

**EchoLife ONT
V500R019C30
Security Maintenance**

Issue **06**
Date **2019-11-21**

Copyright © Huawei Technologies Co., Ltd. 2019. All rights reserved.

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

Trademarks and Permissions



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

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

Notice

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

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

Huawei Technologies Co., Ltd.

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

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

Email: support@huawei.com

About This Document

Product Version

The following table lists the product versions related to this document.

Product Name	Product Version
EchoLife ONT	V500R019C30

Intended Audience

The intended audience of this document is as follows:

- Technical support engineers
- Maintenance engineers








NOTE

Based on your requirements, mirroring feature may involve using, obtaining, or saving some information about users' communications for the purpose of safeguarding network operation and protecting services. Huawei alone is unable to collect or save the content of users' communications. It is suggested that you activate the interception-related functions based on the applicable laws and regulations in terms of purpose and scope of usage. You are obligated to take considerable measures to ensure that the content of users' communications is fully protected when the content is being used and saved.

Symbol Conventions

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

Symbol	Description
 DANGER	Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.
 WARNING	Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.

Symbol	Description
 CAUTION	Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury.
 NOTICE	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.
 NOTE	Calls attention to important information, best practices and tips. NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration.

GUI Conventions

Convention	Description
Boldface	GUI elements such as buttons, menus, parameters, tabs, window, and dialog titles are in boldface . For example, click OK .
>	Multi-level menus are separated by the > sign. For example, choose File > Create > Folder .

Change History

Changes between document issues are cumulative. Therefore, the latest document issue contains all changes made in previous issues.

Issue 06 (2019-11-21)

This issue is the fifth official release. Compared with the previous version, some bugs are fixed.

Issue 05 (2019-08-30)

This issue is the fifth official release. Compared with the previous version, some bugs are fixed.

Issue 04 (2019-06-19)

This issue is the fourth official release. Compared with the previous version, the modifications are as follows:

Section 2.3.1: Added descriptions about the support for IPv6.

Section 2.3.4: Added descriptions about DS-Lite supporting IP address filtering.

Section 2.3.11: Added IPsec VPN.

Issue 03 (2019-02-23)

This issue is the third official release. Compared with the previous version, the modifications are as follows:

Section 2.3.2: Added preventing TCP SYN port scanning.

Issue 02 (2018-10-30)

This is the second official release. Compared with the first version, the modifications are as follows:

Section 1.10.3: Modified URL filtering to parental control.

Delete the contents of URL Filtering in Chapter 2.

Issue 01 (2018-08-30)

This is the first official release.

Contents

About This Document.....	ii
1 Security Maintenance.....	1
1.1 Account Management.....	1
1.2 Maintaining the Web Account and Password.....	2
1.3 Maintaining the CLI Account and Password.....	3
1.4 Maintaining the TR069 Account and Password.....	4
1.5 Maintaining the Multicast Upgrade Account and Password.....	4
1.6 Maintaining the Cloud Platform Upgrade Account and Password.....	5
1.7 Changing the Account and Password.....	5
1.7.1 Changing the root(web) Password.....	5
1.7.2 Changing the telecomadmin Password.....	6
1.7.3 Changing the root(cli) Password.....	7
1.7.4 Changing the mutool Password.....	10
1.7.5 Changing the Cloud Platform Password.....	13
1.7.6 Troubleshooting.....	15
1.8 Viewing the Login Logs.....	16
1.9 Viewing the Configuration Modification Logs.....	16
1.10 Upgrading the Version.....	17
1.11 Security in the Application Layer.....	17
1.11.1 Maintaining MAC Address Filtering.....	17
1.11.2 Maintenance Suggestions for IP Address Filtering.....	18
1.11.3 Maintenance Suggestions for Parent Control.....	18
1.12 Machine-to-Machine Interface.....	19
2 Security Features.....	21
2.1 Secure Packet Mirroring of the Voice Media Stream.....	21
2.2 Device Management Security.....	27
2.2.1 User Management.....	27
2.2.2 HTTPS Connection Security.....	28
2.2.2.1 Introduction.....	28
2.2.2.2 Reference Standards and Protocols.....	29
2.2.2.3 Principles.....	29
2.2.3 M2M Web Interface.....	30

2.2.3.1 Introduction	30
2.2.3.2 Specifications	30
2.2.3.3 Principles	31
2.2.4 NetOpen Security.....	32
2.3 System Security	32
2.3.1 Anti-DoS Attack.....	33
2.3.1.1 Introduction	33
2.3.1.2 Specifications	33
2.3.1.3 Feature Updates	33
2.3.1.4 Principles	34
2.3.2 Preventing TCP SYN Port Scanning.....	37
2.3.2.1 Introduction	37
2.3.2.2 Specifications	38
2.3.2.3 Feature updates	38
2.3.2.4 Principles	38
2.3.3 MAC Address Filtering.....	39
2.3.3.1 Introduction	39
2.3.3.2 Specifications	39
2.3.3.3 Feature Updates	39
2.3.3.4 Principles	39
2.3.4 IP Address Filtering	40
2.3.4.1 Introduction	40
2.3.4.2 Specifications	40
2.3.4.3 Feature Updates	40
2.3.4.4 Principles	41
2.3.5 Firewall.....	41
2.3.5.1 Introduction	41
2.3.5.2 Feature Updates	42
2.3.5.3 Feature Dependency and Limitation.....	42
2.3.5.4 Principles	42
2.3.6 External Host Access Control	43
2.3.6.1 Introduction	43
2.3.6.2 Specifications	44
2.3.6.3 Feature Updates	44
2.3.6.4 Feature Dependency and Limitation.....	44
2.3.6.5 Principles	44
2.3.7 Inband Management VLAN	45
2.3.7.1 Introduction	45
2.3.7.2 Principle.....	45
2.3.8 Parental Control	45
2.3.8.1 Introduction	45
2.3.8.2 Specifications	46

2.3.8.3 Feature Updates	46
2.3.8.4 Principles	46
2.3.9 MAC Anti-spoofing	47
2.3.9.1 Introduction	47
2.3.9.2 Specifications	47
2.3.9.3 Feature Updates	47
2.3.9.4 Principles	47
2.3.10 Internet Access Control	48
2.3.10.1 Introduction	48
2.3.10.2 Specifications	48
2.3.10.3 Feature Updates	48
2.3.10.4 Principles	48
2.3.11 IPsec VPN	48
2.3.11.1 Introduction	48
2.3.11.2 Specifications	49
2.3.11.3 Feature Updates	50
2.3.11.4 Principles	50

1 Security Maintenance


Security maintenance provides guidance for routine security maintenance.




- [1.1 Account Management](#)
- [1.2 Maintaining the Web Account and Password](#)
- [1.3 Maintaining the CLI Account and Password](#)
- [1.4 Maintaining the TR069 Account and Password](#)
- [1.5 Changing the Account and Password](#)
- [1.6 Viewing the Login Logs](#)
- [1.7 Viewing the Configuration Modification Logs](#)
- [1.8 Upgrading the Version](#)
- [1.9 Security in the Application Layer](#)
- [1.10 Machine-to-Machine Interface](#)

1.1 Account Management

You can log in to and manage the ONT by Telnet or web page. Table 1-1 lists the available account, password and management mode.

Table 1-1 ONT account information

Default Account/Password	Scenario	You Can Manage an Account
telecomadmin/admintelecom	You log in to the ONT by web page, M2M web interface, or mobile phone App.	On NMS
root/adminHW  NOTE This account is used for web page login. It is described as	You log in to the ONT by web page, M2M web interface, or mobile phone App.	On web page or NMS

Default Account/Password	Scenario	You Can Manage an Account
root(web) in the following sections.		
root/adminHW  NOTE This account is used for Telnet or SSH login. It is described as root(cli) in the following sections.	You log in to the ONT by Telnet, SSH, or transparent channel.	By running the CLI command/on NMS
smartgateway/#hw#ont\$78A  NOTE This account is used for cloud platform authentication on the ONT. smartplat/#hw#plat%67B  NOTE This account is used for ONT authentication on the cloud platform.	You register the ONT with the cloud platform.	On the cloud platform

 **NOTE**

- The system displays a login failure message if the account and password for logging in to the ONT by Telnet, SSH, or web page are incorrect.
- For account management using the web page, the system will be locked if you input incorrect user name and password three times within two minutes. One minute later, it will be unlocked.
- For account management using the CLI, the system will be locked if you input incorrect user name and password five times within five minutes. Five minutes later, it will be unlocked.
- Change the initial password after logging in to the ONT. The initial account cannot be changed.
- Certain carriers may customize accounts and passwords, which are different from the default accounts and passwords listed in the preceding table. For details, contact the corresponding carrier.
- Currently, the root(cli) account password is the same as the account password of a common user logging in to the ONT by web page. Before using the root(cli) account to manage an ONT, perform security planning.

1.2 Maintaining the Web Account and Password

Suggestions

The security information in web account management includes the account and password.

- To guarantee system security, you need to try to ensure that the account and password are different and ensure that the length and complexity of a password comply with the security requirement. A password must comply with the following requirements:
 - The password must contain a minimum of six characters.
 - The password must contain at least two types of the following characters: digits, upper-case letters, lower-case letters, and special characters.

- The password cannot be the same as the account or the account spelled in the reverse order.
- The account for web login cannot be changed and the password must be changed periodically. It is recommended that you change the password at least once every three months.
- Only one user can log in to the web page at a time.
- The telecomadmin user, having the highest priority in the system, cannot use the default password. Specifically, the telecomadmin user must change the password after logging in to the system.
- The user logs in to the system must exit the system and then leave the system for a long period of time to prevent the system from being used by another user.
- The user logs in to the system but does not enter any information will be forced to go offline. It is recommended that you set the timeout duration to the default 5 minutes.
- The system processes web connections in serial mode. To defend against denial of service (DoS) attacks, you are advised to take security measures in advance, such as configuring ACLs and firewalls.
- You are advised to use HTTPS to access the web page. For the first login, replace the certificate in the **Modify Login Password** window and set SSL certificate parameters.
- When setting SSL certificate parameters on a web page, ensure that the entered certificate and password are matched. Otherwise, SSL is unavailable.
- When the user logs in to the web page through HTTPS, the RC4 algorithm is not recommended. You are advised to use the more secure AES128 algorithm or version-later security algorithm.
- When the user logs in to the web page through HTTPS, SSL negotiation is performed, which occupies lots of system resources. To prevent system overload that affects system performance, you are advised to prepare security assurance measures in advance, such as ACL and firewall settings.



NOTE

There are risks of attacks if the remote access through the WAN side is enabled. Therefore, you need to perform security planning in advance.

1.3 Maintaining the CLI Account and Password

Suggestions

The security information in CLI account management includes the account and password.

- To guarantee system security, you need to try to ensure that the account and password are different and ensure that the length and complexity of a password comply with the security requirement. A password must comply with the following requirements:
 - The password must contain a minimum of six characters.
 - The password must contain at least two types of the following characters: digits, upper-case letters, lower-case letters, and special characters.
 - The password cannot be the same as the account or the account spelled in the reverse order.
- The account for CLI login cannot be changed and the password must be changed periodically. It is recommended that you change the password at least once every three months.

- To prevent sensitive data in a transmission channel from being intercepted or attacked, you are advised to use SSH to log in to an ONT through the CLI at the WAN side.

 **NOTE**

- The Telnet was not designed to be a secure protocol. User sensitive data transmitted over Telnet is prone to captures and attacks. Before you download files using Telnet, make a security plan.
- You are advised to use the more secure SSH to access CLI. For the first CLI login, generate the new SSH login key through the CLI and then you can use the tool supporting SSH to access an ONT.
- The current version supports one TCP connection when Telnet is used and only one TCP connection when SSH is used. If TCP connections are in full configuration, other users cannot log in to the ONT. You are advised to plan the TCP connections in advance.
- When the user logs in to the web page through SSH, SSH negotiation is performed, which occupies lots of system resources. To prevent system overload that affects system performance, you are advised to prepare security assurance measures in advance, such as ACL and firewall settings.

1.4 Maintaining the TR069 Account and Password

Suggestions

When the ONT is managed by a TR069 server, the security sensitive information mainly includes the account and password.

- To guarantee system security, you need to try to ensure that the account and password are different and ensure that the length and complexity of a password comply with the security requirement. A password must comply with the following requirements:
 - The password must contain a minimum of six characters.
 - The password must contain at least two types of the following characters: digits, upper-case letters, lower-case letters, and special characters.
 - The password cannot be the same as the account or the account spelled in the reverse order.
- The account and password for a TR069 server must be changed periodically. It is recommended that you change the password at least once every three months.
- To prevent sensitive data in a transmission channel from being intercepted or attacked, you are advised to use SSL to log in to an ONT through the TR069 server at the WAN side.

 **NOTE**

- When the ONT connects to the ACS through HTTPS, the RC4 algorithm is not recommended. You are advised to use the more secure AES128 algorithm or version-later security algorithm.
- When the ONT connects to the ACS through HTTPS, SSL negotiation is performed, which occupies lots of system resources. To prevent system overload that affects system performance, you are advised to prepare security assurance measures in advance, such as ACL and firewall settings.

1.5 Maintaining the Multicast Upgrade Account and Password

Suggestions

When the ONT is used by using a multicast upgrade tool, the security sensitive information mainly includes the account and password.

- To guarantee system security, you need to try to ensure that the account and password are different and ensure that the length and complexity of a password comply with the security requirement. A password must comply with the following requirements:
 - The password must contain a minimum of six characters.
 - The password must contain at least two types of the following characters: digits, upper-case letters, lower-case letters, and special characters.
 - The password cannot be the same as the account or the account spelled in the reverse order.
- The account and password for a multicast upgrade tool must be changed periodically. It is recommended that you change the password at least once every three months.

1.6 Maintaining the Cloud Platform Upgrade Account and Password

Suggestions

When the ONT is managed by a cloud platform, the security sensitive information mainly includes the account and password.

- To guarantee system security, you need to try to ensure that the account and password are different and ensure that the length and complexity of a password comply with the security requirement. Password setting requirements are as follows:
 - A password must contain at least 6 characters.
 - A password must contain at least two of the following combinations: numbers, uppercase letters, lowercase letters, and special characters.
 - A password cannot be the account or its reverse spelling.
- An account and password need to be changed periodically using the cloud platform. It is recommended that you change the password at least once every three months.

