BLONDER TONGUE
LABORATORIES

CMTS Edge 16/32/32P

V4.1.0

User Manual

Blonder Tongue Laboratories, Inc.
Issue: R02
Date: May 2022

PRELIMINARY
SUBJECT TO CHANGE

Statement

Information in this Manual is subject to update from time to time due to version upgrade of product or for other reasons. Unless otherwise stipulated, this Manual is only for operating guidance. All presentations, information and recommendations in this Manual shall not constitute any express or implied warranty.

Technical Support

Blonder Tongue provides customers with comprehensive technical support. Users buying products from agents of Blonder Tongue can contact their purchase sources directly for initial support.

Version Control

Date	Revision	Description
2020.12	R01	First release
2022.05	R02	Field release

Foreword

Related Manuals

CMTS Edge 16/32/32P Series CLI Manual

Content Introduction

Before installing this device and during the installation, please read this Manual carefully to avoid possible device damage and personal injury. This Manual contains the following chapters:

Chapter 1: Product Introduction.

Chapter 2: Access to CMTS Device introduces access to the CMTS by local console, remote session, etc.

Chapter 3: Command Line and Interface Views describes different user views of the system, command line classification and features of command line operation, etc.

Chapter 4: Basic Operations of the System describes the general operation of the CMTS including terminal services, network interface management, AAA configuration and zero touch functions.

Chapter 5: System Maintenance and Management introduces the configuration parameters for CMTS DOCSIS configuration management, log configuration management and product upgrades.

Chapter 6: VLAN Configuration Management describes the use and configuration of Layer-2 VLAN's and Subnet VLANs (Layer-3).

Chapter 7: DHCP Functions describes how to create bundles, perform DHCP service configuration, keyword configuration of Option60 device identification and DHCP information option82.1 circuit-ID.

Chapter 8: DHCPv6 Functions describes how to create bundles, DHCPv6 server configurations, keyword configuration of Option vendor class identification device and the DHCP information option circuit-prefix.

Chapter 9: Local Provisioning Management describes enabling/disabling Local Provisioning, uploading CM configuration files, configuring the DHCP Address Pool for Local Provisioning, IP Segment Exclusion for DHCP Address Pool, etc..

Chapter 10: TFTP proxy covers the prevention of network attacks using CMTS TFTP proxy.

Chapter 11: Channel RF Management describes basic configuration of upstream/ downstream channels, channel quality management and spectrum function and RCC template configuration.

Chapter 12: CMTS DOCSIS Configuration Management describes the configuration of upstream scheduling parameters, the configuration of MDD message sendingtime interval, the configuration of CM for downstream multicast message forwarding, the configuration ofCMTS shared key, the configuration of piggyback function, the configuration of UDC function, the configuration of CM IP initialization mode and the initialization of ranging interval.

Chapter 13: Terminal Management describes basic management of Cable Modem, Cable Modem QoS management, Cable Modem Remote Query management, CPE management, CM-based downstream frequency shift and change downstream frequency of CM by MAC.

Chapter 14: Load-Balance Management describes management and operating mode of load balancing, management of restricted load-balance groups, and management of forced load balance, etc.

Chapter 15: Channels Bonding describes bonding group function of ProvAttrMask for configuring a single channel, and Configuration of voice flow default AttrMask. **THESE ARE DEPRECATED PRACTICES AND ARE ONLY DISCUSSED FOR LEGACY HISTORICAL PURPOSES OR UNIQUE SITUATIONS – BONDING IS AUTOMATICALLY PERFORMED BY THE CMTS AND HAS BECOME THE DEFACTO STANDARD BONDING PRACTICE.**

Chapter 16: Admission Control describeS admission control principles, admission control switch, the bandwidth threshold parameters for admission control and the alarm threshold for admission control.

Chapter 17: ACL Configuration Management describes ACL matching conditions, actions of ACL sub-rule, ACL node placement and Rule for ACL application on a port.

Chapter 18: Network Security Management describes the blacklist/whitelist configuration, IP firewall and Source Address Verification (SAV) configuration management, etc.

Chapter 19: CM Multicast Authorization Management describes how to enable multicast authorization, the multicast authorization file, the multicast authorization default action and the multicast authorization rule.

Target Readers

This Manual is applicable to the following readers - Network administrators and system maintenance personnel.

Conventions in the Manual

1. Conventions on Command Line Format

Format	Meaning
Bold	Keywords in the command line (the part to be typed in and remaining unchanged in the command line) shall be prepared in bold font.
Italics	Command line parameters (the part to be replaced with actual values in the command line) shall be prepared in italics.
[ ]	Those in [ ] are optional.
(x | y | ...)	Means selecting one from two or more options.
[x | y|…]	Means selecting one or none from two or more options.
<x-y>	Means selecting one from x to y.
$	Means the notes.

2. Conventions on Keyboard Operation

Format	Meaning
Characters in angle brackets	Refer to the key name. For example, <Enter>, <Tab>, <Backspace>, <a>, <?> etc. refer to Enter, Tab, Backspace, lowercase letter “a”, and “?” respectively.
<Key 1 + Key 2>	<Key 1 + Key 2> refers to pressing key 1 and key 2 on the keyboard at the same time. For example, <Ctrl + Alt + A> refers to pressing "Ctrl", "Alt" and "A" keys at the same time.
< Key 1, Key 2>	< Key 1, Key 2> refers to pressing Key 1 first on the keyboard, releasing, and then pressing Key 2; for instance, <Alt, F> refers to pressing <Alt> key first, releasing, and then pressing <F> key.

3. Signs

This Manual also uses a variety of eye-catching signs to indicate what should be paid special attention to during the operation. The significance of such signs is as follows:

Danger — Danger indicates that the described activity or situation may result in serious personal injury or death; for example, high voltage or electric shock hazards.

Warning — Warning indicates that the described activity or situation may, or will, cause equipment damage or serious performance problems.

Note — A note provides information that is, or may be, of special interest.

NOTE: Please reach out to Blonder Tongue if you observe any content within this Manual that does not sufficiently conform with the actual product operation. Due to constant update and improvement of product and technology there may be discrepancies. For information on product updates, please refer to http://blondertongue.com.

Table of Contents

Figures

Tables

Chapter 1 Product Introduction

1.1 Overview

The solution of distributed R-CCAP access network for BT is mainly composed of RC9000 series CMTS Controller, CC8800 series CMTS and NM3000 network element management system. Distributed R-CCAP accessnetwork solution can provide powerful DOCSIS, EQAM, SDV, VoIP functions without changing the original network. BT can fully support future coaxial all-IP solutions.

CC8800 series CMTS is a L2 DOCSIS coaxial access device. It is usually installed in FTTB or FTTC optical nodes. It conforms to DOCSIS 2.0/3.0/3.1 and C-DOCSIS 1.0. It can simultaneously access DOCSIS 2.0/3.0/3.1 CM. CC8800 series CMTS supports the management and configuration based on SNMP, Web and CLI, and has a supporting mobile network management APP, supporting Android and iOS.

Detailed hardware specifications and performance indicators of CC8800 series CMTS can be found in the product specifications.

Dingpoint Video NM3000 Series EMS is a B/S architecture network element level network management system, which supports the management and maintenance of RC9000 Series CMTS Controller, CC8800 Series CMTS, CM and CPE terminals.

1.2 Product Introduction

Full spectrum full service support

- CC8800 Series CMTS is an end-to-end solution that can effectively save optical fiber resources.
- CC8800 series CMTS supports DOCSIS, EQAM and PacketetCable/PCMM, which can satisfy customers'full-service networking applications.
- CC8800 series CMTS fully meets the needs of future coaxial all-IP services, making coaxial access schemes fully competitive with optical access.

High performance, high cost performance

- High Bandwidth Access: Gigabit Access Equipment to Support Gigabit Access
- Compared with the traditional I-CMTS/M-CMTS application, it can reduce the occupancy of spectrum resources, improve the efficiency of spectrum utilization and improve the signal quality.
- Compared with the 16-frequency equipment of the previous generation of C-DOCSIS, the overall performance has been greatly improved and the cost-effective ratio is very high.
- Fully meet the needs of the next 5 to 10 years.
- Support DOCSIS service flow, PacketCable/PCMM and EQAM functions, support Internet, voice, video and

other multi-service applications

Save investment and evolve step by step

- Compatible with existing DOCSIS provisioning system, compatible with existing DOCSIS 2.0/3.0CM, effectively saving front-end and client investment
- Initially, as a large capacity DOCSIS 3.0 equipment, the subsequent smooth evolution to DOCSIS 3.1.
- Compared with traditional I-CMTS/M-CMTS, CAPEX is significantly reduced.
- Significantly reduce the demand for front-end room space and power supply resources
- Supporting passive splitting network access, saving front-end to optical node cable resource occupancy

Reliable engineering design

- Dust-proof and waterproof equipment
- Reverse HPF filter design to effectively filter low-frequency noise and improve signal-to-noise ratio
- Industrial grade temperature design for installation and application in cold and hot areas
- Supporting multiple installation modes to meet diverse installation requirements

Convenient management and maintenance

- Supporting distributed R-CCAP system and unified management of RC9000 series CMTS Controller
- Support IPDR, support network information collection, facilitate customer analysis of user behavior
- Support CLI, stand-alone web, EMS (NM3000), mobile APP and other management and maintenance methods
- Supporting reverse background noise spectrum monitoring, providing real-time, average, minimum and maximum preservation curves of noise spectrum through NM3000, and supporting historical curve display
- Support PNM active network operation and maintenance, find network problems ahead of time, further reduce network failure rate and enhance user experience.

Chapter 2 Accessing the CMTS

CMTS device supports local and remote logon configuration by users, which can be achieved by the following ways:

2.1 Access Via the Physical Port

2.1.1 Achieve Local Logon via Console port

Terminal (a PC in this example) will be connected to Console port on the of CMTS device via Console cable. User access the device through the Console port, to realize the management and configuration of the device.

Foreground Task

- To prepare the Console communication cable.
- PC terminal ready terminal emulation software.

Note:

If the terminal simulation software PC used onboard systems (super terminal such as a Windows XP system), it is not necessary to be prepared. If the system is not with terminal emulation software, please prepare to third party terminal emulation software, and the method of use please refer to the software using a guide or online help.

Process of Configuration

First use the terminal emulation software through the Console port logging device, and then complete the basic device configuration.

The Default Configuration

Parameter requirements: baud rate: 115200; data bit: 8; parity verification: None; Flow control: None; stop bit: 1.

Procedure

Step 1 To connect the cables.

1. connect DB-9 jack plug of Console cable to the serial port of PC or terminal with CMTS to be configured.
2. connect RJ-45 end of Console cable to the Console port of CMTS.

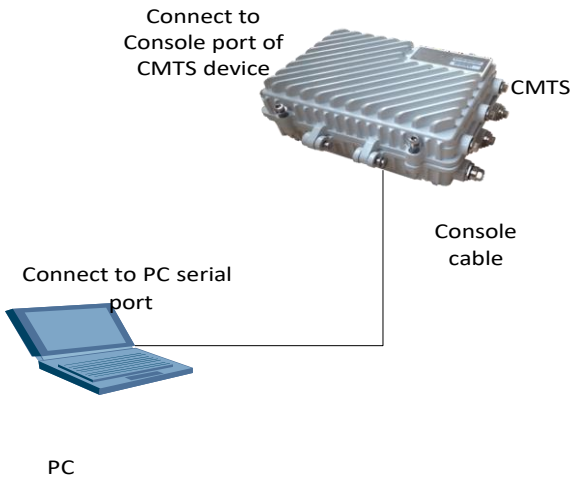

Figure 2-1 Connection to CMTS Console Port

Step 2 Open terminal emulation software, in the PC on the new connection, set up to connect the interface and communication parameters.

Note:

Because the PC end there may be multiple connection interfaces, here is the need to select the interface connecting the Console cable. In general, the selected interface is COM1.

If you modify the serial communication device parameter value, need serial communication parameter replacement communication parameters and device at the PC end of the value consensus, reconnect.

Step 3 Press the Enter key, until the system appears as shown below, prompts the user to enter a user name and password validation. Device for admin the default user name, password for admin. (the following display information is only schematic)

When CMTS device is powered on and starts, the following information output can be seen on the configuration terminal:

```
username:
```

The appearance of the above prompt indicates that the automatic startup of CMTS device finishes, and you will be required to enter the username and password. Both the default username and password are “admin”.

After the password is entered, the terminal shield will display as follows. Users can start CMTS configuration.

```
User Access Verification
Username: admin
Password: ***** BT>
Vty connection is timed out.
```

2.1.2 Access the Device Via MGMT Port

Terminal (a PC in this example) will be connected to MGMT port (out-band management port) on the CMTS device via communication cable. User access the device through the MGMT port (out-band management port), to realize the management and configuration of the device.

Foreground Task

- To prepare the communication cable.
- PC terminal ready terminal emulation software.

Note:

If the terminal simulation software PC used onboard systems (super terminal such as a Windows XP system), it is not necessary to be prepared. If the system is not with terminal emulation software, please prepare to third party terminal emulation software, and the method of use please refer to the software using a guide or online help.

Process of Configuration

First use the terminal emulation software through the MGMT port (out-band management port) logging device, and then complete the basic device configuration.

The Default Configuration

The default configuration: 192.168.0.10.

Procedure

Step 1 Connect one of the two RJ-45 ends of the crossover network cable to the MGMT port (out-band management port) of CMTS device, and another end to the network port of PC.

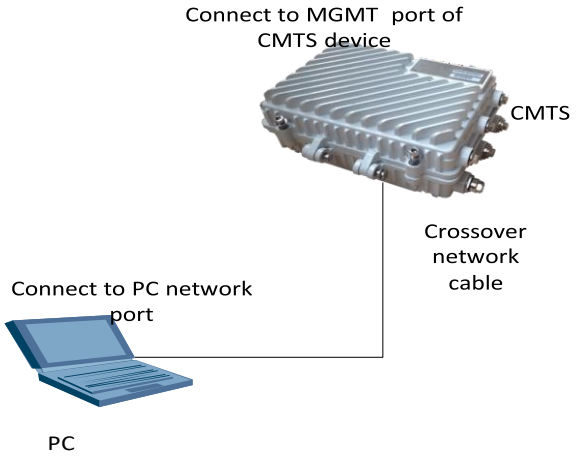

Figure 2-2 Connection to MGMT Port on CMTS Device

Step 2 Open a terminal emulation software in the PC, set the IP address of PC and the MGMT port (out-band management port) IP address consistent, make the new connection, set the IP address and the MGMT port (out-band management port) IP address consistent.

Note:

If this is the first time to use the MGMT port (out-band management port) IP address access the device, choose the default address; if the modifications to the MGMT port (out-band management port), please choose the modified IP address access device.

Step 3 Press the Enter key, until the system appears as shown below, prompts the user to enter a user name and password validation. Device for admin the default user name, password for admin. (the following display information is only schematic)

When CMTS device is powered on and starts, the following information output can be seen on the configuration terminal:

```
**************************************************************
*                                                            *
*  BT software system.                                       *
*  Copyright 2010-2015, All rights Reserved by BT.           *
*                                                            *
**************************************************************
User Access Verification
username:
```

The appearance of the above prompt indicates that the automatic startup of CMTS device finishes, and you will be required to enter the username and password. Both the default username and password are “admin”.

After the password is entered, the terminal shield will display as follows. Users can start CMTS configuration.

```
User Access Verification
Username: admin
Password: ***** BT>
Vty connection is timed out.
```

2.1.3 Access the Device Via Uplink Port

Terminal (a PC in this example) will be connected to uplink port (in-band uplink port) on the CMTS device via communication cable. User access the device through the uplink port (in-band uplink port), to realize the management and configuration of the device.

Foreground Task

- To prepare the communication cable.
- PC terminal ready terminal emulation software.

Note:

If the terminal simulation software PC used onboard systems (super terminal such as a Windows XP system), it is not necessary to be prepared. If the system is not with terminal emulation software, please prepare to third party terminal emulation software, and the method of use please refer to the software using a guide or online help.

Process of Configuration

First use the terminal emulation software through the uplink port (in-band uplink port) logging device, and then complete the basic device configuration.

The Default Configuration

The default configuration: 192.168.168.100. It needs to be configured.

Procedure

Step 1 Connect one of the two RJ-45 ends of the crossover network cable to the uplink port (in-band uplink port) of CMTS device, and another end to the network port of PC.

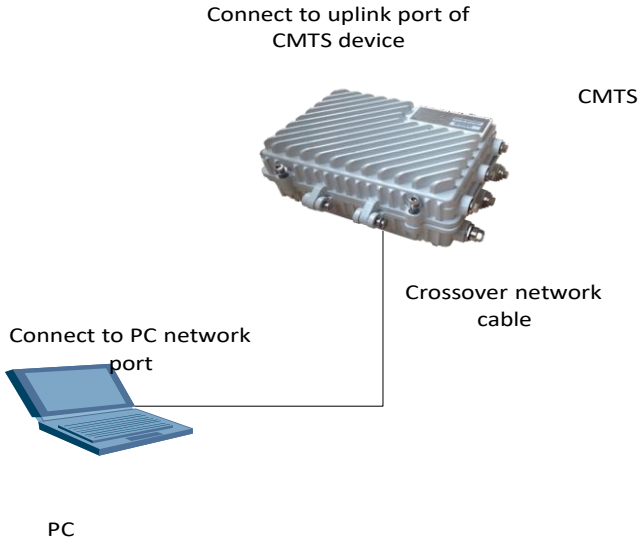

Figure 2-3 Connection to Uplink Port on CMTS Device

Step 2 Open a terminal emulation software in the PC, set the IP address of PC and the MGMT port (in-band uplink port) IP address consistent, make the new connection, set the IP address and the uplink port (in-band uplink port) IP address consistent.

Note:

Before the first use of the uplink port IP address access the device, it need to configure it.

Step 3 Press the Enter key, until the system appears as shown below, prompts the user to enter a user name and password validation. Device for admin the default user name, password for admin. (the following display information is only schematic)

When CMTS device is powered on and starts, the following information output can be seen on the configuration terminal:

```
**************************************************************
*                                                            *
*  BT software system.                                       *
*  Copyright 2010-2015, All rights Reserved by BT.           *
*                                                            *
**************************************************************
User Access Verification
username:
```

The appearance of the above prompt indicates that the automatic startup of CMTS device finishes, and you will be required to enter the username and password. Both the default username and password are “admin”.

After the password is entered, the terminal shield will display as follows. Users can start CMTS configuration.

```
User Access Verification
```

```
Username: admin
Password: *****
BT>
Vty connection is timed out.
```

2.2 Access Via the Software

2.2.1 Access the Device Via Telnet

The PC for remote login need to connect to the network, reachable of the MGMT port or uplink port of the device.

Foreground Task

- To prepare the communication cable.
- PC terminal ready terminal emulation software.

Note:

If the terminal simulation software PC used onboard systems (super terminal such as a Windows XP system), it is not necessary to be prepared. If the system is not with terminal emulation software, please prepare to third party terminal emulation software, and the method of use please refer to the software using a guide or online help.

Process of Configuration

The two RJ-45 cross network cable end, one end connected to the nearest switch or network information socket, the other end is connected to the computer network port.

The Default Configuration

None.

Procedure

Step 1 The two RJ-45 cross network cable end, one end connected to the nearest switch or network information socket, the other end is connected to the computer network port.

Step 2 Open terminal emulation software, in the PC on the new connection, set the IP address the device IP address consistent.

Step 3 Press the Enter key, until the system appears as shown below, prompts the user to enter a user name and password validation. Device for admin the default user name, password for admin. (the following display information is only schematic)

When CMTS device is powered on and starts, the following information output can be seen on the configuration terminal:

```
**************************************************************
*                                                            *
*  BT software system.                                       *
*  Copyright 2010-2015, All rights Reserved by BT.           *
*                                                            *
**************************************************************
User Access Verification
username:
```

The appearance of the above prompt indicates that the automatic startup of CMTS device finishes, and you will be required to enter the username and password. Both the default username and password are “admin”.

After the password is entered, the terminal shield will display as follows. Users can start CMTS configuration.

```
User Access Verification
Username: admin
Password: ***** BT>
Vty connection is timed out.
```

2.2.2 SSH Authentication-based Access

CMTS device supports SSH access. You can access directly via SSH without any configuration on the device. In case of SSH authentication, the port number is 22, and hostname can be filled with available CMTS address.

Foreground Task

- To prepare the communication cable.
- PC terminal ready terminal emulation software.

Note:

If the terminal simulation software PC used onboard systems (super terminal such as a Windows XP system), it is not necessary to be prepared. If the system is not with terminal emulation software, please prepare to third party terminal emulation software, and the method of use please refer to the software using a guide or online help.

Process of Configuration

The two RJ-45 cross network cable end, one end connected to the nearest switch or network information socket, the other end is connected to the computer network port.

The Default Configuration

The port number is 22.

Procedure

Step 1 The two RJ-45 cross network cable end, one end connected to the nearest switch or network information socket, the other end is connected to the computer network port.

Step 2 Open a terminal emulation software, in the PC on the new connection, select the SSH login, The port number: 22, SSH username: admin or the other name which was configured.

Step 3 Press the Enter key, until the system appears as shown below, prompts the user to enter a user name and password validation. Device for admin the default user name, password for admin. (the following display information is only schematic)

When CMTS device is powered on and starts, the following information output can be seen on the configuration terminal:

```
************************************************************
*                                                          *
*  BT software system.                                     *
*  Copyright 2010-2015, All rights Reserved by BT. *
*                                                          *
************************************************************
```

The appearance of the above prompt indicates that the automatic startup of CMTS device finishes.

2.2.3 Access RSH

CMTS support rsh access function, generally only one command can be executed during a single connection to the device. The access needs to be configured on device.

Foreground Task

- To prepare the communication cable.
- PC terminal ready terminal emulation software.

Note:

Relatively rare the rsh client software in Windows, so user can use rsh in Linux NetKit tool.

Process of Configuration

User may need another connection method to achieve these steps.

Step 1 Created CMTS-local user on the CMTS.

Step 2 Open rsh service on the CMTS. The command is"**`ip rcmd enable`**", refer to CLI manual for more details about this command.

Step 3 Configure rsh user association on CMTS. Example, the CMTS user name is admin, the PC IP is 192.168.1.111, the PC login username is root, then the configure command is "**`ip rcmd remote-host admin 192.168.1.111 root enable`**", refer to CLI manual for more details about this command.

The Default Configuration

Port: 514.

Procedure

Step 1 The two RJ-45 cross network cable end, one end connected to the nearest switch or network information socket, the other end is connected to the computer network port.

Step 2 Use the user name "root" login PC, then use the command "**`rsh CMTS-IP -l admin command`**" on Windows operating systems or use the command "**`rsh -l admin CMTS-IP command`**" on Linux operating systems.

Step 3 According to different command in step 2, user can view different show.

2.2.4 Access via Web

For convenient use by the customers, the system offers a special access via web. You can enter IP of the CMTS on the browser, and start the logon access and parameter configurations directly on the screen. For specific configurations, refer to **WebGUI.**

WEBGUI supports HTTP and HTTPS protocols. by default, the HTTP access enabled. When the HTTP access disabled, the connection through the HTTP protocol will automatically be redirected to HTTPS. If you want to use the HTTP protocol, please enter the "**`webgui http-access`**" command to enable HTTP.

2.3 Access Security

In order to enhance access security, the device has malicious user protection and view the access failure function.

2.3.1 Malicious User Protection

To enhance access security, the device has a lock function. If the login failure numble achieved max try numble, the device will block user login until the lock time expired. To use this feature, please refer to CLI manual for "**`user try-num`** *`try-number`*", "**`user lock-time`** *`lock-time`*" and "**`user ext-lock-time`** *`ext-lock-time`*".

Note:

Changing try number will reset login failure number and unlock all users that have been locked.

The maximum total locking time is 24 hours, which will be reset after successful login. This function can only be used in local authentication. When AAA is enabled, this feature is automatically disabled.

Example: Set try-num to 3 and use default configuration for other parameters.

Step 1 Use the **user try-num** command to set the number of login failures to 3

```
BT(config)# user try-num 3
BT(config)# show running-config | include try-num
user try-num 3
```

Step 2 Log out using the quit command

```
BT(config)# quit
```

Step 3 Log in three times with an incorrect password

```
User Access Verification
Username: admin
Password: ******
Password:
% Bad passwords, too many failures!
```

Step 4 Re-use the correct password to login, unable to login successfully.

```
User Access Verification
Username: admin
Password: *****
% The user admin have been locked,please try again after 283
seconds!
Password:
```

2.3.2 View the Access Failure

Every access to the device will generate a event. If the login failed,the device will record failure number. Users can query this counter by using "**show terminal user login failure**" command.

```
BT(config)# show terminal user login failure
-------------------------------------------------------------------------------------------
User fail login information:
-------------------------------------------------------------------------------------------
Access Type IP Address    Failure Count Latest Entered User Name
Time
telnet       10.10.29.206  3                admin
1970-01-01,05:28:27
-------------------------------------------------------------------------------------------
Total record(s) number: 1
```

Chapter 3 Command Line and Interface Views

3.1 Overview of Command Line Interface

CMTS device provides users with a series of configuration commands and command line interfaces to facilitate users to configure and manage CMTS via command lines. The command line interfaces have the following features:

- Configure hierarchy command protection to ensure that the unauthorized users can not invade the system.
- Users can type in "?" at any time to get help information.
- Provide History function for viewing the history commands.
- The command line interpreter adopts the method of inexact matching to search for command line keyword. Users can just enter the conflict-free keyword for interpretation. For command "**`interface`**", just enter "**`interf`**".

3.2 Command Line Hierarchy and Views

3.2.1 Command Line Hierarchy

CMTS device's command lines adopt the hierarchy protection mode to prevent unauthorized users from illegal invasion.

The command lines are classified into three levels: access level, system level and administrator level, with descriptions as follows:

- Access level: the commands are used to view the help information on UI, set the terminal control parameters, view the system configuration, etc., and associate with the "view" view.
- System level: the commands are used for file operation, network diagnosis, system upgrade, device reboot, etc. and associate with the "enable" view.
- Administrator level: the commands are related to the global system configuration and the configuration of interfaces and part of services, and associate with the "config" view, and the interface views of ad, bundle, cmts and line, etc..

The users logging in the system can be classified into two levels, corresponding to the command levels. The users of access level can use the commands of access level, and privileged users can use all commands. Levels of users logging on OLT can be switched by entering the password for corresponding view, which can be set as demand.

Note:

The ex-factory default “admin” user of the device is the privileged user.

3.2.2 Command Line Views

The command line views are achieved based on different configuration requirements, and are related and different from each other. For example, log on successfully with username and password to enter the “view” view, which can only achieve the simple function of viewing the running status and statistics information. Further type in command “**enable**” and it’s password (by default, this password is unavailable, which can be configured by using “enable password”) to enter the enable view, in which typing in command “**configure terminal**” to enter the config view, in which typing in different commands to enter corresponding views.

```
view
  |___enable
      |___config
          |___acl
          |___bundle
          |___cmts
          |___line
          |___syslog
          |___vlan
          |___uplink
          |___bonding-group
          |___ip dhcp-pool
          |___ip-dhcpv6-pool
          |___mauth
          |___sav
          |___eqam template
          |___client-class
```

Table 3-1 List of Command Line Views

Command line mode	Function	Prompt	Command for entering	Command for exit
“view” view	View running	BT>	Establish a connection with	**exit:** disconnect

Command line mode	Function	Prompt	Command for entering	Command for exit
	record and simple help information of CMTS		CMTS, type in the username and password for login and then enter the view	with CMTS **quit:** disconnect with CMTS
enable view	View running information of CMTS, and command for version upgrade	BT#	Type in "**enable**" in the "view" view	**exit:** return to the "view" view **quit:** disconnect with CMTS
config view	Configure global parameters	BT(config)#	Type in "**configure terminal**" in the enable view	**exit:** return to the enable view **quit:** disconnect with CMTS
acl view	Configure and view ACL information	BT(config-if-acl- 1)#	Type in "**acl** *acl-id*" in the enable view	**exit:** return to the enable view **quit:** disconnect with CMTS
bundle view	Configure and view DHCP Relay parameters	BT(config-if-bundle(1)#	Type in "**interface bundle** *bundle-id*" in the config view	**exit:** return to the config view (i.e., global view) **quit:** disconnect with CMTS
cmts view	Configure CMTS parameters	BT(config-if-cmts-1)#	Type in "**interface cmts 1**" in the config view or CC configuration view	**exit:** return to the config view (i.e., global view) **quit:** disconnect with CMTS
line view	Configure and view vty information	BT(config-line)#	Type in "**line vty**" in the config view or CC configuration view	**exit:** return to the config view (i.e., global view) **quit:** disconnect with CMTS
Syslog view	Configure and view syslog information	BT(config-syslog)#	Type in "**syslog**" in the config view (i.e. global view)	**exit:** return to the config view (i.e., global view) **quit:** disconnect with CMTS
vlan view	Configure and view VLAN information	BT(config-if-vlan1)#	Type in "**interface vlanif** *vlan-id*" in the config view (i.e. global view)	**exit:** return to the config view (i.e., global view) **quit:** disconnect with CMTS

Command line mode	Function	Prompt	Command for entering	Command for exit
uplink view	Configure and view syslog information	`BT(config-if-uplink1)#`	Type in "**interface uplink** *uplink-id*" in the config view (i.e. global view)	**exit:** return to the config view (i.e., global view) **quit:** disconnect with CMTS
bonding-group view	Configure and view bonding group information	`BT(config-if-us- bonding-group1)#` or `BT(config-if-ds- bonding-group1)#`	Type in "**interface us bonding-group** *bdg-id*" or "**interface ds bonding-group** *bdg-id*" in the config view (i.e. global view)	**exit:** return to the config view (i.e., global view) **quit:** disconnect with CMTS
ip dhcp-pool view	Configure and view IP dhcp-pool information	`BT(ip-dhcp-pool)#` or `BT(ipv 6-dhcp-pool)#`	Type in "**ip dhcp-pool**" or "**ipv6 dhcp-pool**" in the config view (i.e. global view)	**exit:** return to the config view (i.e., global view) **quit:** disconnect with CMTS
ip-dhcpv6-pool view	Configure and view Ipv6 address pool information.	`BT(ipv6-dhcp-pool)#`	Type in "**ipv6 dhcp-pool**" in the config view (i.e. global view)	**exit:** return to the config view (i.e., global view) **quit:** disconnect with CMTS
mauth view	Configure and view multicast authorization information.	`BT(config-mauth)#`	Type in "**cable multicast authorization profile** *profile-name*" in the config view (i.e. global view)	**exit:** return to the config view (i.e., global view) **quit:** disconnect with CMTS
sav view	Configure and view SAV information	`BT(config-sav)#`	Type in "**cable source verify group** *group-name*" in the config view (i.e. global view)	**exit:** return to the config view (i.e., global view) **quit:** disconnect with CMTS
eqam template view	Configure and view EQAM template information	`BT(config-if-eqam-template-1)#`	Type in "**interface eqam template 1**" in the config view (i.e. global view)	**exit:** return to the config view (i.e., global view) **quit:** disconnect with CMTS
client-class view	Configure and view client-class information	`BT(client-class-1)#`	Type in "**client-class** *class-id*" in the config view (i.e. global view)	**exit:** return to the config view (i.e., global view)

Command line mode	Function	Prompt	Command for entering	Command for exit
				quit: disconnect with CMTS

3.3 Command Line Features

3.3.1 Command Line Online Help

The command line interface provides two kinds of online help: complete help and partial help. Users can acquire relevant help information required for device configuration through online help.

- Complete Help
  a. In any view, type <?>, and the user terminal screen will display the first keyword and a simple description of the current configurable command in that view.
  b. In any view, type **list**, and all commands in that view will be displayed on the user terminal screen.
  c. Type in a command, followed by a space and <?>. If a keyword is for the position, all keywords and their simple descriptions will appear on the screen of user terminal.
  d. Type in a command, followed by a space and <?>. If a parameter is for the position, descriptions of related parameters will appear on the screen of user terminal.
- Partial Help
  a. Type in a string, followed by <?>, and all commands starting with the string will appear on the screen of user terminal.
  b. Type in a command, followed by a string and <?>, and all keywords of the commands starting with the string will appear on the screen of user terminal.
  c. Type in the first few letters of a keyword and press <Tab> key. If the keyword starting with the entered letters is unique, the complete keyword will appear on the screen of user terminal. If the keyword matching with the entered letters is not unique, the keywords matching with the letters will appear on the terminal screen in turn.
  d. <Cr> standards for no parameter for the position. Press <Enter> directly to execute.

3.3.2 Features of Command Line Display

The command line interfaces provide the display features as follows:

- If the information to be displayed exceeds a screen, the function of pause is available, and three options are available for users, as shown in follows.

Table 3-2 List of Display Functions

Key or command	Function
When stopping the display, type in <Ctrl + C>	Stop the display and command execution
When stopping the display, type in q	Stop the display and command execution
When pausing the display, press the <space> key	Continue displaying the next screen of information
When pausing the display, press the <Enter> key	Continue displaying the next line of information

- When you want to search for configuration information containing certain keywords, this task can help screen and output relevant contents according to the screening matching condition. There are three options for screening-based display:
  - begin: select to start display from the first line matching the screening condition.
  - include: display all information matching the screening condition.
  - exclude: display all information not matching the screening condition.

Procedure

Step 1 Display all information matching the screening condition by using the command "**| include**".

Example

Screen out the entries having the show running-config information containing system.

```
BT(config)# show running-config | include system
 system  name  "cmts-test"
 system location "Hong Kong"
 system contact "test@test.com"
```

3.3.3 Command Line Error Message

All commands entered by users will be correctly executed if they pass the syntax check. Otherwise error message will be reported to the users. Common error messages are shown in table below.

Table 3-3 List of common error messages of command line

Error message in English	Cause of error
% Unknown command.	1. Command is not found. 2. Keyword is not found. 3. Wrong parameter type 4. Too many parameters are entered.
%Command incomplete.	Incomplete command is entered.
%Ambiguous command.	Ambiguous command is entered.
% Invalid parameter.	Parameter value is out of the range.

3.3.4 Features of Command Line Editing

The command line interface provides the basic function of command editing and supports multi-line editing. The maximum length of each command is 511 characters(including keywords, parameters and blank spaces), as shown in table below.

