

EG8245W5-8T

Webseitenreferenz

Ausgabe

01

Datum

2020-08-26



Copyright © Huawei Technologies Co., Ltd. 2020. Alle Rechte vorbehalten.

Weitergabe oder Vervielfältigung dieses Dokuments oder von Teilen daraus sind, zu welchem Zweck und in welcher Form auch immer, ohne die ausdrückliche schriftliche Genehmigung von Huawei Technologies Co., Ltd. nicht gestattet.

Marken und Genehmigungen



HUAWEI und andere Huawei-Marken sind Marken von Huawei Technologies Co., Ltd.

Alle in diesem Dokument enthaltenen Marken und Markennamen sind Eigentum der jeweiligen Besitzer.

Beachten Sie:

Die erworbenen Produkte, Dienstleistungen und Features unterliegen dem Vertrag, der zwischen Huawei und dem Kunden geschlossen wird. Die in diesem Dokument beschriebenen Produkte, Dienstleistungen und Funktionen können ganz oder teilweise nicht zum Umfang des Einkaufs bzw. der Nutzung gehören. Sofern nicht anderweitig im Kaufvertrag angegeben, werden alle Angaben, Informationen und Empfehlungen in diesem Dokument „IN DER VORLIEGENDEN FORM“ gegeben, ohne ausdrückliche oder implizierte Gewährleistungen, Garantien oder Darstellungen jeglicher Art.

Die Informationen in diesem Dokument können ohne Vorankündigung geändert werden. Bei der Vorbereitung dieses Dokuments wurde größtmögliche Sorgfalt aufgewendet, um die Genauigkeit der Inhalte sicherzustellen. Dennoch entsteht durch die Aussagen, Informationen und Empfehlungen in diesem Dokument keinerlei ausdrückliche oder implizierte Gewährleistung.

Huawei Technologies Co., Ltd.

Anschrift: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
Volksrepublik China

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

E-Mail: support@huawei.com

Inhalte

1 Lokale Anmeldung bei der Weboberfläche	1
2 Schnelleinstellung	4
3 Startseite.....	5
4 Diagnose per Klick	6
5 Systeminformationen.....	8
5.1 Geräteinformationen	8
5.2 WAN-Daten	9
5.3 Optische Informationen	10
5.4 Status der Servicebereitstellung.....	11
5.5 VoIP-Informationen	12
5.6 Eth-Portinformationen	13
5.7 WLAN-Daten	14
5.8 Informationen zum Heimnetzwerk	15
5.9 Informationen zum Gerät des Benutzers.....	16
6 Erweiterte Konfiguration.....	17
6.1 WAN-Konfiguration	17
6.2 LAN-Konfiguration	17
6.2.1 LAN-Hostkonfiguration.....	17
6.2.2 DHCP-Serverkonfiguration	18
6.2.3 Konfiguration der statischen DHCP-IP.....	21
6.2.4 DHCPv6-Serverkonfiguration	21
6.2.5 Konfiguration der statischen DHCPv6-IP.....	25
6.3 Sicherheitskonfiguration.....	25
6.3.1 IPv4-Adressfilterung.....	25
6.3.2 MAC-Adressfilterung	28
6.3.3 WLAN-MAC-Adressfilterung	29
6.3.4 Jugendschutz.....	30
6.3.5 Präzise Gerätezugriffssteuerung	31
6.3.6 Gerätezugriffssteuerung.....	32
6.3.7 IPv6-Adressfilterung.....	33
6.4 Weiterleitungsregeln	34

6.4.1 DMZ-Funktion.....	35
6.4.2 IPv4-Portzuordnung.....	36
6.4.3 Konfiguration des Port-Triggers	39
6.4.4 IPv6-Portzuordnung.....	40
6.5 Anwendung.....	42
6.5.1 USB-Anwendung.....	42
6.5.2 Gemeinsame Nutzung von Medien.....	43
6.5.3 DDNS-Funktion.....	44
6.5.4 UPnP-Funktion	46
6.5.5 Statischer DNS.....	46
6.6 WLAN	47
6.6.1 Grundeinstellungen für 2,4-GHz-Netzwerke	47
6.6.2 Erweiterte Einstellungen für 2,4-GHz-Netzwerke.....	50
6.6.3 Grundeinstellungen für 5G-Netzwerke.....	52
6.6.4 Erweiterte Einstellungen für 5G-Netzwerke.....	54
6.6.5 Automatische WLAN-Abschaltung	56
6.6.6 Verwaltung der WLAN-Abdeckung	57
6.7 Systemverwaltung.....	59
6.7.1 Kontoverwaltung	59
6.7.2 ONT-Authentifizierung.....	60
6.7.3 Hinweise zu Open Source-Software	60
6.8 Wartungsdiagnose.....	62
6.8.1 Verwaltung von Konfigurationsdateien	62
6.8.2 Wartung.....	62
6.8.3 Benutzerprotokoll	64
6.8.4 Firewallprotokoll	64
6.8.5 Verwaltung des Anzeigestatus.....	66
6.8.6 Neustart.....	66

1 Lokale Anmeldung bei der Weboberfläche

In diesem Abschnitt werden der Datenplan und das Verfahren zur Anmeldung bei der Web-Konfigurationsoberfläche beschrieben.

Kontext

Vergewissern Sie sich vor der Einrichtung der Konfigurationsumgebung, dass die in Tabelle 1-1 aufgeführten Dateninformationen verfügbar sind.

Tabelle 1-1 Datenplan

Element	Beschreibung
Benutzername und Kennwort	Standardeinstellungen: Common User (Endgerätebenutzer) • Benutzername: Epuser • Passwort: ***** HINWEIS • Das Standardkennwort wird zufällig generiert und auf dem Typenschild aufgedruckt. • Das allgemeine Benutzerkonto kann verwendet werden, um den Servicestatus abzufragen. Für ONTs, die WLAN und die USB-Speicherfunktion unterstützen, kann das allgemeine Benutzerkonto für die Konfiguration von Services wie WLAN und Home Sharing verwendet werden. • Wenn Sie innerhalb von fünf Minuten nach Anmeldung bei der Webseite keine Vorgänge durchführen, werden Sie gesperrt und kehren zur Anmeldeoberfläche zurück. Sie können das Konto dann entsperren, indem Sie den Benutzernamen und das Kennwort für die Anmeldung eingeben. • Nach dreimaliger falscher Eingabe des Benutzernamens und des Kennworts wird das System gesperrt und nach einer Minute automatisch wieder entsperrt. • Ändern Sie das Kennwort im Web. • Bestimmte Internetdienstanbieter (ISPs) passen eventuell Konten und Kennwörter an, die sich von den oben angeführten standardmäßigen Konten und Kennwörtern unterscheiden. Wenn Sie nähere Einzelheiten wünschen, wenden Sie sich bitte an den entsprechenden ISP.

Element	Beschreibung
IP-Adresse und Subnetzmaske des LAN	Standardeinstellungen: • IP-Adresse: 192.168.18.1 • Subnetzmaske: 255.255.255.0
IP-Adresse und Subnetzmaske des PCs	Konfigurieren Sie die IP-Adresse des Computers so, dass sie sich im selben Subnetz befindet wie die LAN-IP-Adresse des ONT. Zum Beispiel: • IP-Adresse: 192.168.18.100 • Subnetzmaske: 255.255.255.0

Vorgehensweise

- Schritt 1** Verwenden Sie ein Netzkabel, um den LAN-Anschluss des ONT an einen PC anzuschließen.
- Schritt 2** Stellen Sie sicher, dass der Internet Explorer (IE) des PCs keinen Proxy-Server verwendet. Im folgenden Abschnitt wird der IE 6.0 als Beispiel betrachtet, um zu beschreiben, wie Sie überprüfen können, ob der IE den Proxy-Server verwendet.
1. Starten Sie den IE und wählen Sie im Hauptmenü des IE-Fensters **Tools Internet Options**. Daraufhin wird die Schnittstelle **Internet Options** angezeigt.
 2. Klicken Sie in der Schnittstelle **Internet Options** auf die Registerkarte **Connections** und klicken Sie dann auf **LAN settings**.
 3. Stellen Sie im Bereich **Proxy server** sicher, dass das Kontrollkästchen **Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections)** nicht aktiviert ist (also kein „✓“ vorhanden ist). Wenn das Kontrollkästchen aktiviert ist, deaktivieren Sie es und klicken Sie dann auf **OK**.
- Schritt 3** Legen Sie die IP-Adresse und die Subnetzmaske des PCs fest. Einzelheiten finden Sie unter Tabelle 1-1.
- Schritt 4** Melden Sie sich bei der Web-Konfigurationsoberfläche an.
1. Geben Sie **http://192.168.18.1** in die Adresszeile des IE ein (192.168.18.1 ist die Standard-IP-Adresse des ONT) und drücken Sie dann **Enter**, um die Anmeldeoberfläche anzuzeigen, wie in Abbildung 1-1 gezeigt.

Abbildung 1-1 Login-Oberfläche



HINWEIS

- Aufgrund von Protokollbeschränkungen weisen SSL3.0 und TLS1.0 Sicherheitsrisiken auf. Deshalb wird TLS1.1 oder TLS1.2 empfohlen.
- Der TCP-Port 80 wird für die Erkennung von HTTPS-Paketen verwendet. Sie müssen „https://192.168.18.1:80“ in die Adressleiste des IE eingeben und **Enter** drücken, um sich beim ONT anzumelden.

2. Geben Sie auf der Anmeldeoberfläche den Benutzernamen und das Kennwort ein. Weitere Informationen zu Standardeinstellungen des Benutzernamens und des Kennworts finden Sie in der Tabelle 1-1. Nach bestandener Authentifizierung des Kennworts wird die Web-Konfigurationsoberfläche angezeigt.

----Ende

2 Schnelleinstellung

In diesem Abschnitt wird beschrieben, wie Sie schnell ein ONT einrichten. Wenn sich Common User zum ersten Mal bei der ONT-Webseite anmelden, wird diese Seite angezeigt. In anderen Fällen müssen Sie oben rechts auf der Startseite auf **Fast Setting** klicken, um diese Seite aufzurufen.

Abbildung 2-1 Schnelleinstellung

Welcome to Huawei ONT for connecting you to your family and friends.

Wi-Fi configuration Account management Configuration completion

Set the Wi-Fi name and password

WLAN(2.4 GHz) On/Off: ☒ ON

2.4G Wi-Fi Name: (1-32 characters)

2.4G Wi-Fi Password: ☒ Hide (8-63 characters or 64 hexadecimal characters)

WLAN(5 GHz) On/Off: ☒ ON

5G Wi-Fi Name: (1-32 characters)

5G Wi-Fi Password: ☒ Hide (8-63 characters or 64 hexadecimal characters)

ANMERKUNG

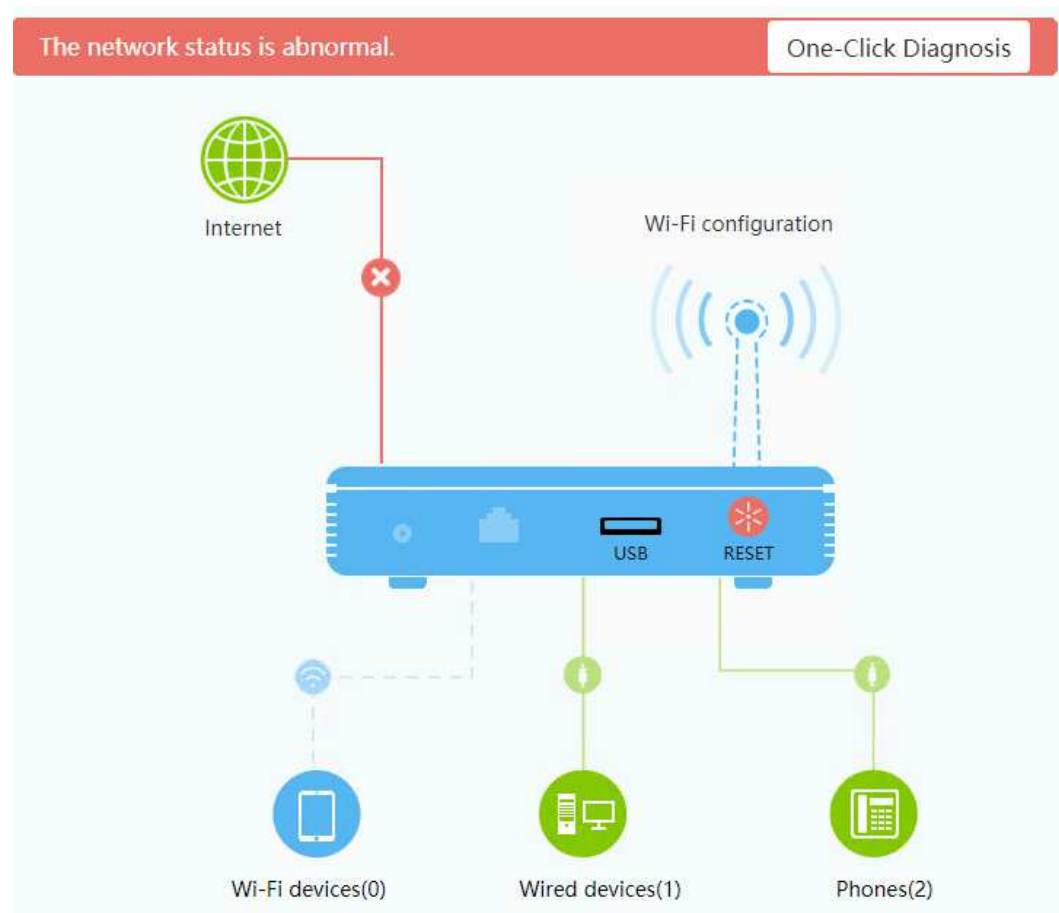
Informationen zur WLAN-Konfiguration finden Sie unter 6.6 WLAN. Informationen zur Kontoverwaltung finden Sie unter 6.7.1 Kontoverwaltung.

3 Startseite

In diesem Abschnitt werden die allgemeinen Konfigurationen des ONT beschrieben, zum Beispiel die WLAN-Konfiguration, die Freigabe des Heimnetzwerks und die Abfrage des Netzwerkstatus.

Mithilfe der Schaltflächen oben rechts auf der Seite können Sie zu den verschiedenen Seiten navigieren.

Abbildung 3-1 Startseite

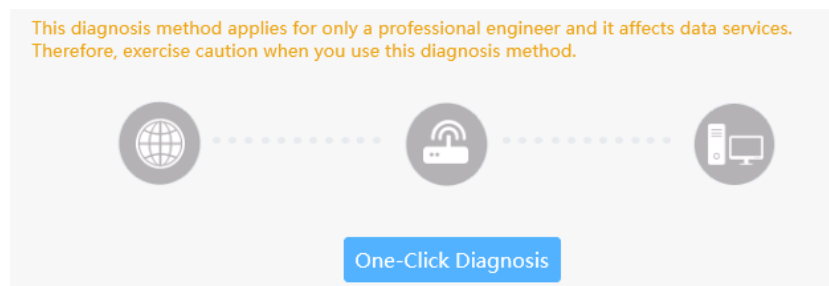


4 Diagnose per Klick

In diesem Abschnitt wird beschrieben, wie Sie ONT-Netzwerkfehler schnell diagnostizieren.