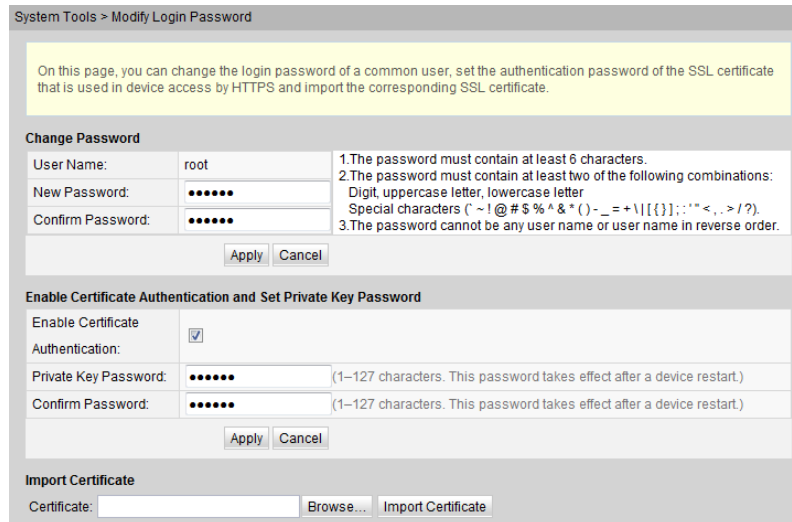
1.7 Changing the Account and Password

1.7.1 Changing the root(web) Password

Procedure

Step 1 Log in to the web page as root or telecomadmin.

Step 2 Navigate to Account by choosing: **Advance > Management > Account Management**.



Step 3 Change the password on the Account interface, and click **Apply**.

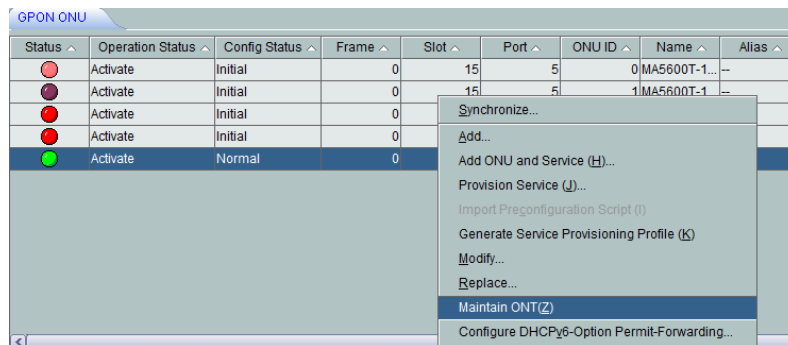
----End

1.7.2 Changing the telecomadmin Password

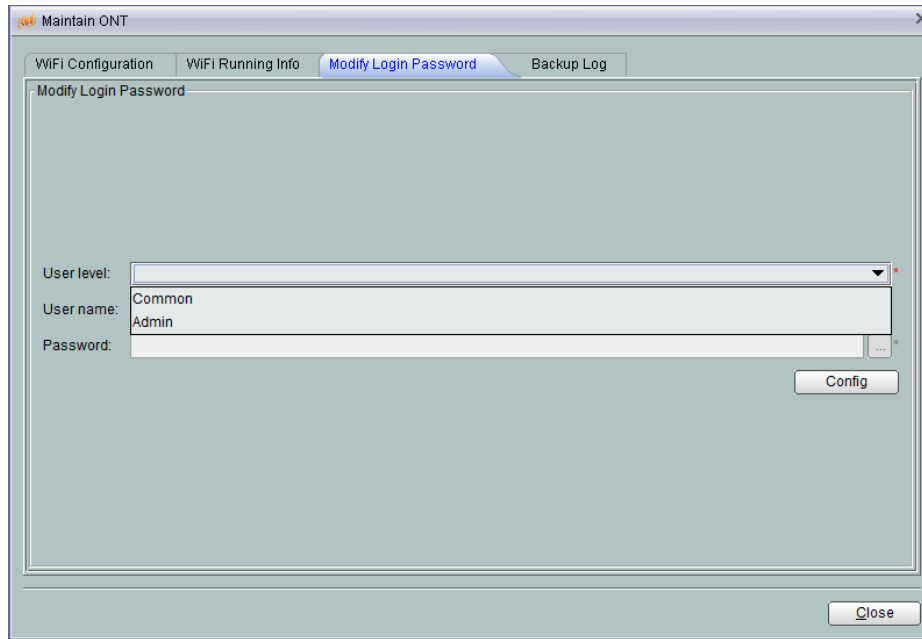
Change the telecomadmin password through the BMS.

Procedure

Step 1 Log in to the BMS, select the ONT whose telecomadmin password needs to be changed, right-click, and choose **Maintain ONT(Z)**.



Step 2 In the dialog box that is displayed, select **Modify Login Password**.



Step 3 Select **Admin** from the **User level** drop-down list, input a new password in **Password**, and click **Config**.



NOTE

This password is encrypted by the BMS.

----End

1.7.3 Changing the root(cli) Password

Procedure

Change the root(cli) password through the BMS.

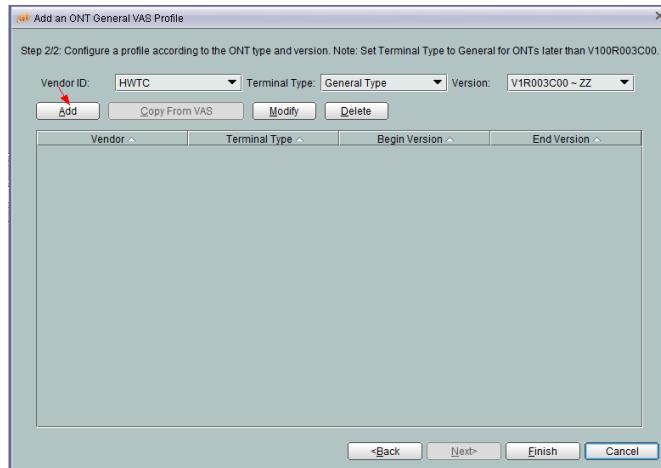
1. (Optional) Add a general ONT VAS profile.



NOTE

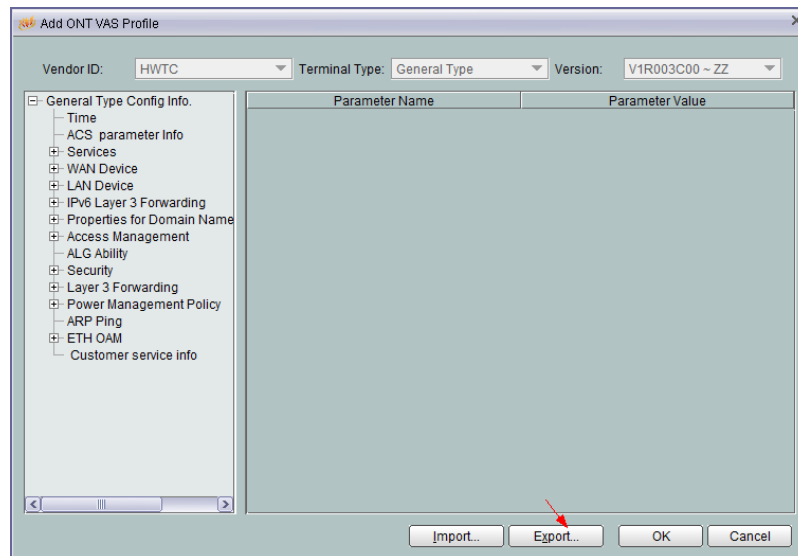
If there is an ONT VAS profile, select this profile, right-click, and choose **Modify** from the shortcut menu.

- a. From the main menu, choose **Configuration > Access Profile Management**. In the navigation tree of the tab page that is displayed, choose **PON Profile > ONT VAS Profile**.
- b. On the **General ONT VAS Profile** tab page, right-click, and choose **Add** from the shortcut menu.
- c. In the dialog box that is displayed, set **Name** of the general VAS profile, and configure the WAN port information and voice service parameters for the ONT.
- d. Click **Next**.
- e. In the dialog box that is displayed, set **vendor ID** to **HWTC**, **Terminal Type** to **General Type**, and **Version** to **V1R003C00-ZZ**, Click **Add**.



- f. In the dialog box that is displayed, configure parameters of the general ONT VAS profile based on requirements.
2. Export the **ONT VAS Profile** to be changed.

In the **Add ONT VAS Profile** dialog box, click **Export** to export an XML configuration file.



3. Use the **Text Document** to open the exported XML file.

```
<Layer3Forwarding X_HW_AutoDefaultGatewayEnable="0" X_HW_WanDefaultWanName="">
</Layer3Forwarding>
<X_HW_policy_route MaxNumber="64" NumberOfInstances="0"/>
<Forwarding MaxNumber="64" NumberOfInstances="0"/>
</Layer3Forwarding>
<X_HW_APPPolicy EnablePowerSavingMode="1">
<BatteryModePolicy NotUseCATVService="0" NotUseLanService="0" NotUseRemoteManagement="0" NotUseUssService="0" NotUseVoiceService="0" NotUseWlanService="0"/>
<BatteryAlarmPolicy AlwaysEnable="1" VoiceServiceEnable="1"/>
</X_HW_APPPolicy>
<X_HW_ABPingIntrusiveness MaxNumber="64" NumberOfInstances="0"/>
<X_HW_Dot1agCfm>
<dot1agCfmMd MaxNumber="64" NumberOfInstances="1">
<dot1agCfmMdInstance InstanceId="1" MdIndex="0" MdLevel="0" MdNameFormat="1" MdNameValue="none">
<dot1agCfmMa MaxNumber="64" NumberOfInstances="1">
<dot1agCfmMaInstance CmInterval="6" InstanceId="1" MdIndex="0" MdNameFormat="2" MdNameValue="none" VlanId="1">
<dot1agCfmMep MaxNumber="8191" NumberOfInstances="1">
<dot1agCfmMepInstance ActiveStatus="enable" CoStatus="disable" Direction="up" InstanceId="1" L2Priority="7" MepId="1" PortId="1" PortType="lan-port" RemoteMepId="8191"/>
</dot1agCfmMep>
</dot1agCfmMaInstance>
</dot1agCfmMa>
</dot1agCfmMdInstance>
</dot1agCfmMd>
</X_HW_Dot1agCfm>
<X_HW_UserServiceInfo ServiceDescription="">
<QueueManagement X_HW_ClassificationEnable="0">
<X_HW_Classification MaxNumber="64" NumberOfInstances="0"/>
</QueueManagement>
</UserInterface>
<X_HW_WebUserInfo NumberOfInstances="1">
<X_HW_WebUserInfoInstance Enable="1" InstanceId="2" Password="UD3F450BF142081D1DC4FC28B83648B" UserLevel="0" UserName="e6588EED7847E46E8E215DD0D1239256"/>
</X_HW_WebUserInfo>
</UserInterface>
</UserInterface>
```


4. Add the following contents and save the file.

```
<UserInterface>
<X_HW_CLIUserInfo NumberOfInstances="1">
<X_HW_CLIUserInfoInstance InstanceID="1" Username="root" Userpassword="Admin&123"/>
</X_HW_CLIUserInfo>
<X_HW_WebUserInfo NumberOfInstances="1">
<X_HW_WebUserInfoInstance Enable="1" InstanceID="2" Password="UD3F450BF1420B1D18C4FC28B836348B" UserLevel="0" UserName="e6588EBD7B47B4668B215DD0D1239256"/>
</X_HW_WebUserInfo>
</UserInterface>
</InternetGatewayDevice>
```

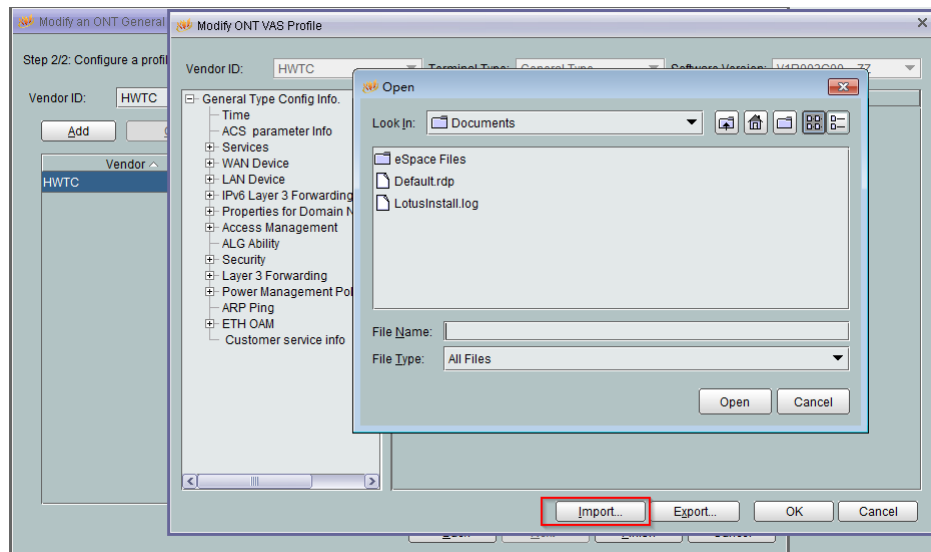


NOTE

- Fill in the password being changed. The BMS automatically encrypts the password.
- **Username** is the user name and **Userpassword** is the password. The user information is changed by changing **Username** and **Userpassword**.
- The default user name of a common user is **root**. The user name can be changed. The common user password in the preceding figure is Admin&123.

5. Import the changed XML file to the BMS.

- From the main menu, choose **Configuration > Access Profile Management**. In the navigation tree of the tab page that is displayed, choose **PON Profile > ONT VAS Profile**.
- Select the created profile, right-click, and choose **Modify** from the shortcut menu.
- In the dialog box that is displayed, click **Next**.
- Select the record where **Terminal Type** is set to **OntGnlrType**, right-click, and choose **Modify** from the shortcut menu.
- In the dialog box, click **Import**, and select the XML configuration file to be imported in the window that is displayed.



- Click **OK**.

6. Bind the changed **General VAS Profile** to the specified ONT.

- In the **Physical Map** navigation tree on the **Main Topology** tab page, double-click the target OLT or select the target OLT, right-click, and choose **NE Explorer**.
- In the navigation tree, choose **GPON > GPON Management**.
- In the window on the right, choose **GPON ONU**.
- On the **GPON ONU** tab page, set the search criteria to find the GPON ONU records.

- e. Select an ONT from the list, right-click, and choose **Bind General VAS Profile** from the shortcut menu. In the dialog box that is displayed, select the created profile, and click **OK** to complete profile binding.

Change the root(cli) password through the CLI.