Table 3-4 Editing Function

Key	Function
Common keys	If the editing buffer is not full, insert in the position of current cursor and move the cursor rightward.
Backspace key	Delete a character ahead of the position of current cursor, and the cursor is moved backward.
Left cursor key ← or <Ctrl + B>	Move the cursor leftward for a character
Right cursor key → or <Ctrl + F>	Move the cursor rightward for a character
Up cursor key ↑ or <Ctrl + P>, down cursor key ↓ or <Ctrl + N>	Display the history command
Tab key	Press Tab key after entering an incomplete keyword, and the system will automatically perform the partial help: if the keyword matching is unique, the system will use this complete keyword to replace the original input; if the keyword matching the entered letters is not unique, keywords matching the letters will be displayed in turn on the terminal screen in line wrap; if the parameter of a command word does not match, the system will make no change, and display the original input in line wrap.

Chapter 4 Basic Operation of the System

4.1 Terminal Service

Describe some operations frequently used for management and maintenance of CMTS via CLI, including setting the system name, setting the terminal timeout and screening the display.

4.1.1 Configure the System Time

Configure the system time and time zone of the device through this task.

Context

- Format of system time: year-month-day, hour:minute:second;
- Default configuration of the system time: 1970-01-01, 00:00:00 at the time of startup;
- The system time takes effect immediately after it is set.

Procedure

Step 1 Configure the system time by using the command "**clock set**";

Step 2 Query the system time and time zone by using the command "**show sys-date**".

Example

Set the system time of the device s 2014-10-11, 8:30:30.

```
BT(config)# clock set 2014-10-11 8:30:30
BT(config)# show sys-date System
time: 2014-10-11 08:30:31 Sat
Timezone: GMT+08:00
```

4.1.2 Configure the System Time Zone

Configure the system time and time zone of the device through this task.

Context

- The time zone information of the CMTS device is to record the time zone for local geographical location of the device, relative UTC (0 time zone) offset time - positive number for eastern hemisphere, negative number for western hemisphere, and the greatest deviation is (-13)-14 hours, generally speaking, the minute offset of the timezone is 0 minute, 30 minutes or 45 minutes;
- Default configuration of the system time zone: GMT +00:00., Time Zone 0;
- The system time takes effect immediately after it is set.

Procedure

Step 1 Configure the system time zone by using the command "**clock timezone**".

Step 2 Query the system time and time zone by using the command "**show sys-date**".

Example

Set the system time zone of the device as East Zone 9.

```
BT(config)# clock timezone 9
BT(config)# show sys-date System
time: 2014-10-11 08:30:31 Sat
Timezone: GMT+09:00
```

4.1.3 Configure the System Name

Configure the system name of the device through this task when you need to distinguish between different CMTS devices by system name.

Context

- When there's any space in the parameter, you're required to mark all contents of the parameter with double quotation marks;
- The system name takes effect immediately after it is set.

Procedure

Step 1 Configure the system name by using the command "**system name**".

Step 2 Query the system name by using the command "**show running-config**".

Example

Set the system name of the device as SystemName1.

```
BT(config-if-cmts-1)# system name SystemName1
BT(config-if-cmts-1)# show running-config | include system
 system name "SystemName1"
```

4.1.4 Configure the System Location

Configure location information of the device through this task when you need to mark location of the device.

Context

- The default configuration of contact information of the system is null;
- When there's any space in the parameter, you're required to mark all contents of the parameter with

double quotation marks;

- The system location information takes effect immediately after it is set.

Procedure

Step 1 Configure local address of the device by using the command "**system location**".

Step 2 Query the address of the device by using the command "**show running-config**".

Example

Set local address of the device as Hong Kong.

```
BT(config-if-cmts-1)# system location "Hong Kong"
BT(config-if-cmts-1)# show running-config | include Hong Kong
 system location "Hong Kong"
```

4.1.5 Configure the Contact Information

Configure system contact information for maintenance of the device through this task, including E-mail, phone number and address, when you need to mark the contact information of the device.

Context

- The default of contact information is null;
- When there's any space in the parameter, you're required to mark all contents of the parameter with double quotation marks;
- The system contact information takes effect immediately after it is set.

Procedure

Step 1 Configure the contact information of the device by using the command "**system contact**".

Step 2 Query the system contact information by using the command "**show running-config**".

Example

Set the contact information of the device as admin@mail.com.

```
BT(config-if-cmts-1)# system contact admin@mail.com
BT(config-if-cmts-1)# show running-config | include contact
 system contact "admin@mail.com"
```

4.1.6 Configure the Terminal Timeout for Exit

Configure the terminal timeout for exit through this task. After configuring the terminal timeout for exit, if no input is available on the terminal within the set period, the terminal will exit automatically.

Context

By default, the terminal will be forced to exit the system if no input is available on the terminal within 10 minutes;

The terminal timeout set for telnet and ssh is applicable only to the connection for this time, and will not affect the timeout of other telnet and ssh.

Procedure

Step 1 Configure the terminal timeout for exit by using the command "**exec-timeout**".

Step 2 Query the terminal timeout for exit by using the command "**show vty**".

Example

Set the terminal timeout for exit as 60 minutes.

```
BT(config-line)# exec-timeout 60
BT(config-line)# show vty
VTY width:      177
VTY height:     57
VTY timeout:    60 min
Monitor status: enabled
```

Related Operations

Table 4-1 Related Operations for Configuring the Terminal Timeout for Exit

Operation	Command	Remarks
Restore the default terminal timeout for exit	**no exec-timeout**	The default terminal timeout for exit is 10 minutes

4.2 Network Interface Management

4.2.1 Configure the Network Interface

CMTS provides the network management interface, takes SNMP (Simple Network Management Protocol) for communication with the network management system, and supports WEB management system (hereinafter referred to as WEB), which can ensure management and maintenance against CMTS device through the network interface on CMTS. For details, refer to the **Web GUI**.

4.2.2 Configure IP Address of Out-band Management Port

Configure the out-band management port IP address (i.e., MGMT port IP address) through this task.

Context

- Out-band management interface IP address supports only one IP, which is allowed to modify but cannot be delete.
- The default out-band management interface IP address is 192.168.0.10;
- The address takes effect immediately after it is set.

Procedure

Step 1 Configure the out-band management IP address by using the command "**outband ip-address**".

Step 2 Query the out-band management IP address by using the command "**show outband-info**".

Example

Configure the out-band management IP as 192.168.100.1 and subnet mask as 255.255.255.0.

```
BT(config)# outband ip-address 192.168.100.1 255.255.255.0
BT(config)# show outband-info
Ip Address          : 192.168.100.1
Ip Mask             : 255.255.255.0
MAC Address         : 0024.683a.0003
```

4.2.3 Configure the In-band Uplink IP address

Configure the in-band network management interface IP address through this task.

Context

- CMTS device can configure the in-band uplink IP address in the config view or the vlan view: In the config view, the uplink IP address forwarding will carry no VLAN tag;In the vlan view, the uplink IP address forwarding will carry VLAN tag;
- In each view, it allows the number of IPv4: It allows to configure at most 1 primary IP address and 62 secondary IP address. it allows the number of IPv6: It supports 1 link local address and 10 global unicastaddress in each view.
- The device supports 63 IPv4 address total, in which are supported 62 secondary IPv4 address. While IPv6address, the device supports 9 link local address and 90 global unicast address total.

Procedure

Step 1 Configure the in-band network uplink primary IP address by using the command "**`ip address primary`**"; Or configure the in-band network uplink primary IP address by using the command "**`ip address secondary`**".

Step 2 Query the in-band network uplink IP address by using the command "**`show running-config`**".

Example

Configure the in-band uplink primary IP as 10.10.28.88 and subnet mask as 255.255.255.0 in the configview.

```
BT(config)# ip address 10.10.28.88 255.255.255.0 primary
BT(config)# show running-config | include ip address
ip address 10.10.28.88 255.255.255.0 primary
```

Related Operations

Table 4-2 Related Operations for Configuring In-band Network Management IP

Operation	Command	Remarks
Delete the in-band network management IP address	**no ip address**	This command can be used to delete the primary IP address and secondary IP address

4.2.4 Configure Static Routing Information

While it is not essential to do so, you may establish route information from the CMTS to other network devices through this method.

Context

- When the IP address of CMTS device and that of other devices are not in the same subnet, this task is used to establish communication between them to forward IP packets to the CMTS gateway.
- The system supports at most twelve (12) unique routes.
- If both the destination IP address and mask are 0.0.0.0, the configured route will be the default one. If route matching fails, the default route will be used for packet forwarding.

Procedure

Step 1 Configure the route information by using the command "**ip route-static**".

Step 2 Query current routing information of the device by using the command "**show ip routing-table**".

Example

Configure the route information, and next-hop address as 10.10.28.1.

```
BT(config)# ip route 0.0.0.0 0.0.0.0 10.10.28.1BT(config)# show
running-config | include route ip route 0.0.0.0 0.0.0.0
10.10.28.1
BT(config)# show ip routing-table
        Destination     Netmask         Nexthop       Type      Interface
        0.0.0.0         0.0.0.0         10.10.28.1    static    gigabitethernet0
        10.10.28.0      255.255.255.0   *             direct    gigabitethernet0
        192.168.168.0   255.255.255.0   *             direct    gigabitethernet0
        192.168.0.0     255.255.255.0   *             direct    fastethernet0
```

Related Operations

Table 4-3 Related Operations for Configuring the Network Management Routing

Operation	Command	Remarks
Delete the unicast static route	**no ip route**	

4.2.5 Configure Gateway Address

Context

When the CMTS device and DHCP Server in the different network, we need to specify the gateway address information, and configure the packet which destination address and the device is not in the same network forwarding to the gateway.

Procedure

Step 1 Configure the gateway address of the CMTS device by using the command "**gateway**".

Step 2 View the gateway address of the CMTS device by using the command "**show running-config**".

Example

Configure gateway address as 10.10.28.1.

```
BT(config)# ip address 10.10.28.89 255.255.255.0 primary
BT(config)# gateway 10.10.28.1
BT(config)# show running-config | include gateway
gateway 10.10.28.1
```

Related Operations

Table 4-1 Related Operations of gateway address

Operation	Command	Remarks
Delete the gateway address	**no gateway**	

4.3 AAA Configuration

4.3.1 AAA Overview

Authentication Authorization Accounting (AAA) provides the CMTS with a unified configuration framework for authenticating, authorizing, and charging users who log on to the system remotely. Here:

- Authentication refers to checking the user identity and determining whether the user is a valid user.

- Authorization refers to authorizing a user who is successfully authenticated to use specified services.
- Accounting refers to recording resource usage of users when they use network services. The recorded information serves as the basis of charging.

Currently, the system supports only authentication and authorization in the following scenarios:

- Authentication and authorization of users logging on to the CMTS:
  - Local authentication and authorization: When a user logs on to the CMTS, the entered user name and password are checked against the user information in the CMTS. If the information is consistent and authentication and authorization are successful, related permissions are granted to the user and the user is allowed to log on to the CMTS.
  - TACACS+ authentication and authorization: When a user logs on to the CMTS, the entered user name and password are sent to the TACACS+ server, and the TACACS+ server checks the user information. If the information is consistent and authentication and authorization are successful, related permissions are granted to the user through the CMTS and the user is allowed to log on to the CMTS.
  - RADIUS authentication and authorization: When a user logs on to the CMTS, the entered user name and password are sent to the RADIUS server, and the RADIUS server checks the user information. If the information is consistent and authentication and authorization are successful, related permissions are granted to the user through the CMTS and the user is allowed to log on to the CMTS.
  - None authentication and authorization: When a user logs on to the CMTS, the entered user name and password pass the authentication directly, and the user is allowed to log on to the CMTS. This type of authentication and authorization can only be used as the last authentication and authorization mode of hybrid authentication and authorization. A user who logs on to the CMTS in this mode is in user level 0 (with lowest permission).
  - Hybrid authentication and authorization: It refers to any combination of the above four authentication and authorization modes. When a user logs on to the CMTS, authentication and authorization are performed in the configured sequence. If no response is received in the current authentication and authorization mode, the next authentication and authorization mode is automatically used. Hybrid authentication and authorization will fail in the following scenarios:
    - No response is received in all authentication and authorization modes (when the none authentication and authorization mode is not configured).
    - If a failure response is received in an authentication and authorization mode, the next authentication and authorization mode is no longer used, a failure is directly returned, and the user is not allowed to log on to the system.
- Authentication before a user accesses the Enable view: If the user level is lower than the enable password level, the user must access the Enable view for authentication.

- Local authentication: The enable password entered by the user is checked against the user information in the CMTS. If the information is consistent, the user is allowed to access the Enable view.
- TACACS+ authentication: The enable password entered by the user is sent to the TACACS+ server, and the TACACS+ server checks the user information. If the information is consistent and authentication is successful, the user is allowed to access the Enable view.
- None authentication: The enable password entered by the user is not verified and the user directly accesses the Enable view. This authentication mode can only be used as the last authentication mode of hybrid authentication.
- Hybrid authentication: It refers to any combination of the above three authentication modes. Authentication is performed on the enable password entered by the user in the configured sequence. If no response is received in the first authentication mode, the next authentication mode is automatically used. If no response is received in all authentication modes (when the none authentication mode is not configured), authentication fails. Hybrid authentication will fail in the following scenarios:
  - No response is received in all authentication modes (when the none authentication mode is not configured).
  - If a failure response is received in an authentication mode, the next authentication mode is no longer used, an authentication failure is directly returned, and the user is not allowed to log on to the system.

➢ Authorization of user executed commands:

- Command local authorization: Specific permissions are configured for specific commands. When a user runs a command, the CMTS server checks the permission. If the user level is not lower than the command level, the user is allowed to run the command. If the user level is lower than the command level, the user is not allowed to run the command.
- Command TACACS+ authorization: Specific permissions are configured for specific commands. When a user runs a command, the TACACS+ server checks the permission. If the user level is not lower than the command level, the user is allowed to run the command. If the user level is lower than the command level, the user is not allowed to run the command.
- Command none authorization: A user can directly run a command without being authorized. This authorization mode can only be used as the last authorization mode in the case of hybrid authorization.
- Command hybrid authorization: It refers to any combination of the above three authorization modes. Authorization is performed on the command entered by the user in the configured sequence. If no response is received in the first authorization mode, the next authorization mode is automatically used. Hybrid authorization will fail in the following scenarios:

- No response is received in all authorization modes (when the none authentication and authorization mode is not configured).
- If a failure response is received in an authorization mode, the next authorization mode is no longer used, a failure is directly returned, and the user is not allowed to log on to the system.

4.3.2 Example of AAA Authentication

Conduct AAA authentication against the remote administrators through this task, in the following way: TACACS+ first and local authentication following. Only after passing corresponding level of authentication, can users implement corresponding maintenance and management against the device.

Networking Diagram

This task is performed to complete hybrid authentication and authorization when a remote management user logs on to the CMTS. In the hybrid authentication, TACACS+ and local authentication are performed in sequence. A user can perform maintenance and management on the CMTS only after the successful authentication and authorization.

When the user logs on to the CMTS server, the TACACS+ and local authentication and authorization are performed sequentially according to the configuration.

Before the user can access the Enable view, the TACACS+ and local authentication are performed sequentially.

Command line authorization is configured on the CMTS server. When the user run the reset command, the TACACS+ and local authorization are performed sequentially.

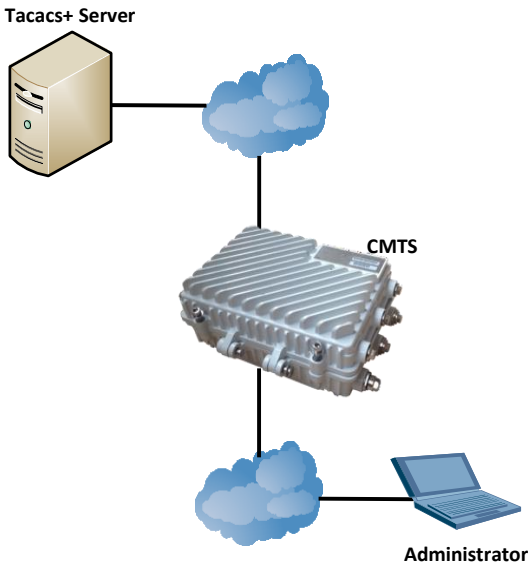

Figure 4-1 Networking Diagram for AAA Authentication

Data Planning

The data planning for the AAA authentication configuration is shown as table below.

Table 4-2 Data Planning for AAA Authentication Configuration

Item	Data
TACACS+ server	Ip address: 192.168.1.1 Encryption key: secretkey1
Local user	User1: Username: user1, password: password1, group: groupname1, level: 13 User2: Username: user1, password: password2, group: administrators, level: 15 Enable password: enablepassword1, level: 14
Log in CMTS device authentication and authorization	

Prerequisite

- Network devices and lines must be in the normal state.
- CMTS device is in normal state.
- TACACS+ server is properly configured.

Configuration flowchart

The process of AAA authentication configuration is shown as figure below.

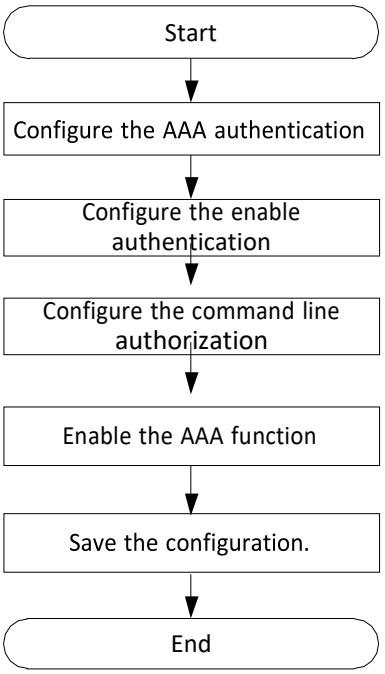

Figure 4-2 Flow of AAA Authentication Configuration

Procedure

Step 1 Configure the AAA authentication authorization mode as TACACS+ authentication first and local authentication following.

1. Configure local user group as groupname;

```
BT(config)# groupname groupname1 privilege 13 BT(config)#
username user1 password password1 BT(config)# username
user1 groupname groupname1 BT(config)# username user2
password password2 BT(config)# username user2 groupname
administratorsBT(config)# show groups
group index         : 0
group name          : administrators
group privilege     : 15
group index         : 1
group name          : default
group privilege     :  3
group index         : 2
group name          : groupname1
group privilege     : 13
show local groups: a total of 3 groups
```

2. Configure IP address and encryption key of TACACS+ server.

```
BT(config)# tacacs-server primary ip-address 192.168.1.1key
secretkey1
BT(config)# show tacacs-server
```

Type	Port	Retry	Timeout	Ip_address	Key
primary	49	1	3	192.168.1.1	secretkey1
secondary	--	--	--	--	--

3. Configure the AAA authentication mode as TACACS+ authentication first and local authentication following.

```
BT(config)#aaa authentication login default group tacacs+local
```

Step 2 Configure the enable authentication mode as TACACS+ authentication first and local authentication following.

1. Configure the password for enable at Level 15.

```
BT(config)# enable password enablepassword1 level 15Configure
```

2. the enable authentication mode as TACACS+ authentication first and local authentication following.

```
BT(config)# aaa authentication enable default grouptacacs+
local
```

Step 3 Configure the command-line authorization mode as TACACS+ authorization.

1. Add Level-15 command line “reboot” to the local command-line authorization database.

```
BT(config)# privilege exec level 15 reboot
```

2. Configure the command-line authorization mode as TACACS+ authorization first and local authorization following.

```
BT(config)# aaa authorization commands 15 default grouptacacs+ local
```

Step 4 Configure to enable AAA.

```
BT(config)# aaa new-model
```

Step 5 Save the configuration.

```
BT(config)# exit
BT# copy running-config startup-config
This will save the configuration to the flash memory.
Are you sure?(y/n) [n]y
Building configuration.....
Configuration saved successfully.
```

Result

Only after passing corresponding level of authentication authorization, can the user implement corresponding maintenance and management against the device.

4.3.3 Configure Login Authentication Authorization

Logon authentication and authorization supported by the system:

- The authentication part authenticates users by checking the user name and password entered by each user. Authentication is implemented based on the principle that every user has a unique permission acquisition standard. The AAA server compares the users' standards with those in the database one by one. If consistent, user authentication is successful. If inconsistent, the server rejects the network connection request.
- A user obtains related task operation permissions by means of authorization. For example, after logging on to the system, the user may run some commands. At this time, the authorization process tests whether the user has the permissions to run these commands.

4.3.3.1 Configure Local Authentication Authorization

Context

- CMTS device supports 16 level of user, Level 0 is the lowest, while Level-15 is the highest.
- CMTS device supports the 2 default user groups, the default user groups do not allow deletion. CMTS device supports the creation of 5 user groups, with each group can be added at most 10 users.
- The default user with username as admin and password as admin is added to the group as administrators.

Users can change the default user's password as required.

Procedure

Step 1 Configure local user group by using the command "**groupname**".

Step 2 Add a new user by using the command "**username password**".

Step 3 Add a local user to a local user group by using the command "**username groupname**".

Step 4 Query information of local user group by using the command "**show groups**".

Step 5 Configure local authentication by using the command "**aaa authentication login default group local**".

Step 6 Configure local authorization by using the command "**aaa authorization login default group local**".

Step 7 Enable the AAA function by using the command "**aaa new-model**".

Step 8 Query configuration of aaa by using the command "**show aaa-configuration**".

Example

Add the user1 to the groupname1, with level as 15, and the login type as local authentication and authorization.

```
BT(config)# groupname groupname1 privilege 15
BT(config)# username user1 password password1
BT(config)# username user1 groupname groupname1
BT(config)# show groups
group index         : 0
group name          : administrators
group privilege     : 15
group index         : 1
group name          : default
group privilege     :  3
group index         : 2
group name          : groupname1
group privilege     : 15
show local groups: a total of 3 groups
BT(config)# aaa authentication login default group local
BT(config)# aaa authorization login default group local
BT(config)# aaa new-model
BT(config)# show aaa-configuration
show aaa configuration:
------------------------------------------------------------------------------------
aaa new-model: enable
authentication local-override: disable
authentication login method: local
authorization login method: local
```

```
authentication enable method:
authorization commands method:
------------------------------------------------------------------------------------------
```

After the above configuration, the user can enter the user name user1 and password password1 to log in to the CMTS device through local authentication and authorization.

Related Operations

Table 4-3 Related Operations for Configuring Local Authentication Authorization

Operation	Command	Remarks
Delete the user group	**no groupname**	
Delete the user	**no username**	
Restore the default authentication mode	**no aaa authentication login default group**	The default authentication mode is local.
Restore the default authorization mode	**no aaa authorization login default group**	The default authorization mode is local.

4.3.3.2 Configure TACACS+ Authentication Authorization

Context

- The CMTS supports configuration of the active and standby TACACS+ servers. If both the active and standby TACACS+ servers are configured, the system first sends an authentication and authorization request to the active TACACS+ server. If the active TACACS+ server does not respond, the system sends an authentication and authorization request to the standby TACACS+ server.
- Except that the active and standby servers and IP addresses are mandatory parameters, the following parameters are optional: encryption key, port number, retransmission times, and timeout. When a command is being configured, if an optional parameter is not configured, the previously configured value takes effect. For example, assume that 192.168.1.1 is already added as the active TACACS+ server. After you configure **tacacs-server primary ip-address 192.168.1.1 port 100**, only the port number is changed to 100, and the settings of the encryption key, retransmission times, and timeout remain unchanged.
- TACACS+ authentication is separated from TACACS+ authorization. You must configure both TACACS+ authentication and TACACS+ authorization to complete the entire logon authentication and authorization process.

Procedure

Step 1 Configure TACACS+ server by using the command "**tacacs-server**".

Step 2 Query configuration information of TACACS+ server by using the command "**show tacacs-server**".

Step 3 Configure TACACS+ authentication by using the command "**aaa authentication login default group tacacs+**".

Step 4 Configure TACACS+ authorization by using the command "**aaa authorization login default group tacacs+**".

Step 5 Enable the AAA function by using the command "**aaa new-model**".

Step 6 Query configuration of aaa by using the command "**show aaa-configuration**".

Example

Configure the IP address and encryption key of TACACS+ server, and the login type as TACACS+ authentication and authorization.

```
BT(config)# tacacs-server primary ip-address 192.168.1.1 key secretkey1
BT(config)# show tacacs-server
-------------------------------------------------------------------------------------------------------------
Type          Port    Retry    Timeout    Ip_address      Key
-------------------------------------------------------------------------------------------------------------
primary      49       1        3          192.168.1.1     secretkey1
secondary    --       --       --         --              --
-------------------------------------------------------------------------------------------------------------
BT(config)# aaa authentication login default group tacacs+
BT(config)# aaa authorization login default group tacacs+
BT(config)# aaa new-model
BT(config)# show aaa-configuration
show aaa configuration:
-----------------------------------------------------------------------------------
aaa new-model: enable
authentication local-override: disable
authentication login method: tacacs+
authorization login method: tacacs+
authentication enable method:
authorization commands method:
-----------------------------------------------------------------------------------
```

After the above configuration, the user can perform TACACS+ authentication and authorization to log in to the CMTS device by entering the user name and password. Users who cannot be authenticated and authorized by TACACS+ are denied access to the CMTS device.

Related Operations

Table 4-4 Related Operations for Configuring TACACS+ Authentication Authorization

Operation	Command	Remarks
Delete the TACACS+ server	**no tacacs-server**	
Restore the default authentication mode	**no aaa authentication login default group**	The default authentication mode is local.
Restore the default	**no aaa authorization**	The default authorization mode is local.

Operation	Command	Remarks
authorization mode	**login default group**	

4.3.3.3 Configure Radius Authentication Authorization

Context

- The CMTS supports configuration of the active and standby radius servers. If both the active and standby radius servers are configured, the system first sends an authentication and authorization request to the active radius server. If the active radius server does not respond, the system sends an authentication and authorization request to the standby radius server.
- Except that the active and standby servers and IP addresses are mandatory parameters, the following parameters are optional: encryption key, port number, retransmission times, and timeout. When a command is being configured, if an optional parameter is not configured, the previously configured value takes effect. For example, assume that 192.168.1.1 is already added as the active radius server. After you configure tacacs-server primary ip-address 192.168.1.1 port 100, only the port number is changed to 100, and the settings of the encryption key, retransmission times, and timeout remain unchanged.
- Radius authentication is separated from radius authorization. You must configure both radius authentication and radius authorization to complete the entire logon authentication and authorization process.

Procedure

Step 1 Configure the radius server by using the command "**radius-server**".

Step 2 Query the configuration information of radius server by using the command "**show radius-server**".

Step 3 Configure the radius authentication by using the command "**aaa authentication login default group radius**".

Step 4 Enable the AAA function by using the command "**aaa new-model**".

Step 5 Query configuration of aaa by using the command "**show aaa-configuration**".

Example

Configure the IP address and encryption key of radius server, and the login type as radius authenticationand authorization.

```
BT(config)# radius-server primary ip-address 192.168.1.1 key secretkey2
BT(config)# show radius-server
-------------------------------------------------------------------------------------------------------------
Type        Port     Retry    Timeout   Ip_address     Key
-------------------------------------------------------------------------------------------------------------
primary     1812     1        3         192.168.1.1    secretkey2
secondary   --       --       --        --             --
-------------------------------------------------------------------------------------------------------------
```

```
BT(config)# aaa authentication login default group radius
BT(config)# aaa new-model BT(config)#
show aaa-configurationshow aaa
configuration:
------------------------------------------------------------------------------
aaa new-model: enable
authentication local-override : disable
authentication login method: radius
authorization login method: local
authentication enable method:
authorization commands method:
------------------------------------------------------------------------------
```

After the above configuration, the user can perform radius authentication and authorization to log in to the CMTS device by entering the user name and password. Users who cannot be authenticated and authorized by radius are denied access to the CMTS device.

Related Operations

Table 4-5 Related Operations for Configuring Radius Authentication Authorization

Operation	Command	Remarks
Delete the radius server	**no radius-server**	
Restore the default authentication mode	**no aaa authentication login default group**	The default authentication mode is local.

4.3.4 Configure Enter the Enable View Authentication

CMTS device supports 2 kinds of AAA authentication modes:

- When the user level is higher than or equal to the enable password level, the user does not need to enter the enable password to directly enter the enable view.
- When the user level is lower than the enable password level, the user needs to enter the enable password and the system performs authentication according to the configured authentication rules.

4.3.4.1 Configure Local Authentication

Context

- CMTS device supports 16 level for users, Level 0 is the lowest, while Level-15 is the highest.
- CMTS device supports 16 level for enable password, Level 0 is the lowest, while Level-15 is the highest.
- The default level of enable password is 3.
- The default user with username as admin and password as admin is added to the group as administrators. Users can select to delete the default user or change the default user's password as required.

- Each level can be configured with one enable password at most, and the duplicate configuration will override the previous configuration.
- When the user's authorization level is lower than the enable password level, an enable password is required for authentication. When the enable password is entered correctly, the enable view is allowed and the user's authorization level does not change. When the enable password is not entered correctly, access to the enable view is denied.

Procedure

Step 1 Configure local enable password by using the command "**enable password** *password* **[level** *level***]**".

Step 2 Configure local authentication by using the command "**aaa authentication enable default group local**".

Step 3 Enable the AAA function by using the command "**aaa new-model**".

Step 4 Query configuration of aaa by using the command "**show aaa-configuration**".

Example

Configure the enable password for Level-13 user as enablepassword2, and the enter enable view type as local authentication.

```
BT(config)# enable password enablepassword2 level 13 BT(config)#
aaa authentication enable default group localBT(config)# aaa
new-model
BT(config)# show aaa-configuration
show aaa configuration:
------------------------------------------------------------------------------------
aaa new-model: enable
authentication local-override : disable
authentication login method : radius
authorization login method   : local
authentication enable method : local
authorization commands method:
------------------------------------------------------------------------------------
```

Related Operations

Table 4-6 Related Operations for Configuring Local Enable Authentication

Operation	Command	Remarks
Delete the local enable password	**no enable password**	The default password for entering the enable view is null.
Restore the default authentication mode	**no aaa authentication enable default group**	The default authentication mode is local.

4.3.4.2 Configure TACACS+ Authentication

Context

- The CMTS supports configuration of the active and standby TACACS+ servers. If both the active and standby TACACS+ servers are configured, the system first sends an authentication request to the active TACACS+ server. If the active TACACS+ server does not respond, the system sends an authentication request to the standby TACACS+ server.
- Except that the active and standby servers and IP addresses are mandatory parameters, the following parameters are optional: encryption key, port number, retransmission times, and timeout. When a command is being configured, if an optional parameter is not configured, the previously configured value takes effect. For example, assume that 192.168.1.1 is already added as the active TACACS+ server. After you configure **`tacacs-server primary ip-address 192.168.1.1 port 100`**, only the port number is changed to 100, and the settings of the encryption key, retransmission times, and timeout remain unchanged.
- Before a user accesses the Enable view, an authentication request is sent to the TACACS+ server. If the user authorization level is not lower than the enable password level, the user can directly access the Enable view without entering the enable password. If the user authorization level is lower than the enable password level, the user must enter the enable password for authentication. If the enable password entered by the user is correct, the user is allowed to access the Enable view and the user authorization level remains unchanged. If the enable password entered by the user is incorrect, the user is not allowed to access the enable view.

Procedure

Step 1 Configure the TACACS+ server by using the command "**`tacacs-server`**".

Step 2 Query the configuration information of TACACS+ server by using the command "**`show tacacs-server`**".

Step 3 Configure the TACACS+ authentication by using the command "**`aaa authentication enable default group tacacs+`**".

Step 4 Enable the AAA function by using the command "**`aaa new-model`**".

Step 5 Query configuration of aaa by using the command "**`show aaa-configuration`**".

Example

Configure the IP address and encryption key of TACACS+ server, and the enter enable view type as TACACS+ authentication.

```
BT(config)# tacacs-server primary ip-address 192.168.1.1 key secretkey3
BT(config)# show tacacs-server
-------------------------------------------------------------------------------------------------------------
Type       Port  Retry  Timeout  Ip_address    Key
-------------------------------------------------------------------------------------------------------------
```

```
primary     49     1       3         192.168.1.1    secretkey3
secondary   --     --      --        --             --
-------------------------------------------------------------------------------------------------------
BT(config)# aaa authentication enable default group tacacs+
BT(config)# aaa new-model BT(config)#
show aaa-configurationshow aaa
configuration:
-------------------------------------------------------------------------------
aaa new-model: enable
authentication local-override: disable
authentication login method: radius
authorization login method: local
authentication enable method: tacacs+
authorization commands method:
-------------------------------------------------------------------------------
```

Related Operations

Table 4-7 Related Operations for Configuring TACACS+ Authentication

Operation	Command	Remarks
Delete the TACACS+ server	**no tacacs-server**	
Restore the default authentication mode	**no aaa authentication enable default group**	The default authentication mode is local.

4.3.5 Configure the Command-Line Authorization

The CMTS device supports the configuration of execute permission for the specified command. Only the user who has reached the permission can execute the command. There are two situations when the user executes this command:

- When the user level is higher than or equal to the command level, the command can be executed.
- When the user level is lower than the command level, the command cannot be executed.

4.3.5.1 Configure Local Command-Line Authorization

Context

- CMTS device supports 16 level for commands, Level 0 is the lowest, while Level-15 is the highest. If the command is level 0, the default authorization is successful.
- The CMTS device supports configuring authorization for 100 local commands.
- The CMTS device supports configuring authorization for 5 keywords matching.
- When the user's authorization level is lower than the command authorization level, users cannot execute commands. Else the users cant execute commands.

Procedure

Step 1 Configure local command-line level by using the command "**privilege exec level command-level** *command1* [*command2* [*command3* [*command4* [*command5*]]]]".

Step 2 Query the locally-added command-line level by using the command "**show privilege exec**".

Step 3 Configure local command-line authorization by using the command "**aaa authorization commands default group local**".

Step 4 Enable the AAA function by using the command "**aaa new-model**".

Step 5 Query configuration of aaa by using the command "**show aaa-configuration**".