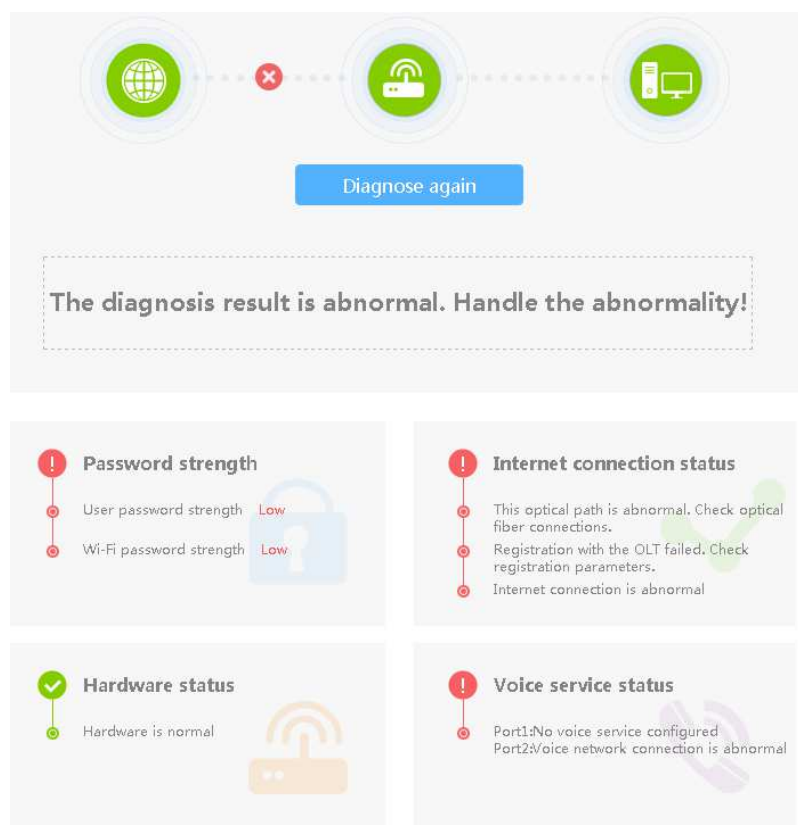
1. Wählen Sie in der Navigationsstruktur im linken Fensterbereich **One-Click Diagnosis**. Klicken Sie dann im rechten Fensterbereich auf **One-Click Diagnosis**, um den Netzwerkstatus zu diagnostizieren, wie in Abbildung 4-1 gezeigt.

Abbildung 4-1 Diagnose per Klick



2. Abbildung 4-2 zeigt die Diagnoseergebnisse an.

Abbildung 4-2 Diagnoseergebnis



ANMERKUNG

Diese Diagnosemethode wirkt sich auf Datenservices aus und sollte nur von einem professionellen Techniker angewendet werden. Gehen Sie mit Vorsicht vor, wenn Sie diese Diagnosemethode anwenden.

Wenn Sie erneut eine Diagnose der Fehler durchführen müssen, klicken Sie auf **Diagnose again**.

5 Systeminformationen

In diesem Abschnitt wird beschrieben, wie Sie die Informationen über das ONT einschließlich der ETH-Portinformationen, optischen Informationen und Benutzergeräteinformationen über die Webseite abfragen.

[5.1 Geräteinformationen](#)

[5.2 WAN-Informationen](#)

[5.3 Optische Informationen](#)

[5.4 Status der Servicebereitstellung](#)

[5.5 VoIP-Informationen](#)

[5.6 Eth-Portinformationen](#)

[5.7 WLAN-Informationen](#)

[5.8 Informationen zum Heimnetzwerk](#)

[5.9 Informationen zum Gerät des Benutzers](#)

5.1 Geräteinformationen

Wählen Sie in der Navigationsstruktur auf der linken Seite **System Information > Device**. Im rechten Fensterbereich können Sie den Produktnamen, die Hardwareversion und die Softwareversion anzeigen, wie in Abbildung 5-1 gezeigt.

Abbildung 5-1 Geräteinformationen

Device Information

On this page, you can view basic device information.

Basic Information

Device Type:	EG8245W5-8T
CPE Description:	OptiXstar EG8245W5-8T (V0000) 100Mbps/32MB/s 4G LTE Cat.4 100Mbps/32MB/s
SN:	XXXXXXXXXXXX
Hardware Version:	V0000
Software Version:	V0000
Manufacture Info:	21500840491234567891.C402
ONT Registration Status:	O1(Initial state)
ONT ID:	255
CPU Usage:	1%
Memory Usage:	45%
Custom Info:	
System Time:	1981-01-01 03:53:22+00:00

Extended Information

Device alias:

[Apply](#)

5.2 WAN-Daten

Wählen Sie in der Navigationsstruktur auf der linken Seite **System Information > WAN**. Im rechten Fensterbereich können Sie den Status der WAN-Schnittstelle, den Modus zum Abrufen einer IP-Adresse, die IP-Adresse und die Subnetz-Maske anzeigen, wie in Abbildung 5-2 gezeigt.

Abbildung 5-2 WAN-Daten

WAN Information

On this page, you can query the connection and line status of the WAN port.

IPv4 Information(Click the form for details)

WAN Name	Status	IP Address	VLAN/Priority	Connect
2_TR069_INTERNET_R_VID_10	Disconnected	--	10/0	AlwaysOn

WAN Information

MAC Address: 00:E0:FC:00:XX:XX

VLAN: 10

Policy: Use the specified value

Priority: 0

NAT: Enable

IP Acquisition Mode: DHCP

IP Address/Subnet Mask: --

Gateway: --

DNS Servers: --

Lease Time: --

Remain Lease: --

NTP Servers: --

Time Zone Info: --

SIP Servers: --

Static Route: --

Vendor Info: --

Online Duration (ddhh:mm:ss): --

ANMERKUNG

Klicken Sie auf einen Datensatz in der WAN-Liste, um weitere Informationen anzuzeigen.

5.3 Optische Informationen

Wählen Sie in der Navigationsstruktur auf der linken Seite **System Information > Optical**. Im rechten Fensterbereich können Sie den optischen Status, die optische Übertragungsleistung und die optische Empfangsleistung des optischen Moduls anzeigen, wie in Abbildung 5-3 gezeigt.

Abbildung 5-3 Optische Informationen

Optical Information		
On this page, you can query the status of the optical module.		
ONT Information		
	Current Value	Reference Value
Optical Signal Sending Status:	--	Auto
TX Optical Power:	-- dBm	0.5 to 5 dBm
RX Optical Power:	-- dBm	-27 to -8 dBm
Working Voltage:	3415 mV	3100 to 3500 mV
Bias Current:	0 mA	0 to 90 mA
Working Temperature:	46 °C	-10 to +85 °C
OLT Information		
	Current Value	Reference Value
Optical module type:	--	--
Transmit optical power:	-- dBm	--
PON port identifier:	--	--

5.4 Status der Servicebereitstellung

Klicken Sie auf die Registerkarte **System Information** und wählen Sie in der Navigationsstruktur auf der linken Seite **Service Provisioning Status**. Im rechten Fensterbereich wird der Status der ONT-Servicebereitstellung angezeigt, wie in Abbildung 5-4 gezeigt.

Abbildung 5-4 Status der Servicebereitstellung

Service Provisioning Status

On this page, you can query the service provisioning status.

ONT Registration Status:

Obtaining the status. Please wait.

OLT Service Configuration Status:

--

EMS Configuration Status:

--

ACS Registration Status:

--

Refresh

5.5 VoIP-Informationen

Wählen Sie in der Navigationsstruktur auf der linken Seite **System Information > VoIP**. Im rechten Fensterbereich können Sie dann Informationen wie den Benutzerstatus und den Anrufstatus abfragen. Die SIP-Konfigurationsseite unterscheidet sich geringfügig von der H.248-Konfigurationsseite, wie in Abbildung 5-5 und Abbildung 5-6 gezeigt.

Abbildung 5-5 VoIP-Informationen – SIP

VoIP Information

On this page, you can query status information of voice users and reset the voice function.

No.	URI	User Name (Phone Number)	Associated POTS Port	User Status	Call Status	Registration Error	Error Code
1	77770857@ont.huawei.com	77770857	1	Registering	Idle	Upstream port disconnected	--
2	77770858@ont.huawei.com	77770858	2	Registering	Idle	Upstream port disconnected	--

Restart VoIP

Abbildung 5-6 VoIP-Informationen – H.248

VoIP Information							
On this page, you can query status information of voice users and reset the voice function.							
No.	Physical TID	Phone Number	Associated POTS Port	User Status	Call Status	Interface Status	Registration Error
1	--	--	1	Initializing	Idle	Closed	Upstream port disconnected
2	--	--	2	Initializing	Idle	Closed	Upstream port disconnected

Wenn der VoIP-Dienst neu gestartet werden muss, klicken Sie im rechten Fensterbereich auf **Restart VoIP**.

5.6 Eth-Portinformationen

Wählen Sie in der Navigationsstruktur auf der linken Seite **System Information > Eth Port**. Im rechten Fensterbereich können Sie den Duplexmodus, die Geschwindigkeit und den Status des ETH-Ports anzeigen, wie in Abbildung 5-7 gezeigt.

Abbildung 5-7 Eth-Portinformationen

Eth Port Information							
On this page, you can query the user-side Ethernet port information.							
Ethernet Port Status							
Port	Status			Receive (RX)		Transmit (TX)	
	Mode	Speed	Link	Bytes	Packets	Bytes	Packets
1	--	--	Down	0	0	193250	1690
2	Full-duplex	1000 Mbit/s	Up	2401372	16064	29226429	27902
3	--	--	Down	0	0	193250	1690
4	--	--	Down	0	0	193250	1690

5.7 WLAN-Daten

Wählen Sie in der Navigationsstruktur auf der linken Seite **System Information > WLAN**. Im rechten Fensterbereich können Sie dann Informationen wie den WLAN-Anschlusststatus, WLAN-Paketstatistiken und SSID abfragen, wie in Abbildung 5-8 gezeigt.

Abbildung 5-8 WLAN-Daten

WLAN Information

On this page, you can query the WLAN information, WLAN packet statistics, and SSID information.

One-Click Diagnosis

☒ 2.4 GHz wireless network information

☐ 5 GHz wireless network information

WLAN Info

WLAN Status:

Enabled

WLAN Channel:

11

WLAN Packet Statistics

SSID Index	SSID Name	Receive (RX)				Transmit (TX)			
		Bytes	Packets	Error	Discarded	Bytes	Packets	Error	Discarded
1	EBG-2G	0	0	0	0	217676	1185	0	0

SSID Information

SSID Index	SSID Name	Security Configuration	Authentication Mode	Encryption Mode
1	EBG-2G	Configured	WPA/WPA2 PreSharedKey	TKIP&AES

STA Information

Query

MAC Address	SSID Name	Connection Duration (s)	Sending Rate (Mbit/s)	Receiving Rate (Mbit/s)	Signal Strength (dBm)	Noise (dBm)	Signal-to-Noise Ratio (dB)	Signal Quality (dBm)	Antenna Num	11k11v
-------------	-----------	-------------------------	-----------------------	-------------------------	-----------------------	-------------	----------------------------	----------------------	-------------	--------

Neighbor AP Information

Query

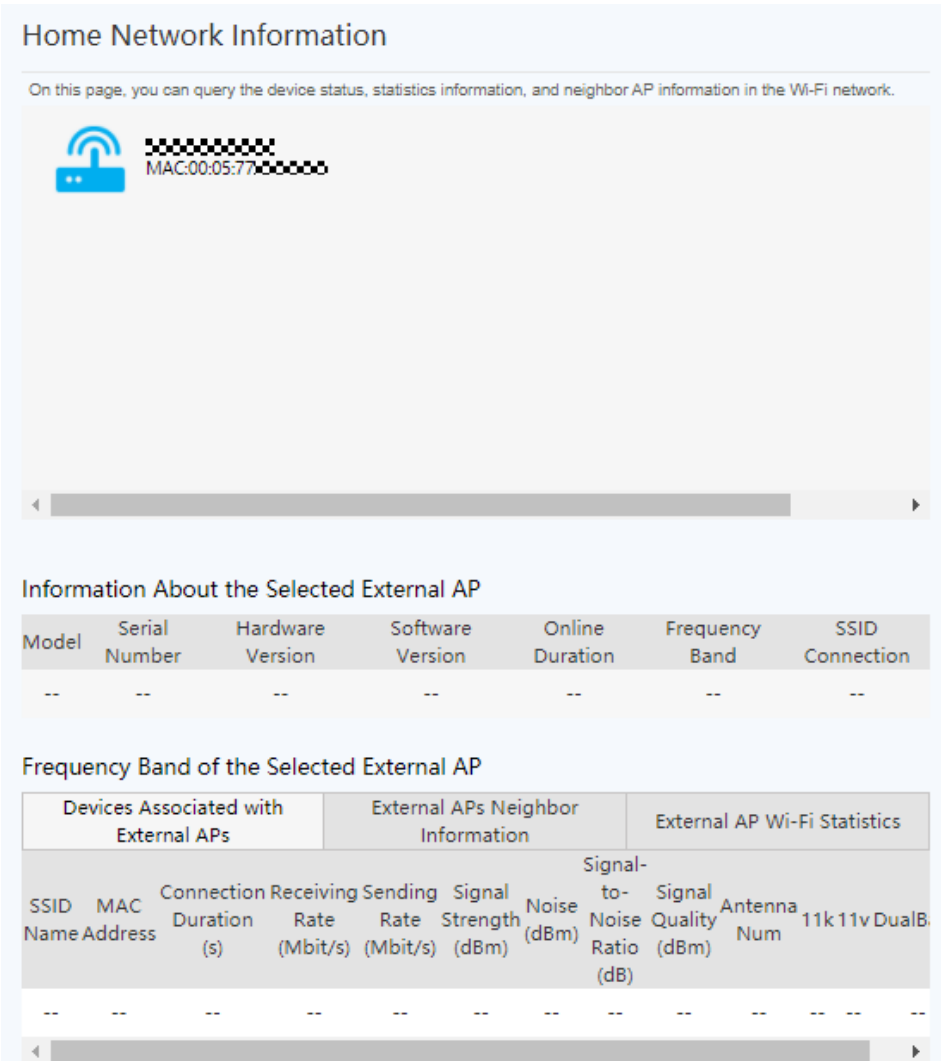
Note: Querying neighbor AP information may disconnect all STA connections.

SSID Name	MAC Address	Network Type	Channel	Signal Strength (dBm)	Noise (dBm)	DTIM Interval	Beacon Period (ms)	Authentication Mode	Working Mode	Ma Ra (Mbi
-----------	-------------	--------------	---------	-----------------------	-------------	---------------	--------------------	---------------------	--------------	------------

5.8 Informationen zum Heimnetzwerk

Klicken Sie auf die Registerkarte **System Information** und wählen Sie in der Navigationsstruktur auf der linken Seite **Home Network**. Überprüfen Sie im rechten Fensterbereich den Gerätestatus, statistische Informationen und Informationen benachbarter APs von externen APs im WLAN-Netzwerk, wie in der Abbildung unten gezeigt.

Abbildung 5-9 Intelligente WLAN-Abdeckung



5.9 Informationen zum Gerät des Benutzers

Klicken Sie auf die Registerkarte **System Information** und wählen Sie in der Navigationsstruktur auf der linken Seite **User Device Information**. Im rechten Fensterbereich werden Informationen zum Gerät des Benutzers angezeigt, einschließlich Hostname, Gerätetyp, IP-Adresse, MAC-Adresse, Gerätestatus, Schnittstelle, Online-Dauer und Leasedauer, wie in Abbildung 5-10 gezeigt.

Abbildung 5-10 Informationen zum Gerät des Benutzers

User Device Information

On this page, you can query the basic information about the user device, including the host name, device type, IP address, MAC address, device status, interface, online duration, and lease time.