1. Connect a PC to the ONT and log in to the ONT by telnet.
2. Run the **set userpasswd root** command to change the password.

```
WAP>set userpasswd root
old password:*****
new password:*****
reenter new password:*****
Password of root has been modified successful!

success!
WAP>
```

1.7.4 Changing the mutool Password

Procedure

Change the mutool password through the BMS.

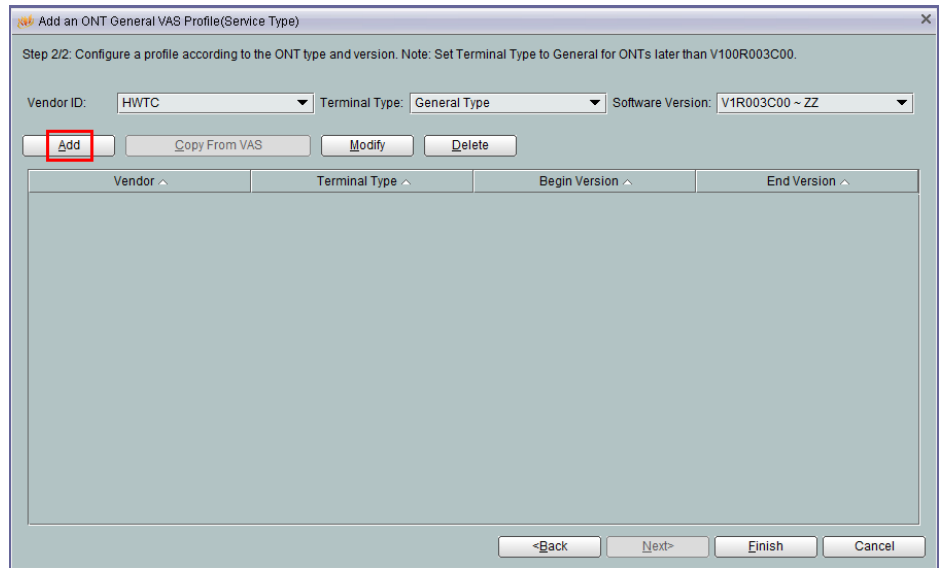
1. (Optional) Add an ONT VAS profile.



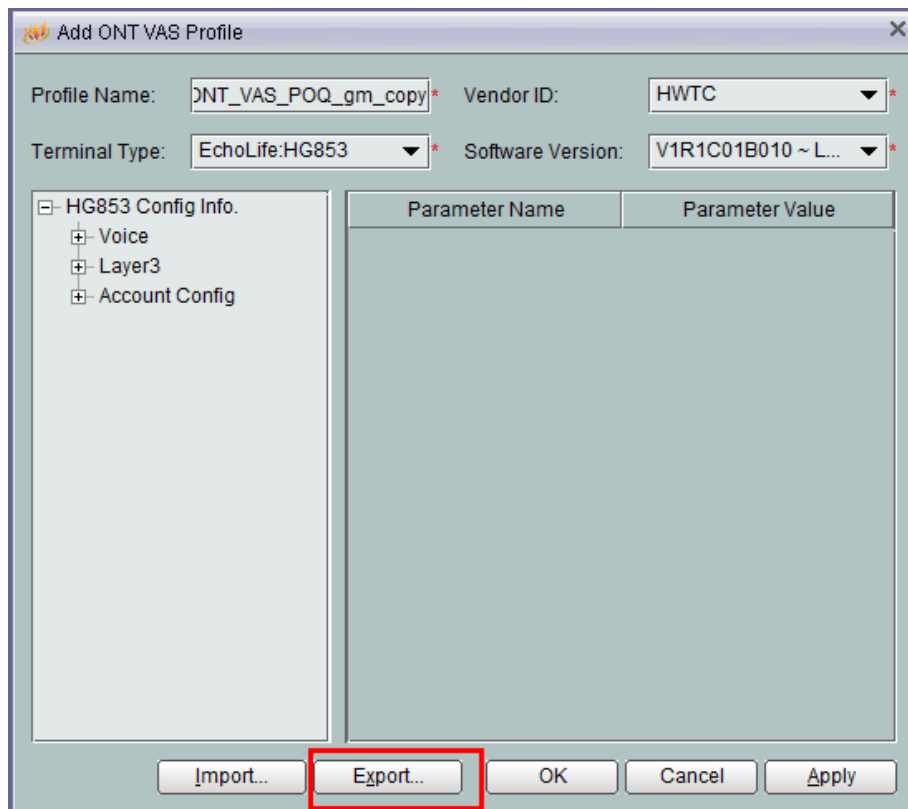
NOTE

If there is an ONT VAS profile, select this profile, right-click, and choose **Modify** from the shortcut menu.

- a. From the main menu, choose **Configuration > Access Profile Management**. In the navigation tree of the tab page that is displayed, choose **PON Profile > ONT VAS Profile**.
- b. On the **General ONT VAS Profile** tab page, right-click, and choose **Add** from the shortcut menu
- c. In the dialog box that is displayed, set **Name** of the general VAS profile, and configure the WAN port information and voice service parameters for the ONT.
- d. Click **Next**.
- e. In the dialog box that is displayed, set **Vendor ID** to **HWTC**, **Terminal Type** to **General Type**, and **Software Version** to **V1R003C00 - ZZ**. Click **Add**.



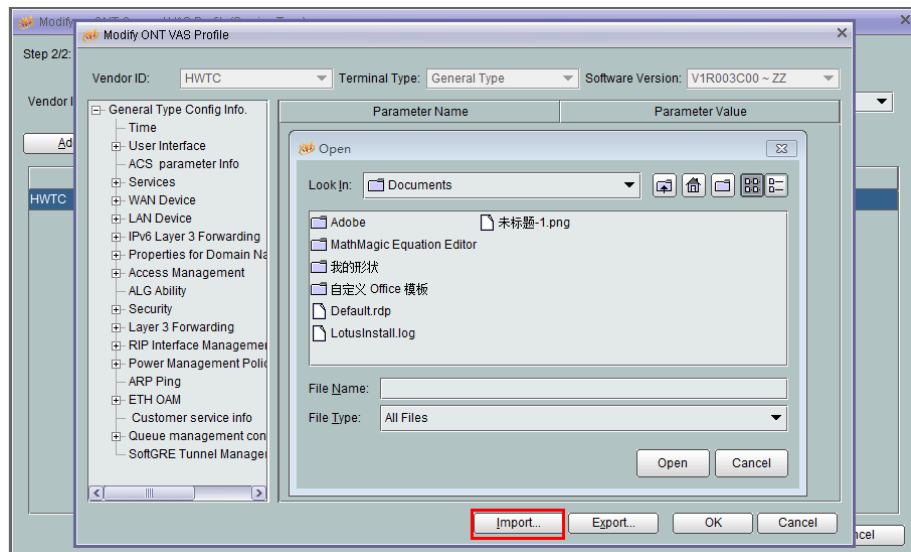
- f. In the dialog box that is displayed, configure parameters of the general ONT VAS profile based on requirements.
- 2. Export the **ONT VAS Profile** to be changed.
In the **Add ONT VAS Profile** dialog box, click **Export** to export an XML configuration file.



- 3. Use the **Text Document** to open the exported XML file. Manually add a mutool node.

```
</WANDevice>
<X_HW_ALG FtpEnable="1" H323Enable="1" RTSPEnable="1" SipEnable="1" TftpEnable="1" />
<X_HW_APMPolicy EnablePowerSavingMode="1">
  <BatteryModePolicy NotUseCATVService="0" NotUseLanService="0" NotUseRemoteManagement="0" NotUseUsbService="0" NotUseVoi
</X_HW_APMPolicy>
<X_HW_AmpInfo EthLoopbackTimeout="0">
  <X_HW_Spec X_HW_EthTrapEnable="1" X_HW_HGDetectEnable="0" X_HW_HGVlan="3999" />
</X_HW_AmpInfo>
<X_HW_DNS SupportedRecordTypes="AAAA">
  <Client>
  </Client>
</X_HW_DNS>
<X_HW_Dot1agCfm>
</X_HW_Dot1agCfm>
<X_HW_IPv6Layer3Forwarding>
  <Forwarding MaxNumber="33" NumberOfInstances="0" />
</X_HW_IPv6Layer3Forwarding>
<X_HW_Security>
  <AcServices FTPLanEnable="1" FTPWanEnable="0" HTTPLanEnable="1" HTTPWanEnable="0" TELNETLanEnable="1" TELNETWanEnable=
  <WANSrcWhiteList WANSrcWhiteListEnable="0" />
</WANSrcWhiteList>
</X_HW_Security>
<X_HW_UserServiceInfo ServiceDescriptions="60000"/>
<X_HW_MUIinterface Username="mutools" password="12!@#&$" />
</InternetGatewayDevice>
```

4. Import the changed XML file to the BMS.
 - a. From the main menu, choose **Configuration > Access Profile Management**. In the navigation tree of the tab page that is displayed, choose **PON Profile > ONT VAS Profile**.
 - b. Select the created profile, right-click, and choose **Modify** from the shortcut menu.
 - c. In the dialog box that is displayed, click **Next**.
 - d. Select the record where **Terminal Type** is set to **General Type**, right-click, and choose **Modify** from the shortcut menu.
 - e. In the dialog box, click **Import**, and select the XML configuration file to be imported in the window that is displayed.



- f. Click **OK**.
5. Bind the changed **General VAS Profile** to the specified ONT.
 - a. In the **Physical Root** navigation tree on the **Main Topology** tab page, double-click the target OLT or select the target OLT, right-click, and choose **NE Profile Management**.
 - b. In the navigation tree, choose **GPON > GPON Management** or **EPON > EPON Management**.
 - c. In the window on the right, choose **GPON ONU** or **EPON ONU** tab page.
 - d. On the **GPON ONU** or **EPON ONU** tab page, set the query criteria to query desired GPON ONU or EPON ONU records.

- e. Select an ONT from the list, right-click, and choose **Bind General VAS Profile** from the shortcut menu. In the dialog box that is displayed, select the created profile, and click **OK** to complete profile binding.

----End

1.7.5 Changing the Cloud Platform Password

Procedure

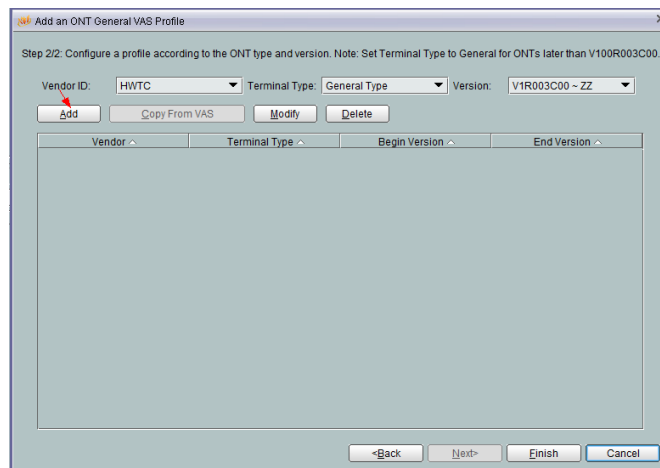
Change the cloud platform password through the BMS.

1. (Optional) Add a general ONT VAS profile.

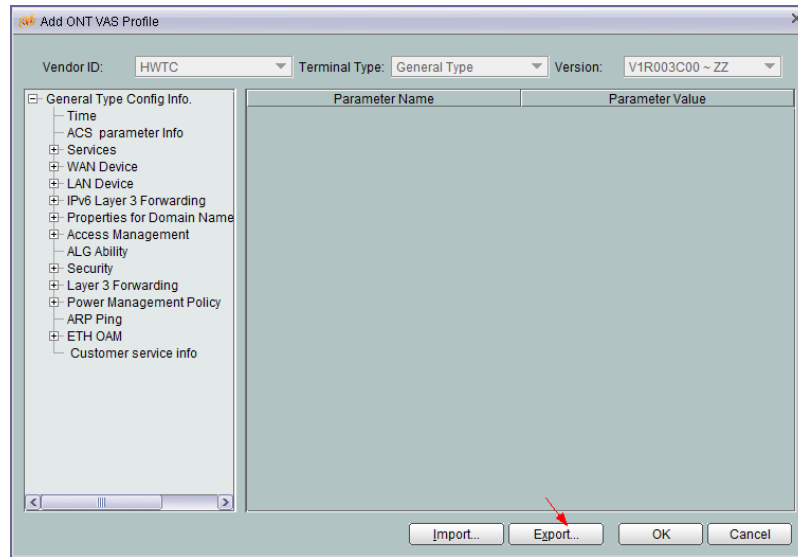
 **NOTE**

If there is an ONT VAS profile, select this profile, right-click, and choose **Modify** from the shortcut menu.

- a. From the main menu, choose **Configuration > Access Profile Management**. In the navigation tree of the tab page that is displayed, choose **PON Profile > ONT VAS Profile**.
- b. On the **General ONT VAS Profile** tab page, right-click, and choose **Add** from the shortcut menu.
- c. In the dialog box that is displayed, set **Name** of the general VAS profile, and configure the WAN port information and voice service parameters for the ONT.
- d. Click **Next**.
- e. In the dialog box that is displayed, set **vendor ID** to **HWTC**, **Terminal Type** to **General Type**, and **Version** to **V1R003C00-ZZ**, click **Add**.



- f. In the dialog box that is displayed, configure parameters of the general ONT VAS profile based on requirements.
2. Export the **ONT VAS Profile** to be changed.
In the **Add ONT VAS Profile** dialog box, click **Export** to export an XML configuration file.