Example

Add Level-15 command line " reset" to local command-line authorization database.

```
BT(config)# privilege exec level 15 reset
BT(config)# show privilege exec
------------------------------------------------------------------------------------------
Index   Level   Commands
------------------------------------------------------------------------------------------
1       15      reset
------------------------------------------------------------------------------------------
show privilege exec: a total of 1 command(s)
BT(config)# aaa authorization commands 15 default group local
BT(config)# aaa new-model BT(config)#
show aaa-configurationshow aaa
configuration:
------------------------------------------------------------------------------------------
aaa new-model: enable
authentication local-override : disable
authentication login method: radius
authorization login method: local
authentication enable method: tacacs+
authorization commands method: local
------------------------------------------------------------------------------------------
```

Related Operations

Table 4-8 Related Operations for Configuring Local Command-line Authorization

Operation	Command	Remarks
Delete the authorized command line	**no privilege exec**	
Restore the default authorization mode	**no aaa authorization commands default group**	The default authorization mode is none.
Enable AAA	**aaa new-model**	To make the configuration take effect,

Operation	Command	Remarks
		you're required to enable AAA after finishing the configuration.
Query the configuration of AAA	**show aaa-configuration**	

4.3.5.2 Configure TACACS+ Command-line Authorization

Context

- CMTS device supports the configuration of the primary and secondary TACACS+ servers.
- Configure the TACACS+ server. Only if the configured primary and secondary server types and IP address are identical to those of the currently-configured server, specifying some a parameter will not make other parameters covered. For example, if 192.168.1.1 has been added as the primary TACACS+ server, configuring tacacs-server primary ip-address 192.168.1.1 port 100 will only modify the port number to 100, and will not modify the encryption key, retry times and timeout to the default value.
- To make the configuration take effect, you're required to enable AAA after finishing the configuration.

Procedure

Step 1 Configure TACACS+ server by using the command "**tacacs-server**".

Step 2 Query the configuration information of TACACS+ server by using the command "**show tacacs-server**".

Step 3 Configure TACACS+ command line authorization by using the command "**aaa authorization commands default group tacacs+**".

Step 4 Enable the AAA function by using the command "**aaa new-model**".

Step 5 Query configuration of aaa by using the command "**show aaa-configuration**".

Example

Configure the IP address and encryption key of TACACS+ server.

```
BT(config)# tacacs-server primary ip-address 192.168.1.1 key secretkey4
BT(config)# show tacacs-server
-------------------------------------------------------------------------------------------------------------
Type        Port   Retry   Timeout   Ip_address       Key
-------------------------------------------------------------------------------------------------------------
primary     49     1       3         192.168.1.1      secretkey4
secondary   --     --      --        --               --
-------------------------------------------------------------------------------------------------------------
BT(config)# aaa authorization commands 15 default group tacacs+
BT(config)# aaa new-model BT(config)#
show aaa-configurationshow aaa
configuration:
```

```
--------------------------------------------------------------------------------
aaa new-model: enable
authentication local-override : disable
authentication login method : radius
authorization login method   : local
authentication enable method : tacacs+
authorization commands method: tacacs+
--------------------------------------------------------------------------------
```

Related Operations

Table 4-9 Related Operations for Configuring TACACS+ Command-line Authorization

Operation	Command	Remarks
Delete the TACACS+ server	**no tacacs-server**	
Restore the default authorization mode	**no aaa authorization commands default group**	The default authorization mode is none.
Enable AAA	**aaa new-model**	To make the configuration take effect, you're required to enable AAA after finishing the configuration.
Query the configuration of AAA	**show aaa-configuration**	

4.4 Zero Touch Function

4.4.1 Zero Touch Overview

Zero touch function can make the device plug and play when entering the network. After the device is powered on, the version is upgraded and the device configuration is issued automatically. This greatly reduces the O&M costs. The zero configuration function supports:

- Plug-and-play of the CMTS device: The zero configuration function works together with the zero configuration backend system. After the CMTS device is connected to the network and powered on, the management IP address and correct configuration files can be automatically obtained, and device configuration is completed automatically. The entire process requires no manual intervention.
- Replace-and-play of the faulty CMTS device: The zero configuration function works together with the zero configuration backend system. When an in-service CMTS device is faulty, another CMTS device of the same model can be used to replace the faulty device. After replacement, the CMTS device automatically completes configuration and starts running. Its IP network configuration parameters and HFC network configuration parameters remain unchanged. The entire process requires no manual intervention.
- Update of the CMTS configuration file (running-config): After the CMTS is connected to the network and starts running, running-config is sent to the CMTS zero configuration backend system according to certain rules.
- You can judge the status of the zero configuration process, such as successful and abnormal, through the

indicators. These LED indicators include the RUN, CABLE, and ALM indicators.

Zero Touch Process	RUN indicators	CABLE indicators	ALARM indicators
DHCP complete/failure	ON / ON	0.5Hz/ 0.5Hz	OFF / ON
Descriptor file uploaded successfully/failure	ON / ON	1Hz/ 1Hz	OFF / ON
Software upgraded successfully/failure	ON / ON	2Hz/ 2Hz	OFF / ON
Config loaded successfully/failure	ON / ON	4Hz/ 4Hz	OFF / ON
Zero config successfully/failure	ON / ON	ON / ON	OFF / ON

Note:

When an exception occurs during the zero touch process, the CABLE light will keep the frequency and ALARM lights long bright. We can find the abnormal process by looking at the frequency of the ALARM light.

When zero touch completed, the device will send event news by the syslog and trap server scanning.

When zero touch completed, the time of indicating the state is able to be set. The command is “auto-update indication wait-time”. User can know more through the CMTS CLI Manual.

4.4.2 Example of CMTS Independent Deployment

Complete CMTS deployment independently through this task.

Networking Diagram

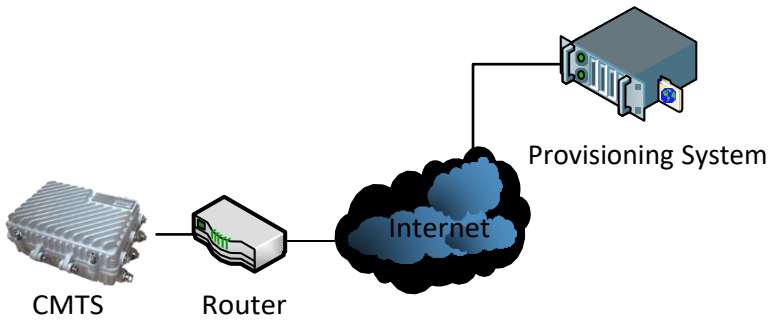

Figure 4-1 CMTS deployment networking diagram

Data Planning

In this case, enable zero touch function, manage VLAN 4089, VLAN 4089 enable dynamic DHCP function.

Zero configuration function and management VLAN can also be specified by factory configuration.

The following example illustrates the scenario of manual configuration.

Table 4-10 CMTS independent deployment data planning

Item	Data
Zero configuration function status	enable
management-vlan	4089
VLAN DHCP status	Turn on dynamic acquisition

Prerequisite

- Network equipment and lines are normal.
- CMTS equipment is in normal condition.
- Pre-configuration system is normal.

Provision server configuration requirements

- If DHCPv4 is used, DHCP option66 and option67 are configured on the device's DHCP server, where option66 is the IP address of the TFTP server and option67 is the CMTS description file name.
- If DHCPv6 is used, suboption32 and suboption33 of DHCPv6 Option17 are configured on the device's DHCP server, where suboption32 is the IP address of the TFTP server and suboption33 is the CMTS description file name.
- Configuration identifies the optio43 field of CMST DHCP message "docsis_device type", such as "docsis_ CC8800-C-P2".

The cmts description file stores the relevant information of the device configuration file, and supports the definition of the following data:

Table 4-11 Zero configuration management server description file data item

Item	Data
!	Represents a comment.
deviceType	Define the device types for this group configuration.
targetVersion=	Target image version number.
imagePath=	Destination image download path, IP address.
imageName=	Target image name.
cmcConfigPath=	The path to the CMC configuration file to be updated.
cmcConfigName=	The filename of the CMC configuration file to be updated.
eqamConfigPath=	Eqam configuration to be updated.
eqamConfigName=	The filename of the eqam configuration file to be updated.

Example:

Edit the cmts description file as follows:

!this is a description file

！first group

targetVersion = V2.2.8.2

imagePath = 10.10.29.207

imageName = imagePacket.img

description = this is update image

cmcConfigPath = 10.10.29.207

cmcConfigName = cmcConfig.cfg

cmcConfigDscr = this is cmc configure file

eqamConfigPath = 10.10.29.207

eqamConfigName = eqamConfig.cfg

eqamConfigDscr = this is eqam configure file

!second group

deviceType = CC8800-C-P2

targetVersion = V4.0.0.32

imagePath = 10.10.29.207

imageName = imagePacket.img

description = this is update image

cmcConfigPath = 10.10.29.207

cmcConfigName = cmcConfig.cfg

cmcConfigDscr = this is cmc configure file

eqamConfigPath = 10.10.29.207

eqamConfigName = eqamConfig.cfg

eqamConfigDscr = this is eqam configure file

!third group

deviceType1 = CC8800-E-P2

targetVersion1 = V4.0.0.33

imagePath1 = 10.10.29.207

imageName1 = imagePacket.img

description1 = this is update image

cmcConfigPath1 = 10.10.29.207

cmcConfigName1 = cmcConfig.cfg

cmcConfigDscr1 = this is cmc configure file

eqamConfigPath1 = 10.10.29.207

eqamConfigName1 = eqamConfig.cfg

eqamConfigDscr1 = this is eqam configure file

If the device obtains the above description file, the C-P2 device will obtain the second group of configuration information, and the E-P2 device will obtain the third group of information. If the device does not obtain the configuration information group matching its own device type, the first group of information will be obtained by default. If the device gets the device type, but it does not match the one in the description file, then if the first group has no devicetype, select the information of the first item, otherwise an error will be returned.

Configuration flowchart

The independent deployment process of CMTS is shown in the following figure.

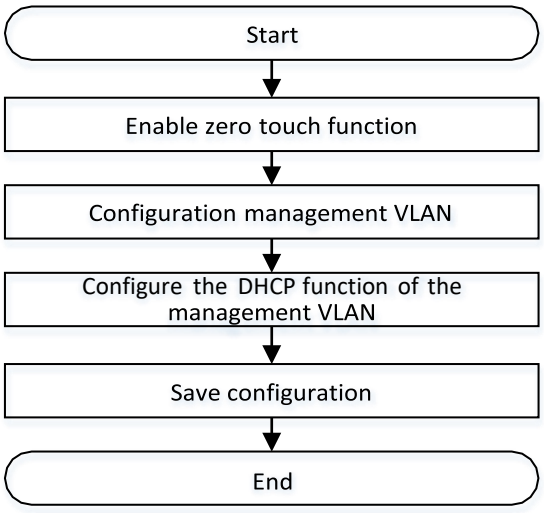

Figure 4-2 CMTS Device Configuration Flow Chart

Procedure

Step 1 Enable zero touch function

```
BT(config)# auto-update config enable
```

Step 2 Configuration management VLAN

```
BT(config)# management-vlan 4089
```

Step 3 Configure the DHCP function of the VLAN

```
BT(config-if-vlan4089)# ip address dhcp-alloc
```

Step 4 Step 4 Save configuration

```
BT(config)# exit
```

```
BT# copy running-config startup-config
This will save the configuration to the flash memory.
Are you sure?(y/n) [n]y
Building configuration.....
Configuration saved successfully.
```

Result

After successful configuration, CMTS can independently complete the deployment function, and can view the deployment status through the indicator lamp in CMTS.

4.4.3 Enable the Zero Touch Function

Context

In automatic mode, the user only needs to advance the configuration information to the production representatives, complete some configuration files written by production representatives.

Simply power up, version upgrades and device configuration can be done automatically.

Procedure

Step 1 Enable the zero touch state by using the command "**auto-update config enable**".

Step 2 Query the status of CMTS device by using the command "**show running-config verbose**".

----The end

Example

Enable the zero touch state of CMTS device.

```
BT(config)# auto-update config enable
BT(config)# show running-config verbose | include update
auto-update config enable
```

4.4.4 Repeat the Zero Touch Function

Context

By default, the CMTS device can only perform a zero touch operation once it is started. After a zero touch operation, the system needs to be restarted to perform zero configuration again.

Users can manually configure the repeat zero configuration function to keep the device version and configuration consistent with the version and configuration in the back-end database.

Procedure

Step 1 Enable the zero touch state by using the command "**auto-update repeat**".

Step 2 Query the status of CMTS device by using the command "**show running-config**".

Example

Enable the zero touch state of CMTS device.

```
BT(config)# auto-update config enable
BT(config)# show running-config | include auto-update
 auto-update repeat
```

4.4.5 Configure Management VLAN

Context

Users can choose to configure the management VLAN for deployment based on the networking plan. If the device is not configured with a management VLAN, you need to manually configure the management VLAN.

The default value of the management VLAN is in the factory default configuration file.

Procedure

Step 1 Configure the management VLAN by using the command "**management-vlan**".

Step 2 Enable the getting IP address automatically by using the command "**ip address dhcp-alloc**".

Step 3

----The end

Example

Query the status of CMTS device by using the command "**`show running-config`**".

Step 3

----The end

Example

Configure the management VLAN as 4089 and enable the getting IP address automatically.

```
BT(config)# management-vlan 4089
BT(config)# show running-config | include management-vlan
management-vlan 4089
BT(config)# interface vlanif 4089 BT(config-if-
vlan4089)# ip address dhcp-allocBT(config-if-
vlan4089)# show running-config interface vlan 4089
ip address dhcp-alloc
exit
```

Related Operations

Table 4-14 Related Operations for Configure the Management VLAN Command-line Authorization

Operation	Command	Remarks
Turn off automatic access to IP Addresses	**no ip address dhcp-alloc**	vlan view

Chapter 5 Management and Maintenance of CMTS

5.1 Log Configuration Management

5.1.1 Log Overview

Log records the status information during the system running in a real time manner, and sends relevant alarm information in case of system abnormity. Users can understand the status of their device by viewing the system log and alarm information, so as to monitor the network operation and provide powerful support for network troubleshooting.

CMTS device supports the following log functions:

- The device supports grading the log and implements reporting by grade:

  The device grades log by importance and reports the message by grade. The device supports eight grades: Emergency | Alert | Critical | Error | Warning | Notice | Informational | Debug.

- Logging mode
  - Local log: it doesn't need to set the server to store log information, but directly stores locally or has log printed to the terminal. It includes the following three modes: stored in the memory, stored in FLASH, and directly printed to the terminal.
  - Syslog: it sends and saves the log information of the device to the syslog server via the uplink port.
  - Trap alarm: it sends and saves the log information of the device to the trap server via the uplink port.
- Supporting speed limit for sending logs, saving system resources and ensuring that network performance will not be degraded due to the high traffic of sending logs.
- CMTS devices support the configuration of four log sending modes.
- Local Record Information Maintenance
  - CMTS devices support viewing local record information through various conditions:
    - Supports the command line filtering function "**| (begin | include | exclude)**" to view local record information. This article can be arbitrarily combined with other conditions. Detailed reference: View LOG information.
    - The keyword "**before-time | after-time | period-time**" is supported to view local record information for the corresponding time period.
    - Supports viewing the local record information of the corresponding ID through the keyword "**eventid**".

- Supports viewing local records of corresponding levels through the keyword "**priority**".
- Supports viewing the latest local record information through the keyword "**last**".
- Supports viewing all local records through the keyword "**all**".

- CMTS devices support the removal of local record information through various conditions:
  - Local record information can be cleared by the keyword "**before-time | after-time**".
  - The local record information of the corresponding ID can be cleared by the keyword "**eventid**".
  - Local record information at the corresponding level can be cleared by the keyword "**priority**".
  - The latest local record information can be cleared by the keyword "**last**".
  - All log information can be cleared by the keyword "**all**".

5.1.2 Example of Reporting Trap Alarms of Warning Level

Send and save the log information of CMTS to the trap server through this example.

Data Planning

The planning of log information in the trap server is shown as follows.

Table 5-1 Data Planning of Alarm Configuration

Item	Data
Logging mode	Alarm
Level of log	Warning
Serial number of trap server	0
IP address of trap server	1.1.1.1
Mode for limiting the syslog sending rate	maintainBelowThreshold
Interval for sending the syslog in current mode	10 seconds
Number of syslog allowed to be sent each interval in current mode	10 syslog

Prerequisite

The network, trap server and CMTS device are normal.

Configuration flowchart

The process of reporting the alarm message is shown as follows.

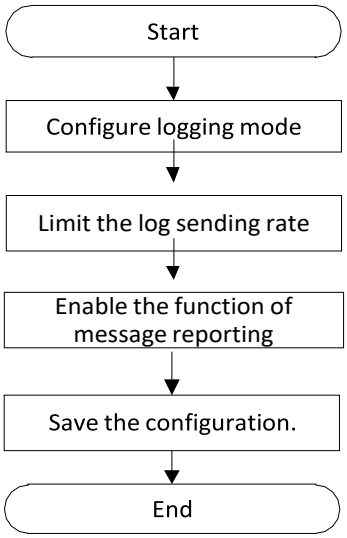

Figure 5-1 Process of configuring the log information in the trap server

Procedure

Step 1 Configure the logging mode.

1. Enter the syslog view.

   ```
   BT(config)# syslog
   ```

2. Configure the trap server for reporting the alarm of warning level.

   ```
   BT(config-syslog)# loglevel warning trapsConfigure
   ```

3. the trap server address.

   ```
   BT(config-syslog)# trap-server-ip 0 1.1.1.1
   ```

Step 2 Limit the log sending rate.

1. Configure the alarm sending rate as maintainBelowThreshold.

   ```
   BT(config-syslog)# throttle-admin maintainBelowThreshold
   ```

2. Configure the interval for sending alarms as 10 seconds.

   ```
   BT(config-syslog)# throttle-interval 10Configure
   ```

3. allowing to send 10 alarms at each interval.

   ```
   BT(config-syslog)# throttle-threshold 10
   ```

Step 3 Enable the function of message reporting.

```
BT(config-syslog)# message-to-event enable
```

Step 4 Save the configuration.

```
BT(config)# exit
BT# copy running-config startup-config
This will save the configuration to the flash memory.
Are you sure?(y/n) [n]y
Building configuration.....
Configuration saved successfully.
```

---- The end

Result

According to the above configurations, the logs of Warning level generated by CMTS will be sent and saved to the trap server.

5.1.3 Report the Log by Level

Context

When CMTS device generates much more syslog, users may be difficult to distinguish which are syslog for normal operation of the device, and which are syslog for troubleshooting. The grading of syslog can help users make coarse judgment and take measures in time to screen out the information which doesn't need any disposal.

The syslog can be classified into eight level by urgency. The higher urgency of syslog is, the smaller value is displayed. The details are shown as table below.

Table 5-2 Grading of Syslog

Value	Level	Description
0	Emergency	The device suffers from fatal abnormity, causing the system unable to use.
1	Alert	The device suffers from significant abnormity, and requires immediate measures for recovery.
2	Critical	The device suffers from abnormity, and requires taking measures or analyzing the reasons.
3	Error	The device suffers from improper operation which will not affect the subsequent service, but requires analyzing the reasons.
4	Warning	The device suffers from abnormity during normal operation, which may be the system malfunction and requires the user to pay attention to.
5	Notice	Important information for normal operation of the device.
6	Informational	General information for normal operation of the device.
7	Debug	Debugging information for normal operation of the device.

- The default emergency, alert, and critical logs are saved on the localnonvol.
- It is the prerequisite for the effectiveness of other configurations of the syslog to configure the logging mode of syslog.
- All levels of log reporting need to enable this task

Procedure

Step 1 Enter the syslog view by using the command "**`syslog`**".

Step 2 Configure the logging mode of syslog by using the command "**`loglevel (emergency | alert | critical | error | warning | notification | informational | debug | none) ( localnonvol | traps | syslog | localvolatile | monitor)`**".

Step 3 Configure the remote server by using the following commands.

- Configure the syslog server by using the command "**log-server-ip (0 | 1 | 2 | 3 | 4)** *ip-address*".
- Configure the trap server by using the command "**trap-server-ip (0 | 1 | 2 | 3 | 4)** *ip-address* **[***community***]**".

(For configuring local server, omit Step 3).

Step 4 Enable the function of reporting syslog by using the command "**message-to-event enable**".

.

Example

Reporting the syslog l to the syslog server with IP address as 1.1.1.1.

```
BT(config)# syslog
BT(config-syslog)# loglevel error syslog
BT(config-syslog)# log-server-ip 0 1.1.1.1
BT(config-syslog)# message-to-event enable
```

Related Operations

Table 5-3 Related Operations of Log Reporting

Operation	Command	Remarks
Restore the logging mode of syslog to the default	**loglevel all default**	
Delete the configurations of syslog server	**no log-server-ip**	
Disable the log reporting function	**message-to-event disable**	

5.1.4 Configure Log to Local Records

Context

Local logging mode includes the following:

- localvolatile: when this mode is used for recording the syslog, the information will be saved to local memory of the device. When the system restarts, the information will be lost.
- localnonvol: when this mode is used for recording the syslog, the information will be saved to local flash of the device permanently.
- monitor: when this mode is used for recording the syslog, the information will be displayed on the terminal only, instead of being saved to any storage medium.

The maximum number of configuration records saved for localnonvol and localvolatile support:

- After the maximum number of locally stored records is configured, when the number of local records generated by the system is greater than the maximum number, the system will overwrite the log records with earlier time.

- The number of local records allowed to be configured in the system is 10-10000.

The output format of syslog saved to the memory or local flash or printed directly to the terminal is shown as follows:

```
<level> TIMESTAMP HOSTNAME CMTS [vendor]: <module> <eventId> text
```

Details of the fields are shown as table below.

Table 5-4 Description of Syslog Output Format

Field	Meaning	Description
level	Level of syslog	Log level includes: Emergency | Alert | Critical | Error | Warning Notice Informational Debug
TIMESTAMP	Time for generating syslog	The format of *TIMESTAMP* is mm dd yy hh:mm:ss
HOSTNAME	Host name	*HOSTNAME* can be represented with either device name, or IP address of the device.
vendor	Vendor name	If the syslog is defined by DOCSIS, fill in DOCSIS; if the syslog is defined by the vendor itself, fill in the name of vendor. All syslog in CMTS are self-defined, therefore by default, all fields for *vendor* are BT.
module	Module name	Local module name of the log
eventId	Event ID	CMTS uses string of numbers to indicate the event ID.
text	Description information	*text* is used for description on the syslog.

Example:

```
<WARNING>Oct 25 2016 15:20:24 Constomer [BT]:<sysMoni><1041> US
Temperature Alarm:red,CMTS-MAC=0024.6851.004e;
```

The level of the syslog is warning, with its delivery time as 2016-10-25, 15:20:24, host name as BT, and the syslog is defined by the vendor-BT itself, with module name as sysMoni, event ID as 1041, and description of the message as “US Temperature Alarm:red,CMTS-MAC=0024.6851.004e;”.

Procedure

Step 1 Enter the syslog view by using the command “**syslog**”.

Step 2 Configure the level of syslog by using the command “**loglevel (emergency | alert | critical | error | warning | notification | informational | debug | none) (localnonvol | localvolatile | monitor)**”.

Step 3 Enable the function of message reporting by using the command “**message-to-event enable**”.

.

Example

Configure the logging mode as saving the log of error level to the memory, and printing the log of notification level to the terminal.

```
BT(config)# syslog
BT(config-syslog)# loglevel error localvolatile
BT(config-syslog)# loglevel notification monitor
BT(config-syslog)# set-log-num 500 BT(config-syslog)#
message-to-event enable
```

Related Operations

Table 5-5 Related Operations of Local Logging Mode

Operation	Command	Remarks
Logging mode	**loglevel (emergency | alert | critical | error | warning | notification | informational | debug | none) syslog**	
Alarm recording mode	**loglevel (emergency | alert | critical | error | warning | notification | informational | debug | none) trap**	

5.1.5 Configure Log to Syslog Server and the Trap Alarm

5.1.5.1 Configure Log to Syslog Server

Context

The output format of syslog saved to the syslog server is shown as follows:

```
<level> TIMESTAMP HOSTNAME CMTS [vendor]: <eventId> text
```

Details of the fields are shown as table below:

Table 5-6 Description of Syslog Output Format

Field	Meaning	Description
level	Level of syslog	*level* is represented with ASCII code; in CMTS, its value is obtained by implementing the "or" operation by using Facility(0x80) of the default process type and the level of syslog (0-7), and is within 128 and 135.
TIMESTAMP	Time for generating syslog	The format of *TIMESTAMP* is mm dd yy hh:mm:ss
HOSTNAME	Host name	*HOSTNAME* can be represented with either device name, or IP address of the device.
vendor	Vendor name	If the syslog is defined by DOCSIS, fill in DOCSIS; if the syslog is defined by the vendor itself, fill in the name of vendor. All syslog in CMTS are self-defined, therefore all fields for *vendor* are BT.
eventId	Event ID	CMTS uses string of numbers to indicate the event ID.

Field	Meaning	Description
text	Description information	*text* is used for description on the syslog.

Example:

```
<WARNING> Nov 21 2017 10:31:20 Constomer [BT]: :<sysMoni><1041> US
Temperature Alarm:red,CMTS-MAC=0024.6851.004e;
```

The level of the syslog is Notice, with its delivery time as 2013-1-29, 17:32:28, host name as BT, and the syslog is defined by the vendor-BT itself, with event ID as 1023, and description of the message as “agent=1 is online,sync db”.

Note:

Trap alarm message and common syslog message are differed just by execution system and storage mode, with other user-configured parameters completely the same.

Procedure

Step 1 Enter the syslog view by using the command “**syslog**”.

Step 2 Configure the level of syslog by using the command “**loglevel (emergency | alert | critical | error | warning | notification | informational | debug | none) syslog**”.

Step 3 Configure the syslog server by using the command “**log-server-ip**”.

Step 4 Enable the function of message reporting by using the command “**message-to-event enable**”.

.

Example

Configure the logging mode as saving the log of warning level to the syslog server, whose IP address as 10.10.29.200, and enable the function of message reporting.

```
BT(config)# syslog
BT(config-syslog)# loglevel warning syslog BT(config-
syslog)# log-server-ip 0 10.10.29.200BT(config-
syslog)# message-to-event enable
```

Related Operations

Table 5-7 Related Operations of Logging Mode

Operation	Command	Remarks
Local logging mode	**loglevel (emergency | alert | critical | error | warning | notification | informational | debug | none)**	

Operation	Command	Remarks
	(localnonvol | localvolatile | monitor)	
Alarm recording mode	**loglevel (emergency | alert | critical | error | warning | notification | informational | debug | none) trap**	

5.1.5.2 Configure Trap Alarm

Context

CMTS devices support log reporting at the log level, sending trap messages to the configured trap server.

Support for configuring 5 trap servers with Index 0-4.

The reported trap messages are stored in the trap server, which can be divided into three types: channel up-and-down trap messages, DCC-RSP event trap messages and other common trap messages.

The different types of messages are as follows:

Table 5-8 Description of Trap Message in System Channel Log Format

Field	Meaning	Description
timestamp	System time	Represents the time when the system triggered the log
alarmSeq	The serial number of the log	Decided by the specific event ID
snmpTrapOID	Oid of corresponding message	LinkUpOid or LinkDownOid
ifIndex	Index value of channel	32 digit integer
ifAdminStatus	Channel switch management status	1 – up, 2- down, 3- test, 4 - ipqam
ifOperStatus	Actual operation status of channel switch	1 – up, 2- down,3 – test, 4- unknown, 5- dormant, 6 – not present, 7 - lowerLayerDown

Table 5-9 Description of System DCC-RSP Log Trap Message Format

Field	Meaning	Description
timestamp	System time	Represents the time when the system triggered the log
alarmSeq	The serial number of the log	Decided by the specific event ID
snmpTrapOID	Oid of corresponding message	docsDevCmtsDCCRspFailTrapOid
EventLevel	Event level	The level of logs contained in the trap message
eventId	Event ID	The ID of the log contained in the trap message
docsDevEvText	Event description	Decided by specific events

Table 5-10 Description of System Common Log Trap Message Format

Field	Meaning	Description
timestamp	System time	Represents the time when the system triggered the log
alarmSeq	The serial number of the log	Decided by the specific event ID
snmpTrapOID	Oid of corresponding message	docsIf3CmtsEventNotifOid
EventLevel	Event level	The level of logs contained in the trap message
eventId	Event ID	The ID of the log contained in the trap message

Field	Meaning	Description
docsDevEvText	Event description	Decided by specific events
docsDevEvLastTime	Log time	Time when the system triggered the log, format YYYYMMDDHmmSS
sysName	System aliases	hostname

Note:

Trap alarm message and common syslog message are differed just by execution system and storage mode, with other user-configured parameters completely the same.

Procedure

Step 1 Enter the syslog view by using the command "**syslog**".

Step 2 Configure the level of syslog by using the command "**loglevel (emergency | alert | critical | error | warning | notification | informational | debug) traps**".

Step 3 Configure the trap server by using the command "**trap-server-ip**".

Step 4 Enable the function of message reporting by using the command "**message-to-event enable**".

.

Example

Configure warning level trap alerts.

```
BT(config)# syslog
BT(config-syslog)# loglevel warning traps
BT(config-syslog)# trap-server-ip 0 1.1.1.1
BT(config-syslog)# message-to-event enable
BT(config)# exit
BT# copy running-config startup-config
This will save the configuration to the flash memory.
Are you sure?(y/n) [n]y
Building configuration.....
Configuration saved successfully
```

Related Operations

Table 5-11 Related Operations of Alarm Logging Mode

Operation	Command	Remarks
Local logging mode	**loglevel (emergency | alert | critical | error | warning | notification | informational | debug**	

Operation	Command	Remarks
	| none) (localnonvol | localvolatile | monitor)	
Logging mode	**loglevel (emergency | alert | critical | error | warning | notification | informational | debug | none) syslog**	

5.1.5.3 Limit the Logging and Alarm Rate

Users can limit the logging and alarm rate to save the resources on the device and ensure that the network performance will not be reduced due to too high traffic for sending logs. The system is only required to limit the rate against the event to be sent to the remote server, i.e., syslog and trap. There are four modes for limiting the log sending rate the device supports:

Table 5-12 Description on Configuration Task of Syslog

Configuration task	Description
Inhibited	In this mode, the device is not allowed to send any syslog to the syslog or trap server.
maintainBelowThreshold	In this mode, the device sends the syslog information normally if the number of syslog sent in the configured sending interval is not larger than the maximum number configured; otherwise, the device will stop sending the syslog information, but will restore sending the information in the next sending interval.
stopAtThreshold	In this mode, the device sends the syslog information normally if the number of syslog sent in the configured sending interval is not larger than the maximum number configured; otherwise, the device will stop sending the syslog information, and will restore sending the information only if configuring the restricted mode again.
unconstrained	In this mode, the device has no limit on the rate when sending the syslog.

Context

- When the system log is sent to the remote server, the sending rate of the system log can be limited by configuring this task.
- When the mode of the sending system log configure as stopAtThreshold or maintainBelowThreshold it need to configuration the of the system log intervals and the log number in each interval.

Procedure

Step 1 Enter the syslog view by using the command "**syslog**".

Step 2 Configure the mode for limiting the syslog sending rate by using the command "**throttle-admin (inhibited | maintainBelowThreshold | stopAtThreshold | unconstrained)**".

Step 3 Configure the interval of the sending log by using the command "**throttle-interval** *interval*".

Step 4 Configure the threshold in each interval by using the command "**throttle-threshold** *threshold*".

.

Example

Configure the mode of the rate is stopAtThreshold , and the interval limiting the syslog sending rate is 15 seconds, allowing 10 log sending in each interval.

```
BT(config)# syslog
BT(config-syslog)# throttle-admin stopAtThreshold
BT(config-syslog)# throttle-interval 15
BT(config-syslog)# throttle-threshold 10
```

Related Operations

Table 5-13 Related Operations of Limiting the Syslog Sending Rate

Operation	Command	Remarks
Restore the default mode for limiting the syslog sending rate	**no throttle-admin**	
Restore the default interval for sending the syslog	**no throttle-interval**	
Restore the default number of syslog allowed to be sent each interval	**no throttle-threshold**	

5.1.6 Configure the Maximum Number of Syslog to Be Saved

Configure the maximum number of syslog to be stored locally through this task.

Context

After configuring the maximum number of syslog to be stored locally, when the number of logs generated by the device is larger than this maximum number, the device will delete the saved old syslog until the number of currently-stored syslog doesn't exceed the maximum number.

Procedure

Step 1 Enter the syslog view by using the command "**syslog**".

Step 2 Configure the maximum number of syslog to be stored locally by using the command "**set-log-num** *log-num*".

Example

Configure the maximum number of syslog to be stored locally as 2,000.

```
BT(config)# syslog
BT(config-syslog)# set-log-num 2000
```

Related Operations

N/A

5.1.7 View the Syslog

View the syslog information through this task.

Context

By the following ways, users can view the syslog information to monitor the running status and locate the faults of the device.

- View the local record information through the command line filtering function **| (begin | include | exclude)**. This condition can be arbitrarily combined with other conditions.
- View the information of syslog before the specified time (Excluding this time point) by logging mode by using the command "**show log (localnonvol | localvolatile) before-time** *time*".
- View the information of syslog after the specified time (Including this time point) by logging mode by using the command "**show log (localnonvol | localvolatile) after-time** *time*".
- View the information of syslog in the specified time range by logging mode by using the command "**show log (localnonvol | localvolatile) period-time** *begin-time end-tim".*
- View the information of syslog with the specified event ID by logging mode by using the command "**show log (localnonvol | localvolatile) eventid** *eventid*".
- View the information of syslog of the specified level by logging mode by using the command "**show log (localnonvol | localvolatile) priority (emergency | alert | critical | error | warning | notification | informational | debug)**".
- View the information of the saved latest syslog in the specified number by logging mode by using the command "**show log (localnonvol | localvolatile) last** *log-num*".
- View the information of all syslog by logging mode by using the command "**show log (localnonvol | localvolatile) all**".

Procedure

Step 1 Enter the syslog view by using the command "**syslog**".

Step 2 View the information of the saved latest syslog in the specified number by logging mode by using the command "**show log (localnonvol | localvolatile) last**".

