidth be 100 Mbit/s.

# 10 FAQs

---

- 10.1 Where can I download the HUAWEI eKit app?
- 10.2 Why does the deployment fail by scanning codes using the eKit app?
- 10.3 Do I need to pay for using the HUAWEI eKit app to manage products and projects?
- 10.4 What is the default user name and password of the F1001-AC?
- 10.5 How many ONU can be connected to the F1001-AC?
- 10.6 Does the MiniFTTO solution support Wi-Fi roaming?
- 10.7 Can the F1001-AC be connected to the optical splitter?
- 10.8 Can the optical gateway F1001-AC connect to APs of other brands?
- 10.9 How do I log in to the web interface of the connected ONU through the primary gateway?
- 10.10 How do I restart the ONU?
- 10.11 How to Identify the Connector Type of Huawei Equipment?
- 10.12 Does the MiniFTTO networking require AP authorization?
- 10.13 Can the MiniFTTO be connected to other ONUs?
- 10.14 Can PoF cable be purchased from other companies?
- 10.15 What is the ambient operating temperature of the F1001-AC?
- 10.16 The password attached to the F1001-AC cannot be used to log in to the F1001-AC
- 10.17 Can P series ONUs be connected to the F1001-AC optical gateway?
- 10.18 How many users can the F1001-AC support?
- 10.19 Does the MiniFTTO need to install the local NMS?
- 10.20 How many users can the F1001-AC support?
- 10.21 Is the F1001-AC input connected through optical fiber?

10.22 Why cannot I log in to the F1001-AC using the default password on the nameplate?

10.23 Does the PoF cable power supply in the MiniFTTO solution adopt the PoE power supply mode?

## 10.1 Where can I download the HUAWEI eKit app?

HUAWEI eKit App is a digital distribution platform that integrates marketing, transaction, service, enablement, and partner operations for numerous distribution partners and enterprise-level users in the enterprise market.

Download HUAWEI eKit App

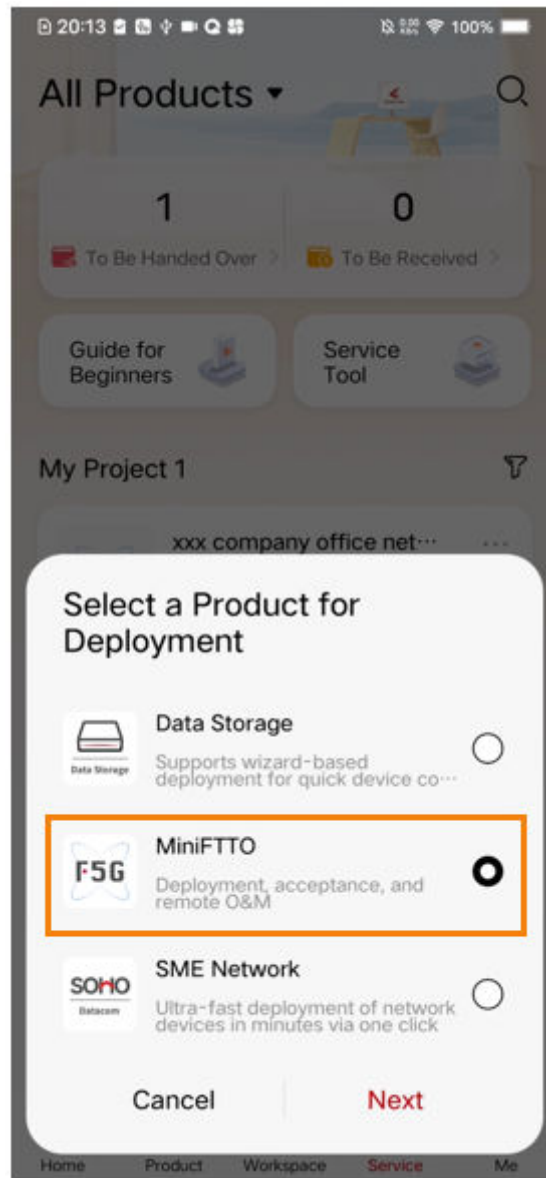
- For Huawei phones, search for **Huawei eKit** in Huawei AppGallery and download it.
- For non-Huawei Android phones, visit <https://app.huawei.com/eplus/soho/front/index.html#/download> in the address box of the browser to download the app.
- Scan the QR code to download.



## 10.2 Why does the deployment fail by scanning codes using the eKit app?

If the deployment fails using the HUAWEI eKit app by scanning the QR code, perform the following operations:

- Check whether the selected product is correct.  
On the Service tab page, tap +, select MiniFTTO.



- Check whether the software version of the optical gateway F1001-AC supports deployment by scanning the QR code.  
The version of the optical gateway at the sites is V500R023C00 or later.

### 10.3 Do I need to pay for using the HUAWEI eKit app to manage products and projects?

The Huawei eKit app is free to download and use without any charge.

## 10.4 What is the default user name and password of the F1001-AC?

You can view the default user name and password of the F1001-AC on the product nameplate.