- Use the **Text Document** to open the exported XML file.

```

</BBSPCustomization>
</X_HW_FeatureList>
<X_HW_OAMFREQUENCY Value="30" />
<X_HW_UserInfo UserName="" UserId="" Status="99" Limit="10" Times="0" Result="99" X_HW_InformStatus="0" X_HW_AcsCn
<X_HW_ServiceManage FtpEnable="0" FtpUserName="root" FtpPassword="admin" FtpPort="21" FtpRootDir="/mnt/usb1
<X_HW_AmpInfo EthLoopbackTimeout="0" />
<X_HW_SSMPPDT>
<Deviceinfo X_HW_CWMPINFO_PRODUCTCLASS_EXTXPON="1" />
</X_HW_SSMPPDT>
<X_HW_PPPOE_BridgeWAN_AutoEmulator Enable="0" Username="" Password="" TimeList="1440" FailedRetryTimeList=
<X_HW_ProductInfo originalVersion="V300R013C00SPC901TA" currentVersion="V100R006" customInfo="AHCT" custom
<!-- SUPPORT_HGW_START-->
<X_HW_AppRemoteManage MgtURL="189cube.com" Port="12112" Heartbeat="60" Ability="0" LocatePort="17998"></X
<!-- SUPPORT_HGW_END-->
<DownloadDiagnostics DownloadDiagnosticMaxConnections="4"/>
</InternetGatewayDevice>

```

- Add the following contents and save the file.

```

</X_HW_FeatureList>
<X_HW_OAMFREQUENCY Value="30" />
<X_HW_UserInfo UserName="" UserId="" Status="99" Limit="10" Times="0" Result="99" X_HW_InformStatus="0" X_HW_AcsCn
<X_HW_ServiceManage FtpEnable="0" FtpUserName="root" FtpPassword="admin" FtpPort="21" FtpRootDir="/mnt/usb1/" Ft
<X_HW_AmpInfo EthLoopbackTimeout="0" />
<X_HW_SSMPPDT>
<Deviceinfo X_HW_CWMPINFO_PRODUCTCLASS_EXTXPON="1" />
</X_HW_SSMPPDT>
<X_HW_PPPOE_BridgeWAN_AutoEmulator Enable="0" Username="" Password="" TimeList="1440" FailedRetryTimeList="15" />
<X_HW_ProductInfo originalVersion="V300R013C00SPC901TA" currentVersion="V100R006" customInfo="AHCT" customInfoData:
<!-- SUPPORT_HGW_START-->
<X_HW_AppRemoteManage PlatUsername="admin" PlatPassword="admin" MgtURL="189cube.com" Port="12112" Heartbeat="60" A
<!-- SUPPORT_HGW_END-->
<DownloadDiagnostics DownloadDiagnosticMaxConnections="4"/>
</InternetGatewayDevice>

```

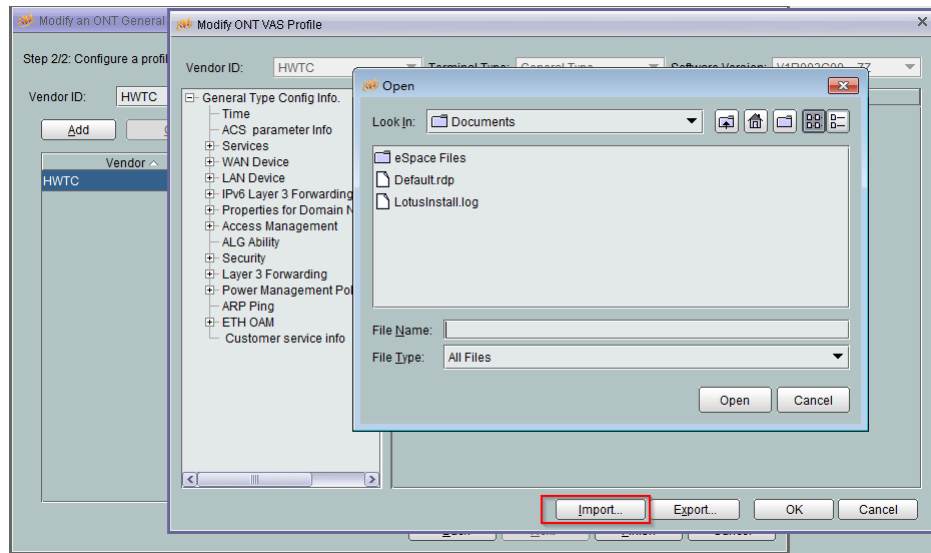
NOTE

- Fill in the password being changed. The BMS automatically encrypts the simple password.
- PlatUsername** is the user name and **PlatPassword** is the user password. The user information is changed by changing **PlatUsername** and **PlatPassword**.

- Import the changed XML file to the BMS.

- From the main menu, choose **Configuration > Access Profile Management**. In the navigation tree of the tab page that is displayed, choose **PON Profile > ONT VAS Profile**.
- Select the created profile, right-click, and choose **Modify** from the shortcut menu.

- c. In the dialog box that is displayed, click **Next**.
- d. Select the record where **Terminal Type** is set to **OntGnlrType**, right-click, and choose **Modify** from the shortcut menu.
- e. In the dialog box, click **Import**, and select the XML configuration file to be imported in the window that is displayed.



- f. Click **OK**.
6. Bind the changed **General VAS Profile** to the specified ONT.
- a. In the **Physical Map** navigation tree on the **Main Topology** tab page, double-click the target OLT or select the target OLT, right-click, and choose **NE Explorer**.
 - b. In the navigation tree, choose **GPON > GPON Management**.
 - c. In the window on the right, choose **GPON ONU**.
 - d. On the **GPON ONU** tab page, set the search criteria to find the GPON ONU records.
 - e. Select an ONT from the list, right-click, and choose **Bind General VAS Profile** from the shortcut menu. In the dialog box that is displayed, select the created profile, and click **OK** to complete profile binding.

1.7.6 Troubleshooting

A user fails to log in to the system because the password is lost.

- The password of a root (common) user is lost.
The telecomadmin user has the right of changing the password of a root user. If the password of a root user is lost, contact the telecomadmin user to change the password.
- The password of a telecomadmin user is lost.
You can request the BMS to reassign the telecomadmin account and password.

1.8 Viewing the Login Logs

Suggestions

To prevent unauthorized users from logging in to the ONT to modify ONT configurations or crack the ONT telnet account/password, view the login logs periodically (at least once in three months) to check whether there are any unauthorized logins or login attempts.

Procedure

Step 1 Log in to the system through Web as a **root/telecomadmin**.

Step 2 Select **Advance > Maintenance Diagnog > user log**, view the contents of the log record of the existence of a large number of logon failures, as shown below:

```
2014-03-31 11:03:36 [Notice][Alarm-Log] AlarmID: 104517, AlarmLevel: Error, [WEB] from ip: 192.168.100.11 login fail!
2014-03-31 11:03:42 [Notice][Alarm-Log] AlarmID: 104517, AlarmLevel: Error, [WEB] from ip: 192.168.100.11 login fail!
2014-03-31 11:03:49 [Notice][Alarm-Log] AlarmID: 104517, AlarmLevel: Error, [WEB] from ip: 192.168.100.11 login fail!
2014-03-31 11:03:49 [Notice][Alarm-Log] AlarmID: 104518, AlarmLevel: Error, [WEB] login times exceed limit times, locked!
2014-03-31 11:04:12 [Notice][Alarm-Log] AlarmID: 104517, AlarmLevel: Error, [CLI]root from ip: 192.168.100.11 login fail!
2014-03-31 11:04:14 [Notice][Alarm-Log] AlarmID: 104517, AlarmLevel: Error, [CLI]ssaa from ip: 192.168.100.11 login fail!
2014-03-31 11:04:17 [Notice][Alarm-Log] AlarmID: 104517, AlarmLevel: Error, [CLI]telecom from ip: 192.168.100.11 login fail!
2014-03-31 11:04:20 [Notice][Alarm-Log] AlarmID: 104517, AlarmLevel: Error, [CLI]aaa from ip: 192.168.100.11 login fail!
2014-03-31 11:04:24 [Notice][Alarm-Log] AlarmID: 104517, AlarmLevel: Error, [CLI]ffs from ip: 192.168.100.11 login fail!
2014-03-31 11:04:24 [Notice][Alarm-Log] AlarmID: 104518, AlarmLevel: Error, [CLI]login times exceed limit times, locked!
```

----End

Troubleshooting

If you identify any unreasonable login records, change the password of the root account through telnet.

1.9 Viewing the Configuration Modification Logs

Suggestions

To prevent users from logging in to the ONT to modify ONT configurations and consequently affecting the user (the user itself or other users) experience, view the configuration modification logs periodically (at least once in three months) to check whether there are any unauthorized configuration modifications.

Procedure

Step 1 Log in to the system through Web as a **root/telecomadmin**.

Step 2 Select **Advance > Maintenance Diagnog > user log**, view the log contents if incorrect configuration changes.

```
2014-03-31 10:48:04 [Notice][Config-Log] Terminal: WEB(192.168.100.11), Result: Success, Type: Set, WANIPConnection: 1.1.1, Ena
2014-03-31 10:48:04 [Notice][Config-Log] Terminal: WEB(192.168.100.11), Result: Success, Type: Set, policy_route: 1
2014-03-31 10:48:04 [Notice][Config-Log] Terminal: WEB(192.168.100.11), Result: Success, Type: Set, WANIPConnection: 1.1.1
2014-03-31 10:48:43 [Notice][Config-Log] Terminal: WEB(192.168.100.11), Result: Success, Type: Set, ManagementServer, Periodic
2014-03-31 10:50:12 [Notice][Config-Log] Terminal: WEB(192.168.100.11), Result: Success, Type: Set, DeviceInfo, X_HW_PonHexP:
```


---End

1.10 Upgrading the Version

Suggestions

Carriers are recommended to upgrade the version if new functions are required or system problems in earlier versions need to be resolved.

Procedure

For details about upgrade, see the Upgrade Guide of the required version.

1.11 Security in the Application Layer

1.11.1 Maintaining MAC Address Filtering

Suggestion

MAC address filtering controls the permission of user terminals on Internet access. After MAC address filtering is configured, only terminals complying with the specified filtering rule can normally access the Internet.

The MAC address of a network device may be changed because of factors such as device replacement and maintenance. If the MAC address of a network device changes, you need to maintain MAC address filtering in time. Specifically, delete filtering for the original MAC address and add it for the new MAC address.

Procedure

- Step 1** In the navigation tree on the left, choose **Security > MAC Filter Configuration**. In the pane on the right, after enabling MAC filter and selecting the filter mode, click **New**. On the dialog box that is displayed, configure the MAC filter rule for the PC to access the Internet, as shown in the following figure.

Security > MAC Filter Configuration

On this page, you can configure MAC filter to prohibit some PCs from accessing the Internet.

Enable MAC Filter:

Filter Mode: Blacklist

New Delete

Source MAC Address	
Source MAC Address:	00:15:17:2C:EF:97 * (AA:BB:CC:DD:EE:FF)

Apply Cancel

- Step 2** Click **Apply**.

---End

1.11.2 Maintenance Suggestions for IP Address Filtering

Suggestion

IP address filtering is a home gateway security mechanism, where rules can be set to permit or deny the packets exchanged between all or specified ports within an IP segment on a private network and all or specified ports on an external IP network.

Use the static IP allocation and disable the DHCP IP allocation for private IP address filtering. This prevents IP address filtering from malfunctioning caused by dynamic change of IP addresses.

Procedure

- Step 1** In the navigation tree on the left, choose **Security > IP Filter Configuration**. In the pane on the right, enable the IP address filter function. After selecting the filter mode, click **New**. Then, in the dialog box that is displayed, configure the rule for filtering IP addresses from the WAN interface to the LAN port, as shown in the following figure.

Security > IP Filter Configuration

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	All	Bidirectional	192.168.100.10	

Rule name: rule

Protocol: All

Direction: Bidirectional

LAN-side Start IP Address: 192.168.100.10

LAN-side End IP Address: 192.168.100.10

WAN-side IP Address: --

Apply Cancel

- Step 2** Click **Apply**.

---End

1.11.3 Maintenance Suggestions for Parent Control

Suggestion

Parent control is a home gateway security mechanism, it allows parents to configure different filtering policy templates to set constraints for network access time and website access. The templates are associated with children's web devices based on MAC addresses.

Procedure

- Step 1** Click the **Security** tab and then choose **Parent Control** from the navigation tree. In the pane on the right, select the filter mode, and configure the URL address, as shown in the following figure.

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](#)

Specify the URL list that a user is allowed or prohibited to access.

Enable website filter

Filter Mode **Blacklist**

[New](#) [Delete](#)

URL Address

URL Address: *An IPv6 address contained in a URL you entered must be enclosed in square brackets [], for example, http://[FE00::1]/test.html.

[Apply](#) [Cancel](#)

<< < 0/0 > >> Page Go

[Return](#)



NOTE

For example, if you need to filter address a.huawei.com and b.huawei.com, set the URL address to huawei.com. Parent control does not support a wildcard character and therefore you cannot set it to *.huawei.com.

- Step 2** Click **Apply**.

---End

1.12 Machine-to-Machine Interface

ONT machine-to-machine interfaces contain OAM/OMCI interface, web interface, TR069 interface, multicast upgrade interface, JSON interface of the mobile phone App and cloud platform, and configuration file interface. These interfaces are used for the OSS, OLT, and GUI to perform configuration management, fault management, performance management, and security management for ONTs. If they are improperly used, the device may be abnormal or services may be interrupted. The document for the ONT machine-to-machine interface is

released with limitation. If you require this document, contact Huawei local office for document acquisition flow and requirements.

2 Security Features

2.1 Secure Packet Mirroring of the Voice Media Stream

This topic describes the secure packet mirroring of the voice media stream.

2.2 Device Management Security

This topic describes features related to device management security.

2.3 System Security

This topic covers the overview, availability, and sub-features of network security.

2.1 Secure Packet Mirroring of the Voice Media Stream

Introduction

In secure packet mirroring of the voice media stream, the mirrored packets do not contain any private user data, such as dialed numbers and communication contents. Therefore, the voice media stream packets can be mirrored for voice service fault locating without being authorized by an end user. The process of secure packet mirroring of the voice media stream is the same as that of remote packet mirroring of the voice service.

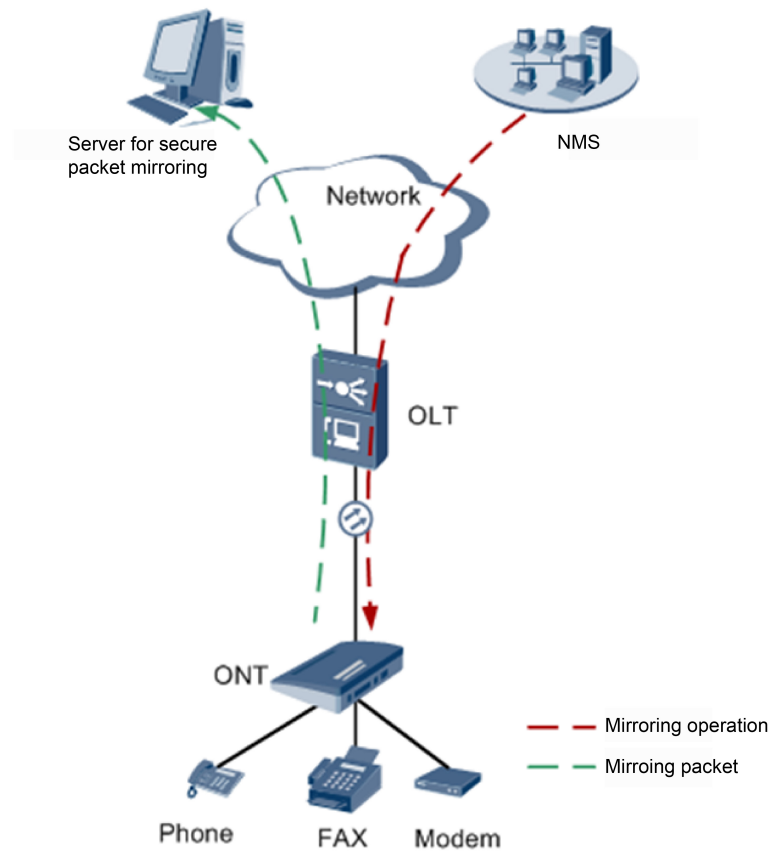
The secure packet mirroring of the voice media stream feature:

- Supports remote fault locating.
- Supports rapid fault locating. Maintenance personnel can enable the voice media stream packet mirroring function based on fault symptoms, which shortens the fault locating time.
- Is secure and reliable. The mirrored voice media stream packets do not contain any private user data, such as dialed numbers and communication contents.