	Host Name	Device Type	IP Address	MAC Address	Device Status	Interface	Online Duration	Lease Time
☐	--	--	192.168.18.2	00:e0:4d:xx:xx:xx	Online	LAN1	0day,00:13:23	--

<< < 1/1 > >>

Page Go

[Details](#) [Delete](#)

6 Erweiterte Konfiguration

In diesem Abschnitt wird die Funktionskonfiguration über die Webseite beschrieben, einschließlich LAN- oder WAN-Konfiguration, Sicherheitskonfiguration usw.

[6.1 WAN-Konfiguration](#)

[6.2 LAN-Konfiguration](#)

[6.3 Sicherheitskonfiguration](#)

[6.4 Weiterleitungsregeln](#)

[6.5 Anwendung](#)

[6.6 WLAN](#)

[6.7 Systemverwaltung](#)

[6.8 Wartungsdiagnose](#)

6.1 WAN-Konfiguration

In diesem Abschnitt wird beschrieben, wie Sie die WAN-Schnittstelle über die Webseite konfigurieren. Common User haben dafür jedoch keine Vorgangsberechtigung.

6.2 LAN-Konfiguration

In diesem Abschnitt wird beschrieben, wie Sie den LAN-Port oder DHCP-Parameter über die Webseite konfigurieren.

6.2.1 LAN-Hostkonfiguration

1. Wählen Sie in der Navigationsstruktur auf der linken Seite **Advanced > LAN > LAN Host**. Legen Sie im rechten Fensterbereich die IP-Adresse für die Verwaltung der primären und sekundären Adresse fest, wie in Abbildung 6-1 gezeigt.

Abbildung 6-1 LAN-Hostkonfiguration

ANMERKUNG

Die IP-Adresse des mit dem LAN-Port verbundenen Geräts muss sich im selben Subnetz befinden wie die IP-Adresse für die Verwaltung. Auf diese Weise können Sie über die Webseite auf ein ONT zugreifen und Abfragen und Verwaltungsaufgaben durchführen.

2. Klicken Sie auf **Anwenden**.

6.2.2 DHCP-Serverkonfiguration

1. Wählen Sie in der Navigationsstruktur auf der linken Seite **Advanced > LAN > DHCP Server**. Im rechten Fensterbereich können Sie den LAN-seitigen DHCP-Adresspool für das ONT konfigurieren, das als Gateway fungiert. Nach der Konfiguration kann der mit dem LAN-Port verbundene PC automatisch eine IP-Adresse aus dem Adresspool abrufen, wie in Abbildung 6-2 gezeigt.

Abbildung 6-2 DHCP-Serverkonfiguration

DHCP Server Configuration

On this page, you can set DHCP server parameters for the LAN-side device to obtain IP addresses.

Primary Address Pool

Enable Primary DHCP Server:

☒

Enable DHCP Relay:

☒

Enable Option125:

☒

LAN Host IP Address:

192.168.18.1

Subnet Mask:

255.255.255.0

Start IP Address:

192.168.18.2

*(It must be in the same subnet as the IP address of the LAN host.)

End IP Address:

192.168.18.254

*

Lease Time:

1

hours

Primary DNS Server:

Secondary DNS Server:

Secondary Address Pool

Enable Secondary DHCP Server:

☒

IP Address:

192.168.2.1

Subnet Mask:

255.255.255.0

Start IP Address:

192.168.2.2

*

End IP Address:

192.168.2.254

*

Lease Time:

1

days

Option 60:

MSFT 5.0

*

Option 43:

NTP Server:

Primary DNS Server:

Secondary DNS Server:

Apply

Cancel

2. Klicken Sie auf **Anwenden**.

Tabelle 6-1 beschreibt die zugehörigen Parameter für den DHCP-Server.

Tabelle 6-1 Zugehörige Parameter für den DHCP-Server

Parameter	Beschreibung
Enable Primary DHCP Server	Gibt an, ob der primäre DHCP-Server aktiviert werden soll. Wenn das Kontrollkästchen aktiviert ist, können Sie den primären DHCP-Server festlegen.

Parameter	Beschreibung
Enable DHCP Relay	Gibt an, ob das DHCP-Relais aktiviert werden soll. Das DHCP-Relais ist ein Prozess, in dem die subnetzübergreifende Weiterleitung von DHCP-Übertragungspaketen zwischen dem DHCP-Client und dem DHCP-Server implementiert wird. Auf diese Weise können die DHCP-Clients in verschiedenen physischen Subnetzen IP-Adressen abrufen, die dynamisch vom gleichen DHCP-Server zugewiesen werden. • Wenn der Mode des WAN-Ports Route lautet, wird die IP-Adresse des ONT von den übergeordneten DHCP-Servern in verschiedenen Subnetzen abgerufen und die IP-Adressen auf der Benutzerseite werden vom DHCP-Adresspool des ONT abgerufen. • Wenn der Mode des WAN-Ports Bridge lautet, fungiert das ONT als Bridge. Auf diese Weise hat das ONT keine IP-Adresse. Die benutzerseitigen IP-Adressen werden von DHCP-Servern der oberen Ebene in unterschiedlichen Subnetzen abgerufen.
Enable Option125	Gibt an, ob die Option125 aktiviert werden soll.
LAN Host IP Address	Gibt die IP-Adresse des Hosts an.
Start IP Address	Gibt die Start-IP-Adresse im IP-Adressenpool auf dem primären DHCP-Server an.
End IP Address	Gibt die End-IP-Adresse im IP-Adressenpool auf dem aktiven DHCP-Server an.
Lease Time	Gibt die Leasedauer des IP-Adressenpools auf dem aktiven DHCP-Server an. Optionen: Minute, Stunde, Tag und Woche.
Enable secondary DHCP server	Gibt an, ob der sekundäre DHCP-Server aktiviert werden soll. Wenn das Kontrollkästchen aktiviert ist, können Sie den sekundären DHCP-Server festlegen.
IP Address	Gibt die IP-Adresse des sekundären DHCP-Servers an.
Subnet Mask	Gibt die Subnetzmaske des sekundären DHCP-Servers an.
Start IP Address	Gibt die Start-IP-Adresse im IP-Adressenpool auf dem sekundären DHCP-Server an.
End IP Address	Gibt die End-IP-Adresse im IP-Adressenpool auf dem sekundären DHCP-Server an.
Lease Time	Gibt die Leasedauer des IP-Adressenpools auf dem sekundären DHCP-Server an. Optionen: Minute, Stunde, Tag und Woche.
Option 60	Gibt das Feld für die Option 60 des sekundären DHCP-Servers an. Ein benutzerseitiger DHCP-Client kann nur dann eine IP-Adresse aus dem IP-Adressenpool auf dem sekundären DHCP-Server abrufen, wenn das Feld für die Option 60 auf dem benutzerseitigen DHCP-Client mit dieser Einstellung identisch ist.

Parameter	Beschreibung
Option 43	Gibt das Feld für die Option 43 des sekundären DHCP-Servers an, wodurch ein TFTP-Server gekennzeichnet wird.
NTP Server	Gibt die IP-Adresse des NTP-Servers ein.
Primary DNS Server	Gibt die IP-Adresse des primären DNS-Servers ein.
Secondary DNS Server	Gibt die IP-Adresse des sekundären DNS-Servers ein.

6.2.3 Konfiguration der statischen DHCP-IP

1. Klicken Sie auf die Registerkarte **Advanced** > **LAN** und wählen Sie in der Navigationsstruktur auf der linken Seite **DHCP Static IP**. Klicken Sie im rechten Fensterbereich auf **New**. Legen Sie im daraufhin angezeigten Dialogfeld die **MAC Address** und die **IP Address** fest, wie in Abbildung 6-3 gezeigt.

Abbildung 6-3 Konfiguration der statischen DHCP-IP

DHCP Static IP Configuration

On this page, you can configure the reserved IP address that is assigned through DHCP for the specified MAC address.

New Delete

	MAC Address	IP Address
----	----	----

MAC Address: (AA:BB:CC:DD:EE:FF)

IP Address:

Apply Cancel

2. Klicken Sie auf **Anwenden**.

6.2.4 DHCPv6-Serverkonfiguration

1. Wählen Sie in der Navigationsstruktur auf der linken Seite die Registerkarte **Advanced** > **LAN** und anschließend in der Navigationsstruktur auf der linken Seite **DHCPv6 Server**. Im rechten Fensterbereich können Sie den LAN-seitigen Adressenpool für das ONT konfigurieren, das als Gateway fungiert, wie in Abbildung 6-4 gezeigt.

Abbildung 6-4 DHCPv6-Serverkonfiguration

DHCPv6 Server Configuration

On this page, you can configure IPv6-related feature parameters.

Interface Address Information

IPv6 Address:

fe80::1

*

Method of obtaining prefixes:

Static configuration

Prefix:

::/0

*

(IPv6 address/n 1 <= n <= 64)

Preferred period:

3600

*

(600s to 4294967295s)

Valid period:

7200

*

(600s to 4294967295s)

MTU:

1472

*

(1280-1500)

DNS Information

DNS source on the LAN side:

DNS agent

Resource Allocation Information

Enable route advertisement:

☒

Enable DHCPv6 server:

☒

Resource allocation mode:

Manual

Address/Prefix Assignment Mode:

☐ DHCPv6 ☒ SLAAC

Other Information Assignment Mode:

☒ DHCPv6 ☐ SLAAC

ULA information

ULA Mode:

Disabled

Apply

Cancel

2. Klicken Sie auf **Anwenden**.

Tabelle 6-2 führt die Parameter für die DHCPv6-Serverkonfiguration auf.

Tabelle 6-2 Parameter für die DHCPv6-Serverkonfiguration

Parameter	Beschreibung
IPv6 Address	Gibt die IP-Adresse für die IPv6-Verwaltung an. Der Standardwert lautet fe80::1 . Wählen Sie LAN > LAN Host , um die IP-Adresse für die IPv4-Verwaltung zu konfigurieren.
Method Of Obtaining Prefixes	Methoden zum Abrufen von Präfixen. • WAN-Agent • Statische Konfiguration
Parent Prefix	Dieser Parameter wird angezeigt, wenn Method Of Obtaining

Parameter	Beschreibung
	Prefixes auf WAN agent gesetzt ist. Gibt die Quelle des übergeordneten Präfix an. In der Regel wird ein Internet-WAN-Port als Quelle für das übergeordnete Präfix verwendet. Standardmäßig wird der erste IPv6-Internet-WAN-Port als Quelle für das übergeordnete Präfix verwendet. Wenn für diese Option kein Wert angegeben wird, wird kein Präfix abgerufen. Das kann dazu führen, dass der Service nicht verfügbar ist.
Child Prefix Mask	Dieser Parameter wird angezeigt, wenn Method Of Obtaining Prefixes auf WAN agent gesetzt ist. Wird für die Zuweisung der LAN-IP-Adresse verwendet. Dieser Parameter muss konfiguriert werden, wenn das abgerufene Präfix kleiner als 64 Bit ist. Beispiel: Wenn das abgerufene Präfix 2012:1111:2222::/48 und der Wert für die untergeordnete Präfixmaske auf 0:0:0:3333::/64 gesetzt ist, ist das IPv6-Adresspräfix 2012:1111:2222:3333::/64.
Prefix	Dieser Parameter wird angezeigt, wenn Method Of Obtaining Prefixes auf Static configuration gesetzt ist. Gibt den Netzwerkadressraum an. IPv6 verwendet ein Präfix, um den Netzwerkadressraum anzugeben. Beispielsweise gibt 2001:251:e000::/48 einen Adressraum mit einem 48-Bit-Präfix an.
Preferred period	Dieser Parameter wird angezeigt, wenn Method Of Obtaining Prefixes auf Static configuration gesetzt ist. Gibt den Zeitraum an, für den eine gültige Adresse den bevorzugten Status aufweist. Nach Ablauf der bevorzugten Lebensdauer ist die Adresse veraltet.
Valid period	Dieser Parameter wird angezeigt, wenn Method Of Obtaining Prefixes auf Static configuration gesetzt ist. Gibt den Zeitraum an, für den eine Adresse gültig ist. Die gültige Lebensdauer muss länger als die bevorzugte Lebensdauer sein. Wenn die gültige Lebensdauer abläuft, wird die Adresse ungültig.
MTU	Gibt die Maximalgröße der Übertragungseinheit (Maximum Transmission Unit, MTU) für IPoE-Pakete an.
DNS Source On the LAN Side	Gibt die LAN-DNS-Quelle an. Für diesen Parameter kann DNS agent, WAN port oder Static configuration eingestellt werden.
WAN name	Dieser Parameter wird angezeigt, wenn DNS Source On the LAN Side auf WAN port gesetzt ist.
Preferred DNS	Dieser Parameter wird angezeigt, wenn DNS Source On the LAN Side auf Static configuration gesetzt ist.
Spare DNS	Dieser Parameter wird angezeigt, wenn DNS Source On the LAN Side auf Static configuration gesetzt ist.
Enable Route Advertisement	Gibt an, ob die Route Advertisement-Funktion aktiviert werden soll.

Parameter	Beschreibung
Enable DHCPv6 Server	Aktivieren Sie diese Funktion, wenn das Gateway angeschlossenen Geräten IPv6-Adressen zuweisen muss.
Resource Allocation Mode	Gibt den Modus an, in dem ein ONT angeschlossenen Geräten Präfixe und Adressen zuweist. Dieser Parameter kann auf Automatic , Manual oder Manual (strict) gesetzt werden.
Address/Prefix Assignment Mode	Gibt den Zuweisungsmodus für Adressen/Präfixe an. Hierfür kann DHCPv6 oder die statusfreie automatische Adresskonfiguration (SLAAC) eingestellt werden. Wenn für diesen Parameter SLAAC festgelegt ist, muss ULA Mode eingestellt werden. • DHCPv6: Gibt an, dass der LAN-seitige Host Adressen im DHCPv6-Modus abrufen. • SLAAC: Gibt an, dass der LAN-seitige Host Adressen im ND-Modus abrufen. Im SLAAC-Modus konfiguriert der Host Adressen automatisch. Die Adressinformationen enthalten das vom lokalen Router angegebene Präfix und die Schnittstellenkennung des Hosts. Wenn auf dem Link kein Router vorhanden ist, muss der Host die lokale Adresse automatisch konfigurieren, um mit lokalen Knoten kommunizieren zu können.
Other Information Assignment Mode	Gibt den Zuweisungsmodus für sonstige Informationen an. Sonstige Informationen beziehen sich auf die IPv6-Adresse der Nutzlast von Paketen wie beispielsweise DNS-Paketen. • DHCPv6: Gibt an, dass die Adresse im DHCPv6-Modus abgerufen wird. • SLAAC: Gibt an, dass die Adresse im ND-Modus abgerufen wird.
ULA Mode	Gibt den Modus der eindeutigen lokalen IPv6-Adresse (ULA) an. Eine ULA-Adresse beginnt mit dem Präfix fd. Ähnlich wie eine reservierte IPv4-Adresse wird die reservierte IPv6-Adresse für private Zwecke verwendet. Dadurch soll die Protokolleinheitlichkeit sichergestellt werden. Dieser Parameter kann auf Manuell, Automatisch oder Deaktiviert eingestellt werden. Deaktiviert wird empfohlen. • Deaktiviert: Diese wurde deaktiviert. • Automatisch: Das System weist Adressen automatisch zu. • Manuell: Die Adresse muss eingegeben werden. Wenn diese Option ausgewählt ist, muss auch jeweils ein Wert für Präfix, Präfixlänge, Bevorzugte Lebensdauer und Gültige Lebensdauer festgelegt werden.
Prefix	Gibt den Netzwerkadressraum an. IPv6 verwendet ein Präfix, um den Netzwerkadressraum anzugeben. Beispielsweise gibt 2001:251:e000::/48 einen Adressraum mit einem 48-Bit-Präfix an.
Prefix Length	Gibt die Präfixlänge der Netzwerkadresse an.