As shown in the following figure, the red box indicates the default user name and password of the device.

### NOTICE

To ensure account security, change the initial password after logging in to the WebUI using the initial user name and password.



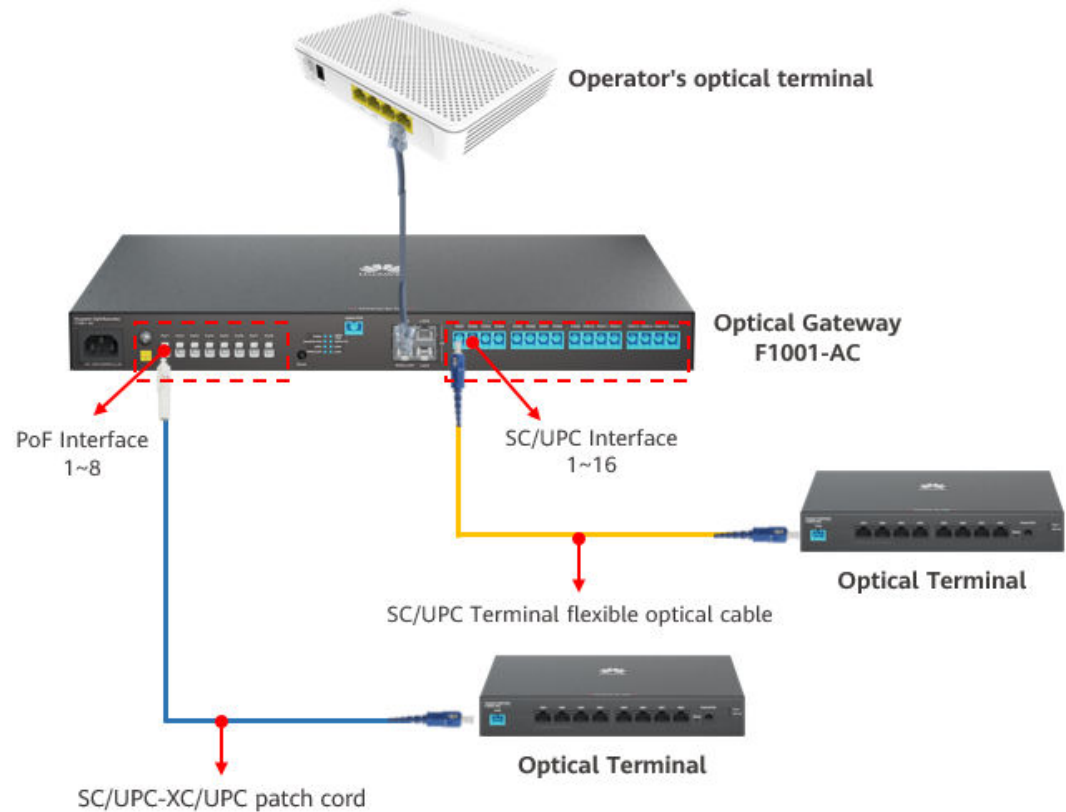
## 10.5 How many ONU can be connected to the F1001-AC?

The F1001-AC can be connected to a maximum of 24 optical terminals (ONUs).

The F1001-AC provides 8 XC/UPC PoF interface and 16 SC/UPC interface.



After XC/UPC-to-SC/UPC patch cords are used, 24 SC/UPC interface can be provided to connect to 24 ONUs.



## 10.6 Does the MiniFTTO solution support Wi-Fi roaming?

Support.

The optical gateway of the MiniFTTO solution integrates the Wi-Fi roaming management function. Multiple optical APs connected to the optical gateway can roam.

## 10.7 Can the F1001-AC be connected to the optical splitter?

NO.

The F1001-AC has a built-in optical splitter, and the downstream port is split by the built-in optical splitter. When the optical splitter is connected to the F1001-AC, the optical power is insufficient after the splitter is connected. As a result, the optical terminal cannot work properly.

## 10.8 Can the optical gateway F1001-AC connect to APs of other brands?

Not supported.

The F1001-AC can be connected only to optical APs of the MiniFTTO solution scope.

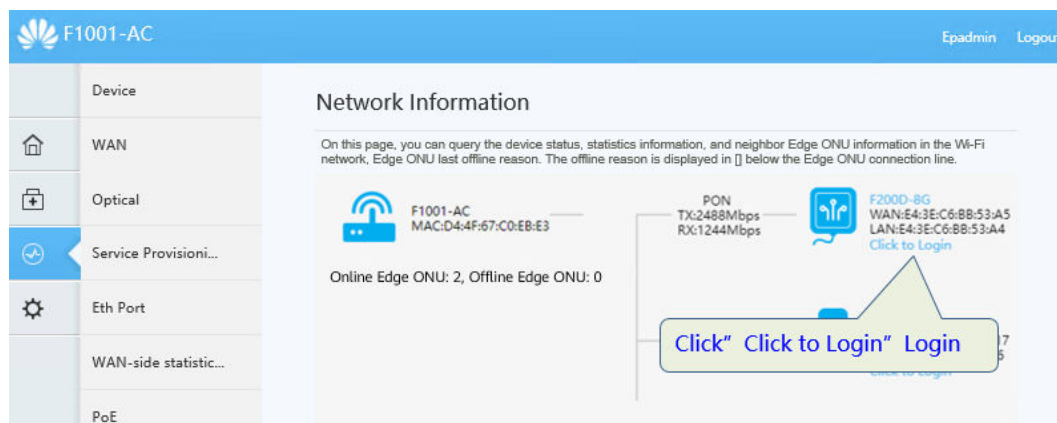
## 10.9 How do I log in to the web interface of the connected ONU through the primary gateway?