Basic Principles

[Figure 2-1](#) shows the networking for the secure packet mirroring of the voice media stream.

Figure 2-1 Principle of the secure packet mirroring of the voice media stream



The ONT duplicates the signaling and media packets on a specified user port, adds headers such as MAC, IP, and UDP to the packets, and sends the packets to a specified server. On the server, a dedicated tool is used to receive UDP packets and remove the added MAC/IP/UDP headers from the packets to restore the original data.

The server for secure packet mirroring can be a specified server, integrated with the NMS, or a specialized server or PC. Therefore, server data (such as the IP address) needs to be configured before secure packet mirroring starts (the data can be configured remotely).

The secure packet mirroring of the voice media stream can be started on the NMS, TR069, or Telnet. After secure packet mirroring is started and a user initiates a call, the entire call process will be recorded. For issues that have been reported with a low probability of recurrence and issues on a specific service (such as fax or modem), secure packet mirroring is an effective maintenance method.

Signaling Mirroring Principle

H.248/SIP/MGCP signaling is in text format. The phone number and user name of a user can be queried by a character string and then be anonymized.

A phone number is processed as follows:

- If a phone number has 1 or 2 digits, it is directly replaced with an asterisk (*).
- If a phone number has more than 8 digits, its first and last 2 digits are displayed in plain text, and other digits are replaced with an asterisk (*).

- If a phone number has 3–7 digits, its last 2 digits are displayed in plain text, and other digits are replaced with an asterisk (*).

A user name is directly replaced with an asterisk (*).

Media Stream Mirroring Principle

Mirroring all voice media stream packets of a call easily discloses user privacy information. Therefore, the ONT device provides differentiated voice media stream mirroring modes. In this way, voice media stream packets can be mirrored without risking disclosing user privacy information.

Table 2-1 lists the voice media stream mirroring modes that the ONT supports.

Table 2-1 Voice media stream mirroring modes

Mode	Description	Usage Scenario
Full packet mirroring	The ONT device does not filter or replace any information in the mirrored Real-Time Transport Protocol (RTP) or time division multiplexing (TDM) tracing packets.	This mode applies when the mirrored packets do not contain user communication content. In this mode, packets can be mirrored as many as possible, which facilitates fault locating. This mode is used to diagnose fax or modem negotiation failures.
Fuzzy packet mirroring	The ONT device retains the minimum data that identifies the fax or modem signal tone in RTP and TDM tracing packets, which prevents the original user communication data from being restored. Specifically, the ONT device retains only 10 ms of data (data generated in a 10-millisecond duration) from every 80 ms of data and erases the 70-ms data. In this way, packets are captured in a discontinuous way and the original communication content cannot be restored.	The ONT device switches to this mode if it cannot determine when a user will initiate a VBD call, or when user data will be transmitted after a VBD call is set up. This mode applies when the local or peer end cannot identify a fax or modem signal tone, or a fax or modem negotiation between the local and peer ends fails.
Packet header-only mirroring	The ONT device mirrors only the IP, UDP, and RTP headers of RTP packets. It replaces the payloads of the RTP packets with fixed data. In addition, the ONT device does not mirror TDM tracing packets.	This mode applies when the VBD negotiation process has ended and locates voice quality faults, such as packet loss, jitter, delay, one-way audio, and no audio. This mode allows for VBD fault locating without mirroring user communication contents.

Figure 2-1 and Figure 2-2 show the application of the voice media stream packet mirroring modes in a fax or modem call and in a common call.

Figure 2-1 Application of the voice media stream packet mirroring modes in a fax or modem call

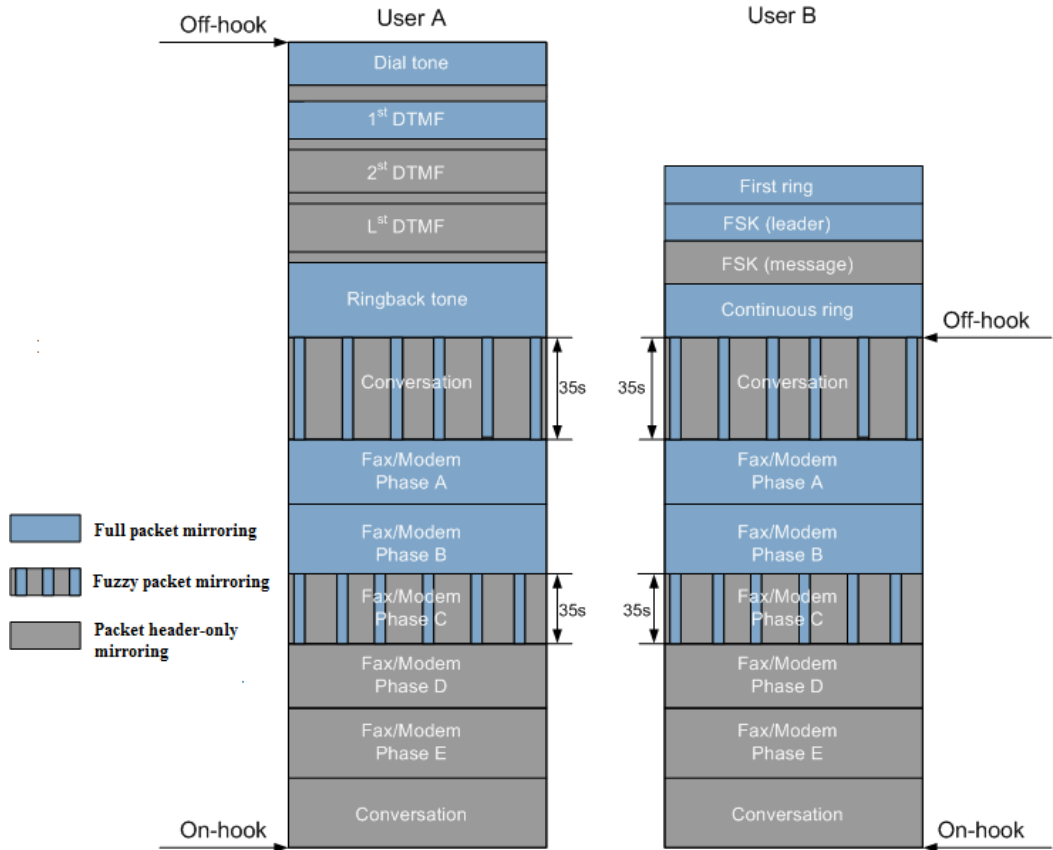
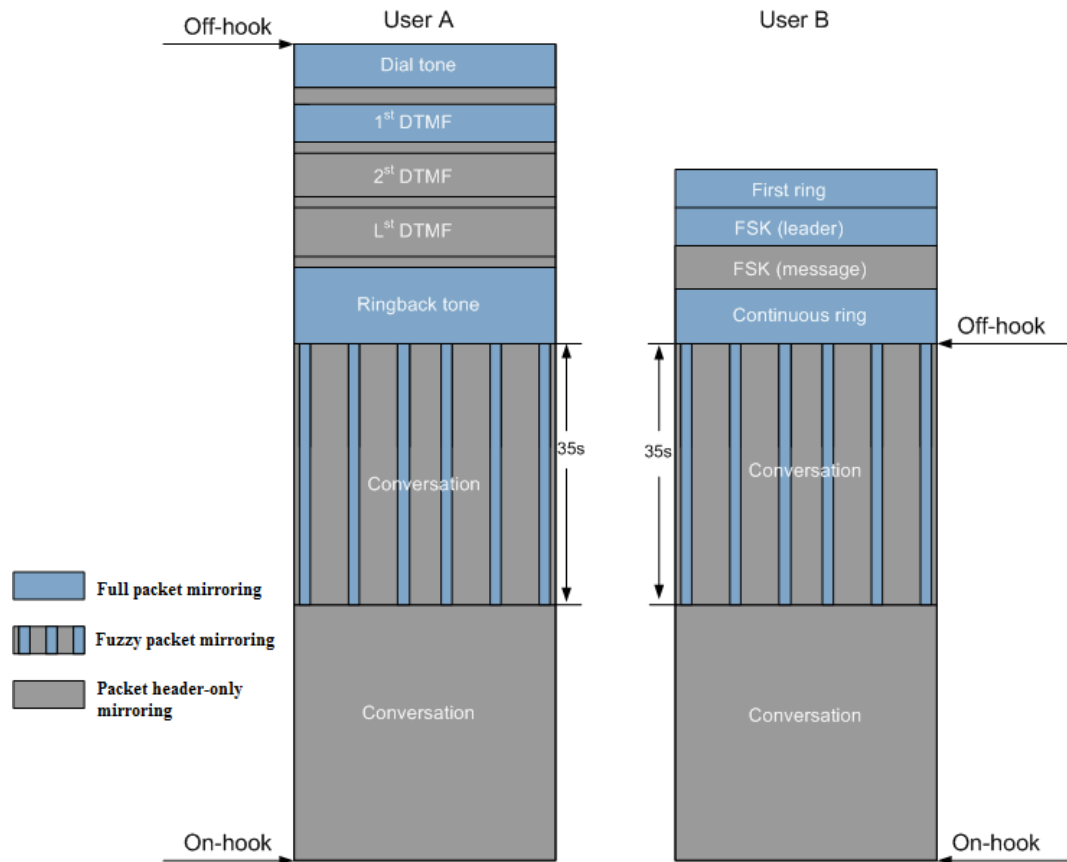


Figure 2-2 Application of the voice media stream packet mirroring modes in a common call



Description

For the calling party:

1. After the calling party picks up the phone, the ONT device starts the full packet mirroring.
2. After detecting the first dual tone multiple frequency (DTMF) number, the ONT device switches to the packet header-only mirroring mode, which prevents disclosure of the user DTMF numbers.
3. When the calling party hears ringback tones, the ONT device switches to the full packet mirroring mode.
4. After the call is set up between the calling and called parties, the ONT device switches to the fuzzy packet mirroring mode and starts a 35-second timer that limits the mirroring time and protects user communication security.



NOTE

The call may be a VBD call, during which the VBD signal tone may not be identified. Therefore, the fuzzy packet mirroring mode is required to locate faults where the VBD signal tone fails to be identified.

5. If the ONT device detects the fax or modem signal tone and the two ends of the fax or modem service are at the negotiation phase, the ONT device switches to the full mirroring mode because no communication data is involved at the negotiation phase. In this way, the ONT device can mirror most fault-related packets, facilitating rapid fault locating.



NOTE

This step is involved only in a fax or modem call.

6. Before the negotiation phase ends, the ONT device switches to the fuzzy packet mirroring mode.



NOTE

This step is involved only in a fax or modem call.

7. When the fuzzy packet mirroring protection timer times out, the ONT device switches to the packet header-only mirroring mode, which protects user communication security.

For the called party:

1. When the phone of the called party is ringing, the ONT device starts the full packet mirroring.
2. When sending frequency shift keying (FSK) signals to the called party, the ONT device switches to the packet header-only mirroring mode, which prevents the user data from being captured.
3. After the call is set up between the calling and called parties, the ONT device switches to the fuzzy packet mirroring mode and starts a 35-second timer that limits the mirroring time and protects user communication security.



NOTE

The call may be a VBD call, during which the VBD signal tone may not be identified. Therefore, the fuzzy packet mirroring mode is required to locate faults where the VBD signal tone fails to be identified.

4. If the ONT device detects the fax or modem signal tone and the two ends of the fax or modem service are at the negotiation phase, the ONT device switches to the full mirroring mode because no communication data is involved at the negotiation phase. In this way, the ONT device can mirror most fault-related packets, facilitating rapid fault locating.



NOTE

This step is involved only in a fax or modem call.

5. Before the negotiation phase ends, the ONT device switches to the fuzzy packet mirroring mode.



NOTE

This step is involved only in a fax or modem call.

6. When the fuzzy packet mirroring protection timer times out, the ONT device switches to the packet header-only mirroring mode, which protects user communication security.



NOTE

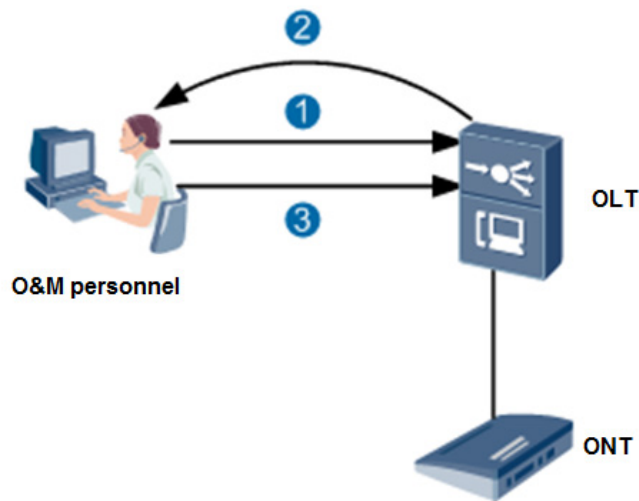
Upon detecting the first DTMF number (or an RFC 2833-compliant DTMF number), the ONT device switches to the packet header-only mirroring mode to protect the numbers dialed by users.

Based on your requirements, the secure packet mirroring of the voice media Stream feature may involve using, obtaining, or saving some information about users' communications for the purpose of safeguarding network operation and protecting services. Huawei alone is unable to collect or save the content of users' communications. It is suggested that you activate the interception-related functions based on the applicable laws and regulations in terms of purpose and scope of usage. You are obligated to take considerable measures to ensure that the content of users' communications is fully protected when the content is being used and saved.