Parameter	Beschreibung
Preferred Lifetime	Gibt an, wie lange eine gültige Adresse den bevorzugten Status aufweist. Nach Ablauf der bevorzugten Lebensdauer ist die Adresse veraltet.
Valid Lifetime	Gibt an, wie lange eine Adresse gültig ist. Die gültige Lebensdauer muss länger als die bevorzugte Lebensdauer sein. Wenn die gültige Lebensdauer abläuft, wird die Adresse ungültig.

6.2.5 Konfiguration der statischen DHCPv6-IP

Klicken Sie auf die Registerkarte **Advanced** > **LAN** und wählen Sie in der Navigationsstruktur auf der linken Seite **DHCPv6 Static IP**. Im rechten Fensterbereich können Sie einer MAC-Adresse mithilfe der Schnittstellen-ID und der IPv6-GUA-Adresse eine IP-Adresse zuweisen. Die IPv6-GUA-Adresse ist eine Kombination aus Schnittstellen-ID und Präfix, die auf der LAN-Seite konfiguriert sind, wie in Abbildung 6-5 gezeigt.

Abbildung 6-5 Konfiguration der statischen DHCPv6-IP

DHCPv6 Static IP Configuration

On this page, you can assign an IP address to a MAC using a reserved interface ID and IPv6 GUA address. The IPv6 GUA address is a combination of the interface ID and prefix configured on the LAN side. If the method of obtaining LAN addresses is set to SLAAC, the configuration on this page does not take effect.

NewDelete

	MAC Address	Interface ID
	----	----

MAC address:

(AA:BB:CC:DD:EE:FF)

Interface ID:

(XXXX:XXXX:XXXX:XXXX)

ApplyCancel

6.3 Sicherheitskonfiguration

In diesem Abschnitt wird beschrieben, wie Sie die Sicherheit über die Webseite konfigurieren.

6.3.1 IPv4-Adressfilterung

1. Klicken Sie auf die Registerkarte **Advanced** > **Security** und wählen Sie in der Navigationsstruktur auf der linken Seite **IPv4 Filtering**. Aktivieren Sie im rechten Fensterbereich die IP-Adressfilterfunktion. Klicken Sie nach der Auswahl des Filtermodus auf **New**. Konfigurieren Sie dann im angezeigten Dialogfeld die Regel zum Filtern von IP-Adressen von der WAN-Schnittstelle zum LAN-Port, wie in Abbildung 6-6 gezeigt.

Abbildung 6-6 IPv4-Adressfilterung

IPv4 Address Filtering

On this page, you can configure WAN-to-LAN filter to prohibit some IP addresses in the WAN from accessing the LAN.

Enable IP Filter:

☐ (Device forwarding performance will deteriorate if the IP filtering function is enabled.)

Filter Mode:

Blacklist

New

Delete

Rule name	Protocol	Direction	LAN-Side IP Address	WAN-Side IP Address
----	----	----	----	----

Rule name:

Protocol:

All

Direction:

Bidirectional

LAN-Side Start IP Address:

Select...

LAN-Side End IP Address:

Select...

WAN-Side IP Address:

--

Apply

Cancel

2. Klicken Sie auf **Anwenden**.

Die IP-Adressfilterfunktion ist ein Sicherheitsmechanismus, der auf dem lokalen Gateway konfiguriert wird. Sie aktiviert oder deaktiviert alle oder einen Teil der Ports in einem Intranet-IP-Adressensegment, um mit allen oder einem Teil der Ports in einem Extranet-IP-Adressensegment zu kommunizieren. Die Konfiguration des IP-Adressfilters dient zur Begrenzung der Kommunikation zwischen einem Intranetgerät und einem Extranetgerät.

Tabelle 6-3 beschreibt die zugehörigen Parameter für den IPv4-Adressfilter.

Tabelle 6-3 Zugehörige Parameter für den IPv4-Adressfilter

Parameter	Beschreibung
Enable IP Filter	Gibt an, ob die IP-Adressfilterfunktion aktiviert werden soll.
Filter Mode	Gibt die IP-Adressfilterregel der Blockierungsliste oder der Vertrauensliste an. Blacklist: Gibt an, dass die Daten, die die Regel in der Filterregelliste erfüllen, nicht passieren dürfen. Whitelist: Gibt an, dass die Daten, die die Regel in der Filterregelliste erfüllen, passieren dürfen.

Parameter	Beschreibung
	• Hybrid: Gibt an, dass Pakete anhand der Upstream- bzw. Downstream-Richtung gefiltert werden. Bestimmte IP-Pakete in der Upstream- oder Downstream-Richtung dürfen (nicht) passieren. Es kann nur einer der vorgenannten Modi ausgewählt werden.
Protocol	Gibt die Art des Protokolls an; möglich sind TCP/UDP, TCP, UDP, ICMP oder ALL.
Rule Name	Gibt den Namen der Regel für die Filterung von IP-Adressen an.
Priority	Gibt die Priorität der IP-Adresse an. Dieser Parameter kann konfiguriert werden, wenn Filter Mode im Hybrid-Modus ausgewählt ist. • Bereich: 0 bis 255.
Direction	Gibt die Richtung an, für die die Filterregel gilt. • Bidirektional: Dieser Wert ist nur verfügbar, wenn Filter Mode auf Blacklist oder Whitelist gesetzt ist. Der Wert kann nicht geändert werden. • Upstream: Wenn dieser Wert im Hybridmodus ausgewählt wird, gilt die Filterregel für die Upstream-Richtung. Im Hybrid-Filtermodus kann nur Upstream oder Downstream ausgewählt werden. • Downstream: Wenn dieser Wert im Hybridmodus ausgewählt wird, gilt die Filterregel für die Downstream-Richtung.
LAN-side Start IP Address	Gibt die Start-IP-Adresse auf der LAN-Seite an.
LAN-side End IP Address	Gibt die End-IP-Adresse auf der LAN-Seite an.
LAN-side TCP Port	Gibt die Port-ID auf der LAN-Seite an. Dieser Parameter ist nur dann konfigurierbar, wenn für Protocol der Wert TCP/UDP oder TCP eingestellt ist.
LAN-side UDP Port	Gibt die Port-ID auf der LAN-Seite an. Dieser Parameter ist nur dann konfigurierbar, wenn für Protocol der Wert TCP/UDP oder UDP eingestellt ist.
WAN-side IP Address	Gibt die IP-Adresse auf der WAN-Seite an.
WAN-side TCP Port	Gibt die ID des WAN-seitigen Ports an. Dieser Parameter ist nur dann konfigurierbar, wenn für Protocol der Wert TCP/UDP oder TCP eingestellt ist.
WAN-side UDP Port	Gibt die ID des WAN-seitigen Ports an. Dieser Parameter ist nur dann konfigurierbar, wenn für Protocol der Wert TCP/UDP oder UDP eingestellt ist.
Action	Gibt die IP-Filteraktion an. Dieser Parameter kann konfiguriert werden, wenn Filter Mode im Hybrid-Modus ausgewählt ist.

Parameter	Beschreibung
	• Accept: akzeptiert Pakete, die der IP-Filterregel entsprechen. • Drop löscht Pakete, die der IP-Filterregel entsprechen.

6.3.2 MAC-Adressfilterung

1. Klicken Sie auf die Registerkarte **Advanced** > **Security** und wählen Sie in der Navigationsstruktur auf der linken Seite **MAC Filtering**. Klicken Sie nach der Aktivierung des MAC-Filters und der Auswahl des Filtermodus im rechten Fensterbereich auf **New**. Konfigurieren Sie in dem daraufhin angezeigten Dialogfeld die MAC-Filterregel so, dass der PC auf das Internet zugreifen darf, wie in Abbildung 6-7 gezeigt.

Abbildung 6-7 MAC-Adressfilterung

2. Klicken Sie auf **Anwenden**.

Die MAC-Adresslisten der PCs im Netzwerk werden im ONT gespeichert. Durch die Konfiguration von MAC-Filterregeln wird der Zugriff auf den Internet-Service für diejenigen PCs, die den Regeln entsprechen, aktiviert bzw. für diejenigen PCs, die den Regeln nicht entsprechen, deaktiviert. Ein PC kann mehrere IP-Adressen, aber nur eine eindeutige MAC-Adresse haben. Daher steuert die Konfiguration der MAC-Filterregeln die Internetdienstzugriffsrechte von PCs in einem LAN.

Tabelle 6-4 beschreibt die zugehörigen Parameter für den MAC-Filter.

Tabelle 6-4 Zugehörige Parameter für den MAC-Adressfilter

Parameter	Beschreibung
Enable MAC Filter	Gibt an, ob die MAC-Adressfilterfunktion aktiviert

Parameter	Beschreibung
	werden soll.
Filter Mode	Gibt die MAC-Adressfilterregel der Blockierungsliste oder der Vertrauensliste an. • Blacklist: Gibt an, dass die Daten, die die Regel in der Filterregelliste erfüllen, nicht passieren dürfen. • Whitelist: Gibt an, dass die Daten, die die Regel in der Filterregelliste erfüllen, passieren dürfen. Der Filtermodus ist der globale Konfigurationsmodus. Daher können der Blockierungslisten- und der Vertrauenslisten-Modus nicht gleichzeitig verwendet werden.
Device Name	Gibt den Gerätenamen in der MAC-Adressfilterregel an.
Source MAC Address	Gibt die MAC-Quelladresse in der MAC-Adressfilterregel an.

6.3.3 WLAN-MAC-Adressfilterung

1. Klicken Sie auf die Registerkarte **Advanced** > **Security** und wählen Sie in der Navigationsstruktur auf der linken Seite **Wi-Fi MAC Filtering**. Wählen Sie im rechten Fensterbereich **Enable WAN MAC filter**, legen Sie den Filtermodus fest und klicken Sie auf **New**. Konfigurieren Sie im daraufhin angezeigten Dialogfeld die SSID-basierte MAC-Adressfilterregel, wie in Abbildung 6-8 gezeigt.

Abbildung 6-8 WLAN-MAC-Adressfilterung

2. Klicken Sie auf **Anwenden**.

Tabelle 6-5 beschreibt die Konfigurationsparameter für die MAC-Filterung im WLAN-Netzwerk.

Tabelle 6-5 Parameter für MAC-Filterung im WLAN-Netzwerk

Parameter	Beschreibung
Enable WLAN MAC Filter	Aktiviert bzw. deaktiviert die WLAN-MAC-Filterfunktion.
Filter Mode	Gibt den MAC-Filtermodus an. Für diesen Parameter kann Blacklist oder Whitelist eingestellt werden. • Blacklist: Datenpakete, die nicht den Regeln in der Blockierungsliste entsprechen, werden nicht durchgelassen. • Whitelist: Datenpakete, die den Regeln in der Vertrauensliste entsprechen, werden durchgelassen. Der Vertrauenslisten- oder Blockierungslistenmodus ist eine globale Konfiguration. Die beiden Modi können nicht gleichzeitig verwendet werden.
SSID Index	Gibt den SSID-Index des WLAN an, für den die MAC-Adressfilterung konfiguriert wird.
Device Name	Gibt den Gerätenamen in der MAC-Adressfilterregel an.
Source MAC Address	Gibt die MAC-Quelladresse in den MAC-Adressfilterregeln an.

6.3.4 Jugendschutz

Klicken Sie auf die Registerkarte **Advanced > Security** und wählen Sie in der Navigationsstruktur auf der linken Seite **Parental Control**. Konfigurieren Sie im rechten Fensterbereich verschiedene Einschränkungen für die Surfdauer im Netzwerk und den Zugriff auf die Website an Arbeits- und Feiertagen. Auf diese Weise können Sie Ihren Kinder den Zugriff auf Netzwerke in bestimmten Zeitsegmenten und frei von unangemessenen Inhalten erlauben, wie in Abbildung 6-9 gezeigt.

Abbildung 6-9 Jugendschutz

Parental Control

On this page, you can set Internet access restrictions to allow your kids to use the Internet safely without direct supervision. Parental control allows you to set the times when your kids can use the Internet and which websites they can access.

[Overview](#) | [Template](#) | [Statistics](#) [Help](#)

☐ Apply on all devices ☒ Apply on specified devices

Device	Description	Binding Templates
---	---	---

Device

Specified Device

00:e0:4c: -- 192.168.18.2

Description

Device Description

Binding Templates

Template

template

Apply

Cancel

ANMERKUNG

Konfigurieren Sie die Vorlage gemäß den Anweisungen im Assistenten. Sie können oben rechts auf **Help** klicken, um bei Bedarf die Online-Hilfe zur Vorlagenkonfiguration anzuzeigen.

6.3.5 Präzise Gerätezugriffssteuerung

Klicken Sie auf die Registerkarte **Advanced** > **Security** und wählen Sie in der Navigationsstruktur auf der linken Seite **Precise Device Access Control**. Klicken Sie auf **New**. Legen Sie im angezeigten Fenster die Informationen für LAN-Port, SSID oder WAN-Port fest, einschließlich **Priority**, **Protocol** und **Mode**, wie in Abbildung 6-10 gezeigt.

Abbildung 6-10 Gerätezugriffssteuerung

Device Access Control

On this page, you can configure precise control for devices based on LAN, SSID, and WAN ports. IPv6 access supports only HTTP, and does not support TELNET, FTP, SSH, ICMP or SAMBA.

Enable precise device access control: ☒

	Priority	Port Name	Source IP Address	Application	Protocol	Port	Mode
☐	1	All LANs	--	TELNET	--	--	Permit
----	----	----	----	----	----	----	----

Type: ☒ Application ☐ User-defined

Priority: (The priority value range is 1-1024.)

Port Type:

Port Name: ☐ All ☐ LAN1 ☐ LAN2 ☐ LAN3 ☐ LAN4

Source IP Address: -- (IPv4 or IPv6 address)

Application: ☐ TELNET ☐ HTTP ☐ SSH ☐ FTP ☐ ICMP ☐ SAMBA

Mode: ☒ Permit ☐ Prohibit

6.3.6 Gerätezugriffssteuerung

Klicken Sie auf die Registerkarte **Advanced** > **Security** und wählen Sie in der Navigationsstruktur auf der linken Seite **Device Access Control**. Im rechten Fensterbereich können Sie die Berechtigung für den Zugriff auf das Gerät aktivieren oder deaktivieren, wie in Abbildung 6-11 gezeigt.

Abbildung 6-11 Gerätezugriffssteuerung

6.3.7 IPv6-Adressfilterung

1. Klicken Sie auf die Registerkarte **Advanced** > **Security** und wählen Sie in der Navigationsstruktur auf der linken Seite **IPv6 Filtering**. Aktivieren Sie im rechten Fensterbereich die IP-Adressfilterfunktion. Klicken Sie nach der Auswahl des Filtermodus auf **New**. Konfigurieren Sie dann im angezeigten Dialogfeld die Regel zum Filtern von IP-Adressen von der WAN-Schnittstelle zum LAN-Port, wie in Abbildung 6-12 gezeigt.

Abbildung 6-12 IPv6-Adressfilterung

2. Klicken Sie auf **Anwenden**.

Die IP-Adressfilterfunktion ist ein Sicherheitsmechanismus, der auf dem lokalen Gateway konfiguriert wird. Sie aktiviert oder deaktiviert alle oder einen Teil der Ports in einem Intranet-IP-Adressensegment, um mit allen oder einem Teil der Ports in einem Extranet-IP-Adressensegment zu kommunizieren. Die Konfiguration des IP-Adressfilters dient zur Begrenzung der Kommunikation zwischen einem Intranetgerät und einem Extranetgerät.