### Question

How do I log in to the web interface of the connected ONU through the primary gateway?

### Answer

Log in to the web interface of the primary gateway, choose **System Information** > **Network Info**, and click **Click to Login** under the ONU icon.



## 10.10 How do I restart the ONU?

### Question

How do I restart the ONU?

### Answer

- **Method 1**  
**Restart the software.**  
In the navigation tree on the left, choose **Advanced** > **Maintenance Diagnosis** > **Edge ONU Software Restart**. In the pane on the right, select a Edge ONU to be restarted, and click **Restart** to restart the Edge ONU.

### Edge ONU Software Restart

Select the Edge ONUs to be restarted and click Restart to restart them in batches.

Restart

<input type="checkbox"/>	Device Model	MAC Address	SN	Software Version	Online Time
--------------------------	--------------	-------------	----	------------------	-------------

- **Method 2**  
**Press the reset button to restart the device.**  
Press the reset button with a needle to restart the device.

## 10.11 How to Identify the Connector Type of Huawei Equipment?

### Question

How to identify the connector type of Huawei equipment?

### Answer

Ensure that the fiber connector type is the same as the adapter type. Otherwise, the fiber connector cannot work properly.

The SC/UPC connector is blue and the SC/APC connector is green. The fiber connector and adapter must be of the same type. That is, the blue fiber connector is connected to the blue fiber connector and the green fiber connector is connected to the green fiber connector. Otherwise, the optical power is abnormal.

For example, if the adapter type of the optical splitter port is SC/APC and the color is green, you must use the SC/APC optical fiber connector.



Corresponding fiber connector type



Optical Fiber Connector Type: SC/APC

For example, if the adapter type of the PON port on the device is SC/UPC and the color is blue, you must use the SC/UPC optical fiber connector.



Adapter Type: SC/UPC

Corresponding fiber connector type



Optical Fiber Connector Type: SC/UPC

## 10.12 Does the MiniFTTO networking require AP authorization?

Doesn't need.

## 10.13 Can the MiniFTTO be connected to other ONUs?

Not supported.

MiniFTTO supports only ONUs within the solution scope.

## 10.14 Can PoF cable be purchased from other companies?

Not recommended.

The pof cable used in the MiniFTTO solution have passed the matching test between the optical gateway and the optical AP. Therefore, the security and adaptability of the optical composite cables cannot be guaranteed.

## 10.15 What is the ambient operating temperature of the F1001-AC?

The operating temperature of the F1001-AC ranges from -10°C to +40°C.

## 10.16 The password attached to the F1001-AC cannot be used to log in to the F1001-AC

The user name and password on the nameplate of the F1001-AC are the initial default account. If you cannot log in to the F1001-AC, check the following:

- For the initial deployment, check whether the entered user name and password are correct.
- If this is not the first deployment, the initial password may have been changed.

## 10.17 Can P series ONUs be connected to the F1001-AC optical gateway?

You can't.

The F1001 optical gateway can be connected to only the ONUs that match the MiniFTTO solution.

## 10.18 How many users can the F1001-AC support?

Maximum of 300 devices connected.

## 10.19 Does the MiniFTTO need to install the local NMS?

No need.

You only need to install the Huawei eKit app on your phone. You can use the Huawei eKit app to implement deployment commissioning, project management, and network maintenance.

## 10.20 How many users can the F1001-AC support?

The F1001-AC supports 300 users.

## 10.21 Is the F1001-AC input connected through optical fiber?

The input end (network-side interface) of the F1001-AC can be connected through optical fibers or network cables.

The F1001-AC provides one XG-PON optical port and four GE electrical ports.



## 10.22 Why cannot I log in to the F1001-AC using the default password on the nameplate?

The user name and password on the nameplate of the F1001-AC are the initial default account. If you cannot log in to the F1001-AC, check the following:

- For the initial deployment, check whether the entered user name and password are correct.
- If this is not the first deployment, the initial password may have been changed.

## 10.23 Does the PoF cable power supply in the MiniFTTO solution adopt the PoE power supply mode?

Not PoE.

The MiniFTTO solution uses power on fiber (PoF) power supply. Optical gateways and APs are equipped with built-in PoF modules to supply power through optical/electrical composite cables.