Process

The O&M personnel set remote diagnosis parameters through the NMS, TR069, or Telnet, start remote diagnosis, and run the Wireshark on the remote diagnosis server. The ONT encapsulates the obtained packet into a UDP packet payload and sends the packet to the remote diagnosis server, as shown in Figure 2-3.

Figure 2-3 Process of obtaining signaling and media during remote security diagnosis



6. The O&M personnel start the universal media stream obtaining software (such as Wireshark) on the remote diagnosis server, and start remote security diagnosis through the NMS, TR069, or Telnet.
7. The ONT sends the obtained security diagnosis signaling and media packets to the remote security diagnosis server specified by the O&M personnel.
8. After the location information is collected, the O&M personnel stop obtaining signaling and media packets, or the ONT automatically stops remote diagnosis after the automatic stop time arrives.



NOTE

Based on your requirements and for the purpose of ensuring network operation and services, the remote security diagnosis feature of voice services may involve the use, acquisition, or storage of certain communication content of individual users. Huawei cannot unilaterally collect or store user communication content. Operators are advised to enable the corresponding functions only within the purpose and scope allowed by the applicable laws and regulations. In the process of using and storing user communication content, operators should take sufficient measures to ensure that the communication content is strictly protected.

2.2 Device Management Security

This topic describes features related to device management security.

2.2.1 User Management

User management includes management of user rights, management of user name and password, and login control.

Introduction

User management involves management of the following two types of users:

- CLI user: A command line interface (CLI) user needs to be authenticated by user name and password when the user attempts to log in to a device through the CLI.

- Web user: A web user needs to be authenticated by user name and password when the user attempts to log in to a device through the web GUI. Web users are classified into two levels: administrator and common user. Users of different levels have different rights.

User management is to secure device management and maintenance by user name+password authentication and level-based rights management.

Specifications

- Web users have two rights levels: administrator and common user.
- The password of a web user or CLI user must contain at least two types of the following characters: upper-case letters, lower-case letters, digits, and special characters.
- The password of a web user or CLI user must not be the same as the user name or the user name spelled in the reverse order.
- A web user will be automatically logged out (that is, locked) if the user does not perform any operation within a specified period of time (also called as the timeout time). The timeout time is defaulted to 5 minutes and can be customized.
- If a web user fails to log in to a device using the same IP address for three times in 2 minutes, the user of this IP address will be locked. The lockout time is 1 minute.
- A CLI user will be automatically logged out if the user does not perform any operation within a specified timeout time. The timeout time is defaulted to 5 minutes and can be customized.
- If a CLI user fails to log in to a device using the same IP address for five times consecutively, the user of this IP address will be locked. The lockout time is 5 minutes.

2.2.2 HTTPS Connection Security

2.2.2.1 Introduction

Definition

Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) is an HTTP protocol that runs on the top of transport layer security (TLS) and Secure Sockets Layer (SSL). It is used to establish a reliable HTTP channel, adding the security capabilities of SSL/TLS to standard HTTP communications. The security of HTTPS is based on SSL/TLS. Therefore, SSL/TLS is required for encryption of the content details.

Purpose

HTTPS can address the following problems:

- Host trust
A server that uses HTTPS must apply from a trusted certificate authority for a certificate that proves the server type and its purpose. The client trusts the host only when the certificate is applied to the corresponding server. In other words, the client trusts the certificate and then trusts the host. This mechanism improves security.
- Data leakage and tampering
 - In HTTPS communication, the ONT must have an authenticated certificate, which ensures that all communication data between the server and client is encrypted, preventing data leakage.

- In HTTPS communication, the client and server communicate with each other using keys. Therefore, even when a third party intercepts data exchanged between the client and server, the third party cannot tamper with it without keys.

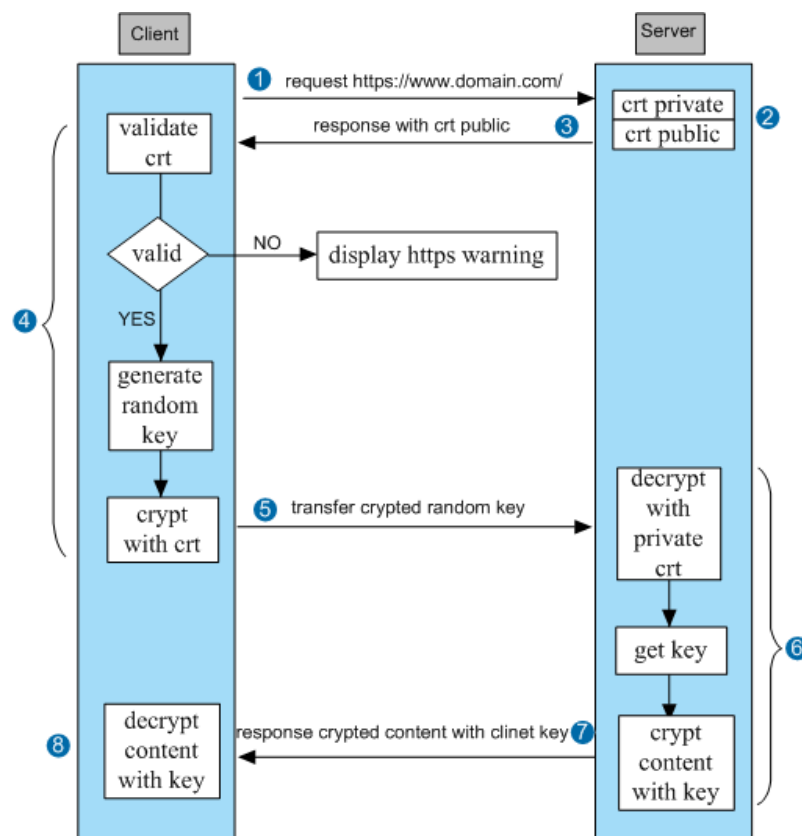
2.2.2.2 Reference Standards and Protocols

- RFC 2246: TLS Protocol Version 1.0
- RFC 5246: Transport Layer Security (TLS) Protocol Version 1.2


2.2.2.3 Principles

HTTPS consists of HTTP and SSL/TLS. A module for processing encrypted information is added based on HTTP. Data of both the server and the client will be encrypted through SSL/TLS. Therefore, data exchanged between the server and the client is encrypted. Figure 2-4 illustrates the data processing procedure.

Figure 2-4 HTTPS data processing



1. The client initiates an HTTPS request.
The user enters an HTTPS website address in the browser and then connects to the 80 port of the server.
2. The server generates a digital certificate.
The server that uses the HTTPS protocol must have a set of digital certificates which contain a public key and a private key. The certificate can be granted by the server itself or applied from a certificate authority. A certificate granted by the server itself must be verified by the client while a certificate applied from a trust certificate authority can be directly used.

3. The server sends the public key to the client.
The public key contains information about the authority that grants the certificate and the valid period of the certificate.
 4. The client parses the certificate.
SSL/TLS of the client parses the certificate. Specifically, SSL/TLS verifies whether the public key is valid, for example, by checking the certificate authority and valid period.
 - If abnormality is found, the client prompts that the certificate is incorrect.
 - If the certificate is correct, the client generates a random value (the private key) and encrypts the random value using the certificate.
 5. The client sends the encrypted random value to the server.
The encrypted random value will be used to encrypt and decrypt communication data between the client and the server.
 6. The server decrypts the random value.
After decryption, the server obtains the random value (the private key) from the client and performs symmetric encryption on data using this value.
-  **NOTE**
Symmetric encryption is to mix the information and private key together using a certain algorithm. In this way, no one can obtain the information unless the private key is known. Data security is ensured because only the client and the server know the private key. The more complex the private key, the more secure the data.
7. The server sends the encrypted information to the client.
The information is encrypted using the private key. Therefore, it can be restored by the client.
 8. The client decrypts the information.
The client uses the private key to decrypt the information sent from the server.

2.2.3 M2M Web Interface

2.2.3.1 Introduction

Definition

Through the machine-to-machine (M2M) web interface, packet formats are unified, which facilitates the development and integration of the operations support system (OSS) and other tools.

Object

M2M web interfaces are a set of HTTP/HTTPS-based interfaces that are defined to ease service provisioning for carriers.

2.2.3.2 Specifications

- The account name, password, and TCP port of the M2M web interface are the same as those of the web page.
- After a user logs in through the web page, the M2M web interface is inaccessible. After a common user logs in to the M2M web interface, the web page is accessible only by using an administrator account.

- Data can be modified and queried through the M2M web interface. The following table lists the items supported by the M2M web interface.

Table 2-2 Item and operation

Item	Operation
SerialNumber	Query
LAN MAC address	Query
Board bar code	Query
HardwareVersion	Query
SoftwareVersion	Query
AdditionalSoftwareVersion	Query
WLAN MAC address	Query
WAN MAC address	Query
ReleaseTime	Query
Main version information	Query
Standby version information	Query
WIFI SSID and password	Query
ProgramKey	Query
Customized configuration name	Query
LAN-side Telnet	Query and modification
ProvinceList	Query

 **NOTE**

The preceding table lists all ONT operations supported by the M2M web interface. However, different carriers' web pages may have different operation rights. The operation rights of a carrier's M2M web interface are the intersection between the operation rights of the web page and the operations listed in the preceding table.

2.2.3.3 Principles

The M2M web interface is defined based on the HTTP/HTTPS protocol. The packets of the M2M web interface are structured as follows:

- Segment 1: common HTTP request field
- Segment 2: common HTTP header
- (Optional) Segment 3: HTTP expansion field (carrying user operation parameters and returned results)

The following figure shows the detailed format of a packet.

```
POST /html/mm/mm.cgi?x=mminterface&RequestFile=html/mm/mminterface.asp  
HTTP/1.1
```

```
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-  
shockwave-flash, application/vnd.ms-excel, application/vnd.ms-powerpoint,  
application/msword, */*
```

```
Referer: http://192.168.100.1/html/mm/mminterface.asp
```

```
Accept-Language: zh-cn
```

```
Content-Type: application/x-www-form-urlencoded
```

```
Accept-Encoding: gzip, deflate
```

```
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
```

```
Host: 192.168.100.1
```

```
Content-Length: 53
```

```
Connection: Keep-Alive
```

```
Cache-Control: no-cache
```

```
Cookie: Cookie=UserName:root:PassWord:YWRtaW4=:Language:english:id=1
```

```
ACTION:ADD/SET/DEL/DSP/LOGINREQ/LOGINSUB/LOGOUT/FILEPUT/  
FILEGET
```

```
TYPE:SECURE
```

```
OPRESULT:
```

```
OPRETURNCODE:
```

```
OPERRORCODE = 0 (SUCCESS)
```

```
Parameter-Length: \r\n\r\n
```

```
<ParameterObjec  
OBJECTNAME="InternetGatewayDevice.ManagementServer" RESULT = "0"  
ERRORCDOE = "SUCCESS">
```

```
<ParaName>ParameterKey</ParaName>
```

```
<Value>0</Value>
```

```
<ParaName>ConnectionRequestURL</ParaName>
```

```
<Value>http://10.1.76.204:5001</Value>
```

```
<ParaName>SoftwareVersion</ParaName>
```

```
<Value>V100R001C05B013</Value>
```

2.2.4 NetOpen Security

Please refer to the related security documentation of NetOpen.

2.3 System Security

This topic covers the overview, availability, and sub-features of network security.

2.3.1 Anti-DoS Attack

The denial of service (DoS) attack refers to an attack initiated from a malicious user who sends a large number of protocol packets to the system, which results in denying service requests of common users by the system. The anti-DoS attack feature refers to the defensive measures taken by the system to control and limit the number of protocol packets sent from a user.

2.3.1.1 Introduction

Definition

The DoS attack indicates an attack from a malicious user who sends a large number of protocol packets, which results in denying service requests of authorized users by the system. The anti-DoS attack feature refers to the defensive measures taken by the system to control and limit the number of protocol packets sent from a user.

Purpose

The DoS attack affects the running of the system. That is, the system may fail to process service requests of authorized users, or even the system may be crashed.

To protect the system, the number of protocol packets received by the system is restricted to a specified range. The packets that are not within the range are discarded.

2.3.1.2 Specifications

The following specifications are supported:

- Anti-SYN flooding attack
- Anti-ICMP echo attack
- Anti-ICMP redirect attack
- Anti-LAND attack
- Anti-Smurf attack
- Anti-WinNuke attack
- Anti-ping sweep attack

2.3.1.3 Feature Updates

Table 2-3 Updates of the anti-DoS attack feature

Product Version	Change Description
V300R019C20&V500R019C20	Supports anti-DoS attack for IPv6 scenarios.
V200R006C00&V200R006C01	This feature is enhanced to support: <ul style="list-style-type: none"> • Anti-tear drop attack • Anti-ping of death attack
V100R002C04&V100R002C05	This feature is enhanced to support: <ul style="list-style-type: none"> • Anti-LAND attack • Anti-Smurf attack

Product Version	Change Description
	<ul style="list-style-type: none"> Anti-WinNuke attack
V100R001C00&V100R001C01	It is the first version that supports this feature.

2.3.1.4 Principles

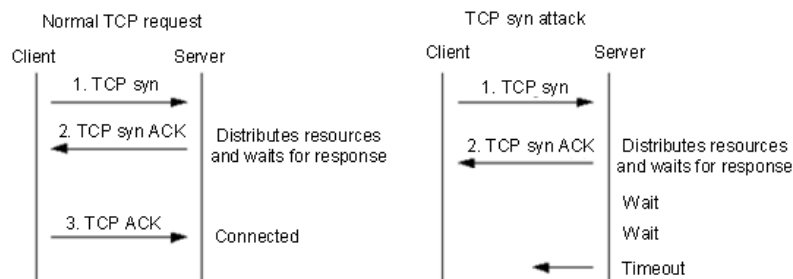
SYN Flooding Attack and Protection

Attack Principle

SYN flooding is a common form of DoS attack. An attacker can initiate attacks from one or several devices at the same time. The attacks result in access failures in the target server. SYN flooding is based on the TCP connection setup mechanism. To set up a TCP connection, the requester and the server must perform the three-way handshake. Then, they can send data to each other.

- Connection request: The requester sends a SYN (synchronize) message to the server to start the three-way handshake.
- Request acknowledgment: The server acknowledges this request by sending a SYN/ACK message to the requester.
- Connection complete: The requester responds with an ACK message and the three-way handshake is complete.

Figure 2-5 Principle of SYN flooding



In the SYN flooding attack, several random source hosts send SYN messages to a destination server. After receiving the SYN/ACK messages from the destination server, the source hosts do not respond. In this way, the destination server establishes many connection queues for the source hosts, and always maintains the queues because no ACK response is received. As a result, resources of the destination server are consumed and the destination server cannot provide services for other connections. In the worst situation, the destination server may crash. The server has to wait until the connections time out and then the server can release the occupied resources.