Tabelle 6-6 beschreibt die zugehörigen Parameter für den IPv6-Adressfilter.

Tabelle 6-6 Zugehörige Parameter für den IPv6-Adressfilter

Parameter	Beschreibung
Enable IP Filter	Gibt an, ob die IP-Adressfilterfunktion aktiviert werden soll.
Filter Mode	Gibt die IP-Adressfilterregel der Blockierungsliste oder der Vertrauensliste an. • Blacklist: Gibt an, dass die Daten, die die Regel in der Filterregelliste erfüllen, nicht passieren dürfen. • Whitelist: Gibt an, dass die Daten, die die Regel in der Filterregelliste erfüllen, passieren dürfen. • Hybrid: Gibt an, dass Pakete anhand der Upstream- bzw. Downstream-Richtung gefiltert werden. Bestimmte IP-Pakete in der Upstream- oder Downstream-Richtung dürfen (nicht) passieren. Es kann nur einer der vorgenannten Modi ausgewählt werden.
Rule name	Gibt den Namen der Regel für die Filterung von IP-Adressen an.
Protocol	Gibt die Art des Protokolls an; möglich sind TCP/UDP , TCP , UDP , ICMPv6 oder All .
Direction	Gibt die Richtung an, für die die Filterregel gilt. • Bidirektional: Dieser Wert ist nur verfügbar, wenn Filter Mode auf Blacklist oder Whitelist gesetzt ist. Der Wert kann nicht geändert werden. • Upstream: Wenn dieser Wert im Hybridmodus ausgewählt wird, gilt die Filterregel für die Upstream-Richtung. Im Hybrid-Filtermodus kann nur Upstream oder Downstream ausgewählt werden. • Downstream: Wenn dieser Wert im Hybridmodus ausgewählt wird, gilt die Filterregel für die Downstream-Richtung.
LAN-Side IP Address	Gibt die IP-Adresse auf der LAN-Seite an.
WAN-Side IP Address	Gibt die IP-Adresse auf der WAN-Seite an.

6.4 Weiterleitungsregeln

In diesem Abschnitt wird beschrieben, wie Sie die DMZ, die Portzuordnung und den Portauslöser über die Webseite konfigurieren.

6.4.1 DMZ-Funktion

1. Klicken Sie auf die Registerkarte **Advanced** > **Forward Rules** und wählen Sie in der Navigationsstruktur auf der linken Seite **DMZ Function**. Klicken Sie im rechten Fensterbereich auf **New**. Legen Sie im angezeigten Dialogfeld die Parameter für die DMZ fest, wie in Abbildung 6-13 gezeigt.

Abbildung 6-13 DMZ-Funktion

2. Klicken Sie auf **Anwenden**.

Die Demilitarized Zone (DMZ) ist eine Technologie, mit der das ONT alle empfangenen Pakete über einen bestimmten internen Server weiterleiten kann. Die Technologie ermöglicht es einem Computer im LAN, sich für alle Benutzern im Internet vollständig zugänglich zu machen, oder ermöglicht die gegenseitige Kommunikation ohne Einschränkungen zwischen einem Host mit einer angegebenen IP-Adresse und anderen Benutzern oder anderen Servern im Internet. Auf diese Weise können viele Anwendungen auf dem Host mit der angegebenen IP-Adresse ausgeführt werden. Der Host mit der angegebenen IP-Adresse erhält alle Verbindungen und Dateien, die erkannt werden können.

HINWEIS

Legen Sie ein LAN-seitiges Gerät, das keinen Website-Service oder andere Netzwerkdienste bereitstellt, nicht als DMZ-Host fest, da alle Ports eines DMZ-Hosts für das Internet geöffnet sind.

Tabelle 6-7 beschreibt die zugehörigen Parameter für die DMZ.

Tabelle 6-7 Zugehörige Parameter für die DMZ

Parameter	Beschreibung
Enable DMZ	Gibt an, ob die DMZ aktiviert werden soll.

Parameter	Beschreibung
WAN Name	Gibt den Namen der WAN-Schnittstelle an. Wenn die WAN-Schnittstelle nicht in der Portzuordnungstabelle enthalten ist, werden die Anwendungsanforderungen von der WAN-Verbindung direkt an den Host in der DMZ weitergeleitet.
Host Address	Gibt die IP-Adresse des DMZ-Hosts an.

6.4.2 IPv4-Portzuordnung

Die Portzuordnung gibt an, dass der Intranetserver offen für das Extranet sein darf (z. B. dass das Intranet einen WWW-Server oder FTP-Server für das Extranet bereitstellt). Die Portzuordnung ist die Zuordnung der IP-Adresse und der Port-ID des Intranethosts zur IP-Adresse und der entsprechenden Port-ID des Extranets, sodass Benutzer aus Extranets auf den Intranetserver zugreifen können. Bei der Portzuordnung können die Benutzer die IP-Adresse des Intranets nicht sehen, aber sie können die IP-Adresse des Extranets sehen.

Navigationsspfad

1. Klicken Sie auf die Registerkarte **Advanced** > **Forward Rules** und wählen Sie **IPv4 Port Mapping**. Legen Sie im angezeigten Dialogfeld die Parameter für die Portzuordnung fest, wie in Abbildung 6-14 gezeigt.

Abbildung 6-14 IPv4-Portzuordnung

IPv4 Port Mapping

On this page, you can set port mapping parameters to set up virtual servers on the LAN network and allow these servers to be accessed from the Internet.
Note: The well-known ports for voice services cannot be in the range of the mapping ports.

NewDelete

Mapping Name	WAN Name	Internal Host	External Host	Enable
----	----	----	----	----

Type: ☒ User-defined ☐ Application
Application: Select...
Enable Port Mapping: ☒
Mapping Name:
WAN Name: 1 TR069 INTERN
Internal Host: 192.168.18.2 * 00:e0:4c
External Source IP Address: --

Protocol: UDP Internal port number: 53 -- 53 *
External port number: 53 -- 53 External source port number: --
Delete
Add

ApplyCancel

- Klicken Sie auf **Anwenden**.

Konfigurationsbeispiel

Aktivieren Sie die Weiterleitung der von der WAN-Seite an das ONT mit der Ziel-WAN-Portnummer 2000 gesendeten Pakete an den LAN-seitigen PC mit der IP-Adresse 192.168.18.121 und die Portnummer wird in 3000 geändert.

IPv4 Port Mapping

On this page, you can set port mapping parameters to set up virtual servers on the LAN network and allow these servers to be accessed from the Internet.
Note: The well-known ports for voice services cannot be in the range of the mapping ports.

	Mapping Name	WAN Name	Internal Host	External Host	Enable
----	----	----	----	----	----

Type: ☒ User-defined ☐ Application

Application:

Enable Port Mapping: ☒

Mapping Name:

WAN Name:

Internal Host:

External Source IP Address: --

Protocol: Internal port number: -- *

External port number: -- External source port number: --

Parameterbeschreibung

Tabelle 6-8 beschreibt die zugehörigen Parameter für die IPv4-Portzuweisung.

Tabelle 6-8 Zugehörige Parameter für die IPv4-Portzuweisung

Parameter	Beschreibung
Type	Gibt den Typ der Portzuweisung an. Für diesen Parameter kann User-defined oder Application eingestellt werden. - Klicken Sie nach Auswahl von User-defined auf Add und konfigurieren Sie Protocol und Port number. - Bei Auswahl von Application müssen Protocol und Port number nicht konfiguriert werden.
Application	Gibt den Anwendungstyp der Portzuweisung an. Dieser Parameter kann nur konfiguriert werden, wenn der Parameter Type auf Application gesetzt ist.
Enable Port Mapping	Gibt an, ob die Portzuordnung aktiviert werden soll.
Mapping Name	Gibt den Namen der Portzuordnungsregel an.

Parameter	Beschreibung
WAN Name	Gibt den Namen der WAN-Schnittstelle an, in der die Portzuordnung aktiviert ist.
Internal Host	Gibt die IP-Adresse des Hosts an, dem der Port zugeordnet ist.
Protocol	Gibt den Protokolltyp des Portzuordnungspakets an, möglich sind TCP, UDP oder TCP/UDP.
External Source IP Address	Gibt die externe Quell-IP-Adresse an.
Internal port number	Gibt den internen Zielport für das Portzuweisungspaket an.
External port number	Gibt den externen Port für das externe Datenpaket an.
External source port number	Gibt den externen Quellport für das externe Datenpaket an.

6.4.3 Konfiguration des Port-Triggers

1. Klicken Sie auf die Registerkarte **Advanced** > **Forward Rules** und wählen Sie **Port Trigger**. Klicken Sie im rechten Fensterbereich auf **New**. Legen Sie im angezeigten Dialogfeld die Parameter für den Portauslöser fest, wie in Abbildung 6-15 gezeigt.

Abbildung 6-15 Konfiguration des Port-Triggers

Port Trigger Configuration

On this page, you can configure the range of the ports that are used by LAN-side applications to access the Internet. You can also enable the port automatically.
Note: The well-known ports for voice services cannot be in the range of open ports.

New
Delete

	WAN Name	Enable Port Trigger	Trigger Port	Open Port	Trigger Protocol	Open Protocol
----	----	----	----	----	----	----

Enable Port Trigger: ☒

WAN Name: 2_TR069_INTERNET_R_VID_10

Trigger Protocol: TCP

Open Protocol: TCP

Start Trigger Port:

End Trigger Port:

Start Open Port:

End Open Port:

Apply
Cancel

2. Klicken Sie auf **Anwenden**.

Der Portauslöser gibt an, dass ein bestimmter Extranet-Port automatisch aktiviert wird, wenn ein entsprechender Intranetport ein Paket sendet und das Paket dem Intranet-Port auf dem Host zugeordnet wird. Ein bestimmtes Zuordnungspaket wird vom ONT über das Intranet gesendet, sodass bestimmte Pakete des Extranets dem entsprechenden Host zugeordnet werden können. Ein bestimmter Port auf der Firewall des Gateways ist für den Fernzugriff durch einige Anwendungen geöffnet. Der Portauslöser kann den offenen Port der Firewall dynamisch aktivieren.

Tabelle 6-9 beschreibt die zugehörigen Parameter für den Portauslöser.

Tabelle 6-9 Zugehörige Parameter für den Portauslöser

Parameter	Beschreibung
Enable Port Trigger	Gibt an, ob der Portauslöser aktiviert werden soll.
WAN Name	Gibt den Namen der WAN-Schnittstelle an, auf der der Portauslöser aktiviert ist.
Trigger Protocol	Gibt den Protokolltyp des Portauslöserpakets an, möglich sind TCP, UDP oder TCP/UDP.
Open Protocol	Gibt den Protokolltyp des offenen Datenpakets an.
Start Trigger Port	Gibt den Startport des Ziels für das Portauslöserpaket an.
End Trigger Port	Gibt den Endport des Ziels für das Portauslöserpaket an.
Start Open Port	Gibt den Startport des Ziels für das offene Paket an.
End Open Port	Gibt den Endport des Ziels für das offene Paket an.

6.4.4 IPv6-Portzuordnung

Die Portzuordnung gibt an, dass der Intranetserver offen für das Extranet sein darf (z. B. dass das Intranet einen WWW-Server oder FTP-Server für das Extranet bereitstellt). Die Portzuordnung ist die Zuordnung der IP-Adresse und der Port-ID des Intranethosts zur IP-Adresse und der entsprechenden Port-ID des Extranets, sodass Benutzer aus Extranets auf den Intranetserver zugreifen können. Bei der Portzuordnung können die Benutzer die IP-Adresse des Intranets nicht sehen, aber sie können die IP-Adresse des Extranets sehen.

Navigationspfad

1. Klicken Sie auf die Registerkarte **Advanced > Forward Rules** und wählen Sie **IPv6 Port Mapping**. Legen Sie im angezeigten Dialogfeld die Parameter für die Portzuordnung fest, wie in Abbildung 6-16 gezeigt.

Abbildung 6-16 IPv6-Portzuordnung

IPv6 Port Mapping

1

In the navigation tree on the left, choose **Advanced > Forwarding > IPv6 Port Mapping**.

On this page, you can set port mapping parameters to set up virtual servers on the LAN network and allow these servers to be accessed from the Internet.
Note: The well-known ports for voice services cannot be in the range of the mapping ports.

< >

NewDelete

2

	Mapping Name	WAN Name	Internal Host	External Host	Enable
---	---	---	---	---	---

Type:

☒ User-defined☐ Application

Application:

Select...

Enable Port Mapping:☒

Mapping Name:

WAN Name:

4 INTERNET_R_GE_V

Internal Host:

External Source IP Address:

User-defined: user-defined port mapping; Application: port mapping for common applications (such as FTP and Telnet).

IP address of the internal server.

Range of ports used by the server.

Protocol:

TCP

Port number:

5030--5030*

Delete

Add

Click to add new port mapping rules.

3

ApplyCancel

2. Klicken Sie auf **Anwenden**.

Parameterbeschreibung

Tabelle 6-10 beschreibt die zugehörigen Parameter für die IPv6-Portzuweisung.

Tabelle 6-10 Zugehörige Parameter für die IPv6-Portzuweisung

Parameter	Beschreibung
Type	Gibt den Typ der Portzuweisung an. Für diesen Parameter kann User-defined oder Application eingestellt werden. - Klicken Sie nach Auswahl von User-defined auf Add und konfigurieren Sie Protocol und Port number. - Bei Auswahl von Application müssen Protocol und Port number nicht konfiguriert werden.
Application	Gibt den Anwendungstyp der Portzuweisung an. Dieser Parameter kann nur konfiguriert werden, wenn der Parameter Type auf

Parameter	Beschreibung
	Application gesetzt ist.
Enable Port Mapping	Gibt an, ob die Portzuordnung aktiviert werden soll.
Mapping Name	Gibt den Namen der Portzuordnungsregel an.
WAN Name	Gibt den Namen der WAN-Schnittstelle an, in der die Portzuordnung aktiviert ist.
Internal Host	Gibt die IP-Adresse des Hosts an, dem der Port zugeordnet ist.
External Source IP Address	Gibt die IP-Adresse der Quelle für das externe Datenpaket an.

6.5 Anwendung

In diesem Abschnitt wird beschrieben, wie Sie Funktionen wie die Zeiteinstellung über die Webseite konfigurieren.

6.5.1 USB-Anwendung

1. Klicken Sie auf die Registerkarte **Advanced** > **Application** und wählen Sie in der Navigationsstruktur auf der linken Seite **USB Application**. Im rechten Fensterbereich können Sie den FTP-Client und die Serverparameter so definieren, dass Dateien auf das Home-Gateway heruntergeladen und Ressourcen freigegeben werden können, wie in Abbildung 6-17 gezeigt.

Abbildung 6-17 FTP-Konfiguration

FTP Configuration

On this page, you can configure the FTP client for downloading a file to a storage device of the home gateway, and configure the FTP server for sharing resources.
When configuring the FTP server, enable the LAN-side or WAN-side FTP function and select character code in UTF-8 format.
Caution:
Do not remove and re-insert the USB storage device in use, because this may damage files in it.

FTP Client Configuration

FTP URL:
Port ID:
User Name:
Password:
Path: *

User Name	Password	Port ID	FTP URL	Path	Status
--	--	--	--	--	--

FTP Server Configuration

Enable FTP Server: ☐
User Name:
Password:
Port ID:
USB Device:
Root Path:

2. Klicken Sie auf **Anwenden**.

6.5.2 Gemeinsame Nutzung von Medien

1. Klicken Sie auf die Registerkarte **Advanced** > **Application** und wählen Sie in der Navigationsstruktur auf der linken Seite **Media Sharing**. Konfigurieren Sie im rechten Fensterbereich die Einstellungen für die gemeinsame Nutzung von Medien, wie in Abbildung 6-18 gezeigt.