Example

View the information of the latest 3 syslog with the logging mode as localnonvol.

```
BT(config)# syslog
BT(config-syslog)# show log localnonvol last 3
<NOTICE>Apr 18 2017 09:21:31 BT CMTS[BT]:<cmtsMgmt><4263314950> CMTS-
MAC=0024.6851.0046;DS 5 changed;adminStatus:down->up;
<NOTICE>Apr 18 2017 09:21:31 BT CMTS[BT]:<cmtsMgmt><4263314950> CMTS-
MAC=0024.6851.0046;DS 6 changed;adminStatus:down->up;
<NOTICE>Apr 18 2017 09:21:31 BT CMTS[BT]:<cmtsMgmt><4263314950> CMTS-
MAC=0024.6851.0046;DS 7 changed;adminStatus:down->up;
total log amount 5,match log amount 3
```

Related Operations

N/A

5.1.8 Clear the Syslog

Clear the information of syslog through this task.

Context

Clear the information of syslog by the following ways, which can save more storage resources for the system.

- Clear the information of syslog before the specified time by logging mode by using the command "**clear log (localnonvol | localvolatile) before-time** *time*".
- Clear the information of syslog after the specified time by logging mode by using the command "**clear log (localnonvol | localvolatile) after-time** *time*".
- Clear the information of syslog with the specified event ID by logging mode by using the command "**clear log (localnonvol | localvolatile) eventid** *eventid*".
- Clear the information of syslog of the specified level by logging mode by using the command "**clear log (localnonvol | localvolatile) priority (emergency | alert | critical | error | warning | notification | informational | debug)**".
- Clear the information of the saved latest syslog in the specified number by logging mode by using the command "**clear log (localnonvol | localvolatile) last** *log-num*".
- Clear the information of all syslog by logging mode by using the command "**clear log (localnonvol | localvolatile) all**".

⚠ Warning:

Since the cleared syslog can not be restored, be sure to confirm the operation before clearing.

Procedure

Step 1 Enter the syslog view by using the command "**syslog**".

Step 2 Clear the information of the saved latest syslog in the specified number by logging mode by using the command "**clear log (localnonvol | localvolatile) last**".

Example

$Clear the information of the latest 3 syslog with logging mode as localnonvol.

```
BT(config)# syslog
BT(config-syslog)# clear log localnonvol last 3
```

Related Operations

N/A

5.1.9 View System-supported Alert and Event Information

View the alert and event list information supported by CMTS devices through this task.

Context

Check the alert and event information supported by CMTS devices through the following two commands.

- Use the **show alarm list (***alarm-id* **| all)** command to view the alert information supported by CMTS devices.
- Use the **show event list (***event-id* **| all)** command to view event information supported by CMTS devices.

Procedure

Step 1 Enter the syslog view by using the command "**syslog**".

Step 2 View the information of the saved latest syslog in the specified number by logging mode by using the command "**show log (localnonvol | localvolatile) last**".
Use the "**show alarm list**" command to view the alert information supported by CMTS devices or use the "**show event list**" command to view the event information supported by CMTS devices.

Example

View the alert information with ID 426316231 and event information with ID 0073055400 supported by CMTS devices.

```
BT(config)# syslog
BT(config-syslog)# show alarm list 4263316231
Alarm ID                Type                          Alarm Name
------------------------------ ----------------------------------- ------------------------------------------
```

```
4263316231(0xfe1d0b07) sysMoni                    DOL_CHIP_TEMP_WARNS
BT(config-syslog)# show event list 73055400
Event ID                Type                      Event Name
------------------------------ ------------------------------- ----------------------------------------
0073055400(0x045abca8) modemMgmt                DOL_CM_PARTIAL_SVC_REGACK_TCS_EVENT
```

Related Operations

N/A

5.2 CMTS Alarm Trap

5.2.1 Configure Temperature Alarm

Context

The temperature alarm function allows you to configure the red and yellow alarm thresholds for the CMTS device. You can use this function to monitor the device temperature. When the temperature is too high, users are notified in time for troubleshooting or service adjustment, providing customers with better services.

If the CMTS device temperature exceeds the temperature alarm threshold, a temperature alarm is generated. Two parameters must be configured to implement the temperature alarm function:

- Red alarm threshold: If the actual temperature is equal to or higher than the red alarm threshold, the CMTS device generates a red alarm. The red alarm threshold must be higher than the yellow alarm threshold. If this parameter is not configured, the value is 75 degrees Celsius by default.
- Yellow alarm threshold: If the actual temperature is equal to or higher than the yellow alarm threshold, the CMTS device generates a yellow alarm. If the CMTS device temperature exceeds both the red and yellow alarm thresholds, the CMTS device generates only a red alarm. If this parameter is not configured, the value is 70 degrees Celsius by default.
- When the actual temperature is lower than the yellow alarm threshold, the CMTS device generates an alarm, indicating that the temperature is back to normal.

Procedure

Step 1 Enter the cmts view by using the command "**`interface cmts`**"

Step 2 Configure the temperature alarm thresholds of CMTS by using the command "**`cable temperature alarm threshold`**".

Step 3 Query the temperature alarm thresholds by using the command "**`show cmts temperature threshold`**".

Example

Configure the red temperature alarm thresholds as 70 celsius, yellow temperature alarm thresholds as 60 celsius.

```
BT(config)# interface cmts 1
BT(config-if-cmts-1)# cable temperature alarm threshold red 70 yellow 60
BT(config-if-cmts-1)# show cmts temperature threshold
        MAC                                  : 0024.6850.128c
        Temperature RED ALARM Threshold      : 70 degC (158 degF)
        Temperature YELLOW ALARM Threshold : 60 degC (140 degF)
```

Related Operations

Table 5-14 Related Operations for Configuring Temperature Alarm

Operation	Command	Remarks
Query the temperature of CMTS device	**show cmts temperature**	

5.2.2 Configure Memory Utilization Alarm

Context

The memory utilization function allows you to configure the alarm and recovery thresholds for the CMTS device. You can use this function to monitor the device memory utilization. When the memory utilization is too high, users are notified in time for troubleshooting or service adjustment, providing customers with better services.

The configuration of the memory utilization alarm function includes two parts: configuring the memory usage alarm threshold and recovery threshold, and enabling the memory utilization alarm. Parameter configuration needs attention:

- Alarm threshold: If the actual memory utilization is equal to or higher than the alarm threshold, the CMTS device generates a alarm. If this parameter is not configured, the value is 85 by default.
- Recovery threshold: If the actual memory utilization is less than the recovery threshold, the CMTS device generates a recovery alarm. If this parameter is not configured, the value is 75 by default.

Procedure

Step 1 Enter the cmts view by using the command "**interface cmts**"

Step 2 Configure the memory utilization alarm thresholds of CMTS by using the command "**cable memory-alarm threshold**".

Step 3 Enable the memory utilization alarm function of CMTS by using the command "**cable memory-alarm enable**".

Step 4 Query the memory utilization alarm thresholds by using the command "**show running-config verbose**".

Example

Configure the alarm thresholds of memory utilization as 80, recovery thresholds as 60, and enable the memory utilization alarm function.

```
BT(config)# interface cmts 1
BT(config-if-cmts-1)# cable memory-alarm threshold warning 80 recovery 60
BT(config-if-cmts-1)# cable memory-alarm enable
BT(config-if-cmts-1)# show running-config verbose | include memory-alarm
 cable memory-alarm enable
 cable memory-alarm threshold warning 80 recovery 60
```

rm

Related Operations

N/A

Context

The CPU utilization function allows you to configure the alarm and recovery thresholds for the CMTS device.You can use this function to monitor the device CPU utilization. When the CPU utilization is too high, users are notified in time for troubleshooting or service adjustment, providing customers with better services.

5.2.3 Configure CPU Utilization Alarm

The configuration of the CPU utilization alarm function includes configuring the CPU usage alarm threshold and recovery threshold. Parameter configuration needs attention:

- Alarm threshold: If the actual CPU utilization is equal to or higher than the alarm threshold, the CMTSdevice generates a alarm. If this parameter is not configured, the value is 60 by default.
- Recovery threshold: If the actual CPU utilization is less than the recovery threshold, the CMTS devicegenerates a recovery alarm. If this parameter is not configured, the value is 50 by default.

Procedure

Step 1 Enter the config view by using the command "**configure terminal**"

Step 2 Configure the CPU utilization alarm thresholds of CMTS by using the command "**sysmoni main-cpu-utili threshold-warning threshold-recovery**".

Step 3 Query the CPU utilization alarm thresholds by using the command "**show sysmoni**".

Example

Configure the alarm thresholds of CPU utilization as 80, recovery thresholds as 70.

```
                                                    BT# configure terminal
BT(config)# sysmoni main-cpu-utili threshold-warning 80 threshold-recovery 70
BT(config)# show sysmoni
```

```
sysmoni main-cpu-utili threshold-warning 80 threshold-recovery 70
```

Related Operations

N/A

5.2.4 Configure Channel Utilization Alarm

Context

The channel utilization function allows you to configure the alarm and recovery thresholds for the CMTS device. You can use this function to monitor the device channel utilization. When the channel utilization is too high, users are notified in time for troubleshooting or service adjustment, providing customers with better services.

The configuration of the channel utilization alarm function includes configuring the channel usage alarm threshold and recovery threshold. Parameter configuration needs attention:

- Alarm threshold: If the actual channel utilization is equal to or higher than the alarm threshold, the CMTS device generates a alarm. If this parameter is not configured, the value are minor: 0, major: 70, critical: 90 for upstream channel and minor: 0, major: 70, critical: 90 for downstream channel by default.
  - If the threshold is 0, the alarm is disabled.
  - When the threshold is not 0, the minor threshold <major threshold <critical threshold and the recovery threshold <identical alarm threshold.
- Recovery threshold: If the actual channel utilization is less than the recovery threshold, the CMTS device generates a recovery alarm. If this parameter is not configured, the value are minor: 0, major: 65, critical: 85 for upstream channel and minor: 0, major: 65, critical: 85 for downstream channel by default.
  - If the threshold is 0, the alarm is disabled.
  - When the threshold is not 0, the minor threshold <major threshold <critical threshold and the recovery threshold <identical alarm threshold.

Procedure

Step 1 Enter the cmts view by using the command "**`interface cmts`**"

Step 2 Configure the upstream channel utilization alarm thresholds of CMTS by using the command "**`cable upstream util threshold-warning threshold-recovery`**", or configure the downstream channel utilization alarm thresholds of CMTS by using the command "**`cable downstream util threshold-warning threshold-recovery`**".

Step 3 Configure the interval of channel utilization alarm of CMTS by using the command "**`cable util-interval`**".

Step 4 Query the channel utilization alarm thresholds by using the command "**`show cable util`**".

Example

The warning thresholds of minor level, major level and critical level are 50, 60 and 70 respectively, and the recovery thresholds of minor level, major level and critical level are 45, 55 and 65 respectively. The channel utilization rate is calculated every 200 seconds.

```
BT(config)# interface cmts 1
BT(config-if-cmts-1)# cable upstream util threshold-warning 50 60 70
threshold-recovery 45 55 65
BT(config)# cable util-interval 200
If the interval is too small, it would cause system performance impact.
A value between 180 to 300 seconds or greater is recommended.
BT(config-if-cmts-1)# show cable util
Channel utilization interval:200s
Upstream(SCQAM OFDMA):
Level          Threshold-warning  Threshold-recovery
Minor          50                 45
Major          60                 55
Critical       70                 65
Channel        Utilization(%)
1              0
2              0
3              0
4              0
5              0
6              0
7              0
8              0
Downstream(SCQAM OFDM):
Level          Threshold-warning  Threshold-recovery
Minor          0                  0
Major          70                 65
Critical       90                 85
Channel        Utilization(%)
1              1
2              1
3              1
4              1
5              1
6              1
7              1
8              1
9              1
10             1
11             1
12             1
```

```
13              1
```

Related Operations

N/A

5.3 Product Upgrade

5.3.1 Upgrade Overview

This section describes in detail the process for the device upgrade. Please operate strictly in accordance with this document when upgrading. The device upgrade can be achieved in two modes:

- Upgrade via TFTP and FTP through the command line;
- Upgrade the software via WEB network management system.

5.3.2 Upgrade through Command Line

There are commands "**load image tftp**", "**load image ftp**" and "**load image curl-ftp**" in the enable view, with which users can perform the online upgrade. After finishing the upgrade, restart the device and the new version of software will take effect. Please upgrade in the following order. The following TFTP method to upgrade example:

5.3.2.1 Enter the Command for Upgrade

Enter "**load image tftp** *192.168.0.206 packetimage*" by command style, where *192.168.0.206* is the IP address of TFTP server, and *packetimage* is the default file name. Keep smooth network and press the Enter key, then the system will start the upgrade automatically.

```
BT# load image tftp 172.16.36.63 CC8800F-V4.0.0.9-build.603.bin
Start to download image packet file...
Download image file successfully.
Start upgrade operation.
Verifying Checksum ...
jffs2: notice: (1691) jffs2_build_xattr_subsystem: complete building xattr subsystem,
0 of xdatum (0 unchecked, 0 orphan) and 0 of xref (0 dead, 0 orphan) found.
Flash whole image...
 Upgrade the system OK!
```

5.3.2.2 Restart the Device

Restart the device, and use the command "**show software-version**" to view the software version after the upgrade.

```
BT(config)# show software-version
Copyright          : Copyright 2010-2019,All rights Reserved by BT
Software Version   : V4.0.0.9
```

```
Product Model       : CC8800-C-P2
Compiled Time       : 2019-03-22 17:23:08
FPGA Version        : V1.0.15
```

5.3.3 Upgrade through Web Interface

CMTS supports the management of web interface, and also supports the upgrade through web interface.

5.4 License Management

In order to facilitate the management of operating equipment, provide Licensee to control equipment resources, so as to adapt to different needs of customers. Controllable resources include:

- Maximum number of available SC downlink channels and NC EQAM channels (total)
- Maximum available SC upstream channel
- Maximum available OFDM/OFDMA channels
- Maximum available BC EQAM channel
- Maximum CM quantity

5.4.1 License Configuration

CMTS device support license function: support import, display, self-access and verification.

- License import:
  - CMTS device supports CLI import license: execute command **`load license ftp`** or **`load license tftp`** (see CLI manual for details)
  - License cannot be deleted, but the system can upgrade the license through the load command
- License display:
  - The content and status of the certificate can be displayed by the **`show license`** command, which currently supports the display of status, subject, public key, fingerprint, serial number, device capability authorization, etc.
- License automatic acquisition
  - In order to facilitate the management of license, the configuration of licensee-server is provided to ensure that if there is no licensee locally, the licensee can be automatically obtained from the licensee-server when the device restarts; if there is a licensee locally, the local license will be used directly.
- License check

  In order to prevent the licensee from being tampered with, a three-level certificate-like structure is provided to ensure the correctness of the license.

That is ROOT-LICENSE, MFG-LICENSE, CMTS-LICENSE. ROOT can test the accuracy of MFG-LICENSE, and MFG can test the accuracy of CMTS-LICENSE.

In addition, E2SN and DEV SN are also provided in CMTS-LICENSE to ensure the matching between LICENSE and equipment.

5.4.2 Example of License Configuration

Through this task, the CMTS license authorization function is realized.

Networking Diagram

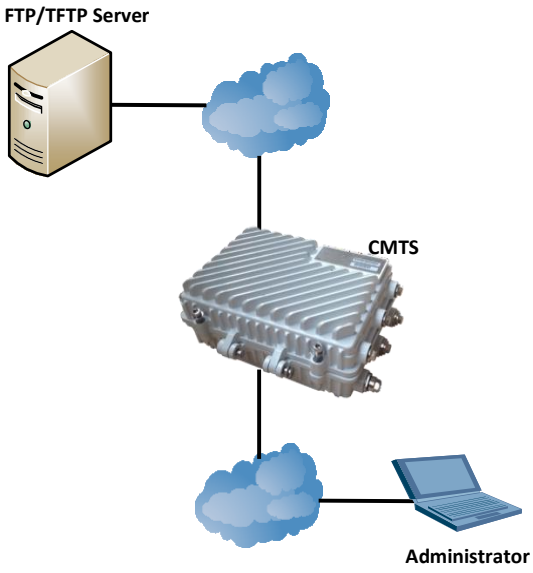

Figure 5-2 CMTS License Authorized Networking Diagram

Data Planning

Table 5-15 CMTS License Authorization Data Planning

Item	Data
Server	FTP/TFTP server
License file	license_1708CCEP220003241.tar.gz
FTP/TFTP server IP	192.166.166.13

Prerequisite

- FTP/TFTP server
- license file
  - license application
  - After CMTS device users obtain the equipment SN and e2sn, they can apply for license from the license authority, which can generate the license files required by the equipment through the license tool.

Configuration flowchart

The configuration license process is shown in the following figure.

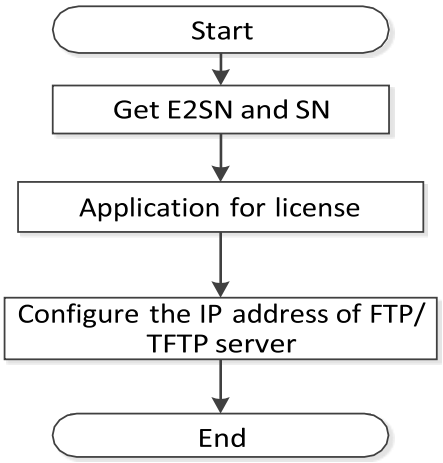

Figure 5.4-1 Configuration license flow chart

Procedure

1. Manual import of equipment license

Step 1 License import

- FTP mode

  BT # **load license ftp 192.166.166.13 admin 123456 license_1708CCEP220003241.tar.gz**

- TFTP mode

  BT # **load license tftp 192.166.166.13 license_1708CCEP220003241.tar.gz**

Step 2 View license information

```
BT(config)# show license
MFG License:
  Subject: Manufacturer License
  License Serial Number: 1550566880310
  MFG License pubkey:
2d:2d:2d:2d:2d:42:45:47:49:4e:20:50:55:42:4c:49:43:20:4b:45:59:2d:2
d:2d:2d:2d:0a:4d:49:47:66:4d
41:30:47:43:53:71:47:53:49:62:33:44:51:45:42:41:51:55:41:41:34:47:4
e:41:44:43:42:69:51:4b:42:67
51:43:75:32:39:2f:48:44:71:6f:4d:58:41:37:72:64:6e:4d:51:2f:62:63:3
8:2f:72:4e:6d:0a:58:2b:73:69
67:72:31:57:32:46:42:6e:65:4c:54:6b:72:74:44:44:59:74:49:69:61:76:2
f:6e:30:47:59:54:55:33:42:72
```

```
4f:64:41:33:36:6e:59:7a:4d:72:51:76:54:33:7a:2f:46:68:57:6c:75:68:3
4:46:43:35:41:70:0a:47:41:4d
61:67:33:6b:38:4d:55:34:58:6c:72:57:56:32:38:71:7a:46:6e:73:35:4b:7
8:43:6f:50:70:2b:51:2f:32:70
33:61:6b:35:66:33:71:32:64:48:73:36:45:57:6f:6a:4c:77:34:74:47:55:4
b:4c:5a:5a:6b:45:72:0a:44:62
4d:7a:61:77:41:57:30:68:2f:6a:6c:44:76:50:2f:77:49:44:41:51:41:42:0
a:2d:2d:2d:2d:2d:45:4e:44:20
  Signature:
48:6e:2f:78:67:6c:53:67:63:47:4a:6c:72:59:6f:34:55:48:6e:47:42:63:5
9:71:37:38:72:48:4a:62:46:56
45:64:61:44:30:31:37:76:4d:2b:75:57:7a:31:51:73:76:31:45:4a:38:4d:6
1:4d:4a:66:4d:39:36:42:49:38
36:55:34:6b:36:41:56:68:59:51:6d:33:48:46:57:35:65:4a:6d:68:39:53:7
6:4f:53:79:69:5a:56:45:4c:56
70:4a:32:55:61:54:6c:65:79:6f:4d:50:79:45:62:46:4e:67:39:74:52:52:6
6:36:41:41:4e:45:4a:72:59:48
70:57:6a:43:36:62:6a:79:56:43:6b:6d:30:64:34:38:78:73:4a:49:63:32:3
8:36:6e:6c:52:46:71:5a:68:64
  Thumbprint:

6a:32:d9:0c:59:c9:7f:4a:5d:0d:af:8c:25:40:e4:a2:57:f0:0c:cd:00:00:0
0:00:00:00:00:00:00:00:00:00
CMTS License:
  License status: active
  Subject: CMTS License
  License Serial Number: 1550646225808
  Authorizationinfo:
      sc ds and nc eqam:     32
      sc us    :     8
      ofdm ds  :     2
      ofdma us :     1
      bc eqam  :     8
      cm       :     400
  Device SN: 1708CCEP220003241
  Signature:
43:47:32:72:52:74:50:62:36:70:31:77:52:46:76:31:73:30:48:75:33:54:6
6:35:72:72:66:67:5a:78:62:4b
36:32:75:46:4d:58:49:33:51:35:50:7a:33:34:52:78:33:4b:42:53:76:45:5
a:75:6c:61:6d:69:77:56:4d:59
```

```
57:41:62:62:75:62:66:63:73:77:6b:68:2f:56:68:47:57:44:7a:71:79:4e:4
a:64:70:74:6f:58:4d:49:46:4e
2b:35:72:70:47:6d:6b:4e:38:77:6c:2b:61:53:46:64:32:6d:31:49:72:4d:5
1:30:79:42:34:57:2b:75:2b:48
4d:78:59:64:69:37:71:46:47:66:46:31:6c:65:74:43:71:38:67:6c:77:51:6
a:7a:4a:34:4d:35:4e:55:31:55
  Thumbprint:
68:e8:c7:f7:22:5a:2e:8c:97:70:88:5b:04:2f:b1:19:e4:ea:15:af:00:00:0
0:00:00:00:00:00:00:00:00:00
```

2. Automatically import license information

Step 1 Configure the IP address of the license's TFTP server

```
BT(config)# license tftp-server ip 192.166.166.13 auto-filename
```

Step 2 Save configuration

```
BT(config)# exit
BT# copy running-config startup-config
This will save the configuration to the flash memory.
Are you sure?(y/n) [n]y
Building configuration.....
Configuration saved successfully.
```

Step 3 Reboot device

```
BT# reboot
Are you sure to reboot?(y/n) [n]y
System is going to reboot...
```

Result

- After importing the device license manually, the user can view the license information of the manufacturer and the device through the **show license** command.
- After importing the license automatically, if the device does not have a license, the license file will be downloaded automatically according to the TFTP server of the license configured; if the device has a license, the license file will not be downloaded from the TFTP server.

Chapter 6 VLAN Configuration Management

6.1 VLAN Overview

Equipment supports two types of VLAN applications:

- Managing VLAN: Supports configuring multiple IP addresses on this VLAN interface. By managing VLAN, the security of access devices can be enhanced.

  IP address of VLAN: According to configuration, it can be divided into static IP address and dynamic IP address.

  - VLAN static IP address: IP address configured by the IP address command.
  - VLAN Dynamic IP Address: IP Address Obtained by DHCP.

- Service VLAN: VLAN based on IP subnet and CM MAC address segment.

  - VLAN partition based on IP subnet: It is mainly used to plan different services by adding different VLAN according to the IP address segment of CPE.
  - VLAN partition based on CM MAC segment: VLAN partition based on CM MAC segment refers to CMTS device according to CM VPN configuration, the CMTS CPE's upstream message is marked with corresponding VLAN tag, the downstream message is stripped; CM's message is not effective.

6.2 Configure IP Address of VLAN Virtual Interface

IP address of VLAN virtual interface can be configured in two modes: static IP address and dynamic IP address.

6.2.1 Configure Static IP Address of VLAN Virtual Interface

Configure static IP address for VLAN virtual interface through this task.

Context

The device supports the creation of 8 VLAN virtual interfaces, and static IP addresses can be configured under each VLAN view.

Procedure

Step 1 Create VLAN and enter the VLAN virtual interface view by using the command "**`interface vlanif`**".

Step 2 Configure IP address of VLAN virtual interface by using the command "**`ip address`**".

Step 3 Use "**`show interface vlanif`**" command to query VLAN information in config view or "**`show running-config`**" command to query VLAN information in VLAN view.

Example

Configure the static IP address for VLAN 100 virtual interface as 10.10.1.1/24.

```
BT(config)# interface vlanif 100
BT(config-if-vlan100)# ip address 10.10.1.1 255.255.255.0 primary
BT(config-if-vlan100)# show running-config
interface vlan 100
 ip address 10.10.1.1 255.255.255.0 primary
exit
BT(config-if-vlan100)# exit
BT(config)# show interface        vlanif
 Vlan ID  MAC Address      Type    Level    Category    Ip Address/Maskbits
 100      0024.6851.0007   static  primary  unicast     10.10.1.1/24
                           static  N/A      link-local  fe80::224:68ff:fe51:7
```

Related Operations

Table 6-1 Related Operations for Configuring Static IP Address of VLAN Virtual Interface

Operation	Command	Remarks
Delete VLAN	**no interface vlanif**	
Delete static IP address of VLAN virtual interface	**no ip address primary**	
Add secondry static IP address of VLAN virtual interface	**ip address secondry**	
Delete secondry static IP address of VLAN virtual interface	**no ip address secondry**	

6.2.2 Configure Dynamic IP Address of VLAN Virtual Interface

Configure the dynamic IP address for VLAN virtual interface through this task.

Context

- Make sure the DHCP of CMTS can work normally before configuring dynamic IP address for VLAN virtual interface.
- After configuring dynamic acquisition of IP address on VLAN virtual interface, the previously-configured static IP address will be deleted automatically, and CMTS is not allowed to configure the static IP address until dynamic acquisition of IP address is disabled.

Procedure

Step 1 Create VLAN and enter the VLAN virtual interface view by using the command "**interface vlanif**".

Step 2 Configure acquiring the IP address of VLAN virtual interface automatically by using the command "**ip address dhcp-alloc**".

Step 3 Use "**show interface vlanif**" command to query VLAN information in config view or "**show running-config**" command to query VLAN information in VLAN view.

Example

Configure automatic acquisition of IP address for VLAN 100 virtual interface.

```
BT(config)# interface vlanif 100 BT(config-if-
vlanif100)# ip address dhcp-allocBT(config-if-
vlanif100)# exit BT(config)# show interface vlanif
 Vlan ID  MAC Address     Type    Level    Category    Ip Address/Maskbits
 100      0024.6851.0007  dhcp    primary  unicast     ( Waiting to assign ip... )
                          static  N/A      link-local  fe80::224:68ff:fe51:7
```

Related Operations

Table 6-2 Related Operations for Configuring Dynamic IP Address of VLAN Virtual Interface

Operation	Command	Remarks
Delete VLAN	**no interface vlanif**	
Disable automatic acquisition of IP address by VLAN virtual interface	**no ip address dhcp-alloc**	

6.3 Configure the IP Subnet-based VLAN

Configure the IP subnet-based VLAN through this task.

Context

Configure this task to help CMTS determine VLAN of the packet by source IP after receiving the Untagged packet in the ingress direction of cable port, and add corresponding VLAN tag to the packet; the VLAN tag will be removed by matching VLAN ID when forwarding the packet in the egress direction of cable port.

Procedure

Step 1 Configure the subnet VLAN by using the command "**ip-subnet-vlan vlan**".

Step 2 (Optional) Configure the subnet VLAN tag protocol identifier by using the command "**ip-subnet-vlan tpid**".

Step 3 (Optional) Configure the subnet VLAN standard format indicator by using the command "**ip-subnet-vlan cfi**".

Step 4 Query the configuration information of subnet VLAN by using the command "**show ip-subnet-vlan vlan**".

Example

Configure the subnet vlan of the packet with source IP 192.168.1.1/32 as 100 and priority as 5.

```
BT(config-if-cmts-1)# ip-subnet-vlan 192.168.1.1 255.255.255.255 vlan 100
priority 5
BT(config-if-cmts-1)# show ip-subnet-vlan all
IP_Address      Subnet Mask       VLAN Id    Priority
192.168.1.1     255.255.255.255   100        5
```

Related Operations

Table 6-3 Related Operations for Configuring the Subnet VLAN

Operation	Command	Remarks
Delete the configuration of subnet VLAN	**no ip-subnet-vlan**	

6.4 Configure VLAN Based on CM MAC Segment

This task can be configured as a VLAN based on CM MAC segment.

Background Information

By configuring this task, CMTS can be divided according to CM MAC segment, the upstream message of CPE under designated CM can be marked with corresponding VLAN tag, and the downstream message can be stripped of the corresponding VLAN tag, which has no effect on the CM message.

Operation Procedures

Step 1 Configure the VLAN mapping of CM specifying the MAC address segment using the "**cable modem mac-range VLAN map**" command.

Step 2 Use the "**show cable mac-range vlan-map**" command to query VLAN mappings for all CM MAC address segments.

Task Example

Configure the VLAN mapping of CM MAC address segment and view the configuration results.

```
BT(config)# cable modem 0014.f8bf.0c68 0014.f8bf.0c78 vlan 1 map priority 0
BT(config)# show cable mac-range vlan-map
 cable modem 00:14:F8:BF:0C:68 00:14:F8:BF:0C:78 vlan 1 map priority 0 " "
```

Related Operations

Table 6-4 Related operations to configuration of VLAN based on CM MAC segment forwarding

Operation	Command	Remark
Delete VLAN based on CM MAC segment	**no cable modem mac-range vlan map**	

Chapter 7 DHCP Relay Function

7.1 Overview

Terminals (including the CM and CPE) can communicate with DHCP servers in other network segments through the DHCP relay. In this way, service terminals can obtain IP addresses in different network segments and go on line normally.

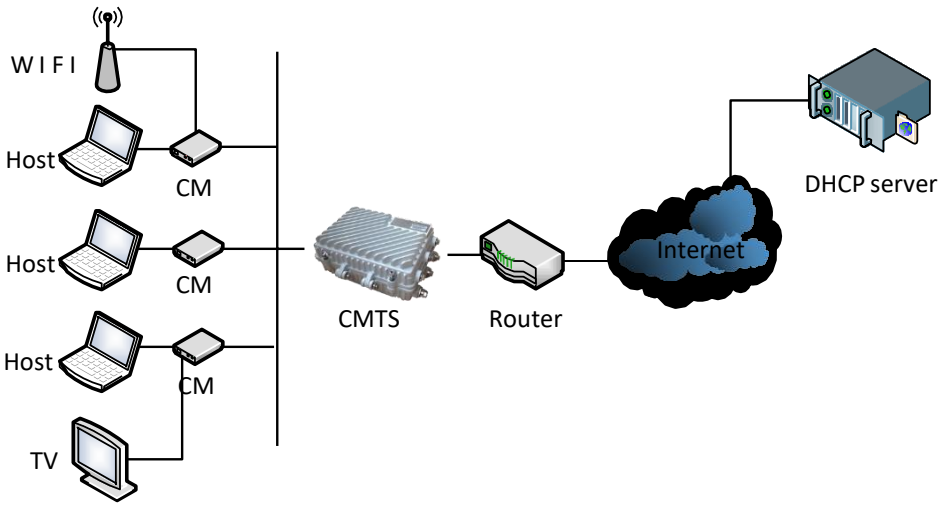

Figure 7-1 Networking Diagram of CMTS Device

The CMTS supports the following DCHP relay function:

- DHCP relay modes

  The CMTS supports the following DHCP forwarding modes:

  - Snooping mode: The CMTS monitors the DHCP interaction process. It directly forwards packets without making any modification. This mode is applicable to the scenario where an upstream device serves as the DHCP relay and the CMTS only forwards data.
  - L2-relay mode: This mode is applicable to the scenario where an upstream device forwards data at L3 and the CMTS only forwards data at L2. It is also applicable to a simple networking scenario. For example, the DCHP server, CMTS, and terminal work in the same network segment, and data does not need to be forwarded across network segments. In this mode, the CMTS supports insertion of option 82 to check the validity of the DHCP packet source.
  - L3-relay mode: In this mode, the CMTS works as a L3 relay so that service terminals can obtain IP addresses in different network segments. The L3-relay mode further consists of the following modes:
    - Primary mode: The same giAddr is used on all devices. The primary IP address is the giAddr of all devices.
    - Policy mode: The CMTS assigns different giAddrs for the CMs and other CPEs. The primary IP address is the giAddr of the CM, and the first secondary IP address is the IP address of the CPE.

- Strict mode: The CMTS assigns a different giAddr for each type of terminals to be used.

Note:

The CMTS is a L2 device, and does not have the traditional giAddr. To maintain consistency with industry standards, the relay address and giAddr are of the same concept.

1. When you configure a giAddr, the CMTS converts the broadcast DCHP packet into the unicast packet and forwards the packet to the DHCP server through the relay. In this way, the DHCP packet can be forwarded across network segments. When configuring L3 forwarding, you must configure the gateway IP address (giAddr) in the DHCP/BOOTP message header. If this field contains the IP address 0.0.0.0, the DHCP relay fills in the IP address of the relay proxy or router in this field, and then forwards the message to the DHCP server. When the DHCP server receives this message, it checks the gateway IP address field (giAddr) in the message. If the DHCP server has multiple address pools, it provides the IP address lease of the address pool based on the giAddr. Therefore, the giAddr determines whether the server allocates the address and determines the address pool from which the address is allocated. The CMTS inserts the giAddrs of different network segments based on the device type. Through flexible insertion of giAddrs, different device types are allocated with different network segments.

2. If you do not configure giAddr, the CMTS supports automatic acquisition of giAddr. Specifically, the DHCP relay module uses the IP address obtained by ip address dhcp-alloc in the config view, or uses the configured primary IP address as the IP address of the device. After dynamic IP address acquisition is configured, the statistic primary IP address cannot be configured in this view. When configuring dynamic IP address acquisition, you only need to configure information about a single bundle. In addition, you do not need to configure the device relay address for the bundle. You can use the no form of the corresponding command to disable dynamic IP address acquisition.

- DHCP server

  The DHCP server configuration includes the common DHCP server and the dedicated DHCP server.

  - Common DHCP server: It is the DHCP server shared by different types of terminals.
  - Dedicated DHCP server: It is the DHCP server used by a specific type of terminals.