Protection Principle

To prevent a SYN flooding attack, you can set a permitted maximum number of half-TCP connections. After the half-TCP connections exceed the maximum number, the half-TCP connections created are disabled randomly or the new SYN messages are discarded.



NOTE

To enable the anti-SYN flooding function, select this function on the ONT web page.

ICMP Echo Attack and Protection

Attack Principle

In general, when a diagnosis application, such as the ping command, is used to diagnose network faults, an ICMP echo request is sent. After receiving the ICMP echo request, the receiving device responds with an ICMP echo reply. The process involves the CPU. In some situations, such as data fragments processing, a lot of CPU resources are consumed. If an attacker sends a large number of ICMP echo requests (known as an ICMP flood) to the target PC, the target PC is busy processing these ICMP echo requests and cannot process other network data packets. In this case, a DoS attack occurs.

Protection Principle

Limiting the rate of ICMP echo requests helps to prevent an ICMP echo attack. When receiving a large number of ICMP echo requests, the device actively discards some of these packets.



NOTE

To enable the anti-ICMP echo function, select this function on the ONT web page.

ICMP Redirect Attack and Protection

Attack Principle

An ICMP redirect attack is a DoS attack targeting at connections. Such an attack can terminate network connections, rendering the connections unavailable. In an ICMP redirect attack, the attacker uses valid ICMP messages to affect all IP devices. Specifically, the attacker forges ICMP redirect messages and sends a large number of such messages to some ports of the destination device. The attack destroys a lot of network connections and consumes CPU resources of the victim network devices. As a result, many network connections are interrupted and a DoS attack occurs.

Protection Principle

Limiting the rate of ICMP redirect packets helps to prevent an ICMP redirect attack. When receiving a large number of ICMP redirect packets, the device actively discards some of these packets.



NOTE

To enable the anti-ICMP redirect function, select this function on the ONT web page.

LAND Attack and Protection

Attack Principle

An attacker sets the source and destination addresses of the TCP SYN message to be the same as the IP address of a target host. In this way, the target host sends an SYN/ACK message to its own IP address and an ACK message carrying the same IP address is returned. Consequently, a null connection is created on the target host. Each null connection remains until it times out. As a result, a large number of connections are unavailable and a DoS attack occurs.

Protection Principle

The host prohibits TCP SYN messages with identical source address and destination address, or intercepts TCP messages with this attribute.



NOTE

To enable the anti-LAND attack function, select this function on the ONT web page.

Smurf Attack and Protection

Attack Principle

In a Smurf attack, an attacker sends ICMP echo requests to a network. The source address of the ICMP echo requests is the address of a victim host (another host), but not the source address of the attacker. Hence, the ICMP echo replies are sent to the victim host, causing the processing capability or network bandwidth usage of the victim host to reach its limit. In a larger network, the attack will cause a more serious impact, because such a network has a larger number of active hosts and the victim host will receive more ICMP echo replies.

Protection Principle

The host does not respond to, or intercepts the ICMP echo requests whose destination address is a network broadcast address.



NOTE

To enable the anti-Smurf attack function, select this function on the ONT web page.

WinNuke Attack and Protection

Attack Principle

WinNuke attack, also called out of band (OOB) attack, is a DoS attack. When the URG flag is set to 1 and the urgent pointer is not set to 0 in the TCP message sent to a target host, the host is attacked. The attack may result in system crash. In a WinNuke attack, the destination port numbers in the messages sent are generally 139, 138, 137, and 113. In addition, the URG flag in the messages is set to 1, indicating the urgent mode.

Protection Principle

The device discards TCP messages in which the destination port numbers are 139, 138, 137, or 113 and the URG flag is 1.



NOTE

To enable the anti-WinNuke attack function, select this function on the ONT web page.

Ping Sweep Attack and Protection

Attack Principle

Ping sweep is implemented by sending ping probing packets in polling mode to multiple IP addresses to determine the running status of hosts on a network and therefore detect live hosts based on the received response packets. A malicious user may attack the live hosts according to the IP addresses.

Protection Principle

After the anti-ping sweep function is enabled, the ONT discards ICMP echo requests and does not respond to ping probing packets.



NOTE

To enable the anti-ping sweep function, select this function on the ONT web page.

Tear Drop Attack and Protection

Attack Principle

Tear drop attack is a denial of service attack based on malformed UDP fragments. An attacker sends the target system multiple fragmented IP packets that contain the information about the packet to which a fragment belongs and the position of a fragment in the packet. After the target system receives the forged packets with overlapping offsets, the system will crash or reboot.

Protection Principle

The operating system checks the malformed packets to prevent tear drop attacks.



NOTE

The anti-tear drop attack function is enabled by default. You are not allowed to disable it.

Ping of Death Attack and Protection

Attack Principle

A ping of death attack is a denial of service attack. An attacker sends the target system a ping packet larger than 65,535 bytes, which causes memory overflow on the target system. As a result, memory allocation fails and TCP/IP stack breaks down.

Protection Principle

After the anti-ping of death function is enabled, the ONT calculates the packet length to prevent oversized packets.



NOTE

The anti-ping of death attack function is enabled by default. You are not allowed to disable it.

2.3.2 Preventing TCP SYN Port Scanning

Port scanning refers to scanning a port or a specified port range one by one by certain technical means. Generally, specific packets are sent and the responses are observed. The scanning result shows the services provided by a device, which helps attackers performed attacks by exploiting known vulnerabilities of the provided services. Most frequently, TCP SYN packets are sent for scanning. The anti-port scanning function is provided to identify scanning behaviors and blocking the IP address of the scanner.

2.3.2.1 Introduction

Definition

Port scanning refers to scanning a port or a specified port range one by one by certain technical means. Generally, specific packets are sent and the responses are observed. The scanning result shows the services provided by a device, which helps attackers performed attacks by exploiting known vulnerabilities of the provided services. Most frequently, TCP SYN packets are sent for scanning. The anti-port scanning function is provided to identify scanning behaviors and blocking the IP address of the scanner.

Purpose

Port scanning provides a way for external attackers to discover device services and helps them launch specific attacks.

To protect the system, a large number of TCP SYN connections initiated from the network side to a device within a unit time are considered as port scanning. In this case, the IP address of the scanner is blocked.

2.3.2.2 Specifications

- Supports the anti-TCP SYN port scanning function.

2.3.2.3 Feature updates

Table 2-4 Enhanced the anti-DoS attack feature

V300R019C20	It is the first version that supports this feature.
-------------	---

2.3.2.4 Principles

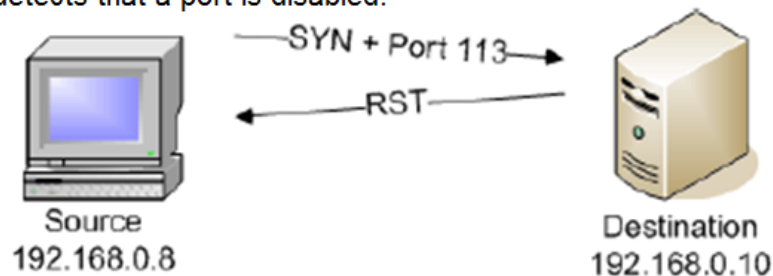
TCP SYN Port Scanning

Attack Principle

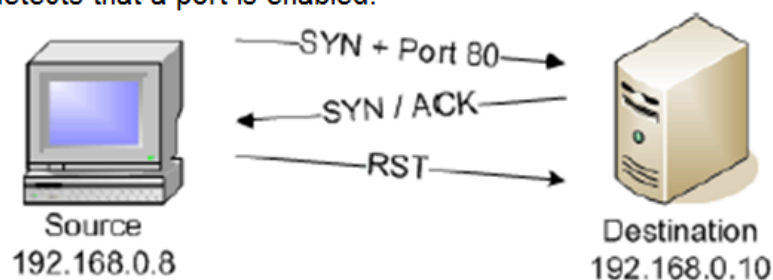
Send SYN to a target port. If the SYN/ACK response is received, the port is enabled. If the RST packet is received, the port is disabled. If no response is received, the port is shielded.

Figure 2-6 TCP SYN port scanning principle

TCP SYN detects that a port is disabled:



TCP SYN detects that a port is enabled:



Protection Principle

A large number of TCP SYN connections initiated from the network side to a device within a unit time are considered as port scanning, and then the IP address of the scanner is blocked.



NOTE

This feature has a certain impact on the system performance and is disabled by default. For customized markets, this feature can be enabled since tr069.

2.3.3 MAC Address Filtering

MAC address filtering is to filter user packets according to the source MAC address of the user packets.

2.3.3.1 Introduction

Definition

MAC address filtering is to filter user packets according to the source MAC address of the user packets.

Purpose

Configuration of MAC address filtering helps control the Internet access rights of user-side PCs. Specifically, the PCs complying with the preset rule are allowed to access the Internet and the unqualified PCs are not allowed to access the Internet.

2.3.3.2 Specifications

The following specifications are supported:

- 8 MAC address filtering rules
- User-side MAC address filtering, including LAN port access and Wi-Fi access on the user side
- SSID-based MAC address filtering. A maximum of 8 MAC addresses can be configured for each SSID.



NOTE

SSID-based MAC address filtering is supported only by ONTs that support the Wi-Fi function.

- Configurations of blacklists and whitelists

2.3.3.3 Feature Updates

Table 2-4 Updates of the MAC address filtering feature

Version	Change Description
V300R013C00	SSID-based MAC address filtering is supported.
V100R001C00&V100R001C01	It is the first version that supports this feature.

2.3.3.4 Principles

A PC may have more than one IP addresses but a unique MAC address. Filtering MAC addresses helps control Internet access of PCs in a LAN.

The MAC address filtering function can be implemented in the following two modes:

- Configuring blacklist of MAC address filtering: The PCs whose MAC addresses are in the blacklist are not allowed to access the Internet while PCs whose addresses that are not in the blacklist are allowed to access the Internet.
- Configuring white list of MAC address filtering: The PCs whose MAC addresses are in the white list are allowed to access the Internet and other PCs are not allowed to access the Internet.



NOTE

Because blacklist and white list are globally configured, only one mode is supported at a time.

2.3.4 IP Address Filtering

2.3.4.1 Introduction

Definition

IP address filtering, a security mechanism of HGs, is a feature of allowing the communication between all or some ports in an IP address segment and all or some ports with public network IP addresses by setting IP address filtering rules.

Purpose

IP address filtering is used to restrict the connection between an intranet host and the public network.

2.3.4.2 Specifications

The following specifications are supported:

- 32 IPv4 address filtering rules (IPv6 address filtering not supported)
- IPv4 address filtering by IP address segment, UCP/TCP port number, and port range
- IPv4 address filtering by IP protocol type

2.3.4.3 Feature Updates

Table 2-5 Updates of the IP address filtering feature

Product Version	Change Description
V300R019C20&V500R019C20	Supports IP address filtering for IPv4 packets in a DS-Lite tunnel.
V300R015C00	Configuration of port number segments is supported. The LAN side and the WAN side each support a maximum of 15 port number segments.
V300R013C00	The blacklist and whitelist hybrid mode is supported. In this mode, IP address filtering can be configured for upstream and downstream.
V100R001C00&V100R001C01	It is the first version that supports this feature.

2.3.4.4 Principles

When an ONT works as an HG for Layer 3 forwarding, it, based on the preconfigured IP address filtering rule, checks data packets one by one to determine whether a data packet matches the filtering rule. The matching information includes the source IP address, destination IP address, encapsulation protocol such as TCP and UDP, TCP/UDP source port, and port range. If a data packet matches a rule and the rule allows the data packet to pass, the data packet will be forwarded according to the information in the route table. If a data packet matches a rule and the rule prohibits the data packet from passing, the data packet will be discarded. If a data packet does not match any rule, the data packet will be forwarded according to the default forwarding rule.



NOTE

The IP address filtering function takes effect only when the ONT works as an HG for Layer 3 forwarding.

2.3.5 Firewall

A firewall is an advanced access control mechanism established between different network security domains. It enables users to control the incoming and outgoing network traffic based on a predetermined set of security rules.

2.3.5.1 Introduction

Currently, the Internet has the following common security threats:

- Unauthorized use of resources: Resources are used by unauthorized users or in an unauthorized mode. For example, attackers gain access to a computer system and use resources by guessing a user account and password combination.
- Denial of service (DoS): Attackers exploit vulnerabilities of network protocol implementation to initiate attacks or maliciously exhaust resources of the attacked object. A DoS attack is an attempt to stop the target object from providing services or resources. For example, attackers send a large number of data packets or deformed packets to a server to request for connections or replies, overloading the server so much that it cannot execute scheduled tasks.
- Data tampering: Attackers modify, delete, delay, or realign system data or message flows, or insert fake messages to compromise data consistency.
- Information theft: Attackers do not invade the target system, but sniff it to steal important data or information.

A firewall monitors data flows and decides whether data flows are allowed to enter an access device. Firewalls protect internal networks against unauthorized or unauthenticated access and attacks initiated from external networks.

Table 2-6 Firewalls supported by the ONT.

Firewall	Function	Characteristics
Stateful packet inspection (SPI) firewall	This firewall inspects information (including the source address, destination address, source port number, destination port number, protocol type, TCP connection status, and	Advantage: high security. Disadvantage: Some connections for online games or P2P downloading may be blocked.

Firewall	Function	Characteristics
	timeout period) of each connection to determine whether to filter data packets.	
Level-based firewall	This firewall controls access to specific services of the ONT from the LAN side and the WAN side and better prevents DoS attacks.	Advantages: provides firewalls with different rules and suits different application scenarios.

2.3.5.2 Feature Updates

Table 2-7 Updates of the firewall feature

Version	Change Description
V200R006C02	It is the first version that supports this feature.

2.3.5.3 Feature Dependency and Limitation

Specifications Limitation

The stateful packet inspection (SPI) firewall is supported only by gateway-type ONTs and bridge+voice ONTs.

The level-based firewall is supported only by gateway-type ONTs.

Feature Dependency

When the level-based firewall is enabled and the firewall level is not the custom level, the following functions are invalid: IP address filtering, URL filtering, anti-DoS attack, and ACL rules.

2.3.5.4 Principles

SPI Firewall

The stateful packet inspection (SPI) firewall not only implements packet filtering but also maintains a connection status recording table in its memory. Therefore, it is more secure than simple packet filtering firewalls.