Abbildung 6-18 Gemeinsame Nutzung von Medien

Media Sharing

In the media sharing service, you can share media information to devices that support DLNA. For example, you can share video, audio, and pictures to PCs, mobile devices, and consumption appliances. On this page, you can configure the sharing service switch and share directories.

⚠ Caution:
Do not remove and re-insert the USB storage device in use, because this may damage files in it.

Enable media sharing: ☐

Share path: ☐ All paths ☒ Specify path

New Delete

	Specify path
--	--

Specified path:

2. Klicken Sie auf **Anwenden**.

6.5.3 DDNS-Funktion

1. Klicken Sie auf die Registerkarte **Advanced** > **Application** und wählen Sie in der Navigationsstruktur **DDNS**. Konfigurieren Sie im rechten Fensterbereich die DDNS-Parameter, einschließlich **Service Provider**, **Service Port**, **Domain Name**, **User Name** und **Password**, wie in Abbildung 6-19 gezeigt.

Abbildung 6-19 DDNS-Funktion

DDNS Function

To obtain the dynamic DNS service, you must apply for a domain name from the dynamic DNS service provider to obtain the configuration information, including the host, user name, and password.

New Delete

WAN Name	Status	Service Provider	Domain Name
----	----	----	----

DDNS Service Information:

Enable DDNS: ☐

WAN Name:

Domain Name: *(1-255 characters)

Service provider Information:

Service Provider:

Host of the service provider: *(1-255 characters)

Service Port: *(1-65535)

User Name: *(1-256 characters)

Password: *(0-256 characters)

Encryption Mode:

Apply Cancel

DDNS Service State:

WAN Name	Domain Name	Run State	Last Update Time	Last Error
--	--	--	--	--

HINWEIS

BASE64 ist ein unsicherer Verschlüsselungsalgorithmus und darf nur in einer sicheren Umgebung verwendet werden.

2. Klicken Sie auf Anwenden.

Dynamic Domain Name Service (DDNS) verknüpft einen statischen Domännennamen mit der dynamischen IP-Adresse des Hosts.

Angenommen, Server A stellt einen HTTP- oder FTP-Dienst bereit und ist über Router mit dem Internet verbunden. Wenn Server A über DHCP eine IP-Adresse erhält oder Server A über PPPoE, PPTP oder L2TP mit dem Internet verbunden ist, dann ist die IP-Adresse eine dynamische IP-Adresse. Das heißt, dass sich die IP-Adresse von Server A jedes Mal ändern kann, wenn er eine Verbindung mit dem Internet initialisiert.

Die Zuordnung zwischen dem Domännennamen und der vom DNS-Server (Domain Name Service) bereitgestellten IP-Adresse ist statisch und die Zuordnung wird nicht aktualisiert, wenn die IP-Adresse geändert wird. Wenn die IP-Adresse des Servers A geändert wird, können Benutzer im Internet daher nicht mit Domännennamen auf Server A zugreifen.

Mit dem DDNS, bei dem ein statischer Domänenname mit der dynamischen IP-Adresse seines Hosts verknüpft wird, können Benutzer im Internet nur mit Domännennamen auf den Server zugreifen.

6.5.4 UPnP-Funktion

1. Klicken Sie auf die Registerkarte **Advanced** > **Application** und wählen Sie in der Navigationsstruktur auf der linken Seite **UPnP**. Legen Sie im rechten Fensterbereich fest, ob UPnP aktiviert werden soll, wie in Abbildung 6-20 gezeigt.

Abbildung 6-20 UPnP-Funktion

UPnP Function

On this page, you can enable or disable the universal plug-and-play (UPnP) function, which supports automatic discovery of multiple types of network devices. If this function is enabled for a device, the device can access networks, obtain an IP address, transmit data, discover other devices, and acquire the data of other devices.

Enable UPnP: ☒

Apply **Cancel**

Number	Description	External Port	Internal Port	Protocol	IP Address	Status
--	--	--	--	--	--	--

<< < 0/0 > >> Page Go

2. Klicken Sie auf **Anwenden**.

Universal Plug and Play (UPnP) ist der Name einer Gruppe von Protokollen. Das UPnP unterstützt konfigurationsfreie Vernetzung und automatische Erkennung verschiedener Netzwerkgeräte. Wenn UPnP aktiviert ist, kann das UPnP-fähige Gerät dynamisch mit dem Netzwerk verbunden werden, um die IP-Adresse zu erhalten, die Übertragungsleistung abzurufen, andere Geräte zu erkennen und die Leistung der anderen Geräte zu ermitteln. Das UPnP-fähige Gerät kann automatisch vom Netzwerk getrennt werden, ohne das Gerät oder andere Geräte zu beeinträchtigen.

Wenn UPnP aktiviert ist, findet der LAN-seitige PC automatisch das ONT, das als Peripheriegerät des PCs betrachtet wird und mittels Plug-and-Play angebunden ist. Nach der Ausführung der Anwendungssoftware auf dem PC werden die Anschlusszuordnungseinträge automatisch durch das UPnP-Protokoll auf dem ONT generiert, wodurch die Ausführungsgeschwindigkeit erhöht wird.

6.5.5 Statischer DNS

1. Klicken Sie auf die Registerkarte **Advanced** > **Application** und wählen Sie in der Navigationsstruktur **Static DNS**.

Konfigurieren Sie im rechten Fensterbereich die DNS-Parameter. Sie können auch die statische DNS-Domännennamenauflösung konfigurieren, wie in Abbildung 6-21 gezeigt.

Abbildung 6-21 Statischer DNS

Static DNS

On this page, you can configure static domain name resolution.

Static DNS Configuration

New Delete

Domain Name	IP Address
---	---

Domain Name:

IP Address:

Apply Cancel

2. Klicken Sie auf **Anwenden**.

6.6 WLAN

In diesem Abschnitt wird beschrieben, wie Sie grundlegende und erweiterte Konfigurationen des WLAN (2,4G und 5G) über die Webseite durchführen.

6.6.1 Grundeinstellungen für 2,4-GHz-Netzwerke

ANMERKUNG

Diese Seite wird nur von Dualband-Produkten unterstützt.

1. Klicken Sie auf die Registerkarte **Advanced** > **WLAN** und wählen Sie in der Navigationsstruktur auf der linken Seite **2.4G Basic Network Settings**. Konfigurieren Sie im rechten Fensterbereich die grundlegenden Parameter des WLAN-Netzwerks, wie in Abbildung 6-22 gezeigt.

Abbildung 6-22 Grundeinstellungen für 2,4-GHz-Netzwerke

2.4G Basic Network Settings

On this page, you can set the basic parameters of 2.4 GHz wireless network(When the 2.4 GHz wireless network is disabled, this page is blank).

⚠ Caution:

1. Wireless network services may be interrupted temporarily after you modify wireless network parameters.

2. It is recommended that you use the WPA2 or WPA/WPA2 authentication mode for security purposes.

☒ Enable WLAN

New

Delete

	SSID Index	SSID Name	SSID Status	Number of Associated Devices	Broadcast SSID	Security Configuration
☐	1	WirelessNet	Enabled	32	Enabled	Configured

SSID Configuration Details

SSID Name:

WirelessNet

* (1-32 characters)

Enable SSID:

☒

Number of Associated Devices:

32

* (1-32)

Broadcast SSID:

☒

Enable WMM:

☒

Authentication Mode:

WPA/WPA2 PreSharedKe

Encryption Mode:

TKIP&AES

WPA PreSharedKey:

.....

☒ Hide * (8-63 characters or 64 hexadecimal characters)

WPA Group Key Regeneration Interval:

3600

* (600-86400s)

Enable WPS:

☐

WPS Mode:

PBC

PBC:

Start WPS

Apply

Cancel

2. Klicken Sie auf **Anwenden**.

Tabelle 6-11 beschreibt die grundlegenden Parameter des WLAN-Netzwerks.

Tabelle 6-11 Grundkonfigurationen für WLAN-Netzwerke

Parameter	Beschreibung
Enable WLAN	Gibt an, ob das WLAN-Netzwerk aktiviert werden soll. Die folgenden Parameter können nur festgelegt werden, wenn das WLAN-Netzwerk aktiviert ist.
SSID Name	Gibt den Namen des WLAN-Netzwerks an. Dieser wird zur Unterscheidung verschiedener WLAN-Netzwerke verwendet. Er besteht aus maximal 32 Zeichen ohne Tabulatorzeichen. Eine Standard-SSID1 namens WirelessNet wird nach der Erstellung

Parameter	Beschreibung
	eines ONT erstellt. Das System kann bis zu vier SSIDs gleichzeitig konfigurieren und WLAN-Endgeräten keine IP-Adressen per SSID zuweisen.
Enable SSID	Gibt an, ob die Verbindung aktiviert werden soll.
Number of Associated Devices	Gibt die Anzahl der STAs an. Diese ist eine Ganzzahl zwischen 1 und 32.
Broadcast SSID	Gibt an, ob Übertragungen aktiviert oder ausgeblendet werden sollen. • Wenn das Optionsfeld aktiviert ist, bedeutet dies, dass die SSID-Übertragungsfunktion aktiviert ist. Das ONT überträgt regelmäßig die SSID, also den Namen des WLAN-Netzwerks. Auf diese Weise kann jede STA nach dem drahtlosen Netzwerk suchen. • Wenn das Optionsfeld nicht aktiviert ist, bedeutet dies, dass die SSID-Übertragungsfunktion deaktiviert ist. Die SSID wird ausgeblendet und die STA kann nicht nach dem drahtlosen Netzwerk suchen. Die SSID kann nur über eine Anfrage abgerufen werden.
Enable WMM	Gibt an, ob WLAN-Multimedia aktiviert werden soll.
Authentication Mode	Gibt den Authentifizierungsmodus für die STA an, die den Zugriff auf das WLAN-Netzwerk anfordert. Der Modus kann Open, Shared, WPA Pre-Shared Key, WPA2 Pre-Shared Key, WPA/WPA2 Pre-Shared Key, WPA Enterprise, WPA2 Enterprise oder WPA/WPA2 Enterprise lauten. Standardmäßig ist „Open“ festgelegt, sodass die STA ohne Authentifizierung auf das Netzwerk zugreifen kann.
Encryption Mode	Gibt den Verschlüsselungsmodus für die STA an, die den Zugriff auf das drahtlose Netzwerk anfordert. Der Verschlüsselungsmodus und die Verschlüsselungsparameter hängen vom Authentifizierungsmodus ab. • Wenn der Authentifizierungsmodus auf Open gesetzt ist, kann None oder WEP als Verschlüsselungsmodus eingestellt werden. • Wenn der Authentifizierungsmodus auf Shared gesetzt ist, ist die Verschlüsselung WEP. • Wenn als Authentifizierungsmodus WPA Pre-Shared Key, WPA2 Pre-Shared Key, WPA/WPA2 Pre-Shared Key, WPA Enterprise, WPA2 Enterprise oder WPA/WPA2 Enterprise eingestellt ist, kann für den Verschlüsselungsmodus AES, TKIP oder TKIP&AES festgelegt werden. HINWEIS WEP ist ein unsicherer Verschlüsselungsalgorithmus. Deshalb werden AES, TKIP, TKIP&AES oder ein Algorithmus mit einer höheren Sicherheitsstufe empfohlen.

ANMERKUNG

- Der auf einem WLAN-Terminal konfigurierte Sicherheitsmodus und die Verschlüsselung müssen mit den Einstellungen für das ONT übereinstimmen. Wenn der Verschlüsselungsmodus TKIP&AES oder AES auf dem WLAN-Terminal nicht konfiguriert ist, verfügt das WLAN-Terminal möglicherweise über eine alte Treiberversion. Wenn dies der Fall ist, aktualisieren Sie die Treiberversion.
- Wenn zwei SSIDs konfiguriert sind und Sie die Informationen einer SSID ändern, wählt die andere SSID erneut einen Kanal aus. Dadurch wird der Service für einige Minuten unterbrochen.
- Die WPS-Funktion kann für SSID1 nur in einem Band verwendet werden. Aktivieren Sie WPS außerdem nicht für mehrere SSIDs in demselben Band. Andernfalls funktioniert die WLAN-Verbindung möglicherweise nicht ordnungsgemäß.

6.6.2 Erweiterte Einstellungen für 2,4-GHz-Netzwerke

ANMERKUNG

Diese Seite wird nur von Dualband-Produkten unterstützt.

1. Klicken Sie auf die Registerkarte **Advanced** > **WLAN** und wählen Sie in der Navigationsstruktur auf der linken Seite **2.4G Advanced Network Settings**. Konfigurieren Sie im rechten Fensterbereich die grundlegenden Parameter des WLAN-Netzwerks, wie in Abbildung 6-23 gezeigt.

ANMERKUNG

Diese Seite ist leer, wenn **Enable WLAN** in **Advanced Configuration** nicht ausgewählt wurde.

Abbildung 6-23 Erweiterte Einstellungen für 2,4-GHz-Netzwerke

2.4G Advanced Network Settings

On this page, you can set the advanced parameters of 2.4 GHz wireless network(When the 2.4 GHz wireless network is disabled, this page is blank).

 **Caution:**
Wireless network services may be interrupted temporarily after you modify wireless network parameters.

Advanced Configuration

TX Power:	100%	
Channel:	Automatic	
Channel Width:	Auto 20/40 MHz	
Mode:	802.11b/g/n	
DTIM Period:	1	(1-255, default: 1)
Beacon Period:	100	(20-1000 ms, default: 100)
RTS Threshold:	2346	(1-2346 bytes, default: 2346)
Fragmentation Threshold:	2346	(256-2346 bytes, default: 2346)

2. Klicken Sie auf **Anwenden**.

Tabelle 6-12 beschreibt die WLAN-Parameter des WLAN-Netzwerks.

Tabelle 6-12 Erweiterte Parameter für das WLAN-Netzwerk

Parameter	Beschreibung
TX Power	Gibt die optische Übertragungsleistung von Funksignalen an. Für den Parameter kann 20% , 40% , 60% , 80% oder 100% eingestellt werden. Je größer der Wert ist, desto besser ist die Abdeckung der Funksignale.
Channel	Gibt den Kanal des WLAN-Netzwerks an. Der Kanal richtet sich nach dem Wert von Regulatory Domain .
Channel Width	Gibt die Breite des WLAN-Kanals an. Für den Parameter kann Auto 20/40 MHz , 20 MHz oder 40 MHz eingestellt werden.
Mode	Gibt den unterstützten WLAN-Netzwerkmodus an. Für den Parameter kann 802.11b , 802.11g , 802.11b/g oder 802.11b/g/n eingestellt werden.
DTIM Period	Gibt den Lieferzeitraum der Delivery Traffic Indication Map (DTIM) an. Der Wert liegt zwischen 1 und 255. Der Standardwert ist 1.
Beacon Period	Gibt die Lieferdauer der Signalleuchte an. Die Signalleuchte wird zur Kontaktaufnahme mit anderen AP-Geräten oder Netzwerksteuerungsgeräten verwendet. Der Wert liegt zwischen 20 ms und 1000 ms. Der Standardwert ist 100 ms.
RTS Threshold	Gibt den Schwellenwert für die zu sendende Anforderung (RTS) an. Dieser dient zur Vermeidung von Konflikten bei der Datenübertragung im WLAN. Je kleiner der RTS-Schwellenwert ist, desto höher ist die Übertragungsfrequenz von RTS-Paketen und desto schneller wird das System nach einer Unterbrechung oder einem Konflikt wiederhergestellt. Es werden jedoch mehr Bandbreiten verwendet, die den Durchsatz anderer Netzwerkdatenpakete beeinflussen. Der Wert liegt zwischen 1 Byte und 2346 Byte. Der Standardwert ist 2346 Byte.
Fragmentation Threshold	Gibt den Fragmentschwellenwert an. Wenn die Größe eines Pakets diesen Schwellenwert übersteigt, wird das Paket fragmentiert. Wenn die Übertragung der Fragmente unterbrochen wird, müssen nur diejenigen Teile erneut übertragen werden, die nicht erfolgreich übertragen worden sind. Der Wert liegt zwischen 256 Byte und 2346 Byte. Der Standardwert ist 2346 Byte.