- Option60 keyword

  Option60 is used to identify different terminal types so that service types can be differentiated based on the terminal type. It is applicable to the snooping, L2-relay, and L3-relay modes.

- dhcp-tag

  With the dhcp-tag function, a VLAN tag can be added to different device types by bundle. It is applicable to the snooping, L2-relay, and L3-relay modes.

- Option82 keyword

The Option82.1 circuit ID is used to configure the user information so as to determine the source of network packets. It is mainly used for security check. It is applicable to the L2-relay and L3-relay modes.

7.2 Example of DHCP Snooping

Achieve the transparent data transmission by CMTS device through this task.

Context

CMTS device provides DHCP Snooping service, and just listens to DHCP data instead of processing. At this time, the terminal devices such as CM/CPE can acquire the IP address from DHCP Server at the network side via Relay that is the layer-3 device connected the CMTS's uplink port. And CMTS can support identifying the device type with VLAN tag.

Data Planning

In this example, configure transparent transmission of the data of CM | HOST | MTA | STB, and have the layer-3 switch to implement the Relay operation, and set VLAN tags for several kinds of terminal devices to determine the device types.

The data planning for configuring the DHCP transparent transmission example is shown as table below.

Table 7-1 Data Planning for DHCP Snooping Mode

Item	Data
CM transmission mode	snooping
HOST transmission mode	snooping
MTA transmission mode	snooping
STB transmission mode	snooping
bundle item	bundle 1
CM DHCP Tag	vlan 1 priority 7
HOST DHCP Tag	vlan 2 priority 7
MTA DHCP Tag	vlan 3 priority 4
STB DHCP Tag	vlan 4 priority 4
DHCP Server	Normal configuration. It can communicate with the device by means of ping; CMTS is not required to configure the address of DHCP Server, but just transmit transparently the packet to the layer-3 device for relay to DHCP Server by the uplink port.

Prerequisites

- Network devices and lines must be in the normal state.
- DHCP Server is configured normally.

Configuration flowchart

The process for configuring DHCP transparent mode is shown as figure below.

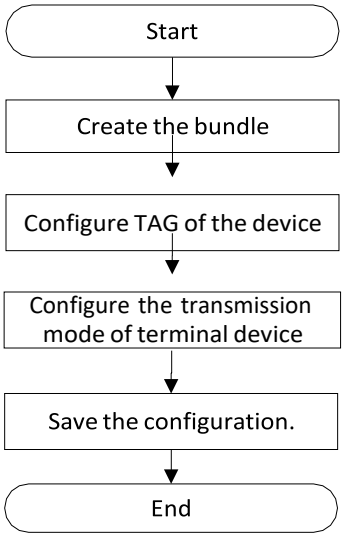

Figure 7-2 Flowchart of DHCP Snooping

Procedure

Step 1 Create the bundle.

```
BT(config)# interface bundle 1
```

Step 2 Add a VLAN tag to data of the terminal device.

1. Add VLAN 1 tag to the data of CM, with priority as 7.

```
BT(config-if-bundle1)# cable dhcp-tag cm vlan 1 priority 7
```

2. Add VLAN 2 tag to the data of HOST, with priority as 7.

```
BT(config-if-bundle1)# cable dhcp-tag host vlan 2 priority 7
```

3. Add VLAN 3 tag to the data of MTA, with priority as 4.

```
BT(config-if-bundle1)# cable dhcp-tag mta vlan 3 priority 4
```

4. Add VLAN 4 tag to the data of STB, with priority as 4.

```
BT(config-if-bundle1)# cable dhcp-tag stb vlan 4 priority 4
```

Step 3 Configure the data of terminal device type for transparent transmission.

1. Exit the bundle view.

```
BT(config-if-bundle1)# exit
```

2. Configure the data with terminal device type as CM for transparent transmission.

```
BT(config)# cable dhcp-mode cm snooping
```

3. Configure the data with terminal device type as HOST for transparent transmission.

```
BT(config)# cable dhcp-mode host snooping
```

4. Configure the data with terminal device type as MTS for transparent transmission.

```
BT(config)# cable dhcp-mode mta snooping
```

5. Configure the data with terminal device type as STB for transparent transmission.

```
BT(config)# cable dhcp-mode stb snooping
```

Step 4 Save the configurations.

```
BT(config)# end
BT# copy running-config startup-config
```

```
This will save the configuration to the flash memory.
Are you sure?(y/n) [n]y
Building configuration.....
Configuration saved successfully.
```

Result

After finishing the configurations, the terminals under CMTS such as CM/HOST/MTA/STB can acquire IP address automatically from DHCP Server by transparent transmission, and identify the device type with VLAN.

7.3 Example of DHCP L2 Relay

Achieve data transparent transmission by CMTS device through this task.

Context

CMTS device provides the DHCP layer-2 Relay service. The device receives the packet from client, and add option82 for forwarding; the device receives the packet from DHCP Server, and removes option82 for forwarding. At this time, the terminal devices such as CM/CPE can acquire the IP address from DHCP Server at the network side via Relay that is the layer-3 device connected the CMTS's uplink port. And CMTS can support identifying the device type with VLAN tag.

Data Planning

In this example, configure L2 Relay against the data of terminals such as HOST | MTA | STB | cablemodem, and have the layer-3 switch to implement the Relay operation, and set Option60 field to distinguish the terminal types.

The data planning for configuring the DHCP transparent transmission example is shown as table below.

Table 7-2 Data Planning for DHCP Transparent Mode

Item	Data
HOST transmission mode	l2-relay
MTA transmission mode	l2-relay
STB transmission mode	l2-relay
cablemodem transmission mode	l2-relay
bundle item	bundle 1
HOST Option60	host-option60
MTA Option60	mta-option60
STB Option60	settopbox-option60
User-defined cablemodem option60	userdefine-cabmo

Item	Data
DHCP Server	Normal configuration. It can communicate with the device by means of ping; CMTS is not required to configure the address of DHCP Server, but just forward the Layer-2 packet to the layer-3 uplink device for relay to DHCP Server by the uplink port.

Prerequisites

- Network devices and lines must be in the normal state.
- DHCP Server is configured normally.

Configuration flowchart

The process for DHCP transparent transmission is shown as figure below.

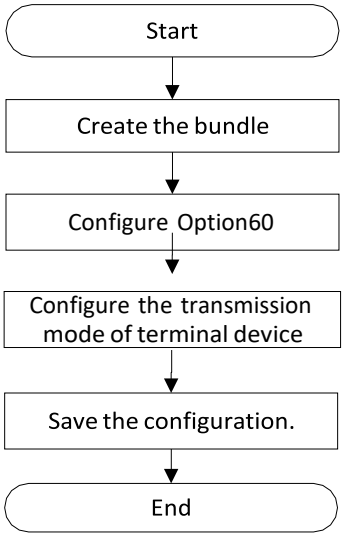

Figure 7-3 Flowchart of DHCP L2 Relay

Procedure

Step 1 Create the bundle.

```
BT(config)# interface bundle 1
```

Step 2 Configure Option60 identifiers for the terminal device.

1. Option60 identifier of HOST is host-option60.

```
BT(config-if-bundle1)# cable dhcp-option60 host host-option60
```

2. Option60 identifier of MTA is mta-option60.

```
BT(config-if-bundle1)# cable dhcp-option60 mta mta-option60
```

3. Option60 identifier of STB is settopbox.

```
BT(config-if-bundle1)# cable dhcp-option60 stb settopbox
```

4. IPv4 option60 identifier of the user-defined device type “cablemodem” is userdefine-cabmo.

```
BT(config-if-bundle1)# cable dhcp device cablemodem
BT(config-if-bundle1)# cable dhcp-option60 cablemodem
userdefine-cabmo
```

Step 3 Configure the layer-2 forwarding against the data of terminal device.

1. Exit the bundle view.

   ```
   BT(config-if-bundle1)# exit
   ```

2. Configure the data of terminal device-HOST for layer-2 forwarding.

   ```
   BT(config)# cable dhcp-mode host l2-relay
   ```

   Configure

3. the data of terminal device-MTA for layer-2 forwarding.

   ```
   BT(config)# cable dhcp-mode mta l2-relay
   ```

4. Configure the data of terminal device-STB for layer-2 forwarding.

   ```
   BT(config)# cable dhcp-mode stb l2-relay
   ```

   Configure the

5. data of terminal device-cablemodem for layer-2 forwarding. `BT(config)# cable dhcp-mode cablemodem l2-relay`

Step 4 Save the configurations.

```
BT(config)# end
BT# copy running-config startup-config
This will save the configuration to the flash memory.
Are you sure?(y/n) [n]y
Building configuration.....
Configuration saved successfully.
```

Result

After finishing the configurations, the terminals under CMTS such as HOST/MTA/STB and user-defined device can acquire IP address automatically from DHCP Server by transparent transmission.

7.4 Example of Primary Mode

The terminal device acquires IP address via DHCP L3 Relay through this task.

Context

In case of L3 Relay mode, CMTS device translates the broadcast DHCP packet via relay into the unicast packet and send it to the DHCP Server for cross-network-segment forwarding of DHCP packet. In primary mode, all CMs and CPEs acquire IP address from DHCP Server at network side through the same relay.

Data Planning

In this example, the data of all CM/CPE is assured of L3 Relay via the same relay, STB device acquires IP address by using the dedicated DHCP Server, while other terminal devices acquire the IP address through the common DHCP Server.

The data planning for configuring DHCP Relay primary mode example is shown as table below.

Table 7-3 Data Planning for DHCP Relay Primary Mode Example

Item	Data
CM transmission mode	l3-relay
HOST transmission mode	l3-relay
MTA transmission mode	l3-relay
STB transmission mode	l3-relay
Global primary IP (IP/MASK)	10.10.28.2/24
bundle item	bundle 1
GiAddr relay mode	primary
Relay address (IP/MASK)	10.10.28.2/24
Universal DHCP Server IP	10.10.29.211
STB dedicated DHCP Server IP	10.10.29.209
Routing information	0.0.0.0 0.0.0.0 10.10.28.1

Prerequisites

- Network devices and lines must be in the normal state.
- DHCP Server is configured normally.

Configuration flowchart

The process for configuring DHCP Relay primary mode is shown as figure below.

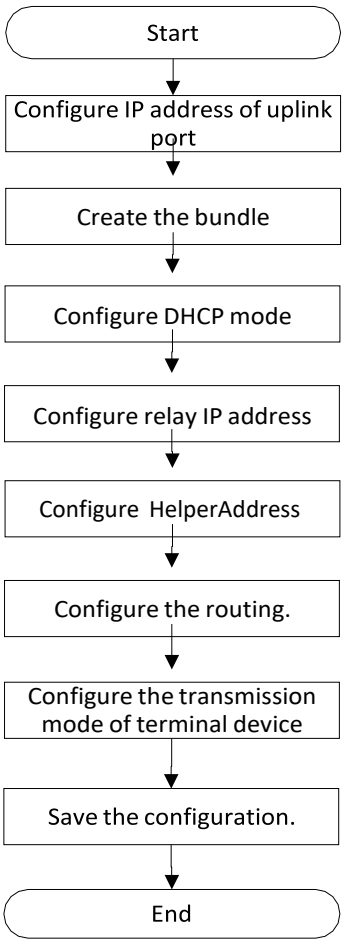

Figure 7-4 Flowchart of DHCP L3 Relay Primary mode

Procedure

Step 1 Configure the primary IP address of the uplink port.

```
BT(config)# ip address 10.10.28.2 255.255.255.0 primary
```

Step 2 Create the bundle.

```
BT(config)# interface bundle 1
```

Step 3 Select DHCP Relay mode as primary.

```
BT(config-if-bundle1)# cable dhcp-giaddr primary
```

Step 4 Configure the relay address set for the terminal.

```
BT(config-if-bundle1)# ip address 10.10.28.2 255.255.255.0
```

Step 5 Configure IP of DHCP server.

1. Configure the universal Helper-Address.

```
BT(config-if-bundle1)# cable helper-address all
10.10.29.211
```

2. Configure STB dedicated Helper-Address.

```
BT(config-if-bundle1)# cable helper-address stb
10.10.29.209
```

Step 6 Configure the routing.

1. Exit the bundle view.

```
BT(config-if-bundle1)# exit
```

2. Configure the routing information.

```
BT(config)# ip route 0.0.0.0 0.0.0.0 10.10.28.1
```

Step 7 Configure the data of terminal device type for Layer-3 forwarding.

1. Configure the data with terminal device type as CM for Layer-3 forwarding.

```
BT(config)# cable dhcp-mode cm l3-relay
```

2. Configure the data with terminal device type as HOST for Layer-3 forwarding.

```
BT(config)# cable dhcp-mode host l3-relay
```

3. Configure the data with terminal device type as MTA for Layer-3 forwarding.

```
BT(config)# cable dhcp-mode mta l3-relay
```

4. Configure the data with terminal device type as STB for Layer-3 forwarding.

```
BT(config)# cable dhcp-mode stb l3-relay
```

Step 8 Save the configurations.

```
BT(config)# exit
BT# copy running-config startup-config
This will save the configuration to the flash memory.
Are you sure?(y/n) [n]y
Building configuration.....
Configuration saved successfully.
```

Result

After finishing the configuration, all terminal devices use the same relay, and STB acquires IP address from the dedicated DHCP server, while other terminal devices acquire IP address automatically from the universal DHCP server.

7.5 Example of Policy Mode

CM and CPE acquire IP address automatically via different relays through this task.

Context

In case of L3 Relay mode, CMTS device translates the broadcast DHCP packet via relay into the unicast packet and send it to the DHCP Server for cross-network-segment forwarding of DHCP packet. In policy mode, CM and CPE acquire IP address from DHCP Server at network side through two different relays respectively.

Data Planning

In this example, the data of CM and CPE is assured of L3 Relay via two different relays respectively, all terminal devices acquire IP address by using the universal DHCP Server.

The data planning for configuring DHCP Relay policy mode example is shown as table below.

Table 7-4 Data Planning for DHCP Relay Policy Mode Example

Item	Data
CM transmission mode	l3-relay
HOST transmission mode	l3-relay
MTA transmission mode	l3-relay
STB transmission mode	l3-relay
Global primary IP (IP/MASK)	10.10.28.2/24
Global secondary IP (IP/MASK)	10.10.27.2/24
bundle item	bundle 1
GiAddr relay mode	policy
Relay address (IP/MASK) of CM	10.10.28.2/24
Relay address (IP/MASK) of other terminal devices including HOST	10.10.27.2/24
DHCP Server IP	10.10.29.211
Routing information	0.0.0.0 0.0.0.0 10.10.28.1

Prerequisites

- Network devices and lines must be in the normal state.
- DHCP Server is configured normally.

Configuration flowchart

The process for configuring DHCP Relay Policy mode is shown as figure below.

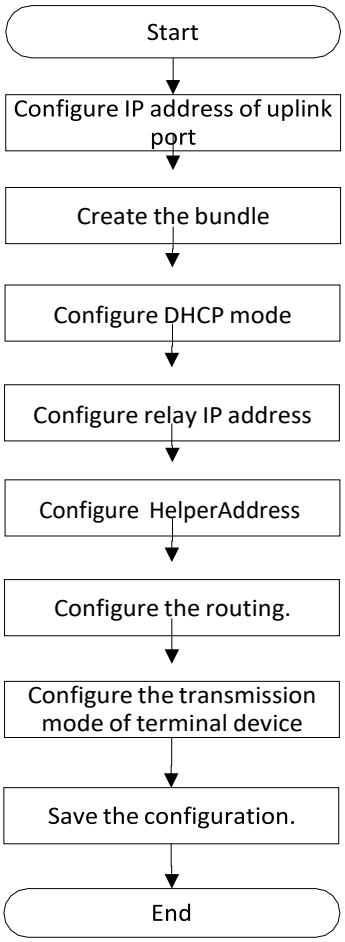

Figure 7-5 Flowchart of DHCP L3 Relay Policy Mode

Procedure

Step 1 Configure the primary IP address of the uplink port.

1. Configure the primary IP address of the uplink port.

   ```
   BT(config)# ip address 10.10.28.2 255.255.255.0 primary
   ```

2. Configure the secondary IP address of the uplink port.

   ```
   BT(config)# ip address 10.10.27.2 255.255.255.0 secondary
   ```

Step 2 Create the bundle.

```
BT(config)# interface bundle 1
```

Step 3 Select DHCP Relay mode as policy.

```
BT(config-if-bundle1)# cable dhcp-giaddr policy
```

Step 4 Configure the relay address set for the terminal.

1. Configure the relay address of CM.

   ```
   BT(config-if-bundle1)# ip address 10.10.28.2
   255.255.255.0
   ```

2. Configure the relay address of other CPE.

   ```
   BT(config-if-bundle1)# ip address 10.10.27.2
   255.255.255.0 secondary
   ```

Step 5 Configure IP of DHCP server.

```
BT(config-if-bundle1)# cable helper-address all 10.10.29.211
```

Step 6 Configure the routing.

1. Exit the bundle view.

   ```
   BT(config-if-bundle1)# exit
   ```

2. Configure the routing information.

   ```
   BT(config)# ip route 0.0.0.0 0.0.0.0 10.10.28.1
   ```

Step 7 Configure the data of terminal device type for Layer-3 forwarding.

1. Configure the data with terminal device type as CM for Layer-3 forwarding.

   ```
   BT(config)# cable dhcp-mode cm l3-relay
   ```

   Configure the

2. data with terminal device type as HOST for Layer-3 forwarding.

   ```
   BT(config)# cable dhcp-mode host l3-relay
   ```

   Configure the

3. data with terminal device type as MTA for Layer-3 forwarding.

   ```
   BT(config)# cable dhcp-mode mta l3-relay
   ```

   Configure the

4. data with terminal device type as STB for Layer-3 forwarding.

   ```
   BT(config)# cable dhcp-mode stb l3-relay
   ```

Step 8 Save the configurations.

```
BT(config)# exit
BT# copy running-config startup-config
This will save the configuration to the flash memory.
Are you sure?(y/n) [n]y
Building configuration.....
Configuration saved successfully.
```

Result

After finishing the configuration, CM and other CPE devices acquire IP address from DHCP server automatically via different relays.

7.6 Example of Strict Mode

CM and other terminal devices acquire IP address automatically via different relays through this task.

Context

In case of L3 Relay mode, CMTS device translates the broadcast DHCP packet via relay into the unicast packet and send it to the DHCP Server for cross-network-segment forwarding of DHCP packet. In strict mode, CM and each kind of CPE acquire IP address from DHCP Server at network side through two different relays respectively.

Data Planning

In this example, the data of CM and each kind of CPE are assured of L3 Relay via different relays, all terminal devices acquire IP address by using the universal DHCP Server.

The data planning for configuring DHCP Relay strict mode example is shown as table below.

Table 7-5 Data Planning for DHCP Relay Strict Mode Example

Item	Data
CM transmission mode	l3-relay
HOST transmission mode	l3-relay
MTA transmission mode	l3-relay
STB transmission mode	l3-relay
Global primary IP (IP/MASK)	10.10.28.2/24
Global secondary IP (IP/MASK)	10.10.27.2/24
Global secondary IP (IP/MASK)	10.10.26.2/24
Global secondary IP (IP/MASK)	10.10.25.2/24
bundle item	bundle 1
GiAddr relay mode	strict
Primary relay address (IP/MASK)	10.10.28.2/24
Secondary relay address (IP/MASK)	10.10.27.2/24
Secondary relay address (IP/MASK)	10.10.26.2/24
Secondary relay address (IP/MASK)	10.10.25.2/24
Specify CM to use the relay	10.10.28.2
Specify HOST to use the relay	10.10.27.2
Specify MTA to use the relay	10.10.26.2
Specify STB to use the relay	10.10.25.2
DHCP Server IP	10.10.29.211
Routing information	0.0.0.0 0.0.0.0 10.10.28.1

Prerequisites

- Network devices and lines must be in the normal state.
- DHCP Server is configured normally.

Configuration flowchart

The process for configuring DHCP Relay strict mode is shown as figure below.

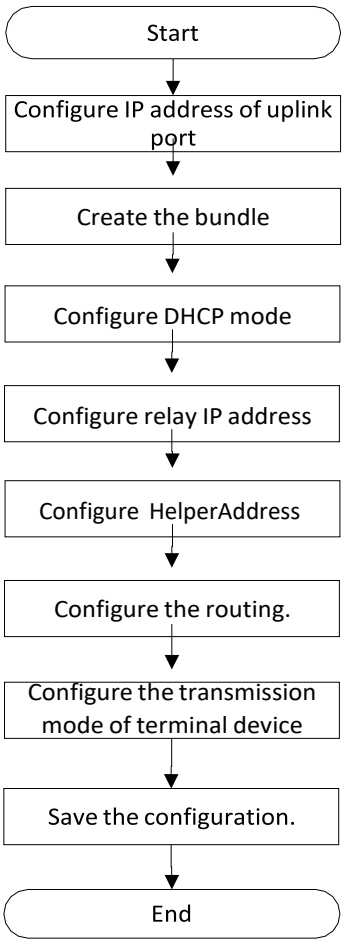

Figure 7-6 Flowchart of DHCP L3 Relay strict Mode

Procedure

Step 1 Configure the primary IP address of the uplink port.

1. Configure the primary IP address of the uplink port.

```
BT(config)# ip address 10.10.28.2          255.255.255.0 primary
```

2. Configure the secondary IP address of the uplink port.

```
BT(config)# ip address 10.10.27.2          255.255.255.0 secondary
```

3. Configure the secondary IP address of the uplink port.

```
BT(config)# ip address 10.10.26.2          255.255.255.0 secondary
```

4. Configure the secondary IP address of the uplink port.

```
BT(config)# ip address 10.10.25.2          255.255.255.0 secondary
```

Step 2 Create the bundle.

```
BT(config)# interface bundle 1
```

Step 3 Select DHCP Relay mode as strict.

```
BT(config-if-bundle1)# cable dhcp-giaddr strict
```

Step 4 Configure the relay address set for the terminal.

1. Configure the primary relay address.

```
BT(config-if-bundle1)# ip address 10.10.28.2
255.255.255.0
```

2. Configure the secondary relay address.

```
BT(config-if-bundle1)# ip address 10.10.27.2
255.255.255.0 secondary
```

3. Configure the secondary relay address.

```
BT(config-if-bundle1)# ip address 10.10.26.2
255.255.255.0 secondary
```

4. Configure the secondary relay address.

```
BT(config-if-bundle1)# ip address 10.10.25.2
255.255.255.0 secondary
```

5. Specify the relay address to be used by CM.

```
BT(config-if-bundle1)# cable dhcp-giaddr cm 10.10.28.2
```

6. Specify the relay address to be used by HOST.

```
BT(config-if-bundle1)# cable dhcp-giaddr host 10.10.27.2
```

7. Specify the relay address to be used by MTA.

```
BT(config-if-bundle1)# cable dhcp-giaddr mta 10.10.26.2
```

8. Specify the relay address to be used by STB.

```
BT(config-if-bundle1)# cable dhcp-giaddr stb 10.10.25.2
```

Step 5 Configure IP of DHCP server.

```
BT(config-if-bundle1)# cable helper-address all 10.10.29.211
```

Step 6 Configure the routing.

1. Exit the bundle view.

```
BT(config-if-bundle1)# exit
```

2. Configure the routing information.

```
BT(config)# ip route 0.0.0.0 0.0.0.0 10.10.28.1
```

Step 7 Configure the data of terminal device type for Layer-3 forwarding.

1. Configure the data with terminal device type as CM for Layer-3 forwarding.

```
BT(config)# cable dhcp-mode cm l3-relay
```

2. Configure the data with terminal device type as HOST for Layer-3 forwarding.

```
BT(config)# cable dhcp-mode host l3-relay
```

3. Configure the data with terminal device type as MTA for Layer-3 forwarding.

```
BT(config)# cable dhcp-mode mta l3-relay
```

4. Configure the data with terminal device type as STB for Layer-3 forwarding.

```
BT(config)# cable dhcp-mode stb l3-relay
```

Step 8 Save the configurations.

```
BT(config)# exit
BT# copy running-config startup-config
This will save the configuration to the flash memory.
```

```
Are you sure?(y/n) [n]y

Building configuration.....
Configuration saved successfully.
```

Result

After finishing the configuration, CM and each kind of CPE device will acquire IP address automatically from the secondary DHCP server via different relays.

7.7 Example of Dynamic IP Acquired

CMTS device achieves data transparent transmission through this task.

Context

In case of L3 Relay mode, CMTS device translates the broadcast DHCP packet via relay into the unicast packet and send it to the DHCP Server for cross-network-segment forwarding of cross-DHCP packet. When the terminal device fails to find giAddr, it takes the dynamically-acquired IP address as the device address.

Data Planning

In this example, configure all terminal devices take the dynamic IP for data transmission, and acquire IP address from DHCP Server.

The data planning for the example of configuring DHCP dynamic IP acquired is shown as table below.

Table 7-6 Data Planning for Dynamic IP Acquired

Item	Data
CM transmission mode	l3-relay
HOST transmission mode	l3-relay
MTA transmission mode	l3-relay
STB transmission mode	l3-relay
Relay address	Dynamic IP address
bundle item	bundle 1
DHCP Server	10.10.29.211

Prerequisites

- Network devices and lines must be in the normal state.
- DHCP Server is configured normally.

Configuration flowchart

The process for configuring dynamic IP as relay address is shown as figure below.

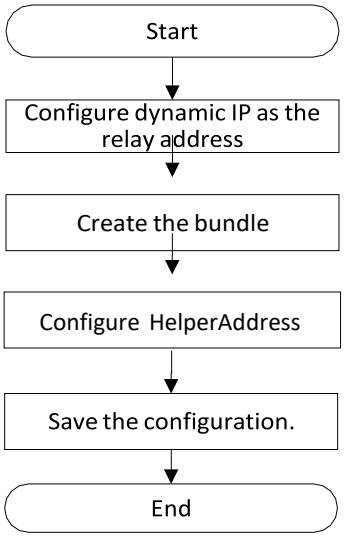

Figure 7-7 Flowchart of Dynamic IP Relay Address

Procedure

Step 1 Configure dynamic IP acquired.

```
BT(config)# ip address dhcp-alloc
```

Step 2 Create the bundle.

```
BT(config)# interface bundle 1
```

Step 3 Configure IP of DHCP server.

```
BT(config-if-bundle1)# cable helper-address all 10.10.29.211
```

Step 4 Configure the data of terminal device type for Layer-3 forwarding.

1. Configure the data with terminal device type as CM for Layer-3 forwarding.

   `BT(config)# cable dhcp-mode cm l3-relay` Configure the

2. data with terminal device type as HOST for Layer-3 forwarding.

   `BT(config)# cable dhcp-mode host l3-relay` Configure the

3. data with terminal device type as MTA for Layer-3 forwarding.

   `BT(config)# cable dhcp-mode mta l3-relay` Configure the

4. data with terminal device type as STB for Layer-3 forwarding.

   `BT(config)# cable dhcp-mode stb l3-relay`

Step 5 Save the configurations.

```
BT(config)# exit
BT# copy running-config startup-config
This will save the configuration to the flash memory.
Are you sure?(y/n) [n]y
Building configuration.....
Configuration saved successfully.
```

Result

After finishing the configuration, all terminal devices under CMTS can acquire IP address automatically from DHCP server via dynamic IP.

7.8 Example of Multiple Bundles under DHCP Snooping

A bundle is a collection of DHCP configurations, which is just a logical division without any actual physical significance. It allows to set different giAddr for the CM/CPE for different services, and divides CM into different address pools. CM/CPE becomes online through different configuration files to achieve the division of different services.

Data Planning

In this example, configure transparent transmission of the data of CM | host | MTA | STB,

We need create two bundles, bundle 2 with relay address 10.10.27.50/24 & 2000::x/64 and bundle 3 with the address 10.10.28.50/24 & 3000::x/64. The relay IP address is only a virtual address, used to select bundle, not a real IPv4 or IPv6 address.

CMs will select the smallest number bundle 2 at the discovery stage, and at the request stage, according to server configuration select the matched bundle 2 or 3.

CPE will directly select the CM bundle it connected. When select bundle 2, the CMTS device will add VLAN tag 100 for the packets it forwards; and when select bundle 3, the CMTS device will add VLAN tag 200 for the packets it forwards.

The data planning for configuring the multiple bundles under DHCP snooping example is shown as table below.

Table 7-7 Data Planning for Multiple Bundles under DHCP Snooping

Item	Data
Bundle item	bundle 2/3
Relay address for bundle 2	IPv4: 10.10.27.50/24 IPv6:2000::x/64
Relay address for bundle 3	IPv4: 10.10.28.50/24 IPv6:3000::x/64
CM DHCP tag for bundle 2	100
Host DHCP tag for bundle 2	100
MTA DHCP tag for bundle 2	100
STB DHCP tag for bundle 2	100
CM DHCP tag for bundle 3	200
Host DHCP tag for bundle 3	200
MTA DHCP tag for bundle 3	200
STB DHCP tag for bundle 3	200
CM transmission mode	snooping
Host transmission mode	snooping
MTA transmission mode	snooping

STB transmission mode	snooping

Item	Data
DHCP Server	Normal configuration. It can communicate with the device by means of ping; CMTS is not required to configure the address of the DHCP Server, but just transmit transparently the packet to the layer-3 device for relay to the DHCP Server by the uplink port.

Prerequisites

- Network devices and lines must be in the normal state.
- DHCP Server is configured normally.

Configuration flowchart

The process for configuring multiple bundles under DHCP snooping is shown as figure below.

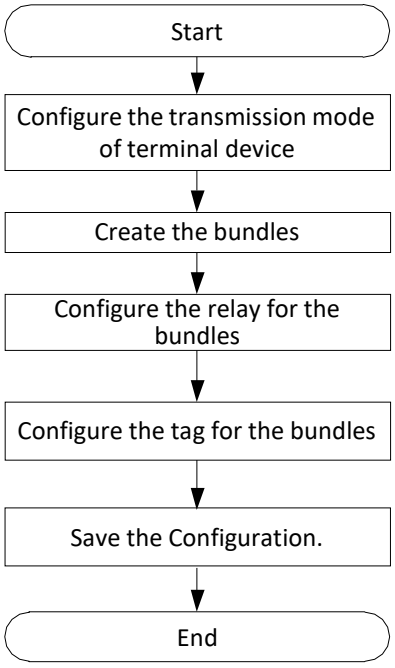

Figure 7-8 Flowchart for Multiple Bundles under DHCP Snooping

Procedure

Step 1 Configure the data of terminal device type for transparent transmission.

1. Configure the data with terminal device type as CM for transparent transmission.
   `BT(config)# cable dhcp-mode cm snooping`
2. Configure the data with terminal device type as host for transparent transmission.
   `BT(config)# cable dhcp-mode host snooping` Configure the data
3. with terminal device type as MTS for transparent transmission.`BT(config)# cable dhcp-mode mta snooping`
4. Configure the data with terminal device type as STB for transparent transmission.
   `BT(config)# cable dhcp-mode stb snooping`

➢ For the bundle 2:

Step 1 Create the bundle 2.

```
BT(config)# interface bundle 2
```

Step 2 Add the DHCP relay for the bundle 2.

1. Add the DHCP relay 10.10.27.50/24 for the bundle 2. `BT(config-if-bundle2)# ip address 10.10.27.50255.255.255.0`
2. Add the DHCP relay 2000::2/64 for the bundle 2.

```
BT(config-if-bundle2)# ipv6 address 2000::2/64
```

Step 3 Add a VLAN tag to data of the CPE.

1. Add the IPv4 VLAN tag 100 to the packets of CM, with priority as 7. `BT(config-if-bundle2)# cable dhcp-tag cm vlan 100priority 7`
2. Add the IPv4 VLAN tag 100 to the packets of host, with priority as 7.

```
BT(config-if-bundle2)# cable dhcp-tag host vlan 100
priority 7
```

3. Add the IPv4 VLAN tag 100 to the packets of MTA, with priority as 7.

```
BT(config-if-bundle2)# cable dhcp-tag mta vlan 100
priority 7
```

4. Add the IPv4 VLAN tag 100 to the packets of STB, with priority as 7.

```
BT(config-if-bundle2)# cable dhcp-tag stb vlan 100
priority 7
```

5. Add the IPv6 VLAN tag 100 to the packets of CM, with priority as 7.

```
BT(config-if-bundle2)# cable dhcpv6-tag cm vlan 100
priority 7
```

6. Add the IPv6 VLAN tag 100 to the packets of host, with priority as 7.

```
BT(config-if-bundle2)# cable dhcpv6-tag host vlan 100
priority 7
```

7. Add the IPv6 VLAN tag 100 to the packets of MTA, with priority as 7.

```
BT(config-if-bundle2)# cable dhcpv6-tag mta vlan 100
priority 7
```

8. Add the IPv6 VLAN tag 100 to the packets of STB, with priority as 7.

```
BT(config-if-bundle2)# cable dhcpv6-tag stb vlan 100
priority 7
```

➢ For the bundle 3:

Step 1 Create the bundle 3.

```
BT(config)# interface bundle 3
```

Step 2 Add the DHCP relay for the bundle 3.

1. Add the DHCP relay 10.10.28.50/24 for the bundle 3.

```
BT(config-if-bundle3)# ip address 10.10.28.50
255.255.255.0
```

2. Add the DHCP relay 3000::2/64 for the bundle 3.

```
BT(config-if-bundle3)# ipv6 address 3000::2/64
```

Step 3 Add a VLAN tag to data of the CPE.

1. Add the VLAN tag 200 to the packets of CM, with priority as 7. `BT(config-if-bundle3)# cable dhcp-tag cm vlan 200priority 7`
2. Add the VLAN tag 200 to the packets of host, with priority as 7.

```
BT(config-if-bundle3)# cable dhcp-tag host vlan 200
priority 7
```

3. Add the VLAN tag 200 to the packets of MTA, with priority as 7.

```
BT(config-if-bundle3)# cable dhcp-tag mta vlan 200
priority 7
```

4. Add the VLAN tag 200 to the packets of STB, with priority as 7.

```
BT(config-if-bundle3)# cable dhcp-tag stb vlan 200
priority 7
```

Step 4 Save the configurations.

```
BT(config)# end
BT# copy running-config startup-config
This will save the configuration to the flash memory.
Are you sure?(y/n) [n]y
Building configuration.....
Configuration saved successfully.
```

Result

After finishing the configurations, the terminals under CMTS such as CM/HOST/MTA/STB can acquire IP address automatically from DHCP Server by transparent transmission, and identify the device type with VLAN.