The most advanced SPI firewall provides the highest level of security. By default, it rejects all requests from external networks and dynamically maintains communication status of all connections for requests sent from the internal network. Only packets that are returned for internal users' connection requests and that match the existing state database can pass through the firewall. This solution allows network users to access Internet resources while preventing hackers on the Internet from accessing internal network resources.

Level-based Firewall

The level-based firewall provides five configuration options (high, medium, low, disabled, and custom level) for different users. Based on the SPI firewall, the level-based firewall controls access to specific services of the gateway from the LAN side and the WAN side and better prevents DoS attacks, enabling the gateway to stably serve authorized users.

Table 2-8 describes the rules for each firewall level.

Table 2-8 Level-based firewall rules

Level	Rule
Disabled	The firewall is disabled.
High	<ul style="list-style-type: none"> • Allows SPI firewall packets. • Allows unsolicited packets sent from the LAN side to the FTP, DNS, and HTTP ports on the WAN side. • Allows unsolicited packets sent from the LAN side to the HTTP port on the gateway side.
Medium	<ul style="list-style-type: none"> • Allows SPI firewall packets. • Allows all unsolicited packets sent from the LAN side to the WAN side. • Allows unsolicited packets sent from the LAN side to the HTTP, ICMP, and Telnet ports on the gateway side. • Allows unsolicited packets sent from the WAN side to the ICMP and ACS ports on the gateway side.
Low	<ul style="list-style-type: none"> • Allows SPI firewall packets. • Allows all unsolicited packets sent from the LAN side to the WAN side. • Allows unsolicited packets sent from the LAN side to the HTTP, ICMP, and Telnet ports on the gateway side. • Allows unsolicited packets sent from the WAN side to the ICMP, FTP, HTTP, and ACS ports on the gateway side.
Custom level	The firewall rules are defined by users.

2.3.6 External Host Access Control

2.3.6.1 Introduction

Definition

The external host access control feature allows certain external hosts to access Telnet/HTTP/FTP connections of the ONT from the WAN side when a firewall is enabled.

Purpose

By default, for security purposes, the firewall rejects remote connection requests, such as Telnet/HTTP/FTP connection requests, from the WAN side. However, remote access to the ONT from the ACS is required during service maintenance. Therefore, this feature is developed to enable the ONT to accept connection requests from certain specified addresses (hosts) even when the firewall rejects remote connections from the WAN side.

2.3.6.2 Specifications

Table 2-9 Items and specifications

Item	Specifications
Maximum number of access control rules	8

2.3.6.3 Feature Updates

Table 2-10 Updates of the external host access control feature

Version	Change Description
V300R012C00	It is the first version that supports this feature.

2.3.6.4 Feature Dependency and Limitation

Specifications Limitation

This feature is supported only by gateway-type ONTs and bridge+voice ONTs.

The configured access control rules apply to WAN-side connection services that are disabled but do not apply to services that are enabled.

External host access rules can be configured only in IPv4 address format. External host access rules in IPv6 address format are not supported.

2.3.6.5 Principles

When the firewall does not allow for connection requests from the WAN side, the ONT rejects all Telnet/HTTP/FTP connection request packets sent from the WAN side. The external host access control feature enables users to add a whitelist of external hosts (WAN side) that are allowed to access the Telnet/HTTP/FTP connections.

The added whitelist rule is "IP address/network segment in the whitelist" with the corresponding rule action "accept". WAN-side hosts that have the specified IP addresses or whose IP addresses are within the network segment specified in the whitelist can access the ONT through the Telnet/HTTP/FTP connections.

2.3.7 Inband Management VLAN

2.3.7.1 Introduction

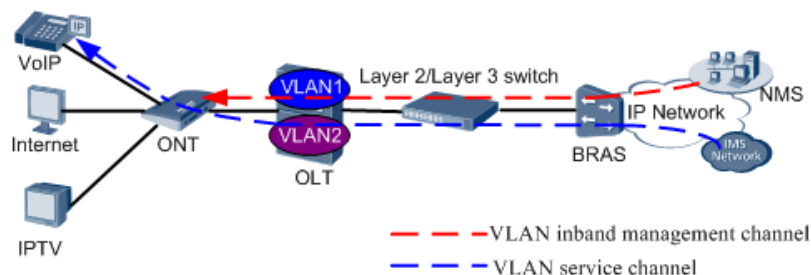
Definition

In an inband management VLAN, carriers manage and maintain ONTs over a remote network. Associated inband management protocols support specified VLAN instances (that is, WAN instances), and virtual routes are planned for the VLAN to receive and forward management packets at the upper-layer network. In this way, carriers can use private IP addresses to manage and maintain devices remotely. This method saves public network IP addresses and isolates the management network from the public network.

2.3.7.2 Principle

Virtual local area network (VLAN) is a communications technology that divides a physical LAN into multiple logical broadcast domains (multiple VLANs). NEs in a VLAN can communicate with each other but NEs in different VLANs cannot.

Figure 2-7 Example network of inband management VLAN



In Figure 2-7, two VLANs are configured for the ONT, where VLAN1 serves as the VoIP service channel and VLAN2 as the inband management channel.

2.3.8 Parental Control

2.3.8.1 Introduction

Definition

The parental control function allows parents to configure different filtering policy templates to set constraints for network access time and website access. The templates are associated with children's web devices based on MAC addresses.

Purpose

Parental control is intended for parents to control the network access time and website access of their children, which ensures that their children access allowed websites in specified time segments and are away from age inappropriate contents.

Benefits

Benefits to users

Parents can configure different network access time and website access constraints on working days and holidays and keep their children away from age inappropriate contents.

2.3.8.2 Specifications

Table 2-11 Items and specifications

Item	Specification	Remarks
Number of filtering policy templates supported	8	-
Number of web devices that can be used by children	8	Web devices are identified by MAC addresses and are associated with specified templates for network access control.
Number of network access time segments that can be configured in a template	4	This item specifies the number of network access time segments that can be configured in a template. Different network access time segments can be configured for working days and holidays.
Number of URL address filtering rules that can be configured in a template	128	-

2.3.8.3 Feature Updates

Table 2-12 Updates of the parental control feature

Product Version	Change Description
V300R015C00	Different filtering policy templates are configured and associated with different children web devices for network access control. The IPv6 is supported.
V300R013C10	It is the first version that supports this feature.

2.3.8.4 Principles

The ONT serves as the home gateway. When the ONT performs Layer 3 forwarding, it checks data packets and determines whether the data packets are allowed to pass based on the filtering scope, MAC address, network using time segment, and URL address configurations.

1. The ONT checks whether the web device is under control based on the filtering settings. If the filtering settings place limits on packets sent from all web devices or from children

web devices, the ONT proceeds with the next step. Otherwise, the ONT forwards the packets based on preconfigured rules.

2. For the network access packets sent from a device under control, the ONT searches out the filtering policy associated with the device and checks whether the current time is in the allowed network access time segment. If yes, the ONT proceeds with the next step. If not, the ONT discards the packets.
3. The ONT checks whether the target URL is in the list of accessible websites based on the URL filtering rules. If yes, the ONT forwards the packets. If not, the ONT discards the packets.

2.3.9 MAC Anti-spoofing

2.3.9.1 Introduction

Definition

MAC anti-spoofing prevents the dynamic MAC address of a gateway from being learned by other ports.

Purpose

MAC anti-spoofing can be configured on a gateway to prevent the dynamic MAC address of the gateway from being learned by other ports. In this way, the packets that need to be sent to the gateway are not incorrectly sent to other ports, preventing service interruption and information leakage.

2.3.9.2 Specifications

The following specifications are supported:

- Whether the dynamic MAC address of the NNI port can be learned by other ports can be customized.
- Only EG8080P and EG8280P are involved.

2.3.9.3 Feature Updates

Table 2-13 Updates of the MAC anti-spoofing feature

Product Version	Change Description
V800R019C00	It is the first version that supports this feature.

2.3.9.4 Principles

Based on the chip that supports configuration of the MAC address learning priority, users can set the MAC address learning priority of the NNI port to be higher than that of the LAN port.

- When a device sends packets whose source MAC address is the dynamic MAC address of the NNI port through the LAN port, the MAC address of the NNI port is not overwritten by that of the LAN port based on priority judgment.

- When a device receives packets whose source MAC address is the MAC address of the LAN port through the NNI port, the MAC address of the LAN port is overwritten by that of the NNI port based on priority judgment.

2.3.10 Internet Access Control

2.3.10.1 Introduction

Definition

For the networks that cover dormitories in schools, ONT Internet access can be disabled at a fixed time point.

Purpose

The Internet access control feature is intended for schools which want to control the time period for students to access Internet. For example, prohibit them from accessing Internet at bed time.

2.3.10.2 Specifications

Table 2-14 Items and specifications

Item	Specification	Remarks
Number of time periods for controlling ONT Internet access	2	

2.3.10.3 Feature Updates

Table 2-15 Updates of the Internet access control feature

Product Version	Change Description
V300R019C00	It is the first version that supports this feature.

2.3.10.4 Principles

Internet access is controlled based on time periods and related forwarding packets from the user side are identified. If forwarding packets are sent during the period when Internet access is prohibited, they will be dropped, preventing users from accessing Internet.

2.3.11 IPsec VPN

2.3.11.1 Introduction

Definition

This feature Provides IPsec tunnel access capabilities for enterprises.

Purpose

Using this feature, branches of small- and medium-sized enterprises can access one another on the Internet through tunnels, and employees on business trips can access the enterprise servers on the Internet through tunnels. IPsec tunnels have security features such as encryption, authentication, and anti-replay. They are secure tunnels suitable for enterprises.

2.3.11.2 Specifications

Item	Specification	Remarks
Supports IPsec tunnels.	10	This feature depends on chips that support hardware encryption and decryption. Currently, this feature is enabled only for government and enterprise gateway products of China Telecom.
Supports the site-to-site and PC-to-site (RoadWarrior) scenarios.	Supports the site-to-site and PC-to-site (RoadWarrior) scenarios, which are respectively used by branches and employees on business trips to access the enterprise network.	In the site-to-site scenario, the transmission mode or tunnel mode is supported. In the PC-to-site scenario, only the tunnel mode is supported.
Supports the transmission mode and tunnel mode.	An IPsec tunnel works in transmission mode or tunnel mode.	
Supports the IKE protocol.	Supports IKEv1 and IKEv2 protocols.	
Supports bidirectional identity authentication with the IPsec peer.	Uses the pre-shared key (PSK) and X.509 digital certificate to authenticate an IPsec peer. An IP address or name can be used as the identity ID.	
Supports NAT-T.	NAT-T is supported to transparently transmit IKE and IPsec packets through the firewall between the local end and the IPsec peer end.	
Supports DPD.	The DPD protocol is supported, and the DPD interval and retry times can be configured.	
Supports ESP and AH security protocols.	The ESP and AH protocols can be used to protect data packets in tunnels.	The AH+ESP mode is not supported.

NOTE

- When configuring the pre-shared key, you are advised to set a long and complex password that is difficult to guess and configure different passwords for different tunnels.

2.3.11.3 Feature Updates

Table 2-16 Updates in the IPsec feature

Product Version	Change Description
V500R019C20	It is the first version that supports this feature.

2.3.11.4 Principles

Overview

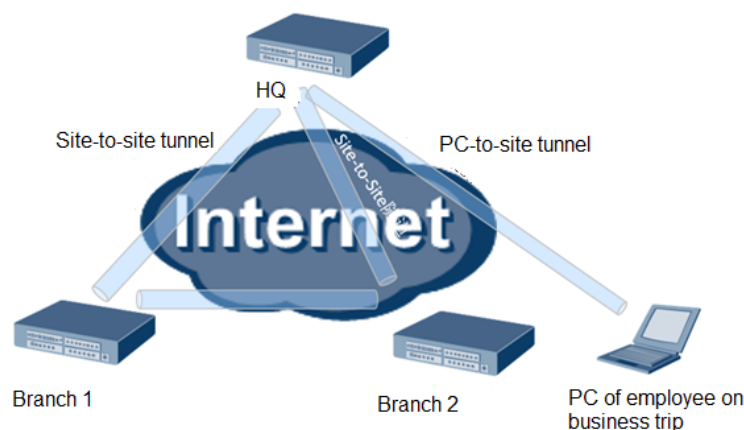
The Internet Protocol Security (IPsec) protocol suite is a series of protocols defined by the Internet Engineering Task Force (IETF). It provides IP packets with high-quality and cryptography-based secure transmission. Specified communication parties encrypt data and authenticate data sources at the IP layer to ensure confidentiality, integrity, and anti-replay of IP data packets during transmission over the network.

- Confidentiality: User data is encrypted and transmitted in ciphertext for security.
- Data integrity: Received data is authenticated to determine whether the packets are tampered.
- Anti-replay: The attacks from malicious users who repeatedly send obtained data packets are prevented. Specifically, the receiver rejects old or repeated data packets.

The IPsec VPN on the government and enterprise gateway can be used in the following scenarios:

- Site-to-Site: The branches of an enterprise connect securely with the headquarters through IPsec tunnels.
- PC-to-Site: Employees on business trips access enterprise services through IPsec tunnels.

Figure 2-8 Typical IPsec scenarios



Basic Concepts

- IPsec peer: IPsec is used to provide secure IP communications between two endpoints. The two endpoints are called IPsec peers.
- A security association (SA) defines the encryption algorithm, digest, and keys for secure data conversion and transmission between IPsec peers. An SA is unidirectional. Bidirectional communication between two participants requires at least two SAs to protect data flows in two directions. An SA is identified by a triplet consisting of a security parameter index (SPI), destination IP address, and security protocol (AH or ESP) identifier. An SPI is a 32-bit value and transmitted in AH and ESP headers. An ONT supports the ISAKMP protocol for dynamic negotiation of the SA.

IPsec VPN Encapsulation Format

The IPsec protocol has two encapsulation modes:

- Tunnel mode: In tunnel mode, AH or ESP is inserted before the original IP header, and a new IP header is generated before AH or ESP. Figure 2-9 take TCP as an example.

Figure 2-9 IPsec tunnel mode

Mode \ Protocol	Tunnel						
AH	New IP Header	AH	Raw IP Header	TCP Header	data		
ESP	New IP Header	ESP	Raw IP Header	TCP Header	data	ESP Tail	ESP Auth data

- Transport mode: In transport mode, AH or ESP is inserted after the IP header but before the transport layer protocol. Figure 2-10 take TCP as an example.

Figure 2-10 Transport mode

Mode \ Protocol	transport						
AH	IP Header	AH	TCP Header	data			
ESP	IP Header	ESP	TCP Header	data	ESP Tail	ESP Auth data	

Protocol Principle

The principles of IPsec are complex. For details, see the corresponding technical white paper.