6.6.3 Grundeinstellungen für 5G-Netzwerke

ANMERKUNG

Diese Seite wird nur von Dualband-Produkten unterstützt.

1. Klicken Sie auf die Registerkarte **Advanced** > **WLAN** und wählen Sie in der Navigationsstruktur auf der linken Seite **5G Basic Network Settings**. Konfigurieren Sie die grundlegenden Parameter des 5G-WLAN-Netzwerks im rechten Fensterbereich, wie in Abbildung 6-24 gezeigt.

Abbildung 6-24 Grundeinstellungen für 5G-Netzwerke

5G Basic Network Settings

On this page, you can set the basic parameters of 5 GHz wireless network(When the 5 GHz wireless network is disabled, this page is blank).

Caution:

1. Wireless network services may be interrupted temporarily after you modify wireless network parameters.
2. It is recommended that you use the WPA2 or WPA/WPA2 authentication mode for security purposes.

☒ **Enable WLAN**

New

Delete

	SSID Index	SSID Name	SSID Status	Number of Associated Devices	Broadcast SSID	Security Configuration
☐	5	WirelessNet-5G	Enabled	32	Enabled	Configured

SSID Configuration Details

SSID Name: * (1-32 characters)

Enable SSID: ☒

Number of Associated Devices: * (1-32)

Broadcast SSID: ☒

Enable WMM: ☒

Authentication Mode:

Encryption Mode:

WPA PreSharedKey: ☒ Hide * (8-63 characters or 64 hexadecimal characters)

WPA Group Key Regeneration Interval: * (600-86400s)

Enable WPS: ☐

WPS Mode:

PBC:

Apply

Cancel

2. Klicken Sie auf **Anwenden**.

Tabelle 6-13 beschreibt die Grundeinstellungen für 5G-WLAN-Netzwerke.

Tabelle 6-13 Grundeinstellungen für 5G-Netzwerke

Parameter	Beschreibung
Enable WLAN	Gibt an, ob das WLAN-Netzwerk aktiviert werden soll. Die folgenden Parameter können nur festgelegt werden, wenn das WLAN-Netzwerk aktiviert ist.
SSID Name	Gibt den Namen des WLAN-Netzwerks an. Dieser wird zur Unterscheidung verschiedener WLAN-Netzwerke verwendet. Er besteht aus maximal 32 Zeichen ohne Leer- und Tabulatorzeichen. Eine Standard-SSID1 namens WirelessNet wird nach der Erstellung eines ONT erstellt. Das System kann bis zu vier SSIDs gleichzeitig konfigurieren und WLAN-Endgeräten keine IP-Adressen per SSID zuweisen.
Enable SSID	Gibt an, ob die Verbindung aktiviert werden soll.
Number of Associated Devices	Gibt die Anzahl der STAs an. Diese ist eine Ganzzahl zwischen 1 und 32.
Broadcast SSID	Gibt an, ob Übertragungen aktiviert oder ausgeblendet werden sollen. - Wenn das Optionsfeld aktiviert ist, bedeutet dies, dass die SSID-Übertragungsfunktion aktiviert ist. Das ONT überträgt regelmäßig die SSID, also den Namen des WLAN-Netzwerks. Auf diese Weise kann jede STA nach dem drahtlosen Netzwerk suchen. - Wenn das Optionsfeld nicht aktiviert ist, bedeutet dies, dass die SSID-Übertragungsfunktion deaktiviert ist. Die SSID wird ausgeblendet und die STA kann nicht nach dem drahtlosen Netzwerk suchen. Die SSID kann nur über eine Anfrage abgerufen werden.
Enable WMM	Gibt an, ob WLAN-Multimedia aktiviert werden soll.
Authentication Mode	Gibt den Authentifizierungsmodus für die STA an, die den Zugriff auf das WLAN-Netzwerk anfordert. Der Modus kann „Open“, „Shared“, „WPA Pre-Shared Key“, „WPA2 Pre-Shared Key“, „WPA/WPA2 Pre-Shared Key“, „WPA Enterprise“, „WPA2 Enterprise“ oder „PA/WPA2 Enterprise“ lauten. Standardmäßig ist „Open“ festgelegt, sodass die STA ohne Authentifizierung auf das Netzwerk zugreifen kann.
Encryption Mode	Gibt den Verschlüsselungsmodus für die STA an, die den Zugriff auf das drahtlose Netzwerk anfordert. Der Verschlüsselungsmodus und die Verschlüsselungsparameter hängen vom Authentifizierungsmodus ab. Wenn der Authentifizierungsmodus auf Open gesetzt ist, kann None oder WEP als Verschlüsselungsmodus eingestellt werden.

Parameter	Beschreibung
	• Wenn der Authentifizierungsmodus auf Shared gesetzt ist, ist die Verschlüsselung WEP. • Wenn als Authentifizierungsmodus WPA Pre-Shared Key, WPA2 Pre-Shared Key, WPA/WPA2 Pre-Shared Key, WPA Enterprise, WPA2 Enterprise oder WPA/WPA2 Enterprise eingestellt ist, kann für den Verschlüsselungsmodus AES, TKIP oder TKIP&AES festgelegt werden. HINWEIS WEP ist ein unsicherer Verschlüsselungsalgorithmus. Deshalb werden AES, TKIP, TKIP&AES oder ein Algorithmus mit einer höheren Sicherheitsstufe empfohlen.

ANMERKUNG

- Der auf einem WLAN-Terminal konfigurierte Sicherheitsmodus und die Verschlüsselung müssen mit den Einstellungen für das ONT übereinstimmen. Wenn der Verschlüsselungsmodus TKIP&AES oder AES auf dem WLAN-Terminal nicht konfiguriert ist, verfügt das WLAN-Terminal möglicherweise über eine alte Treiberversion. Wenn dies der Fall ist, aktualisieren Sie die Treiberversion.
- Wenn zwei SSIDs konfiguriert sind und Sie die Informationen einer SSID ändern, wählt die andere SSID erneut einen Kanal aus. Dadurch wird der Service für einige Minuten unterbrochen.
- Die WPS-Funktion kann für SSID1 nur in einem Band verwendet werden. Aktivieren Sie WPS außerdem nicht für mehrere SSIDs in demselben Band. Andernfalls funktioniert die WLAN-Verbindung möglicherweise nicht ordnungsgemäß.

6.6.4 Erweiterte Einstellungen für 5G-Netzwerke

ANMERKUNG

Diese Seite wird nur von Dualband-Produkten unterstützt.

1. Klicken Sie auf die Registerkarte **Advanced** > **WLAN** und wählen Sie in der Navigationsstruktur auf der linken Seite **5G Advanced Network Settings**. Konfigurieren Sie die grundlegenden Parameter des 5G-WLAN-Netzwerks im rechten Fensterbereich, wie in Abbildung 6-25 gezeigt.

ANMERKUNG

Diese Seite ist leer, wenn **Enable WLAN** in **5G Basic Network Settings** nicht ausgewählt wurde.

Abbildung 6-25 Erweiterte Einstellungen für 5G-Netzwerke

5G Advanced Network Settings

On this page, you can set the advanced parameters of 5 GHz wireless network(When the 5 GHz wireless network is disabled, this page is blank).

⚠ Caution:

Wireless network services may be interrupted temporarily after you modify wireless network parameters.

Advanced Configuration

TX Power:

100%

Channel:

Automatic

Channel Width:

Auto 20/40/80 MHz

Mode:

802.11a/n/ac

Band Steering:

☒

DTIM Period:

1

(1-255, default: 1)

Beacon Period:

100

(20-1000 ms, default: 100)

RTS Threshold:

2346

(1-2346 bytes, default: 2346)

Fragmentation Threshold:

2346

(256-2346 bytes, default: 2346)

Apply

Cancel

2. Klicken Sie auf **Anwenden**.

Tabelle 6-14 beschreibt die WLAN-Parameter des 5G-WLAN-Netzwerks.

Tabelle 6-14 Erweiterte Parameter für das WLAN-Netzwerk

Parameter	Beschreibung
TX Power	Gibt die optische Übertragungsleistung von Funksignalen an. Für den Parameter kann 20% , 40% , 60% , 80% oder 100% eingestellt werden. Je größer der Wert ist, desto besser ist die Abdeckung der Funksignale.
Channel	Gibt den Kanal des WLAN-Netzwerks an. Der Kanal richtet sich nach dem Wert von Regulatory Domain .
Channel Width	Gibt die Breite des WLAN-Kanals an. Für den Parameter kann Auto 20/40/80 MHz , Auto 20/40 MHz , 20 MHz oder 40 MHz eingestellt werden.
Mode	Gibt den unterstützten WLAN-Netzwerkmodus an. Für den Parameter kann 802.11b , 802.11g , 802.11b/g oder 802.11b/g/n eingestellt werden.
Band steering	Gibt an, ob das Band Steering aktiviert werden soll.
DTIM Period	Gibt den Lieferzeitraum der Delivery Traffic Indication Map (DTIM) an. Der Wert liegt zwischen 1 und 255. Der Standardwert ist 1.
Beacon Period	Gibt die Lieferdauer der Signalleuchte an. Die Signalleuchte wird zur Kontaktaufnahme mit anderen AP-Geräten oder

Parameter	Beschreibung
	Netzwerksteuerungsgeräten verwendet. Der Wert liegt zwischen 20 ms und 1000 ms. Der Standardwert ist 100 ms.
RTS Threshold	Gibt den Schwellenwert für die zu sendende Anforderung (RTS) an. Dieser dient zur Vermeidung von Konflikten bei der Datenübertragung im WLAN. Je kleiner der RTS-Schwellenwert ist, desto höher ist die Übertragungsfrequenz von RTS-Paketen und desto schneller wird das System nach einer Unterbrechung oder einem Konflikt wiederhergestellt. Es werden jedoch mehr Bandbreiten verwendet, die den Durchsatz anderer Netzwerkdatenpakete beeinflussen. Der Wert liegt zwischen 1 Byte und 2346 Byte. Der Standardwert ist 2346 Byte.
Fragmentation Threshold	Gibt den Fragmentschwellenwert an. Wenn die Größe eines Pakets diesen Schwellenwert übersteigt, wird das Paket fragmentiert. Wenn die Übertragung der Fragmente unterbrochen wird, müssen nur diejenigen Teile erneut übertragen werden, die nicht erfolgreich übertragen worden sind. Der Wert liegt zwischen 256 Byte und 2346 Byte. Der Standardwert ist 2346 Byte.

6.6.5 Automatische WLAN-Abschaltung

- Klicken Sie auf die Registerkarte **Advanced** > **WLAN** und wählen Sie in der Navigationsstruktur auf der linken Seite **Automatic WiFi Shutdown**. Konfigurieren Sie im rechten Fensterbereich das Zeitsegment für die geplante WLAN-Abschaltung, damit das WLAN-Netzwerk bei Inaktivität automatisch heruntergefahren wird, wie in Abbildung 6-26 gezeigt.

Abbildung 6-26 Automatische WLAN-Abschaltung

Automatic Wi-Fi Shutdown

On this page, you can enable automatic Wi-Fi shutdown in a specified period as required.

Automatic Shutdown Configuration

☒ Enable automatic Wi-Fi shutdown

	Start	End	Mon	Tues	Wed	Thur	Fri	Sat	Sun	All
1	:	:	☒	☒	☒	☒	☒	☒	☒	☒
2	:	:	☒	☒	☒	☒	☒	☒	☒	☒
3	:	:	☒	☒	☒	☒	☒	☒	☒	☒
4	:	:	☒	☒	☒	☒	☒	☒	☒	☒

2. Klicken Sie auf **Anwenden**.

6.6.6 Verwaltung der WLAN-Abdeckung

1. Klicken Sie auf die Registerkarte **Advanced** > **WLAN** und wählen Sie in der Navigationsstruktur auf der linken Seite **WiFi Coverage**. Geben Sie im rechten Fensterbereich die für die intelligente WLAN-Abdeckung verwendete SSID an und fügen Sie dem WLAN-Netzwerk die erkannten externen AP-Geräte hinzu, wie in Abbildung 6-27 und Abbildung 6-28 gezeigt.

Abbildung 6-27 Konfiguration der WLAN-Parameter

Wi-Fi Coverage Management

On this page, you can specify the SSID for a Wi-Fi network and add the scanned external AP to this Wi-Fi network. Then, the external AP and this device construct an entire Wi-Fi network and your wireless devices can seamlessly access this network.

Wi-Fi Parameter Setting

Wi-Fi Network Management

Set 2.4G Parameters

Go to the 2.4G Basic Network Settings web page

SSID Name	Broadcast SSID	Authentication and Encryption Mode	Password
SSID1	Enabled	WPA-WPA2-Personal	•••••••• ☒ Hide

Set 5G Parameters

Go to the 5G Basic Network Settings web page

SSID Name	Broadcast SSID	Authentication and Encryption Mode	Password
SSID2	Enabled	WPA-WPA2-Personal	•••••••• ☒ Hide

Select a policy to synchronize Wi-Fi parameters to the newly detected external AP.

☐ Do not enable automatic synchronization.

☒ Specify the SSID for automatic synchronization.

SSID1(2.4G) ▼

SSID2(5G) ▼

☐ Enable best-effort synchronization based on AP capabilities.

External AP List

Device Model	Serial Number	Status	Online Duration	Configuration Status
--	--	--	--	--

Abbildung 6-28 WLAN-Netzwerkverwaltung

Wi-Fi Coverage Management

On this page, you can specify the SSID for a Wi-Fi network and add the scanned external AP to this Wi-Fi network. Then, the external AP and this device construct an entire Wi-Fi network and your wireless devices can seamlessly access this network.

Wi-Fi Parameter Setting

Wi-Fi Network Management

☐ Synchronize WLAN frequency band status to the external AP

☐ Enable Video Retransmission Switch

RTCP Port

8027

1~65535, default value:8027

Apply

Cancel

Wi-Fi Link Switching Sensitivity

LowMediumHigh

Apply

Cancel

Wi-Fi Operation for Entire Network

Forced channel reselection

Start

Automatic Network Topology Adjustment Policy

☐ No cascaded STAs

☒ Deteriorated cascade link

☒ The cascade link rate is lower than the threshold.

☐ The air interface packet loss rate of the cascade link exceeds the threshold.

Apply

Cancel

Cascade Link Threshold

Name	Value	Description
Low rate threshold	200	kbps (0 to 65535; default value: 200)
PLR threshold	5	% (0 to 100; default value: 5)

Apply

Cancel

2. Klicken Sie auf **Anwenden**.

6.7 Systemverwaltung

In diesem Abschnitt wird beschrieben, wie Sie das System über die Webseite verwalten, einschließlich der Konfiguration von TR-069, Kontoverwaltung und ONT-Authentifizierung.