7.9 Example of Multiple Bundles under DHCP Layer3

Context

Refer to 7.8 Configuring multiple instances bundle under snooping mode.

Data Planning

In this example, the configuration terminal device includes three layers of data forwarding from CM | host | STB.

It is necessary to set bundle 2 and bundle 3, where the relay address of bundle 2 is 10.10.10/24 and that of bundle 3 is 11.11.11/24. The relay IP address needs to be real on CMTS.

CM chooses bundle 2 in Discovery phase, bundle 2 in Request phase according to DHCP server, and CPE directly chooses to connect the bundle to which CM belongs. When CM/CPE chooses bundle 2, the message is forwarded by relay 10.10.10/24, and when CM/CPE chooses bundle 3, the message is forwarded by relay 11.11.11/24.

Configuring multi-bundle data planning is shown in the following table.

Table 7-8 Data Planning for Multiple Bundles under DHCP Layer3

Item	Data
bundle item	bundle 2/3
relay address for bundle 2	10.10.10.10/24
relay address for bundle 3	11.11.11.11/24
DHCP Server address	172.168.10.10
Route address	172.168.10.10 10.10.10.10
CM transmission mode	l3-relay
Host transmission mode	l3-relay
STB transmission mode	l3-relay

Prerequisites

- Network devices and lines must be in the normal state.
- DHCP Server is configured normally.

Configuration flowchart

The process for configuring multiple bundles under DHCP layer3 is shown as figure below.

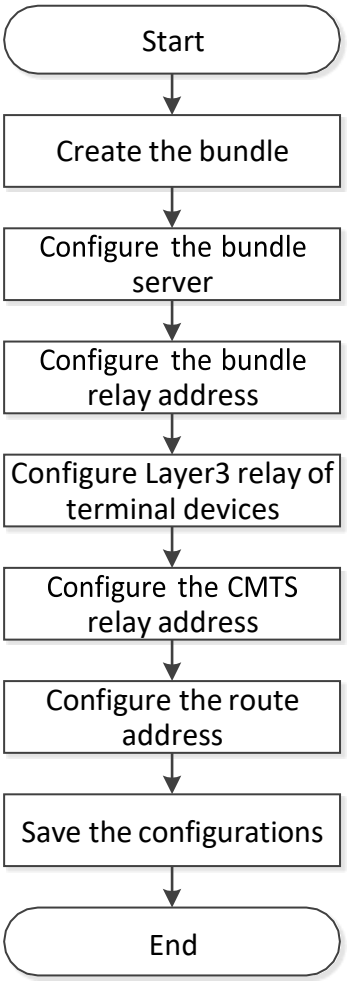

Figure 7-9 Flowchart for Multiple Bundles under DHCP Layer3

Procedure

➢ For the bundle 2:

Step 1 Create the bundle 2.

```
BT(config)# interface bundle 2
```

Step 2 Add the DHCP server as 172.168.10.10 for the bundle 2.

```
BT(config-if-bundle2)# cable helper-address all
172.168.10.10
```

Step 3 Add the DHCP relay as 10.10.10.10/24 for the bundle 2.

```
BT(config-if-bundle2)# ip address 10.10.10.10 255.255.255.0
```

➢ For the bundle 3:

Step 1 Create the bundle 3.

```
BT(config)# interface bundle 3
```

Step 2 Add the DHCP server as 172.168.10.10 for the bundle 3.

```
BT(config-if-bundle3)# cable helper-address all
172.168.10.10
```

Step 3 Add the DHCP relay as 11.11.11.11/24 for the bundle 3.

```
BT(config-if-bundle3)# ip address 11.11.11.11 255.255.255.0
```

Step 4 Configuring Layer 3 forwarding packets of terminal device type.

1. Configuring Layer 3 forwarding packets of CM. `BT(config)#`
   `cable dhcp-mode cm l3-relay`Configuring Layer 3
2. forwarding packets of host.
   `BT(config)#` **`cable dhcp-mode host l3-relay`**
3. Configuring Layer 3 forwarding packets of STB. `BT(config)#`
   `cable dhcp-mode stb l3-relay`

Step 5 Configuring the CMTS device relay address.

1. Configuring the CMTS device relay address as 10.10.10.10/24.
   `BT(config)#` **`ip address 10.10.10.10 255.255.255.0 primary`**
2. Configuring the CMTS device relay address as 11.11.11.11/24.
   `BT(config)#` **`ip address 11.11.11.11 255.255.255.0 primary`**

Step 6 Configuring the CMTS device route address.

`BT(config)#` **`ip route 172.168.10.10 10.10.10.10`**

Step 7 Save the configurations.

```
BT(config)# end
BT# copy running-config startup-config
This will save the configuration to the flash memory.
Are you sure?(y/n) [n]y
Building configuration.....
Configuration saved successfully.
```

Result

After finishing the configurations, CMs will select the smallest number bundle 2 at the discovery stage, and at the request stage, according to server configuration select the matched bundle 2 or 3.

CPE will directly select the CM bundle it connected. When select bundle 2, the CMTS device will forward the packets through the relay 10.10.10.10/24; and when select bundle 3, the CMTS device will forward the packets through the relay 11.11.11.11/24.

7.10 Create Bundles and Selection Rules

A bundle is a collection of DHCP configurations, which is just a logical division without any actual physical significance. It allows to set different giAddr for the CM/CPE for different services, and divides CM into different address pools. CM/CPE becomes online through different configuration files to achieve the division of different services.

Context

CMTS device supports 32 bundles, the range of 1-32.

When the device in a multi-bundle, bundle selection rules are as follows:

During DHCPv4 Discover Process of CM:

1. CM select the smallest number bundle matching the packet VLAN and the bundle VLAN;
2. When the selection of bundle is not successful, if the DHCP mode is l3-relay, packets will be discarded; if the DHCP mode is l2-relay | snooping, it transparently transmits the packet.

During DHCPv4 Request Process of CM:

1. CM prefers the bundle which the request IP + packet VLAN and the bundle IP address VLAN matches, the packet VLAN and bundle VLAN matches.
2. If condition 1 is not met, then CM select the bundle which the request IP + untag and the IP address VLAN + untag matches, the packet VLAN and bundle VLAN matches.
3. If condition 2 is not met, then CM select the smallest number bundle which the packet VLAN and the I bundle VLAN matches.
4. When the selection of bundle is not successful, if the DHCP mode is l3-relay, packets will be discarded; if the DHCP mode is l2-relay | snooping, it transparently transmits the packet.

During DHCPv4 Discover Process of CPE:

1. CPE prefers the bundle which the CPE connected CM selected, packet VLAN and bundle VLAN matches.
2. When the selection of bundle is not successful, if the DHCP mode is l3-relay, packets will be discarded; if the DHCP mode is l2-relay | snooping, it transparently transmits the packet.

During DHCPv4 Request Process of CPE:

1. CPE prefers the bundle which the request IP and the bundle IP address matches, the packet VLAN and bundle VLAN matches.
2. When the selection of bundle is not successful, if the DHCP mode is l3-relay, packets will be discarded; if the DHCP mode is l2-relay | snooping, it transparently transmits the packet.

Procedure

Step 1 Create a bundle and enter the bundle view by using the command "**`interface bundle`**".

Step 2 View the information of the bundles by using the command "**`show interface bundle all`**".

Example

$ Create bundle 3 and enter bundle view:

```
BT(config)# interface bundle 3
BT(config-if-bundle3)# show interface bundle all
!
```

```
interface bundle 3
 cable  dhcp-giaddr  primary
 cable source verify enable
 cable ipv6 source verify enable
 cable source verify leasequery-filter upstream 5 10
exit
```

Related Operations

Table 7-9 Related Operations of Create Bundles

Operation	Command	Remarks
Delete the bundle and its configuration	**no interface bundle**	

7.11 Configure Helper-Address

Some DHCP messages, for example DHCP Discover, are broadcast packets. When the DHCP Relay required to forward packets across the network, while broadcast packets are usually unable to pass through the layer 3 device, so you need to specify the destination address to forward DHCP messages that is helper-address, this address is usually the IP address of the DHCP Server.

Different types of devices may share the same DHCP server, or use different DHCP server. Therefore DHCP Relay provides two helper-address configuration modes: 1. Universal helper-address; 2. The specified helper-address for the device type.

Meanwhile DHCP Relay allows to set more than one helper-address for the device. After setting, it will forward multiple DHCP packets to multiple helper-address simultaneously. This configuration is mainly applicable to the redundant backup scenario.

7.11.1 Configure the Universal Helper-Address

Context

- The device supports DHCP general server configuration in IPv4 environment.
- All devices without configuring the dedicated Helper-Address use the universal Helper-Address.
- It allows to configure multiple (at most 5) universal Helper-Address. After finishing the configuration, CMTS device will forward DHCP packet to multiple Helper-Address.
- The configurations of universal Helper-Address can be deleted by using the corresponding “no” command.

Procedure

Step 1 Set universal Helper-Address of the device by using the command “**cable helper-address all**”.

Step 2 View the Helper-Address configured for the device by using the command "**show running-config**".

Example

Configure the universal Helper-Address:

```
BT(config-if-bundle1)#  cable  helper-address  all  10.10.29.211
BT(config-if-bundle1)#  cable  helper-address  all  10.10.29.209
BT(config-if-bundle1)# show running-config
 cable helper-address all 10.10.29.211
 cable helper-address all 10.10.29.209
 ip address 10.10.28.88 255.255.255.0
```

Related Operations

Table 7-10 Related Operations for Configure the Universal Helper-Address

Operation	Command	Remarks
Delete the universal Helper-Address	**no cable helper-address**	

7.11.2 Configure the Dedicated Helper-Address

Context

- It allows to configure the dedicated Helper-Address for all terminals such as CM, HOST, MTA, STB and device (user-defined). After the configuration, CMTS device will forward the DHCP packet to the dedicated Helper-Address by terminal device type.
- After the dedicated Helper-Address is configured for a terminal device type, CMTS will not forward the DHCP request of such terminal device to the universal Helper-Address.
- Each terminal device can be configured multiple (at most 5) dedicated Helper-Address. After finishing the configuration, CMTS device will forward DHCP packet to multiple dedicated Helper-Address simultaneously.
- The configuration of universal Helper-Address can be deleted by using the corresponding "no" command.

Procedure

Step 1 Set dedicated Helper-Address of the device by using the command "**cable helper-address (cm | host | mta | stb |** *device*)".

Step 2 View the configured Helper-Address of the device by using the command "**show running-config**".

Example

Configure the dedicated Helper-Address of CM:

```
BT(config-if-bundle1)#   cable   helper-address   cm   10.10.29.211
BT(config-if-bundle1)#   cable   helper-address   cm   10.10.29.213
BT(config-if-bundle1)# show running-config | include cm
 cable helper-address cm 10.10.29.211
 cable helper-address cm 10.10.29.213
```

Related Operations

Table 7-11 Related Operations for Configure the Dedicated Helper-Address

Operation	Command	Remarks
Delete the dedicated Helper-Address	**no cable helper-address (cm | host | mta | stb** | *device*)	When all dedicated Helper-Addresses of a terminal device, such terminal will be online with universal Helper-Address.

7.12 Configure User-defined Device

Option 60 is used to identify different terminal types, so L3 relay can assign different IP addresses according to terminal types.

- CMTS devices default support for C-DOCSIS standard defined strings.
- CMTS supports configuring options 60 strings for terminal types in order to be more compatible with vendors'devices.
- When users need to plan their business according to different terminal types and standard terminal types (CM/HOST/MTA/STB) can not meet the requirements, users can also configure custom terminal types, and configure option 60 string for custom terminal types.

Option 60 strings are specified in the C-DOCSIS standard as shown in the following table. Users need to avoid the default strings specified in the standard when configuring them. (Option fields are case-insensitive, i.e., characters such as "STB" or "sTb" will be recognized as "stb".) :

Table 7-12 Option60 Keyword Configuration Parameter

Device	Option60 string	Description
Cable Modem	String starting with “docsis”	The subsequent string can include docsis version and capability supported by CM; Cable Modem includes independent CM terminal and embedded CM, such as embedded CM in STB.
MTA	String starting with “pktc”	The subsequent string can include PacketCable version and capability supported by the device.
Set-top box	String starting with “stb”	The subsequent string can describe the capability of the device.

Context

- If Option60 can match multiple strings simultaneously, the priority is: the defined string > longer string > front string.
- 4 different Option60 strings can be configured for the same terminal type.
- Option 60 supports up to 16 characters.
- The configuration of Option60 can be deleted by using the corresponding "no" command.

Procedure

Step 1 Configure user-defined device by using the command "**cable dhcp device**".

Step 2 Configure Option60 string of the device by using the command "**cable dhcp-option60**".

Step 3 View the configured option60 of the device by using the command "**show running-config**".

Example

Configure user-defined device:

```
BT(config-if-bundle1)# cable dhcp device cablemodem
BT(config-if-bundle1)# cable dhcp-option60 cablemodem cablemodemIPv4
BT(config-if-bundle1)# show running-config | include option
cable dhcp-option60 cablemodem 1 "cablemodemIPv4"
```

Related Operations

Table 7-13 Related Operations Option 60

Operation	Command	Remarks
Delete the user-defined device type	**no cable dhcp device**	
Delete the option60 configuration	**no cable dhcp-option60**	

7.13 Configure DHCP Tags

Dhcp-tag function can be used to add VLAN tags to different device type by bundle. The upper device of CMTS such as switch will perform the DHCP relay by the tag. By this approach, different giAddr can be inserted in different devices and classified into different address pools.

Context

- Dhcp-tag function supports the DHCP mode is l2-relay, snooping, and l3-relay.
- Dhcp-tag function can be used to add VLAN tag to different devices by bundle, and the upper device of CMTS such as switch will perform the DHCP relay by the tag further. By this approach, different giAddr can be inserted in different devices and classified into different address pools.
- In case of multiple bundles, by default, CM belongs to the first bundle, and CPE belongs to the bundle of

CM. in case of request, confirm bundle by the network segment again. If it is impossible to match with the ip address segment, configure the forwarding by the default bundle.

Procedure

Step 1 Configure VLAN tags of the device by using the command "**cable dhcp-tag**".

Step 2 View the configured VLAN tags of the device by using the command "**show running-config**".

Example

Configure STB to add VLAN 100 tag, with priority as 7:

```
BT(config-if-bundle2)# cable dhcp-tag stb vlan 100 priority 7
BT(config-if-bundle2)# show running-config | include dhcp-tag
 cable dhcp-tag stb vlan 100 priority 7
```

Related Operations

Table 7-14 Related Operations of Dhcp-tag

Operation	Command	Remarks
Delete DHCP Tag of dedicated terminal type	**no cable dhcp-tag**	

7.14 DHCP information option circuit-id-prefix

Option 82.1 Circuit ID is used to configure user information, which is conducive to judging the source of network messages. It is mainly used for security checking, such as preventing IP spoofing, user identifier spoofing and MAC address spoofing.

Working process:

- CMTS receives DHCP messages from terminal devices and forwards them to DHCP server with option 82. DHCP server is responsible for identifying the option82 information added to the DHCP message and making corresponding processing according to the information.
- CMTS receives DHCP message from DHCP server, removes option 82 and forwards it to the corresponding terminal device.

Context

- Format of circuit-id-prefix: Hexadecimal or String
- Default configuration of circuit-id-prefix: *hostname*(BT)
- Option 82 strings support input of up to 64 characters.
- Option 82 configuration can be deleted by the corresponding "no" command.

Procedure

Step 1 Configure the circuit-id-prefix by using the command "**dhcp information option circuit-id-prefix (hex | string)**".

Step 2 Query the **circuit-id-prefix** value by using the command "**show dhcp circuit-id-prefix**".

Example

Configure the circuit ID as string representation BT .

```
BT(config)# dhcp information option circuit-id-prefix string BT
BT(config)# show dhcp circuit-id-prefix
Hex Format        :746f7076697369f6e
String Format     :BT
```

Related Operations

Table 7-15 Related Operations of DHCP information option circuit-id-prefix

Operation	Command	Remarks
Delete the circuit-id-prefix value	**no dhcp information option circuit-id-prefix**	The default value is hostname.
Display the configuration of circuit-id-prefix	**show dhcp circuit-id-prefix**	

Chapter 8 DHCPv6 Relay Function

8.1 Overview

Terminals (including the CM and CPE) can communicate with DHCPv6 servers in other network segments through the DHCPv6 relay. In this way, service terminals can obtain IP addresses in different network segments and go on line normally.

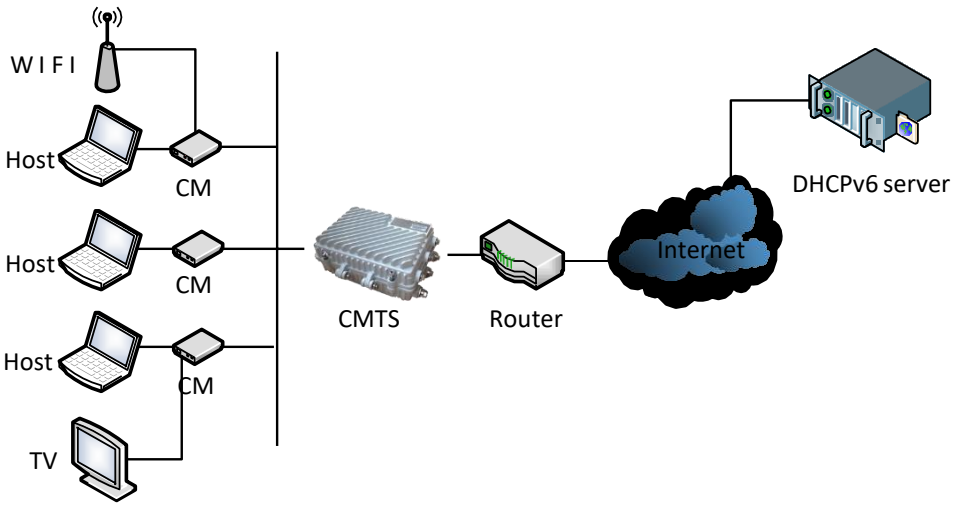

Figure 8-1 Networking Diagram of CMTS Device

The CMTS supports the following DCHP relay function:

- DHCPv6 relay modes

  The CMTS supports the following DHCPv6 forwarding modes:

  - Snooping mode: The CMTS monitors the DHCPv6 interaction process. It directly forwards packets without making any modification. This mode is applicable to the scenario where an upstream device serves as the DHCPv6 relay and the CMTS only forwards data.
  - L2-relay mode: This mode is applicable to the scenario where an upstream device forwards data at L3 and the CMTS only forwards data at L2. It is also applicable to a simple networking scenario. For example, the DCHP server, CMTS, and terminal work in the same network segment, and data does not need to be forwarded across network segments. In this mode, the CMTS supports insertion of option 82 to check the validity of the DHCPv6 packet source.
  - L3-relay mode: In this mode, the CMTS works as a L3 relay so that service terminals can obtain IP addresses in different network segments. The L3-relay mode further consists of the following modes:

- DHCPv6 server

  The DHCPv6 server configuration includes the common DHCPv6 server and the dedicated DHCPv6 server.

  - Common DHCPv6 server: It is the DHCPv6 server shared by different types of terminals.

- Dedicated DHCPv6 server: It is the DHCPv6 server used by a specific type of terminals.

➢ Option vendor class keyword

Option vendor class is used to identify different terminal types so that service types can be differentiated based on the terminal type. It is applicable to the snooping, L2-relay, and L3-relay modes.

➢ Dhcpv6-tag

With the dhcpv6-tag function, a VLAN tag can be added to different device types by bundle. It is applicable to the snooping, L2-relay, and L3-relay modes.

➢ Option18 keyword

The Option18 circuit ID is used to configure the user information so as to determine the source of network packets. It is mainly used for security check. It is applicable to the L2-relay and L3-relay modes.

8.2 Example of DHCPv6 Snooping

Achieve data transparent transmission by CMTS device through this task.

Context

CMTS device provides the DHCPv6 layer-2 Relay service. The device receives the packet from client, and add option82 for forwarding; the device receives the packet from DHCPv6 Server, and removes option82 for forwarding. At this time, the terminal devices such as CM/CPE can acquire the IP address from DHCPv6 Server at the network side via Relay that is the layer-3 device connected the CMTS's uplink port. And CMTS can support identifying the device type with VLAN tag.

Data Planning

In this example, configure L2 Relay against the data of terminals such as HOST | MTA | STB | cablemodem, and have the layer-3 switch to implement the Relay operation, and set Option60 field to distinguish the terminal types.

The data planning for configuring the DHCPv6 transparent transmission example is shown as table below.

Table 8-1 Data Planning for DHCPv6 Transparent Mode

Item	Data
CM transmission mode	DHCPv6 snooping
HOST transmission mode	DHCPv6 snooping
MTA transmission mode	DHCPv6 snooping
STB transmission mode	DHCPv6 snooping
bundle item	bundle 1
HOST option vendor class	host-option
MTA option vendor class	mta-option
STB option vendor class	settopbox-option

Item	Data
User-defined cablemodem option option vendor class	userdefine-cabmo
CM initial maintenance	IPv6 only mode
DHCPv6 Server	Normal configuration. It can communicate with the device by means of ping; CMTS is not required to configure the address of DHCPv6 Server, but just forward the Layer-2 packet to the layer-3 uplink device for relay to DHCPv6 Server by the uplink port.

Prerequisites

- Network devices and lines must be in the normal state.
- DHCPv6 Server is configured normally.

Configuration flowchart

The process for DHCPv6 transparent transmission is shown as figure below.

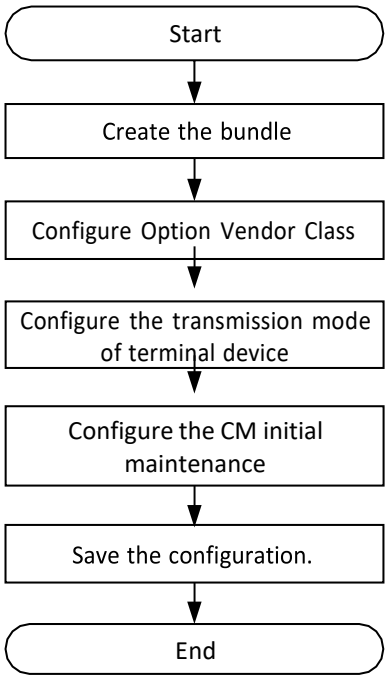

Figure 8-2 Flowchart of Configuring Option Identification Terminal in Snooping Mode

Procedure

Step 1 Create the bundle.

```
BT(config)# interface bundle 1
```

Step 2 Configure the option60 identifiers for the terminal device.

1. Option vendor class identifier of HOST is host-option.

```
BT(config-if-bundle1)# cable dhcpv6-option vendor-classhost
host-option
```

2. Option vendor class of MTA is mta-option.

```
BT(config-if-bundle1)# cable dhcpv6-option vendor-classmta
mta-option
```

3. Option vendor class identifier of STB is settopbox-option.

```
BT(config-if-bundle1)# cable dhcpv6-option vendor-classstb
settopbox-option
```

4. Option vendor class identifier of the user-defined device type “cablemodem” is userdefine-cabmo. IPv6 vendor class of the user-defined device type “cusprequip” is userdefine-cpe.

```
BT(config-if-bundle1)# cable dhcpv6 device cablemodem
BT(config-if-bundle1)# cable dhcpv6-option vendor-class
cablemodem userdefine-cabmo
```

Step 3 Configure the data of terminal device type for transparent transmission.

1. Exit the bundle view.

```
BT(config-if-bundle1)# exit
```

2. Configure the DHCPv6 data with terminal device type as HOST for transparent transmission.

```
BT(config)# cable dhcpv6-mode host snooping
```

3. Configure the data with terminal device type as MTS for transparent transmission.

```
BT(config)# cable dhcpv6-mode mta snooping
```

4. Configure the data with terminal device type as STB for transparent transmission.

```
BT(config)# cable dhcpv6-mode stb snooping
```

5. Configure the data with terminal device type as cablemodem for transparent transmission.

```
BT(config)# cable dhcpv6-mode cablemodem snooping
```

Step 4 Configure the CM initial maintenance.

1. Enter the cmts view.

```
BT(config)# interface cmts 1
```

2. Configure the CM initial maintenance as DHCPv6 only.

```
BT(config-if-cmts-1)# cable ip-init ipv6
```

Step 5 Save the configurations.

```
BT(config-if-cmts-1)# end
BT# copy running-config startup-config
This will save the configuration to the flash memory.
Are you sure?(y/n) [n]y
Building configuration.....
Configuration saved successfully.
```

Result

After finishing the configurations, the terminals under CMTS such as HOST/MTA/STB and user-defined device can acquire IP address automatically from DHCPv6 Server by transparent transmission.

8.3 Example of DHCPv6 L2 Relay

Achieve the transparent data transmission by CMTS device through this task.

Context

CMTS device provides DHCPv6 Snooping service, and just listens to DHCPv6 data instead of processing. At this time, the terminal devices such as CM/CPE can acquire the IP address from DHCPv6 Server at the network side via Relay that is the layer-3 device connected the CMTS's uplink port. And CMTS can support identifying the device type with VLAN tag.

Data Planning

In this example, configure transparent transmission of the data of CM | HOST | MTA | STB| cablemodem, and have the layer-3 switch to implement the Relay operation, and set VLAN tags for several kinds of terminal devices to determine the device types.

The data planning for configuring the DHCPv6 transparent transmission example is shown as table below.

Table 8-2 Data Planning for DHCPv6 Snooping Mode

Item	Data
CM transmission mode	DHCPv6 l2-relay
HOST transmission mode	DHCPv6 l2-relay
MTA transmission mode	DHCPv6 l2-relay
STB transmission mode	DHCPv6 l2-relay
Custom type cablemodem transmission mode	l2-relay
bundle item	bundle 1
CM DHCP Tag	vlan 1 priority 7
HOST DHCP Tag	vlan 2 priority 7
MTA DHCP Tag	vlan 3 priority 4
STB DHCP Tag	vlan 4 priority 4
Custom type cablemodem tag transmission mode	vlan 5 priority 7
DHCP Server	Normal configuration. It can communicate with the device by means of ping; CMTS is not required to configure the address of DHCP Server, but just transmit transparently the packet to the layer-3 device for relay to DHCP Server by the uplink port.

Prerequisites

- Network devices and lines must be in the normal state.
- DHCPv6 Server is configured normally.

Configuration flowchart

The process for configuring DHCPv6 transparent mode is shown as figure below.

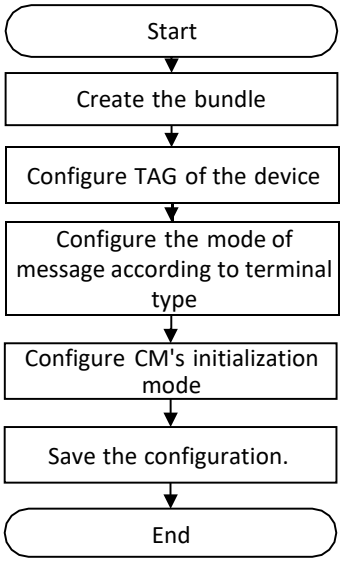

Figure 8-3 Flowchart of Configuring Option Terminal Type in Relay Mode

Procedure

Step 1 Create the bundle.

```
BT(config)# interface bundle 1
```

Step 2 Add a VLAN tag to data of the terminal device.

1. Add VLAN 1 tag to the data of CM, with priority as 7.

```
BT(config-if-bundle1)# cable dhcpv6-tag cm vlan 1 priority 7
```

2. Add VLAN 2 tag to the data of HOST, with priority as 7.

```
BT(config-if-bundle1)# cable dhcpv6-tag host vlan 2 priority7
```

3. Add VLAN 3 tag to the data of MTA, with priority as 4.

```
BT(config-if-bundle1)# cable dhcpv6-tag mta vlan 3 priority4
```

4. Add VLAN 4 tag to the data of STB, with priority as 4.

```
BT(config-if-bundle1)# cable dhcpv6-tag stb vlan 4 priority4
```

5. Option vendor class identifier of the user-defined device type “cablemodem” is userdefine-cabmo. Add VLAN 4 tag to the data of STB, with priority as 7.

```
BT(config-if-bundle1)# cable dhcp device cablemodem BT(config-if-bundle1)# cable dhcpv6-tag cablemodem vlan 5priority 7
```

Step 3 Configure the layer-2 forwarding against the data of terminal device.

1. Exit the bundle view.

```
BT(config-if-bundle1)# exit
```

2. Configure the data of terminal device-CM for layer-2 forwarding.

```
BT(config)# cable dhcpv6-mode cm l2-relay
```

3. Configure the data of terminal device-HOST for layer-2 forwarding.

```
BT(config)# cable dhcpv6-mode host l2-relayConfigure
```

4. the data of terminal device-MTA for layer-2 forwarding.

```
BT(config)# cable dhcpv6-mode mta l2-relay
```

5. Configure the data of terminal device-STB for layer-2 forwarding. `BT(config)# cable dhcpv6-mode stb l2-relay` Configure the data of terminal
6. device-cablemodem for layer-2 forwarding. `BT(config)# cable dhcpv6-mode cablemodem l2-relay`

Step 4 Configure the CM initial maintenance.

1. Enter the cmts view.

```
BT(config)# interface cmts 1
```

2. Configure the CM initial maintenance as DHCPv6 only.

```
BT(config-if-cmts-1)# cable ip-init ipv6
```

Step 5 Save the configurations.

```
BT(config-if-cmts-1)# end
BT# copy running-config startup-config
This will save the configuration to the flash memory.
Are you sure?(y/n) [n]y
Building configuration.....
Configuration saved successfully.
```

Result

After finishing the configurations, the terminals under CMTS such as CM/HOST/MTA/STB can acquire IPv6 address automatically from DHCPv6 Server by transparent transmission, and identify the device type with VLAN.

8.4 Example of Multiple Bundles under DHCPv6 Snooping

A bundle is a collection of DHCPv6 configurations, which is just a logical division without any actual physical significance. It allows to set different giAddr for the CM/CPE for different services, and divides CM into different address pools. CM/CPE becomes online through different configuration files to achieve the division of different services. Reference chapter for selection rules of multiple bundles: 8.6Create Bundles and Selection Rules

Data Planning

In this example, configure transparent transmission of the data of CM | host | MTA | STB,

We need create two bundles, bundle 2 with relay address 2000::x/64 and bundle 3 with the address 3000::x/64. The relay IP address is only a virtual address, used to select bundle, not a real IPv4 or IPv6 address.

CMs will select the smallest number bundle 2 at the discovery stage, and at the request stage, according to server configuration select the matched bundle 2 or 3.

CPE will directly select the CM bundle it connected. When select bundle 2, the CMTS device will add VLAN tag 100 for the packets it forwards; and when select bundle 3, the CMTS device will add VLAN tag 200 for the packets it forwards.

The data planning for configuring the multiple bundles under DHCP snooping example is shown as table below.

Table 8-3 Data Planning for Multiple Bundles under DHCPv6 Snooping

Item	Data
Bundle item	bundle 2/3
Relay address for bundle 2	2000::x/64
Relay address for bundle 3	3000::x/64
CM DHCP tag for bundle 2	100
Host DHCP tag for bundle 2	100
MTA DHCP tag for bundle 2	100
STB DHCP tag for bundle 2	100
CM DHCP tag for bundle 3	200
Host DHCP tag for bundle 3	200
MTA DHCP tag for bundle 3	200
STB DHCP tag for bundle 3	200
CM transmission mode	snooping
Host transmission mode	snooping
MTA transmission mode	snooping
STB transmission mode	snooping
DHCP Server	Normal configuration. It can communicate with the device by means of ping; CMTS is not required to configure the address of the DHCP Server, but just transmit transparently the packet to the layer-3 device for relay to the DHCPv6 Server by the uplink port.

Prerequisites

- Network devices and lines must be in the normal state.
- DHCPv6 Server is configured normally.

Configuration flowchart

The process for configuring multiple bundles under DHCPv6 snooping is shown as figure below.

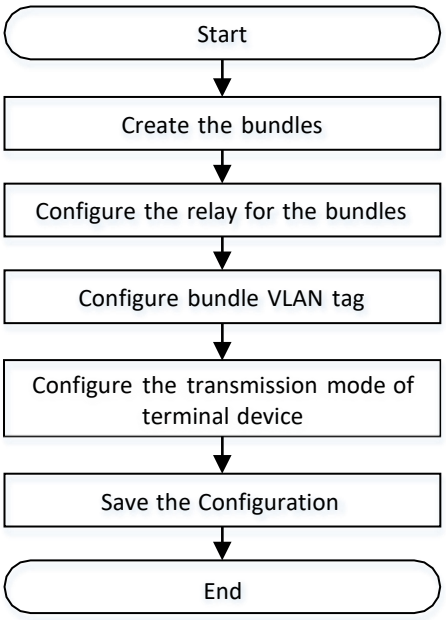

Figure 8-4 Flowchart for Multiple Bundles under DHCP Snooping

Procedure

➢ For the bundle 2:

Step 1 Create the bundle 2.

```
BT(config)# interface bundle 2
```

Step 2 Add the DHCP relay 2000::2/64 for the bundle 2.

```
BT(config-if-bundle2)# ipv6 address 2000::2/64
```

Step 3 Add a VLAN tag to data of the CPE.

1. Add the IPv6 VLAN tag 100 to the packets of CM, with priority as 7. `BT(config-if-bundle2)# cable dhcpv6-tag cm vlan 100priority 7`
2. Add the IPv6 VLAN tag 100 to the packets of host, with priority as 7.

```
BT(config-if-bundle2)# cable dhcpv6-tag host vlan 100 priority 7
```

3. Add the IPv6 VLAN tag 100 to the packets of MTA, with priority as 7.

```
BT(config-if-bundle2)# cable dhcpv6-tag mta vlan 100 priority 7
```

4. Add the IPv6 VLAN tag 100 to the packets of STB, with priority as 7.

```
BT(config-if-bundle2)# cable dhcpv6-tag stb vlan 100 priority 7
```

➢ For the bundle 3:

Step 1 Create the bundle 3.

```
BT(config)# interface bundle 3
```

Step 2 Add the DHCP relay 3000::2/64 for the bundle 3.

```
BT(config-if-bundle3)# ipv6 address 3000::2/64
```

Step 3 Add a VLAN tag to data of the CPE.