6.7.1 Kontoverwaltung

1. Wählen Sie in der Navigationsstruktur auf der linken Seite **Advanced > System Management > Account Management**. Ändern Sie im rechten Fensterbereich das Kennwort des Common User, wie in Abbildung 6-29 gezeigt.

Abbildung 6-29 Kontoverwaltung

The screenshot shows the 'Account Management' web page. At the top, it says 'On this page, you can change the password of the current login user to ensure security and make it easy to remember.' Below this, the 'User Name' is listed as 'Epuser'. There are three password input fields: 'Old Password', 'New Password', and 'Confirm Password'. To the right of these fields, three password rules are listed: 1. The password must contain at least 6 characters. 2. The password must contain at least two of the following combinations: digits, uppercase letters, lowercase letters; and special characters. Special characters can be the following: ` ~ ! @ # \$ % ^ & * () _ = + \ | [{ }] ; : ' " < , . > / ? . 3. The password cannot be any user name or user name in reverse order. At the bottom of the form, there are two buttons: 'Apply' and 'Cancel'.

HINWEIS

- Nachdem sich der Benutzer mit dem Standardnamen und -kennwort des Common User bei der Weboberfläche des ONT angemeldet hat, wird die Schnittstelle **Account Management** automatisch angezeigt und der Benutzer wird aufgefordert, das ursprüngliche Kennwort zu ändern. Nachdem der Benutzer das Kennwort erfolgreich geändert hat, wird die Schnittstelle **Account Management** bei den folgenden Anmeldungen nicht mehr angezeigt.
- Um die Systemsicherheit zu erhöhen, ändern Sie das Kennwort anforderungsgemäß nach der ersten erfolgreichen Anmeldung. Sie sollten das Kennwort in regelmäßigen Abständen ändern.

2. Klicken Sie auf **Anwenden**.

6.7.2 ONT-Authentifizierung

1. Wählen Sie in der Navigationsstruktur auf der linken Seite **Advanced > System Management > ONT Authentication**. Im rechten Fensterbereich können Sie den Authentifizierungsmodus für die Registrierung des ONT auf dem OLT anzeigen oder ändern, wie in Abbildung 6-30 gezeigt.

Abbildung 6-30 ONT-Authentifizierung

ONT Authentication

On this page, you can change ONT authentication parameters to ensure that it can be authenticated on the OLT.

Authentication Mode: ☐ LOID ☒ Password

Password Mode: ASCII string ▼

Password: ☒ Hide(a string of 10 characters at most)

Apply Cancel

2. Klicken Sie auf **Anwenden**.

6.7.3 Hinweise zu Open Source-Software

Wählen Sie in der Navigationsstruktur auf der linken Seite **Advanced > System Management > Open Source Software Notice**. Im rechten Fensterbereich können Sie den Open-Source-Software-Hinweis für das Produkt anzeigen, wie in Abbildung 6-31 gezeigt.

Abbildung 6-31 Hinweise zu Open Source-Software

OPEN SOURCE SOFTWARE NOTICE

This part contains an open source software notice for this product. The open source software licenses are granted by the respective right holders. The open source licenses prevail all other license information with regard to the respective open source software contained in the product.

Warranty Disclaimer

THE OPEN SOURCE SOFTWARE IN THIS PRODUCT IS DISTRIBUTED IN THE HOPE THAT IT WILL BE USEFUL, BUT WITHOUT ANY WARRANTY, WITHOUT EVEN THE IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SEE THE APPLICABLE LICENSES FOR MORE DETAILS.

Copyright Notice and License Texts

License: Linux GPL v2 License

NOTE! This copyright does *not* cover user programs that use kernel services by normal system calls - this is merely considered normal use of the kernel, and does *not* fall under the heading of "derived work";. Also note that the GPL below is copyrighted by the Free Software Foundation, but the instance of code that it refers to (the Linux kernel) is copyrighted by me and others who actually wrote it.

Also note that the only valid version of the GPL as far as the kernel is concerned is this particular version of the license (ie v2, not v2.2 or v3.x or whatever), unless explicitly otherwise stated.

Linus Torvalds

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public

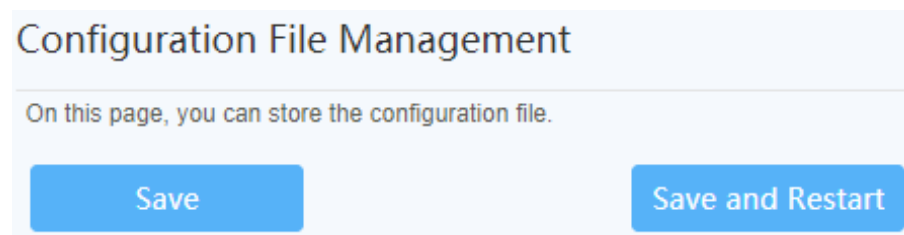
6.8 Wartungsdiagnose

In diesem Abschnitt wird beschrieben, wie Sie das System über die Webseite warten, einschließlich der Methode für den Neustart des Geräts, die Fehlerdiagnose und die Aktualisierung der Softwareversion.

6.8.1 Verwaltung von Konfigurationsdateien

Klicken Sie auf die Registerkarte **Advanced > Maintenance diagnose** und wählen Sie in der Navigationsstruktur auf der linken Seite **Configuration File Management**. Klicken Sie im rechten Fensterbereich nach Bedarf auf die Schaltfläche, wie in Abbildung 6-32 gezeigt.

Abbildung 6-32 Verwaltung von Konfigurationsdateien



- Klicken Sie auf **Save**, um die Konfigurationsdatei im Flashspeicher zu speichern. Dies verhindert Datenverluste durch den Neustart des Geräts.
- Klicken Sie auf **Save and Restart**, um die Konfigurationsdatei zu speichern und das ONT neu zu starten.

6.8.2 Wartung

Wählen Sie in der Navigationsstruktur auf der linken Seite **Advanced > Maintenance Diagnose > Maintenance**.

1. Geben Sie im rechten Fensterbereich die Ziel-IP-Adresse oder den Hostnamen unter **Target** und **WAN name** ein und klicken Sie anschließend auf **Start**, wie in Abbildung 6-33 gezeigt.

Abbildung 6-33 Ping-Test

The screenshot shows a web interface titled "Maintenance". Below the title is a subtitle: "On this page, you can use the maintenance and diagnosis function to check LAN or Internet connectivity." There are two main sections: "Ping Test" and "Traceroute Test".

Ping Test section:

- Target:
- WAN Name:
- Data Block Size: (32-65500; default: 56)
- Repetitions: (1-3600; default without inputting: 4)
- Maximum Timeout Time: (1-4294967s; default: 10)
- DSCP Value: (0-63; default without inputting: 0)

Buttons:

Traceroute Test section:

- Target:
- WAN Name:
- Data Block Size: (38-32768; default: 38)

Buttons:

- Bei einem erfolgreichen Ping-Test wird für **The result PASS** angezeigt, das heißt, das ONT kann mit dem Gerät mit der Ziel-IP-Adresse interagieren.
 - Ist der Ping-Test nicht erfolgreich, wird für **The result FAIL** angezeigt, das heißt, das ONT kann nicht mit dem Gerät mit der Ziel-IP-Adresse interagieren.
2. Klicken Sie im rechten Fensterbereich auf **Start Hardware Fault Detection**, um die Hardwarefehlererkennung zu starten, wie in Abbildung 6-34 gezeigt.

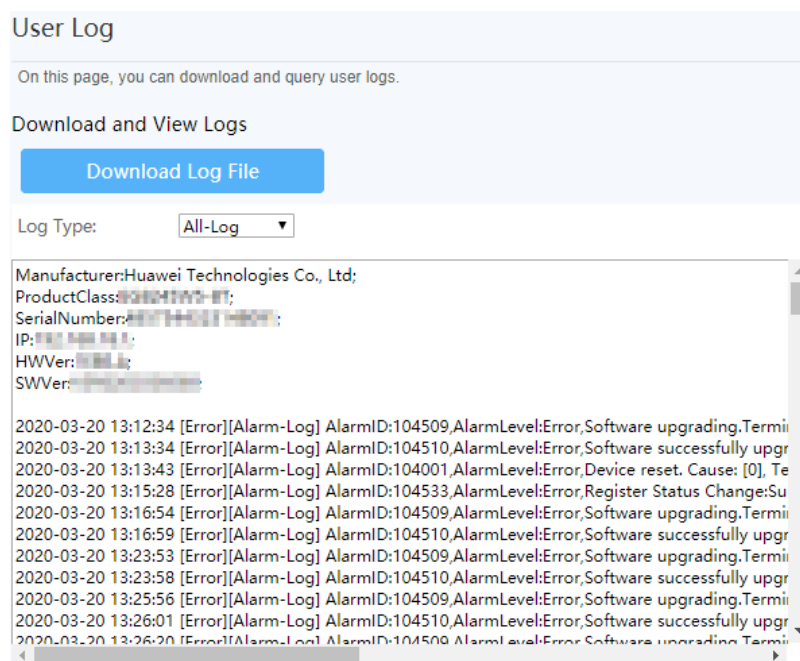
Abbildung 6-34 Hardware-Fehlererkennung

The screenshot shows a web interface titled "Hardware Fault Detection". Below the title is a button labeled "Start Hardware Fault Detection". Below the button, the text "Performing hardware fault detection...Please wait." is displayed in red.

6.8.3 Benutzerprotokoll

Wählen Sie in der Navigationsstruktur auf der linken Seite **Advanced > System Management > User Log**. Klicken Sie im rechten Fensterbereich auf **Download log File**. Klicken Sie im angezeigten Dialogfeld auf **Save**, geben Sie den Pfad zum Speichern der Protokolldatei an und speichern Sie die Datei auf der lokalen Festplatte, wie in Abbildung 6-35 gezeigt.

Abbildung 6-35 Benutzerprotokoll



HINWEIS

Wenn der IE8 zum Herunterladen der Protokolldatei verwendet wird und Sie mehr als 10 Sekunden nach dem Herunterladen auf die Schaltfläche „Speichern“ klicken, ist die heruntergeladene Protokolldatei unvollständig.

6.8.4 Firewallprotokoll

Klicken Sie auf die Registerkarte **Advanced > Maintenance Diagnose** und wählen Sie in der Navigationsstruktur auf der linken Seite **Firewall Log**. Im rechten Fensterbereich können Sie Protokolle anzeigen und Protokolldateien herunterladen, wie in Abbildung 6-36 gezeigt.

Abbildung 6-36 Firewallprotokoll

Firewall Log

On this page, you can configure, download, and query a firewall log.

Enable Firewall ☐ (If enabled, device forwarding performance will be deteriorated)

Log:

New Delete

	Log Rule Status	Log Access Direction	Log Rule Action
----	----	----	----

Enable Log Rule: ☒

Log Access Direction: From Internet to LAN ▼*

Log Rule Action: Accept ▼*

Apply

Cancel

Download and View Logs

Download Log File

Manufacturer:Huawei Technologies Co., Ltd;

ProductClass: ;

SerialNumber: ;

IP:192.168.100.1;

HWVer:150D.A;

SWVer: ;

Klicken Sie auf **Enable Firewall Log**, um die Funktion zu aktivieren oder zu deaktivieren. Bei Aktivierung ist die Weiterleitungsleistung des Geräts beeinträchtigt.

Klicken Sie auf **New**, um die Firewall-Regeln zu konfigurieren.

Klicken Sie auf **Download Log File**. Klicken Sie im angezeigten Dialogfeld auf **Save**, geben Sie den Pfad zum Speichern der Protokolldatei an und speichern Sie die Protokolldatei auf der lokalen Festplatte.

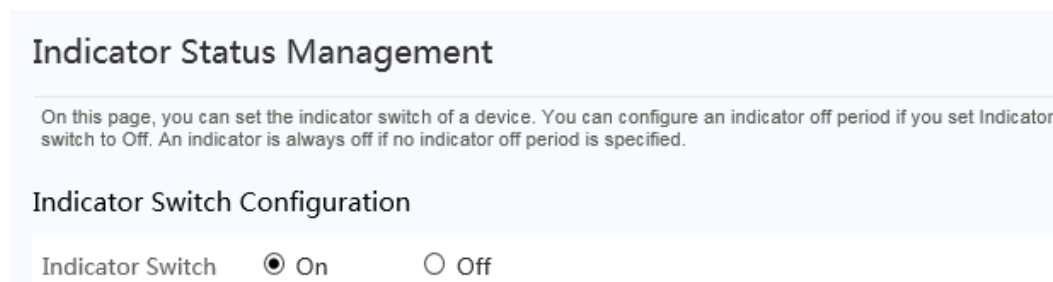
HINWEIS

Wenn der IE8 zum Herunterladen der Protokolldatei verwendet wird und Sie mehr als 15 Sekunden nach dem Herunterladen auf die Schaltfläche „Speichern“ klicken, ist die heruntergeladene Protokolldatei unvollständig.

6.8.5 Verwaltung des Anzeigestatus

Klicken Sie auf die Registerkarte **Advanced > Maintenance Diagnose** und wählen Sie in der Navigationsstruktur auf der linken Seite **Indicator Status Management**. Legen Sie im rechten Fensterbereich den Anzeigeschalter fest, wie in Abbildung 6-37 gezeigt.

Abbildung 6-37 Verwaltung des Anzeigestatus



Indicator Status Management

On this page, you can set the indicator switch of a device. You can configure an indicator off period if you set Indicator switch to Off. An indicator is always off if no indicator off period is specified.

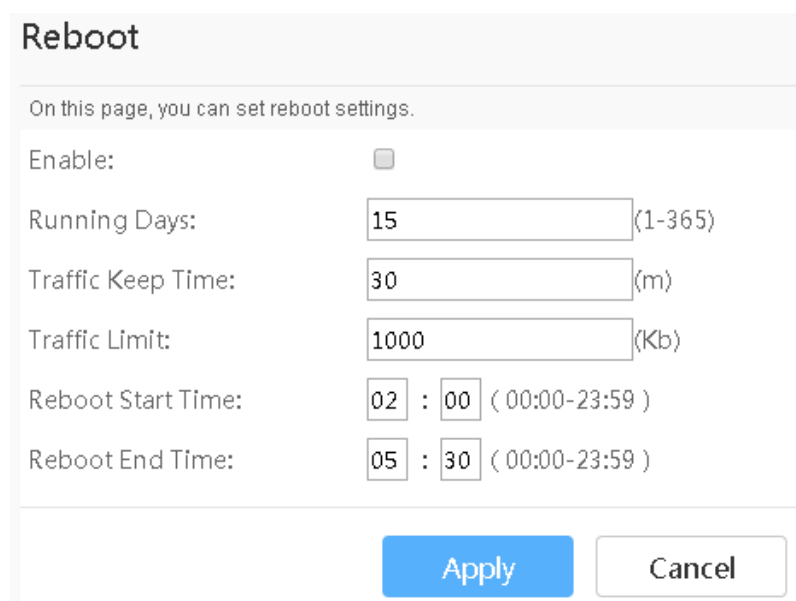
Indicator Switch Configuration

Indicator Switch ☒ On ☐ Off

6.8.6 Neustart

Klicken Sie auf die Registerkarte **Advanced > Maintenance Diagnose** und wählen Sie in der Navigationsstruktur auf der linken Seite **Reboot**. Im rechten Fensterbereich können Sie die Einstellungen für den Neustart festlegen, wie in Abbildung 6-38 gezeigt.

Abbildung 6-38 Einstellungen für den Neustart



Reboot

On this page, you can set reboot settings.

Enable: ☐

Running Days: (1-365)

Traffic Keep Time: (m)

Traffic Limit: (Kb)

Reboot Start Time: : (00:00-23:59)

Reboot End Time: : (00:00-23:59)