1. Add the VLAN tag 200 to the packets of CM, with priority as 7. `BT(config-if-bundle3)# cable dhcpv6-tag cm vlan 200priority 7`
2. Add the VLAN tag 200 to the packets of Host, with priority as 7.
   `BT(config-if-bundle3)# cable dhcpv6-tag host vlan 200 priority 7`
3. Add the VLAN tag 200 to the packets of MTA, with priority as 7.
   `BT(config-if-bundle3)# cable dhcpv6-tag mta vlan 200 priority 7`
4. Add the VLAN tag 200 to the packets of STB, with priority as 7.
   `BT(config-if-bundle3)# cable dhcpv6-tag stb vlan 200 priority 7`

Step 4 Configure the data of terminal device type for transparent transmission.

1. Configure the data with terminal device type as CM for transparent transmission.
   `BT(config)# cable dhcpv6-mode cm snooping` Configure the data
2. with terminal device type as host for transparent transmission.`BT(config)# cable dhcpv6-mode host snooping` Configure the data with terminal
3. device type as MTS for transparent transmission.`BT(config)# cable dhcpv6-mode mta snooping` Configure the data with terminal device type
4. as STB for transparent transmission.`BT(config)# cable dhcpv6-mode stb snooping`

Step 5 Save the configurations.

```
BT(config)# end
BT# copy running-config startup-config
This will save the configuration to the flash memory.
Are you sure?(y/n) [n]y
Building configuration.....
Configuration saved successfully.
```

Result

After finishing the configurations, the terminals under CMTS such as CM/HOST/MTA/STB can acquire IP address automatically from DHCPv6 Server by transparent transmission, and identify the device type with VLAN.

8.5 Example of Multiple Bundles under DHCPv6 Layer3

Context

Refer to 8.4 Example of Multiple Bundles under DHCPv6 Snooping.

Data Planning

In this example, configure DHCPv6 layer 3 forwarding packets of CM | host | STB.

We need create two bundles, bundle 2 with relay address 2000::x/64 and bundle 3 with the address 3000::x/64. The relay IP address must be a real IP address in the CMTS.

CMs will select the smallest number bundle 2 at the discovery stage, and at the request stage, according to server configuration select the matched bundle 2 or 3.

CPE will directly select the CM bundle it connected. When select bundle 2, the CMTS device will forward the packets through the relay 2000::x/64; and when select bundle 3, the CMTS device will forward the packets through the relay 3000::x/64.

The data planning for configuring the multiple bundles under DHCPv6 layer3 example is shown as table below.

Table 8-4 Data Planning for Multiple Bundles under DHCPv6 Layer3

Item	Data
bundle item	bundle 2/3
relay address for bundle 2	2000::2/64
relay address for bundle 3	3000::2/64
relay address for bundle 3 CM	3000::2/64
relay address for bundle 3 host	3000::2/64
relay address for bundle 3 STB	3000::2/64
DHCPv6 Server	1000::1000
Route address	1000:: 64 2000::1
CM transmission mode	l3-relay
Host transmission mode	l3-relay
STB transmission mode	l3-relay

Prerequisites

- Network devices and lines must be in the normal state.
- DHCP Server is configured normally.

Configuration flowchart

The process for configuring multiple bundles under DHCPv6 layer3 is shown as figure below.

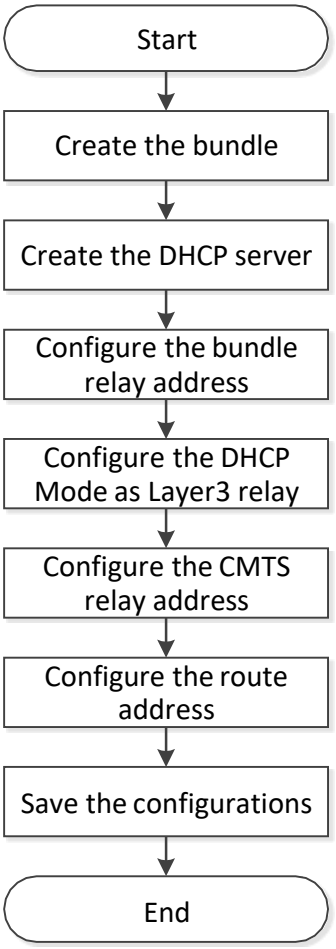

Figure 8-5 Flowchart for Multiple Bundles under DHCPv6 Layer3

Procedure

➢ For the bundle 2:

Step 1 Create the bundle 2.

```
BT(config)# interface bundle 2
```

Step 2 Add the DHCPv6 server 1000::1000 for the bundle 2.

```
BT(config-if-bundle2)# ipv6 dhcp relay destination
1000::1000
```

Step 3 Add the DHCPv6 relay 2000::2/64 for the bundle 2.

```
BT(config-if-bundle2)# ipv6 address 2000::2/64
```

➢ For the bundle 3:

Step 1 Create the bundle 3.

```
BT(config)# interface bundle 3
```

Step 2 Add the DHCPv6 server 1000::1000 for the bundle 3.

```
BT(config-if-bundle3)# ipv6 dhcp relay destination
1000::1000
```

Step 3 Add the DHCPv6 relay for the bundle 3.

1. Add the DHCPv6 relay 3000::2/64 for the bundle 3.

   ```
   BT(config)# ipv6 address 3000::2/64
   ```

2. Configuring Layer 3 forwarding packets of CM.

   ```
   BT(config)# ipv6 dhcp relay link-address cm 3000::2
   ```

3. Configuring Layer 3 forwarding packets of host.

   ```
   BT(config)# ipv6 dhcp relay link-address host 3000::2
   ```

4. Configuring Layer 3 forwarding packets of STB.

   ```
   BT(config)# ipv6 dhcp relay link-address stb 3000::2
   ```

Step 4 Configuring Layer 3 forwarding packets of terminal device type.

1. Configuring Layer 3 forwarding packets of CM. `BT(config)#`

   `cable dhcpv6-mode cm l3-relay`Configuring Layer 3

2. forwarding packets of host.

   ```
   BT(config)# cable dhcpv6-mode host l3-relay
   ```

3. Configuring Layer 3 forwarding packets of STB.

   ```
   BT(config)# cable dhcpv6-mode stb l3-relay
   ```

Step 5 Configuring the CMTS device relay address.

1. Configuring the CMTS device relay address as 2000::2/64.

   ```
   BT(config)# ipv6 address 2000::2/64
   ```

2. Configuring the CMTS device relay address as 3000::2/64.

   ```
   BT(config)# ipv6 address 3000::2/64
   ```

Step 6 Configuring the CMTS device route address.

```
BT(config)# ipv6 route 1000:: 64 2000::1
```

Step 7 Save the configurations.

```
BT(config)# end
BT# copy running-config startup-config
This will save the configuration to the flash memory.
Are you sure?(y/n) [n]y
Building configuration.....
Configuration saved successfully.
```

Result

After finishing the configurations, CMs will select the smallest number bundle 2 at the discovery stage, and at the request stage, according to server configuration select the matched bundle 2 or 3.

CPE will directly select the CM bundle it connected. When select bundle 2, the CMTS device will forward the packets through the relay 2000::x/64; and when select bundle 3, the CMTS device will forward the packets through the relay 3000::x/64.

8.6 Create Bundles and Selection Rules

A bundle is a collection of DHCP configurations, which is just a logical division without any actual physical significance.

Context

CMTS device supports 32 bundles, the range of 1-32.

When the device in a multi-bundle, bundle selection rules are as follows:

During DHCPv6 Solicit Process of CM:

1. CM select the smallest number bundle matching the packet VLAN and the bundle VLAN;
2. When the selection of bundle is not successful, if the DHCP mode is l3-relay, packets will be discarded; if the DHCP mode is l2-relay | snooping, it transparently transmits the packet.

During DHCPv6 Request Process of CM:

1. CM prefers the bundle which the request IP + packet VLAN and the bundle IP address VLAN matches, the packet VLAN and bundle VLAN matches.
2. If condition 1 is not met, then CM select the bundle which the request IP + untag and the IP address VLAN + untag matches, the packet VLAN and bundle VLAN matches.
3. If condition 2 is not met, then CM select the smallest number bundle which the packet VLAN and the I bundle VLAN matches.
4. When the selection of bundle is not successful, if the DHCP mode is l3-relay, packets will be discarded; if the DHCP mode is l2-relay | snooping, it transparently transmits the packet.

During DHCPv6 Solicit Process of CPE:

1. CPE prefers the bundle which the CPE connected CM selected, packet VLAN and bundle VLAN matches.
2. When the selection of bundle is not successful, if the DHCP mode is l3-relay, packets will be discarded; if the DHCP mode is l2-relay | snooping, it transparently transmits the packet.

During DHCPv6 Request Process of CPE:

1. CPE prefers the bundle which the request IP and the bundle IP address matches, the packet VLAN and bundle VLAN matches.
2. When the selection of bundle is not successful, if the DHCP mode is l3-relay, packets will be discarded; if the DHCP mode is l2-relay | snooping, it transparently transmits the packet.

Procedure

Step 1 Create a bundle and enter the bundle view by using the command "**`interface bundle`**".

Step 2 View the information of the bundles by using the command "**`show interface bundle all`**".

Example

Create bundle 3 and enter bundle view:

```
BT(config)# interface bundle 3
BT(config-if-bundle3)# show interface bundle all
!
interface bundle 3
 cable  dhcp-giaddr  primary
 cable source verify enable
 cable ipv6 source verify enable
 cable source verify leasequery-filter upstream 5 10
exit
```

Related Operations

Table 8-5 Related Operations of Create Bundles

Operation	Command	Remarks
Delete the bundle and its configuration	**no interface bundle**	

8.7 Configure DHCPv6 Server

CMTS supports the configuration of two servers:

- Universal DHCPv6 server: DHCPv6 server used by different terminal types.
- Dedicated DHCPv6 servers: DHCPv6 servers for specific terminal types.

8.7.1 Configure the Universal DHCPv6 Server

Context

- The device supports DHCPv6 universal server configuration in IPv6 environment.
- Universal DHCPv6 servers are used for all terminal types that are not configured with dedicated DHCPv6 servers.
- The device supports up to five general-purpose DHCPv6 servers. After configuration is completed, the CMTS device will forward DHCPv6 messages to multiple servers at the same time.
- Universal DHCPv6 server configuration can be deleted by corresponding “no” command.

Procedure

Step 1 Set universal Helper-Address of the device by using the command “**ipv6 dhcp relay destination**”.

Step 2 View the Helper-Address configured for the device by using the command “**show running-config**”.

Example

Configure the universal Helper-Address:

```
BT(config-if-bundle1)# ipv6 dhcp relay destination 1000::1000
BT(config-if-bundle1)# show running-config | include destination
 ipv6 dhcp relay destination 1000::1000
```

Related Operations

Table 8-6 Related Operations for Configure the Universal Helper-Address

Operation	Command	Remarks
Delete the universal Helper-Address	**no ipv6 dhcp relay destination**	

8.7.2 Configure the Dedicated DHCPv6 Server

Context

- The device supports DHCPv6 dedicated server configuration in IPv6 environment.
- CMTS devices are supported to configure dedicated DHCPv6 servers for CM, host, MTA, STB and each custom terminal device. After configuring, CMTS devices will forward DHCPv6 messages to dedicated DHCPv6 servers according to terminal type.
- After a terminal type is configured with a dedicated DHCPv6 server, the CMTS device no longer forwards DHCPv6 requests of that terminal type to the general server.
- Device supports up to five dedicated DHCPv6 servers for each terminal. When CMTS is configured, DHCPv6 messages will be forwarded to multiple dedicated DHCPv6 servers at the same time.
- Dedicated DHCPv6 server configuration can be deleted by the corresponding “no” command.

Procedure

Step 1 Set dedicated Helper-Address of the device by using the command “**ipv6 dhcp relay destination (cm | host | mta | stb |** *device*)”.

Step 2 View the configured Helper-Address of the device by using the command “**show running-config**”.

Example

Configure the dedicated DHCPv6 server of CM:

```
BT(config-if-bundle1)# ipv6 dhcp relay destination cm 2 2000::1000
BT(config-if-bundle1)# show running-config | include destination
 ipv6 dhcp relay destination cm 2 2000::1000
```

Related Operations

Table 8-7 Related Operations for Configure the Dedicated DHCPv6 server

Operation	Command	Remarks
Delete the dedicated DHCPv6 server	**no ipv6 dhcp relay destination (cm | host | mta | stb |** *device*)	When all dedicated Helper-Addresses of a terminal device, such terminal will be online with universal Helper-Address.

8.8 Configure Option Vendor Class to identify terminal types

Option vendor class (applied to IPv6 network) is used to identify different terminal types, so that L3 relay can assign different IP addresses according to terminal types.

- CMTS devices default support for C-DOCSIS standard defined strings.
- CMTS supports the configuration of option vendor class strings for terminal types in order to be more compatible with vendors'devices.
- When users need to plan business according to different terminal types and standard terminal types (CM/HOST/MTA/STB) can not meet the requirements, users can also configure custom terminal types and configure option vendor class strings for custom terminal types.
- The option vendor class string in the C-DOCSIS standard is specified in the following table. Users need to avoid the default string specified in the standard when configuring it (the option field is case-insensitive, i.e. characters such as "STB" or "sTb" will be recognized as "stb". :

Table 8-8 Option Vendor Class Keyword Configuration Parameter

Device	Option60 string	Description
Cable Modem	String starting with “docsis”	The subsequent string can include docsis version and capability supported by CM; Cable Modem includes independent CM terminal and embedded CM, such as embedded CM in STB.
MTA	String starting with “pktc”	The subsequent string can include PacketCable version and capability supported by the device.
Set-top box	String starting with “stb”	The subsequent string can describe the capability of the device.

Context

- If Option60 can match multiple strings simultaneously, the priority is: the defined string > longer string > front string.
- 4 different Option60 strings can be configured for the same terminal type.
- Option60 string is case insensitive, that is, strings like “STB” or “sTb” will be identified as “stb”.
- The configuration of Option60 can be deleted by using the corresponding “no” command.

Procedure

Step 1 Configure user-defined device by using the command "**cable dhcpv6 device**".

Step 2 Configure option vendor class of the device by using the command "**cable dhcpv6-option vendor-class**".

Step 3 View the configured option vendor class of the device by using the command "**show running-config**".

Example

Configure the custom terminal type cablemodem in IPv6 environment, and configure the option vendorclass string as cablemodemIPv6.

```
BT(config-if-bundle1)# cable dhcpv6 device cablemodem
BT(config-if-bundle1)# cable dhcpv6-option vendor-class cm cablemodemIPv6
BT(config-if-bundle1)# show running-config | include option
cable dhcp-option60 cablemodem 1 "cablemodemIPv4"
```

Related Operations

Table 8-9 Related Operations Option Vendor Class

Operation	Command	Remarks
Delete the user-defined device type	**no cable dhcpv6 device**	
Delete the option vendor class string of the terminal type.	**no cable dhcpv6-option vendor-class**	

8.9 Configure DHCPv6 Tags

DHCPv6-tag function can be used to add VLAN tags to different device type by bundle. The upper device of CMTS such as switch will perform the DHCP relay by the tag.

Context

- Dhcp-tag function supports the DHCP mode is l2-relay, snooping, and l3-relay.
- Dhcp-tag function can be used to add VLAN tag to different devices by bundle, and the upper device of CMTS such as switch will perform the DHCP relay by the tag further. By this approach, different giAddr can be inserted in different devices and classified into different address pools.

Procedure

Step 1 Configure VLAN tags of the device by using the command "**cable dhcpv6-tag**".

Step 2 View the configured VLAN tags of the device by using the command "**show running-config**".

Example

Configure STB to add VLAN 100 tag, with priority as 7:

```
BT(config-if-bundle2)# cable dhcpv6-tag stb vlan 100 priority 7
BT(config-if-bundle2)# show running-config | include dhcp-tag
 cable dhcpv6-tag stb vlan 100 priority 7
```

Related Operations

Table 8-10 Related Operations of Dhcp-tag

Operation	Command	Remarks
Delete DHCPv6 tag of dedicated terminal type	**no cable dhcpv6-tag**	

8.10 DHCP information option circuit-id-prefix

Option 18 (interface-id) is used to configure user information, which is conducive to judging the source of network messages. It is mainly used for security checking, such as preventing IP spoofing, user identifier spoofing and MAC address spoofing.

Working process:

- CMTS receives the DHCPv6 message from the terminal device and forwards it to DHCPv6 server with option 18. DHCPv6 server is responsible for identifying the option18 information added to the DHCPv6 message and making corresponding processing according to the information.
- CMTS receives DHCPv6 message from DHCPv6 server, removes option 18 and forwards it to the corresponding terminal device.

Context

- CMTS devices support both hexadecimal and string configuration options 18.
- If not configured, CMTS defaults to host name value (BT) for option 18.
- Option 18 strings support input of up to 64 characters.
- Option 18 configuration can be deleted by the corresponding “no” command.

Procedure

Step 1 Configure the circuit-id-prefix by using the command “**dhcp information option circuit-id-prefix (hex | string)**”.

Step 2 Query the circuit-id-prefix value by using the command “**show dhcp circuit-id-prefix**”.

Example

Configure the circuit ID and the interface ID in hexadecimal as 414c55.

```
BT(config)# dhcp information option circuit-id-prefix string sumavision
BT(config)# show dhcp circuit-id-prefix
Hex Format         :73756d6176973696f6e
String Format      :sumavision
```

Related Operations

Table 8-11 Related Operations of DHCP information option circuit-id-prefix

Operation	Command	Remarks
Delete the circuit-id-prefix value	**no dhcp information option circuit-id-prefix**	The default value is *hostname*.
Display the configuration of circuit-id-prefix	**show dhcp circuit-id-prefix**	

Chapter 9 Local Provisioning Management

This section mainly describes Local Provisioning management for the CMTS. Users can refer to this section to build a provisioning system for the CMs and CPEs that will allow the CMs and CPEs to obtain IP addresses and upload/download configuration files to complete the registration process.

9.1 Overview

When miniaturized network deployment or operators do not need complex network scenarios, CMTS Local Provisioning system can be used to provide local provisioning services for CM and CPE. IP addresses and configuration files can be allocated online according to CM configuration, and IP addresses can also be allocated for CPE. CMTS Local Provisioning system also supports CM automatic upgrade.

Equipment support:

- CM Profile Management: It supports downloading CM Profile from FTP/TFTP Server to CMTS File System by command "**`load (cm-config | cm-class-config)"`** command, and supports assigning specified Profile to CM of specified MAC address segment.
- CM Auto Upgrade: Devices support CM upgrades of specified types. When the device opens the CM automatic upgrade function, the device will check CM Model Number and software version information after CM goes online. When the information meets the requirement of automatic upgrade, CM upgrade will be triggered automatically, and CM will restart automatically after the upgrade is completed.

Note:

1. The precondition of configuring CM automatic upgrade is that CM software version needs to support automatic upgrade function.
2. The device also supports upgrade of a single CM image using the command upgrade cable modem.

- IPv4 local provisioning address pool:
  - DHCP address pool segment: In order to facilitate operators to better plan IP addresses, devices support the configuration of IPv4 large segment (through command "**`network`**" configuration) and small segment (through command "**`network start-ip end-ip`**" configuration). If the small segment information is not configured, the large segment will take effect; if the small segment information is configured, the intersection of the large segment and the small segment will take effect.
  - DHCP lease: CM/CPE uses DHCP IP address lease period, need to renew before expiration, otherwise terminal equipment will not be able to access the network.
  - Default routing address

- DNS address

➢ IPv6 local provisioning address pool:

- DHCP address pool segment: The device supports configuring IPv6 segment, which can assign a single IP address to the terminal device (by command "**address-prefix lifetime**") or IP address segment (by command "**prefix-delegation lifetime**") via IAPD.
- Effective Life Cycle: When CM/CPE uses the effective life cycle of DHCP IP address, it needs to be renewed before the expiration date, otherwise the terminal device will not be able to access the network.
- Preferred Life Cycle: CM/CPE uses DHCP IP address's preferred life cycle. CMTS devices allocate IP address pools, giving priority to IP addresses whose preferred life cycle has expired.
- DNS address

➢ Exclude the DHCP address pool segment: Provisioning system excludes the designated segment and does not assign it to the terminal.

➢ CM gets the specified configuration file by MAC address when it goes online.

9.2 Example of Configure CM and CPE to go online via Local Provisioning System

Through this example, CM and CPE can be online through Local Provisioning system.

Data Planning

With the following configuration, CM whose MAC address segment is 0012.0000.0000-0012.0000.0012 is assigned IPv4 and IPv6 address pool network segment (except excluding address segment), and the CM configuration file "online.cfg" is obtained to go online. Online planning through the Local Provisioning system is shown in the following table.

Table 9-1 Data Planning for Local Provisioning System online

Item	Data
Device global IPv4 address.	172.168.100.136/24
Device global IPv6 address.	3000:: 136/64
CM message request.	Initiate IPv4 and IPv6 at the same time, i.e. dual-stack mode
CM supports IPv4 local provisioning.	Enable
CPE supports IPv4 local provisioning.	Enable
CM supports IPv6 local provisioning.	Enable
CPE supports IPv6 local provisioning.	Enable
Local provisioning excludes address segments.	172.168.100.20-172.168.100.30 and 172.168.100.50-172.168.100.55
IPv4 address pool segment.	172.168.100.0/24

Item	Data
Rental period of IP address in IPv4 address pool.	1 day
Default routing address for IPv4 address pool.	172.168.100.1
DNS address of IPv4 address pool.	10.10.28.2
IPv6 address pool segment.	3000:: /64
The effective life cycle of IP addresses in IPv6 address pool.	6400 seconds
The preferred lifecycle of IP addresses in the IPv6 address pool.	6400 seconds
IAPD's address pool network segment.	3000:: /64
The effective life cycle of IAPD.	6400 seconds
IAPD's preferred life cycle.	6400 seconds
DNS address of IPv6 address pool.	Dns-server 3000::111
Description information for client-class 1.	Client class 1
CM configuration file for client-class binding.	Online.cfg
CM MAC address in client-class.	0012.0000.0000-0012.0000.0012

Prerequisite

Network and CMTS equipment are normal.

Configuration flowchart

CM and CPE go online through Local Provisioning as shown in the following figure.

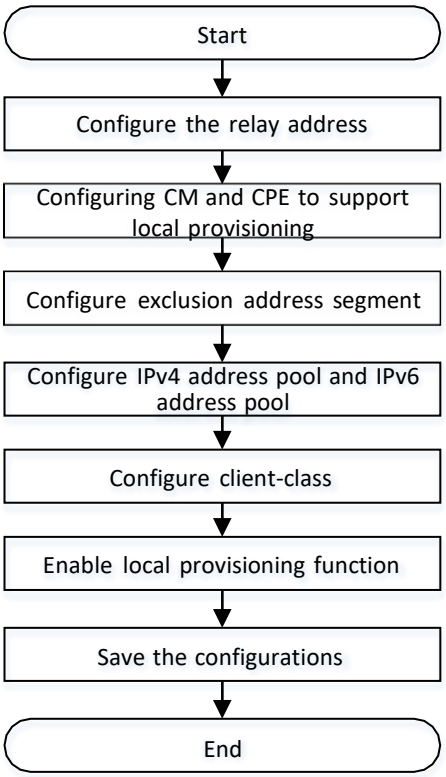

Figure 9-1 Flowchart for CM and CPE are configured online through the local provisioning system

Procedure

Step 1 Configure the relay address.

1. Configure the global IPv4 primary address.

   `BT(config)# ip address 172.168.100.136 255.255.255.0primary`

2. Configure the global IPv6 address.

   `BT(config)# ipv6 address 3000::136/64`

Step 2 Configure CM and CPE to support local provisioning.

1. Enter the CMTS view.

   `BT(config)# interface cmts 1`

2. Configure CM to initiate both IPv4 and IPv6 message requests. `BT(config-if-cmts-1)# cable ip-init dual-stack`Exit the CMTS view.

3. `BT(config-if-cmts-1)# exit`

4. Open CM to support IPv4 local provisioning

   `BT(config)# cable local-provisioning support cm`

5. Open CPE to support IPv4 local provisioning

   `BT(config)# cable local-provisioning support cpe`

6. Open CM to support IPv6 local provisioning

   `BT(config)# cable ipv6 local-provisioning support cm`

7. Open CPE to support IPv6 local provisioning

   `BT(config)# cable ipv6 local-provisioning support cpe`

Step 3 Configure exclusion address segments.

1. Configuration exclusion address segment 172.168.100.20-172.168.100.30

   `BT(config)# ip dhcp excluded-address 172.168.100.20 172.168.100.30`

2. Configuration exclusion address segment 172.168.100.50-172.168.100.55

   `BT(config)# ip dhcp excluded-address 172.168.100.50 172.168.100.55`

Step 4 Configure IPv4 address pool and IPv6 address pool

1. Enter the ip-dhcp-pool view

   `BT(config)# ip dhcp-pool`

2. Configuration of DHCP service IPv4 address pool segment 172.168.100.0/24 `BT(ip-dhcp-pool)# network 172.168.100.0 255.255.255.0`The lease time for

3. configuring IP addresses in the IPv4 address pool is 1 day `BT(ip-dhcp-pool)# lease days 1`

4. The default routing address for configuring IPv4 address pool is 172.168.100.1

   `BT(ip-dhcp-pool)# default-router`

5. Configure the DNS address of IPv4 address pool to 10.10.28.2

```
BT(ip-dhcp-pool)# dns-server 10.10.28.2
```

6. Exit the ip-dhcp-pool view `BT(ip-dhcp-pool)# exit`Enter the ip-dhcpv6-pool
7. view
   `BT(config)# ipv6 dhcp-pool`
8. Configure DHCP service IPv6 address pool segment to 3000::/64, effective life cycle to 64000 seconds, preferred life cycle to 64000 seconds
   `BT(ip-dhcpv6-pool)# address-prefix 3000::/64 lifetime64000 64000`
9. Configure DHCP service IPv6 address pool segment to 3000::/64, effective life cycle to 64000 seconds, preferred life cycle to 64000 seconds
   `BT(ip-dhcpv6-pool)# prefix-delegation 3000::/64 96 lifetime 64000 64000`
10. DNS address for IPv6 address pool configuration is 3000::111
    `BT(ip-dhcpv6-pool)# dns-server 3000::111`
11. Exit the ip-dhcpv6-pool view
    `BT(ip-dhcpv6-pool)# exit`

Step 5 Configuration of client-class

1. Enter the client-class view
   `BT(config)# client-class 1`
2. Configure client-class description information as "client class 1". `BT(client-class-1)# description "client class 1"`Configure CM in client-
3. class to go online using online.cfg configuration file `BT(client-class-1)# client-class bind cm-config "online.cfg"`
4. Configure the CM MAC address in client-class to be 0012.0000.0000-0012.0000.0012
   `BT(client-class-1)# member mac 0012.0000.00000012.0000.0012`

Step 6 Save configuration

```
BT(client-class-1)# end
BT# copy running-config startup-config
This will save the configuration to the flash memory.
Are you sure?(y/n) [n]y
Building configuration.....
Configuration saved successfully.
```

Result

According to the above configuration, CM with MAC address 0012.0000.0000-0012.0000.0012 obtains both IPv4 and IPv6 addresses and goes online through the configuration file online.cfg. The range of addresses obtained is: 3000://64 and 172.168.100.0/24, excluding 172.168.100.20-172.168.100.30 and 172.168.100.50-172.168.100.55.

9.3 CM Configuration File Management

Users can refer to this section to understand how to download the CM configuration file from the server to the CMTS or upload the CM configuration file from the CMTS to the server.

Download the CM configuration file from the FTP/TFTP server to the specified folder using the FTP/TFTP protocol. When the CM configuration file is downloaded to the device, the user can modify the filename as needed. If the user does not modify the filename, the default is the original filename.

Operation Procedures

Step 1 Determine how the file will be downloaded (FTP or TFTP), prepare the CM configuration file on the server, and build the required connection to make sure that the device can communicate with the server network.

Step 2 In the enable view, use the command "**load (cm-config | cm-3.0-config)**" to download the default CM configuration file from the server or use the command "**load cm-class-config**" to download the CM configuration file from the server.

Step 3 In the client-class view, use the command "**client-class bind cm-config**" to bind the CM configuration file to the client-class. (Omit this step when using the command "**load (cm-config | cm-3.0-config)**" in step 2).

Step 4 In the config view, use the command "**show running-config**" to display the CM configuration file or in the enable view,use the command "**show system file**" to display downloads from the server.

Task Example

Download CM configuration file, in_service.cfg, from FTP server 10.10.29.209 and store as cm.cfg in the device.

```
BT# load cm-config ftp 10.10.29.209 wp wp in_service.cfg cm.cfg
File saved to /app/cm-config/cm.cfg
```

Related Operations

Table 9-2 Related operations to download CM configuration file management

Operation	Command	Remark
Upload default CM configuration file to a PC using FTP/TFTP	**upload (cm-config | cm-3.0-config) (ftp | tftp)**	Get the CM configuration file from the /app/cm-config/ directory cm-3.0-config: Default configuration file of 3.0

Operation	Command	Remark
		CM, higher priority than cm-config. cm-config: Default configuration file of all CM. If cm-3.0-config is already configured, 3.0 CM's default configuration file is cm-3.0-config.
Use TFTP/TFTP to download the default CM configuration file to the device	**load (cm-config | cm-3.0-config) (ftp | tftp)**	Save the CM configuration file to /app/cm-config/ cm-3.0-config: Default configuration file of 3.0 CM, higher priority than cm-config. cm-config: Default configuration file of all CM. If cm-3.0-config is already configured, 3.0 CM's default configuration file is cm-3.0-config.
Enable the configuration file select function of 3.0 CM	**bootfile cm-3.0**	
Disable the configuration file select function of 3.0 CM	**no bootfile cm-3.0**	
Upload CM configuration file to a PC using FTP/TFTP	**upload cm-class-config (ftp | tftp)**	Get the CM configuration file from the /app/cm-config/ directory
Use TFTP/TFTP to download the CM configuration file to the device	**load cm-class-config (ftp | tftp)**	
Remove the the CM configuration file	**remove cm-class-config**	
Rename the the CM configuration file	**rename cm-class-config**	

9.4 CM Automatic Upgrade

Context

Users can configure CM automatic upgrade through this section. When CM is online, users can specify the following parameters to upgrade CM (if three parameters are not configured, upgrade all CM by default):

- CM model number: CM model number is designated by CM manufacturer. Different batches of CM from different manufacturer have different CM model number.
- CM Version Number: The target version number of CM upgrade. All CMs that do not match the CM version number will be upgraded to the target version number.
- CM Upgrade Mirror File: The Mirror File for CM Upgrade.

Procedure

Step 1 Determine the use of download mode (FTP or TFTP), and prepare CM image files on the server, build the relevant environment, determine the device and server network accessibility.

Step 2 downloads CM image file from FTP/TFTP server to CMTS file system by command "**load cm-class-image**" in enable view.

Step 3 Upgrade CM through the command "**cable modem auto-upgrade**" in the config view.

Step 4 Views the CM version in the enable view by the command "**show cable modem version**".

Example

Download CM image file cm-class-image from TFTP server 192.168.1.100 and upgrade it to CM model number BCM93383DCM, version number is not all CM of SC011_Tv_151128.

```
BT# load cm-class-image tftp 192.168.1.100 cm-class-image
File saved to /app/cm-image/cm-class-image
BT# configure terminal
BT(config)# cable modem auto-upgrade BCM93383DCM SC011_Tv_151128 cm-class-image
BT(config)# show cable modem version
MAC Address          Model Number        Software Version
001c.1df5.72e1       BCM93383DCM         SC011_Tv_151128
```

Related Operations

Table 9-3 Related Operations of CM Automatic Upgrade

Operation	Command	Remarks
FTP uploads CM image file to PC	**upload cm-class-image ftp**	
TFTP uploads CM image file to device	**upload cm-class-image tftp**	
Delete CM image files in CMTS file system	**remove cm-class-image**	
Rename the CM image file in the CMTS file system	**rename cm-class-image**	

9.5 Configure IPv4 Local Provisioning Address Pool

Users can configure IPv4 Local Provisioning address pool through this section.

Context

Manage the IPv4 address and lease time allocated to CMTS by CMTS Local Provisioning address pool.

Procedure

Step 1 Configures the relay address in IPv4 through the command "**ip address**" in the config view.

Step 2 Enters the ip-dhcp-pool view by commanding "**ip dhcp-pool**" in the config view.

Step 3 Use the command "**network**" to configure the DHCP address pool segment in the ip-dhcp-pool view to be the same segment as the device Primary IP.

Step 4 Configure the lease time using the command "**lease**" in the ip-dhcp-pool view.

Step 5 Configures the default routing address of the address pool using the command "**default-router**" in the ip-dhcp-pool view.

Step 6 Configures the DNS address of the address pool using the command "**dns-server**" in the ip-dhcp-pool view.

Step 7 Uses the command "**show dhcp-server config**" to view the Provisioning address configuration in the ip-dhcp-pool view.

Step 8 Uses the command "**show IP dhcp-pool used-status**" in the ip-dhcp-pool view to view the IP address allocation of Local Provisioning.

Example

$ The IP allocated by Provisioning is 10.0.0.1 and the mask is 255.255.255.0. At the same time, the IP allocated by address pool is limited to 10.0.0.11-10.0.0.112 segments, and the address lease time is 9 days, 11 hours, 11 minutes and 22 seconds.

```
BT(config)# ip address 10.0.0.1 255.255.255.0 primary
BT(config)# ip dhcp-pool
BT(ip-dhcp-pool)# network 10.0.0.1 255.255.255.0
BT(ip-dhcp-pool)# network start-ip 10.0.0.11 end-ip 10.0.0.112
BT(ip-dhcp-pool)# lease days 9 hours 11 minutes 11 seconds 22
BT(ip-dhcp-pool)# show dhcp-server config
Server host MAC    :0024.68ab.cdcc
Server host IP     :10.0.0.1
Next sever IP      :10.0.0.1
Boot file name     :cm.cfg
Network  IP        :10.0.0.1/24
Lease              :9d11h11m22s
Default route      :
Primary DNS        :
Secondary DNS      :
BT(ip-dhcp-pool)# show ip dhcp-pool used-status Client MAC
                    IP Address       LeaseEnd
001a.c369.8746      10.0.0.11        1970 Jan 10  11:14:51
0016.9259.7d14      10.0.0.12        1970 Jan 10  11:14:57
BT(ip-dhcp-pool)# show running-config
network 10.0.0.1 255.255.255.0
network start-ip 10.0.0.11 end-ip 10.0.0.112
lease days 9 hours 11 minutes 11 seconds 22
```

Related Operations

Table 9-4 Related Operations ofpaikallinen osoite kokoonpanon ipv4-varauksia

Operation	Command	Remarks
View address pool configuration	**show ip dhcp-pool**	In the config view
View the address pool configuration in detail	**show running-config [verbose]**	In the view of ip-dhcp-pool
Enable 3.0 CM configuration file selection function	**bootfile cm-3.0**	

Operation	Command	Remarks
Disable 3.0 CM configuration file selection	**no bootfile cm-3.0**	
Delete address pool related configuration	**no ip dhcp-pool**	In the config view
Configure the address pool to specify the IP address segment	**network start-ip end-ip**	In the view of ip-dhcp-pool, the maximum specification is 10 pairs
Delete the IP address segment of the address pool	**no network start-ip end-ip**	In the view of ip-dhcp-pool

9.6 Configure IPv6 Local Provisioning Address Pool

Users can configure IPv6 Local Provisioning address pool through this section.

Context

Manage the IPv6 address and lease time allocated to CMTS by CMTS Local Provisioning address pool.

Procedure

Step 1 Configures the relay address of IPv6 through the command "**ipv6 address**" in the config view.

Step 2 Enters the "**ip dhcp-pool**" view by commanding IP dhcp-pool in the config view.

Step 3 Configures the DHCP address pool segment in the ip-dhcpv6-pool view using the command "**address-prefix lifetime**", effective life cycle and preferred life cycle.

Step 4 Configures the address pool segment used by IAPD in the ip-dhcpv6-pool view using the command "**prefix-delegation lifetime**", effective lifecycle and preferred lifecycle.

Step 5 Configure the DNS address of the address pool using the command "**dns-server**" in the ip-dhcpv6-pool view.

Step 6 Uses the command "**show ipv6 dhcp-pool used-status**" in the ip-dhcpv6-pool view to view the IP address allocation of Local Provisioning.

Example

$ Provisioning allocates 3000:/64 segments, 3000:/64 prefix proxy and 96 prefix lengths respectively, while limiting both effective and preferred lives to 64000s, and DNS servers to 3000::111 and 3000::222.

```
BT(config)# ipv6 address 3000::136/64
BT(config)# ipv6 dhcp-pool
BT(ip-dhcp-pool)# address-prefix 3000::/64 lifetime 64000 64000
BT(ip-dhcp-pool)# prefix-delegation 3000::/64 96 lifetime 64000 64000
BT(ip-dhcp-pool)# dns-server 3000::111 3000::222 BT(ip-
dhcp-pool)# show ipv6 dhcp-pool used-status Client MAC
                    IP Address       LeaseEnd
001a.c369.8746      3000::/64        1970 Jan 10  11:14:51
0016.9259.7d14      3000::/65        1970 Jan 10  11:14:57
BT(ip-dhcp-pool)# show running-config
```

```
address-
prefix
3000::/64
lifetime
64000
64000
```

```
prefix-delegation 3000::/64 96 lifetime 64000 64000
dns-server 3000::111 3000::222
```

Related Operations

Table 9-5 Related Operations of Configure IPv6 Local Provisioning Address Pool

Operation	Command	Remarks
View address pool configuration in detail	**show running-config [verbose]**	In the view of ip-dhcpv6-pool
Delete address pool related configuration	**no ipv6 dhcp-pool**	In the config view

9.7 Configure IP Segment Exclusion for DHCP Address Pool

Background Information

Manage how CMTS Local Provisioning assigns IP addresses to the CMs/CPEs. After the IP address segment has been configured using the address pool, the user needs to specify the IP address segment for separate use, the maximum specification is 20 pairs.

Operation Procedures

Step 1 First verify if the address pool configuration is complete and that the CM/CPE can operate normally online.

Step 2 In the config view, use the command "**ip dhcp excluded-address 10.0.0.11 10.0.0.15**" to exclude IP addresses in the segment 10.0.0.11-10.0.0.15.

Step 3 Use **show running-config** to view the configuration. When the CM/CPE is online again, the network segment 10.0.0.11-10.0.0.15 will not be assigned to the devices.

Task Example

Exclude network segment IP.

```
BT(config)# ip dhcp excluded-address 10.0.0.11 10.0.0.15
BT(config)# show running-config | include excluded-addressip dhcp
excluded-address 10.0.0.11 10.0.0.15
```

Related Operations

Table 9-6 Related operations to configure excluded address pool

Operation	Command	Remark
Delete the IP segment in the excluded address pool	**no ip dhcp excluded-address**	Delete the IP segment in the excluded address pool

9.8 Get designated configuration file based on MAC once CM is brought online using local-provision

Background Information

When CM is online using built-in DHCP server. After configuring this function, CM gets the specified configuration file online according to CM MAC.

Operation Procedures

Step 1 Use the command "**cable local-provisioning enable**" to turn on the built-in DHCP server, and use ip dhcp-pool to configure the address pool.

Step 2 Use the command "**load cm-config**" to download the CM configuration file.

Step 3 Use the command "**client-class**" to create a class and enter this class.

Step 4 In the class, use the command "**member mac**" to add the MAC member.

Step 5 Use the command "**client-class bind cm-config**" to bind the CM configuration file.

Step 6 Once the CM uses the built-in DHCP server to get online, use the command "**show cable modem verbose**" to check if the CM is already using the designated configuration file.

Task Example

Configure CM[001c.1df2.a4eb] to use configuration file, online.cfg, to get online.

```
BT(config)# cable local-provisioning enable
BT(config)# exit
BT# load cm-config ftp 10.10.29.58 top top online.cfg
BT# configure terminal
BT(config)# client-class 1
BT(client-class-1)# member mac 001c.1df2.a4eb BT(client-class-1)#
client-class bind cm-config online.cfgBT(config)# show cable
modem 001c.1df2.a4eb verbose
```

Related Operations

Table 9-7 Related operations to Based on MAC once CM is Brought Online

Operation	Command	Remark
Delete the client-class and its associated configuration	**no client-class**	Delete the IP segment in the excluded address pool
Delete the CM configuration file which binding to the client-class	**no client-class bind cm-config**	
Delete the CM MACRange from the client class.	**no member mac**	

9.9 Enable Local Provisioning Support CM

Users can refer to this section to enable the Local Provisioning system.

Background Information

When CMTS Local Provisioning system is enabled, the DHCPv4 message of CM will be terminated within the device. CM DHCPv4 message will no longer be forwarded upward, nor will it be required to configure the command related to forwarding CM DHCPv4 message in bundle. However, the configuration can still take effect according to device type and VLAN function.

By default, CMTS does not enable the Local Provisioning function. If you need to use this function, you need to turn it on.

- If used in IPv6 environment, CM IP Provisioning mode should be set to support IPv6, that is, IPv6 Only, alternate or dual-stack.
- Local Provisioning defaults to the Primary IP address as its own IP address to communicate with CM. It is necessary to ensure that the Primary IP address of the device exists, otherwise CM cannot be online.

Operation Procedures

Step 1 In the config view, use the **"cable [ipv6] local-provisioning support cm"** command to enable local provisioning support cm.

Step 2 Use **"show running-config"** to view the configuration for local provisioning.

Task Example

Enable local provisioning support cm.

```
BT(config)# cable local-provisioning support cm BT(config)# show
running-config | include local-provisioningcable local-provisioning
support cm
```

Related Operations

Table 9-8 Related operations to enable local provisioning support cm

Operation	Command	Remark
Disable local provisioning support cm	**no cable [ipv6] local-provisioning support cm**	
View the switch status for local provisioning	**show cable [ipv6] local-provisioning**	
Enable local provisioning support CPE	**cable local-[ipv6] provisioning support cpe**	
Disable local provisioning support CPE	**no cable [ipv6] local-provisioning support cpe**	

Chapter 10 TFTP Proxy

10.1 Function Overview

To prevent network embezzlement and attack, CMTS supports TFTP proxy function to prevent server IP leakage according to DOCSIS security requirements.

As a TFTP server of CM, CMTS downloads configuration files from TFTP server as TFTP client, and ensures that the settings registered by CM are consistent with those obtained from legal TFTP server.

10.2 Example of Configure TFTP Proxy Function

Context

When CM obtains IP through DHCP, CMTS monitors the message returned by DHCP server to CM, which carries TFTP server address and configuration file name required by CM. CMTS changes the TFTP server address to the IP address of CMTS, and records the profile name.

CM starts to send request to TFTP server and download configuration file after acquiring IP address. Because CMTS modifies the TFTP server address, for CM, TFTP server is CMTS. After CMTS receives CM's request, it first verifies whether the requested configuration file name is correct. After the authentication, add CM IP and / or CM MAC options in TFTP request to send the request to TFTP server. CMTS receives the message replied by TFTP server and forwards it to CM. While accomplishing the agent task between CM and TFTP server, CMTS also learned the content of configuration file and recorded it for use.

After CM finishes downloading configuration file, it forms REG-REQ message and sends registration request to CMTS. CMTS parses the configuration content from REG-REQ, matches and verifies the configuration file learned before, and prevents CM from tampering with the configuration content. If the verification is successful, allow CM to continue to register, otherwise send an event to inform CM that the content of the configuration file does not match.

In the case of high security requirements for operators, in order to prevent TFTP server address disclosure and ensure that CM registered configuration is the correct configuration downloaded from TFTP server, TFTP proxy function needs to be used.

Data Planning

Table 10-1 Data Planning for Configure the TFTP Proxy Feature

Item	Data
TFTP-Proxy switch	Enable
TFTP-Proxy options	Enable IP and MAC options (optional, TFTP server support required)
TFTP-Proxy profile learning	Enable

Prerequisites

- Network and CMTS equipment are normal.
- If option is enabled, TFTP server support is required
- DHCP function is normal

Configuration Flowchart

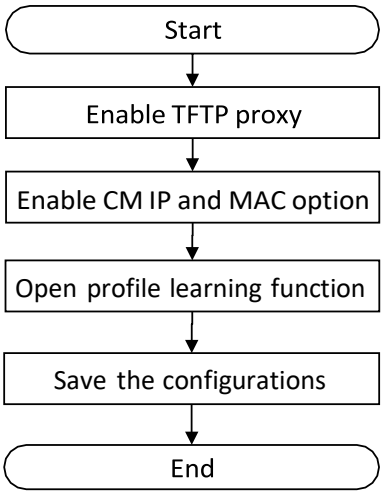

Figure 10-1 Flowchart for TFTP Proxy Function Configuration

Procedure

Step 1 Enable TFTP proxy:

1. Enter CMTS view

   `BT(config)# interface cmts 1`

2. Enable TFTP proxy

   `BT(config-if-cmts-1)# cable tftp-proxy`

Step 2 Enable CM IP and MAC option:

1. Enter config view

   `BT(config-if-cmts-1)# exit`

2. Turn on the IP with the specified option cm. `BT(config)#`

   `cable tftp-proxy option ip`Turn on the Mac with the

3. specified option cm.

   `BT(config)# cable tftp-proxy option mac`

Step 3 Open the profile learning function:

`BT(config)# cable tftp-proxy config-file learning`

Step 4 Save the configurations:

```
BT(config)# end
BT# copy running-config startup-config
This will save the configuration to the flash memory.
Are you sure?(y/n) [n]y
```

```
Building configuration.....
Configuration saved successfully.
```

Result

The TFTP process of CM to get the configuration file will be forwarded by CMTS. CMTS verifies the registration request content of CM to prevent the inconsistency between the request content and that issued by TFTP server. After verification, CM will go online successfully.

10.3 Example of Configure TFTP Server Address Replacement

Context

In order to prevent TFTP Server address leakage, network embezzlement and attack.

After enabling TFTP Proxy:

In the Next server IP address of Offer and ACK messages, replace TFTP server IP with CMTS IP (DHCPv4);

Replace the suboption TFTP server address (option 17.32) of the vendor specific information content in the advertisement and reply messages with the CMTS IP address (DHCPv6).

After the TFTP proxy function is turned off, the TFTP server address is not replaced.

The priority of address selection of TFTP server replacement function is as follows:

1. The address configured through "**`cable tftp server (ipv4 | ipv6)`**" command is preferred.
2. From the interface VLAN interface configuration, select the address of the same network segment allocated to cm in the offer / ACK or advertisement / reply message.
3. The dynamic address obtained by using the controller or stand-alone activation.
4. If the appropriate address cannot be obtained in the above three cases, use the TFTP server address in the original message.

Network Diagram

Provisioning includes DHCP server and TFTP server.

When TFTP proxy is turned on, CMTS serves as the TFTP server of CM and downloads configuration files from TFTP server as TFTP client.

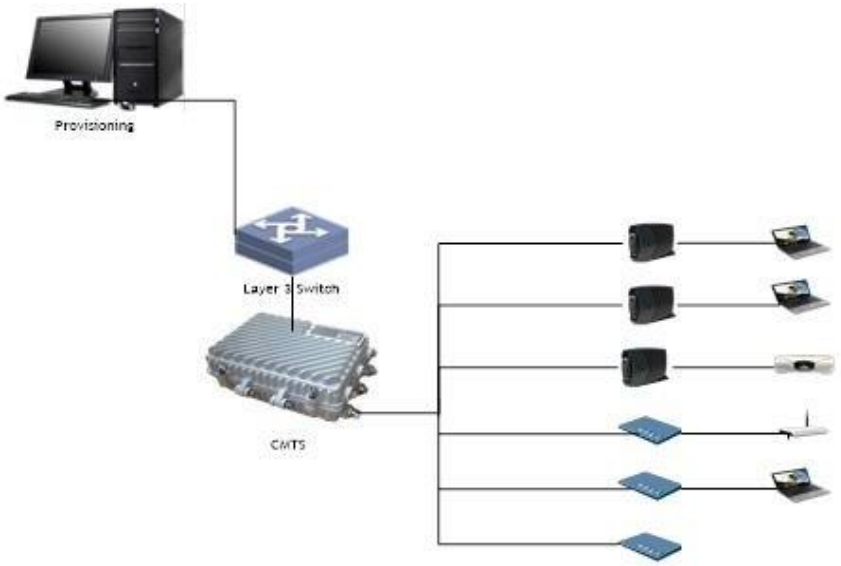

Figure 10-1 Networking Diagram of Configure TFTP Server Address Replacement

Data Planning

Table 10-2 Data Planning for Configure TFTP Server Address Replacement

Item	Data
TFTP-Proxy switch	Enable
TFTP-Proxy server	IPv4: 172.16.10.2; IPv6: 2003::2

Prerequisites

- Network and CMTS equipment are normal.
- The address configured by TFTP server shall exist in CMTS interface interface and can ping with TFTP server address.

Configuration Flowchart

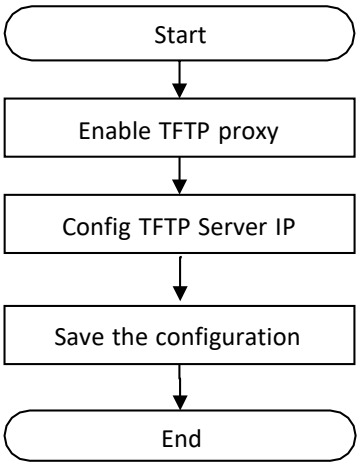

Figure 10-2 Flow Chart of Configure TFTP Server Address Replacement

Procedure

Step 1 Enable TFTP proxy:

1. Enter CMTS view

```
BT(config)# interface cmts 1
```

2. Enable TFTP proxy

```
BT(config-if-cmts-1)# cable tftp-proxy
```

Step 2 Config TFTP Server IPv4:

```
BT(config-if-cmts-1)# cable tftp-proxy server ipv4
172.16.10.2
```

Step 3 **Config** TFTP Server IPv6:

```
BT(config-if-cmts-1)# cable tftp-proxy server ipv6 2003::2
```

Step 4 Save the configuration.

```
BT(config)# end
BT# copy running-config startup-config
This will save the configuration to the flash memory.
Are you sure?(y/n) [n]y
Building configuration.....
Configuration saved successfully.
```

Result

The next server IP address of DHCP offer / ack message will be replaced with 172.16.10.2; the suboption TFTP server address (option17.32) of DHCPv6 advertisement and reply message vendor specific information will be replaced with 2003:: 2.

The IPv4 TFTP request for CM will be sent to 172.16.10.2.

IPv6 TFTP request of CM will be sent to 2002:: 2.

Chapter 11 RF Channel Management

The device supports DOCSIS2.0 and DOCSIS3.0 channels. This chapter mainly describes the configuration of radio frequency parameters, quality control, automatic frequency hopping technology and modulation template management of SC (Single Carrier) channel.

- Configure the basic parameters of upstream and downstream SC channel: configure the central frequency, bandwidth, modulation mode and other parameters of the channel.
- Channel quality monitoring: Set the threshold of signal quality monitoring. When the channel quality becomes worse, the equipment automatically alarms, reminding users to monitor problems or adjust business.
- Automatic Frequency Hopping Management: Configuration of frequency hopping strategy, when the channel quality changes, through pre-set conditions for automatic frequency hopping.
- Modulation template management: When the default modulation template cannot meet the actual deployment of customers, we can customize the modulation template to achieve the desired purpose.

11.1 Configure Basic Parameters of SC Channels

The basic parameters of SC channel include:

Table 11-1 Basic Parameters of SC Channel for CMTS Equipment

Item	Parameter
Upstream SC channel ID	1-8
Upstream SC channel center frequency	5M Hz-85M Hz
Upstream SC channel bandwidth	1.6M|3.2M|6.4M
Upstream SC channel modulation mode	ATDMA: qpsk | qam16 | qam32 | qam64 | qam256
Upstream SC channel mode	v3.0 | v2.0
Upstream SC channel reception level	(-14.0) dBmV -14.0dBmV
Downstream SC channel ID	1-32
Downstream SC channel center frequency	European standard: 87 ~ 1006MHz American Standard: 54 ~ 1002MHz
Downstream SC channel modulation mode	qam64 | qam256 | qam1024
Downstream SC channel format	Annex a: European standard, bandwidth fixed to 8MHz Annex b: US Standard, bandwidth fixed at 6MHz
Receiving level of downstream SC channel	Relevant to the type of equipment

11.1.1 Example of SC Channel Basic Parameters

Configure basic parameters of the upstream/downstream channels through this task, to ensure normal RF signal of CMTS device.

Data Planning

The data planning for configuring the parameters of upstream/downstream channel of CMTS is shown as follows.

Table 11-2 Data Planning for Configuring Basic Parameters of Upstream/Downstream Channel of CMTS

Item	Data
Upstream SC channel ID	2
Upstream SC channel central frequency	15400000 Hz
Upstream SC channel bandwidth	6.4M
Upstream SC channel transmission mode	atdma
Upstream SC channel modulation mode	qam64
Upstream SC channel mode	v2.0
Downstream SC channel ID	2
Downstream SC channel central frequency	448000000 Hz
Downstream SC channel modulation mode	qam256
Downstream SC channel system	a
Downstream SC channel sending power level	42.6 dBmV
All parameters of the remaining channels	Default value

Prerequisite

The network CMTS is online normally.

Configuration flowchart

Configuration the parameters of upstream/downstream channel of the device is shown as figure below.

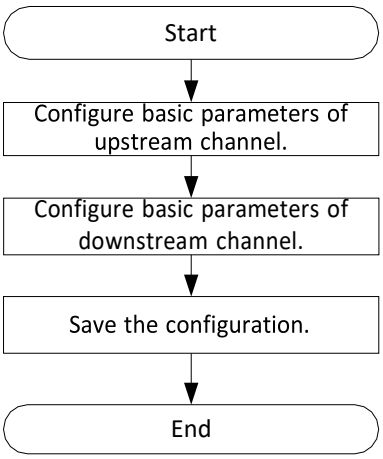

Figure 11-1 Flowchart for Configuration the Parameters of Upstream/Downstream Channel

Procedure

Step 1 Configure basic parameters of upstream channel.

```
BT(config-if-cmts-1)# cable upstream 2 frequency 15400000channel-width 6.4M atdma profile-type qam64 channel-mode v2.0
```

Step 2 Configure basic parameters of downstream channel.

```
BT(config-if-cmts-1)# cable downstream 2 frequency
448000000 modulation qam256 annex a power-level 42.6
It will take some time with a large number of CMs,please wait a
moment.
Modulation, annex and interleave on a group changed!
```

Step 3 Save the configurations.

```
BT(config-if-cmts-1)# end
BT# copy running-config startup-config
This will save the configuration to the flash memory.
Are you sure?(y/n) [n]y
Building configuration.....
Configuration saved successfully.
```

Result

According to the parameters of upstream/downstream channels of CMTS configured above, the CM which is online via the configured channels will use the parameters such as the channel frequency and bandwidth.

11.1.2 Configure Basic Parameters of Upstream Channel

Basic parameters of upstream channel include the following. Different parameters configure different functions. For details, refer to the sections for specific configurations of each parameter:

- Upstream SC channel state
- Upstream SC channel central frequency
- Upstream SC channel bandwidth
- Upstream SC channel transmission mode
- Upstream SC channel modulation mode
- Upstream SC channel mode
- Upstream SC channel receiving power level

11.1.2.1 Configure Upstream SC Channel State

Context

- By default, the upstream channel is disabled.
- After CMTS device online for the first time, it requires enabling manually the upstream SC channel to be used, and save it as the startup configuration.
- The CMTS device supports batch change the upstream SC channels state.

Procedure

Step 1 Disable the upstream channels by using the command "**cable upstream shutdown**" or enable the upstream channels by using the command "**no cable upstream shutdown**".

Step 2 View the channel state of the device by using the command "**show cable upstream**".

Example

Enable upstream channel 2-3 of CMTS device.

```
BT(config-if-cmts-1)# no cable upstream 2-3 shutdown
BT(config-if-cmts-1)# show cable upstream 2
upstream 2 is up
Channel utilization interval:180s , Avg channel utilization:0% , Curr Speed:0 bps
0 discarded, 11284 bytes input
Segments: 0 valid, 0 discarded
BT(config-if-cmts-1)# show cable upstream 3
upstream 3 is up
Channel utilization interval:180s , Avg channel utilization:0% , Curr Speed:0 bps
0 discarded, 10185 bytes input
Segments: 0 valid, 0 discarded
```

Related Operations

N/A

11.1.2.2 Configure Upstream SC Channel Central Frequency

Context

- The configuration prompt of upstream channel central frequency 5000000-85000000 indicates the operating frequency range instead of the central frequency allowed to be configured.
- The central frequency is determined jointly by the operating frequency range and bandwidth, i.e., 5000000 Hz <= minimum configuration frequency-bandwidth / 2 <= maximum configuration frequency + bandwidth / 2 <= 85000000 Hz.
- If the central frequency is not configured, the default center channel frequency for upstream SC channel 1 is 9000000 Hz, followed by an additional 6400000 Hz for the next channel.
- The CMTS device supports batch central frequency of upstream channel modification.The device supports configure begin upstream channel ID, begin frequency, frequency bandwidth or offset frequency, In order to realize batch central frequency of upstream channel modification.

Procedure

Step 1 Configure the upstream channel central frequency of CMTS device by using the command "**cable upstream frequency**", or configure the batch central frequency of upstream channel modification by using the command "**cable upstream frequency-batch**".

Step 2 View the configured central frequency of the device by using the command "**show running-config**".

Example

Configure the central frequency of upstream channel 2 as 15400000 Hz.

```
BT(config-if-cmts-1)# cable upstream 2 frequency 15400000 channel-width 6.4M atdma
profile-type qam64 channel-mode v2.0
BT(config-if-cmts-1)# show running-config | include upstream 2 frequency
 cable upstream 2 frequency 15400000 channel-width 6.4M atdma profile-type qam64
channel-mode v2.0
```

11.1.2.3 Configure Upstream SC Channel Bandwidth

Context

- The configuration range of upstream SC channel bandwidth is : 1.6M, 3.2M and 6.4M.
- The central frequency and bandwidth jointly constitute the operating frequency range of upstream SC channel, 5000000 <= minimum configuration frequency-bandwidth / 2 <= maximum configuration frequency + bandwidth / 2 <= 85000000.
- If it is not configured, the default upstream SC channel bandwidth is 3.2M.
- The CMTS device supports batch configure the upstream SC channels bandwidth.

Procedure

Step 1 Configure the channel bandwidth of CMTS device by using the command "**cable upstream channel-width**".

Step 2 View the configured bandwidth of the device by using the command "**show running-config**".

Example

Configure the bandwidth of upstream channel 2 as 1.6 MHz.

```
BT(config-if-cmts-1)# cable upstream 2 channel-width 1.6M
BT(config-if-cmts-1)# show running-config | include channel-width
 cable upstream 2 frequency 15400000 channel-width 1.6M atdma profile-type qam64-best
channel-mode v3.0
```

Related Operations

Table 11-3 Related Operations of Upstream Channel Bandwidth

Operation	Command	Remarks
Configure the upstream SC channel center frequency, bandwidth, modulation and other parameters	**cable upstream frequency channel-width profile-type channel-mode**	Specific command: **cable upstream** *channel-id* **frequency** *frequency* **channel-width (1.6M | 3.2M | 6.4M) atdma profile-type (qpsk | qam16 | qam32 | qam64 | qam256) channel-mode (v3.0 | v2.0)**

11.1.2.4 Configure Upstream Channel Modulation Mode

Context

- The upstream channel support ATDMA transmission mode.
- The modulation mode supported by ATDMA: qpsk | qam16 | qam32 | qam64 | qam256.
- If it is not configured, the default upstream channel modulation is "ATDMA QPSK".
- The CMTS device supports batch configure the upstream channels modulation mode.

Procedure

Step 1 Configure the channel modulation mode of CMTS device by using the command "**cable upstream profile-type**".

Step 2 View the configurations of the device by using the command "**show running-config**".

Example

Configure the transmission mode of upstream channel 1-2 as ATDMA and modulation mode as QAM64.

```
BT(config-if-cmts-1)# cable upstream 1-2 atdma profile-type qam64
BT(config-if-cmts-1)# show running-config | include qam64
 cable upstream 1 frequency 9000000 channel-width 3.2M atdma profile-type qam64
channel-mode v2.0
 cable upstream 2 frequency 15400000 channel-width 3.2M atdma profile-type qam64
channel-mode v2.0
```

Related Operations

Table 11-4 Related Operations of Upstream Channel Modulation Mode

Operation	Command	Remarks
Configure the upstream SC channel center frequency, bandwidth, modulation and other parameters	**cable upstream frequency channel-width profile-type channel-mode**	Specific command: **cable cable upstream** *channel-id* **frequency** *frequency* **channel-width (1.6M | 3.2M | 6.4M) atdma profile-type (qpsk | qam16 | qam32 | qam64 | qam256) channel-mode (v3.0 | v2.0)**

11.1.2.5 Configure Upstream SC Channel Receiving Power level

Context

- If you configure single or multiple channel levels, all channel levels are adjusted to this value at the same time.
- If it is not configured, for the default upstream channel receiving power level is 6 dBmV..

Procedure

Step 1 Configure the upstream channel receiving power level of CMTS device by using the command "**cable upstream power-level**".

Step 2 View the configurations of the device by using the command "**show cable upstream power-level**".

Example

Set the power level of upstream channel 2 as 13 dBmV.

```
BT(config-if-cmts-1)# show cable upstream power-level
Channel     Power(dBmV)
1           6.0
2           6.0
3           6.0
4           6.0
5           6.0
6           6.0
7           6.0
8           6.0
BT(config-if-cmts-1)# cable upstream 2 power-level 13
Power on all upstream channels changed!
BT(config-if-cmts-1)# show cable upstream power-level
Channel     Power(dBmV)
1           13.0
2           13.0
3           13.0
4           13.0
5           13.0
6           13.0
7           13.0
8           13.0
```

Related Operations

Table 11-5 Related Operations of Upstream Channel Receiving Power level

Operation	Command	Remarks
View the upstream channel receiving power level	**show cable upstream power-level**	
Enable automatic adjustment of upstream channel power level along with the temperature	**cable upstream power-level auto-adjust temperature**	After the function is enabled, the upstream channel power level of CMTS will adjust automatically along with the temperature, thus ensuring stable performance of the device. By default, the function is disabled.
Disable automatic adjustment of upstream channel power level along with the temperature	**no cable upstream power-level auto-adjust temperature**	

11.1.2.6 Configure Upstream SC Channel Mode

Context

- The upstream channel supports two modes: V2.0 and V3.0.
- V2.0 identifier of A-TDMA channel uses SAC1/SINC1/UCD29, and V3.0 identifier uses SAC2/SINC2/UCD35.
- If it is not configured, for the default upstream channel bandwidth.
- The CMTS device supports batch configure the upstream channels mode.

Procedure

Step 1 Configure the channel mode of CMTS device by using the command "**cable upstream channel-mode**".

Step 2 View the configurations of the device by using the command "**show running-config**".

Example

Configure the channel mode of upstream channel 2 as 3.0.

```
BT(config-if-cmts-1)# cable upstream 2 channel-mode v3.0 BT(config-if-cmts-
1)# show running-config | include channel-mode cable upstream 1 frequency
9000000 channel-width 3.2M atdma profile-type qpskchannel-mode v2.0
 cable upstream 2 frequency 15400000 channel-width 3.2M atdma profile-type qam64
channel-mode v3.0
 cable upstream 3 frequency 21800000 channel-width 3.2M atdma profile-type qpsk
channel-mode v2.0
 cable upstream 4 frequency 28200000 channel-width 3.2M atdma profile-type qpsk
channel-mode v2.0
```

Related Operations

Table 11-6 Related Operations of Upstream Channel Mode

Operation	Command	Remarks
Configure the upstream SC channel center frequency, bandwidth, modulation and other parameters	**cable upstream frequency channel-width profile-type channel-mode**	Specific command: **cable upstream** *channel-id* **frequency** *frequency* **channel-width (1.6M | 3.2M | 6.4M) atdma profile-type (qpsk | qam16 | qam32 | qam64 | qam256) channel-mode (v3.0 | v2.0)**

11.1.3 Configure Basic Parameters of Downstream SC Channel

Basic parameters of downstream channel include the following. Different parameters configure different functions. For details, refer to the sections for specific configurations of each parameter:

- Downstream SC channel state
- Downstream SC channel central frequency
- Downstream SC channel modulation mode
- Downstream SC channel annex
- Downstream SC channel sending power level

11.1.3.1 Configure Downstream SC Channel State Management

Context

- By default, the downstream channel is disabled.
- After CMTS is online for the first time, it requires enabling manually the downstream channel to be used, and save it as the startup configuration.
- The CMTS device supports batch change the downstream channels state.

Procedure

Step 1 Disable the downstream channels by using the command "**cable downstream shutdown**" or enable the downstream channels by using the command "**no cable downstream shutdown**".

Step 2 View the channel state of the device by using the command "**show running-config**".

Example

Enable the second downstream channel of CMTS.

```
BT(config-if-cmts-1)# no cable downstream 2 shutdown
It will take some time with a large number of CMs,please wait a moment.
BT(config-if-cmts-1)# show running-config | include downstream 2
 no cable downstream 2 shutdown
```

Related Operations

Table 11-7 Related Operations of Downstream Channel State

Operation	Command	Remarks
Enable the downstream channel	**no cable downstream shutdown**	

11.1.3.2 Configure Downstream SC Channel Type

Context

- The downstream channel supports two kinds of channels: DOCSIS and EQAM. The default channel is DOCSIS channel.
- The number of EQAM channels can be configured depending on the CMTS device type.
- The CMTS device supports batch configure the downstream channels type.

Procedure

Step 1 Configure EQAM channel by using the command "**cable downstream eqam**" or configure DOCSIS channel by disabling and then enabling the channel.

Step 2 View the channel type of the device by using the command "**show running-config**".

Example

Set the second downstream channel of CMTS EQAM type.

```
BT(config-if-cmts-1)# show running-config | include downstream 2
 no cable downstream 2 shutdown
BT(config-if-cmts-1)# cable downstream 2 eqam
It will take some time with a large number of CMs,please wait a moment.
BT(config-if-cmts-1)# show running-config | include downstream 2
 no cable downstream 2 shutdown
 cable downstream 2 eqam annex a symbolrate 6952
```

11.1.3.3 Configure Downstream Channel Central Frequency

Context

- The central frequency is determined jointly by the operating frequency range and bandwidth, 52000000 Hz <= minimum configuration frequency-bandwidth / 2 <= maximum configuration frequency + bandwidth / 2 <= 1002000000 Hz. The downstream frequency range of European standard is 87 ~ 1006 MHz, and the downstream frequency range of American standard is 54 ~ 1002 MHz.
- If the central frequency is not configured, for the default downstream channel 1 central frequency is 440000000 Hz, and other central frequencies in order to increase 8000000 Hz.
- The device supports batch downstream channel modification. The device supports configure begin downstream channel ID, begin frequency, offset frequency, In order to realize batch central frequency of downstream channels modification.

Procedure

Step 1 Configure the downstream channel central frequency of CMTS device by using the command "**cable downstream frequency**" or configure the batch central frequency of downstream channel modification by using the command "**cable downstream frequency-batch**".

Step 2 View the configured central frequency of the device by using the command "**show running-config**".

Example

Configure the central frequency of downstream channel 2 as 448000000 Hz.

```
BT(config-if-cmts-1)# cable downstream 2 frequency 448000000 modulationqam256
annex a power-level 42.6
It will take some time with a large number of CMs,please wait a moment.
BT(config-if-cmts-1)# show running-config | include downstream 2
 cable downstream 2 frequency 448000000 modulation qam256 annex a power-level 42.6
```

11.1.3.4 Configure Downstream SC Channel Annex

Context

- The downstream channel annex can be configured as European standard annex a or American standard annex b.
- When it is configured as annex a, the downstream channel bandwidth is 8MHz; when it is configured as annex b, the downstream channel bandwidth is 6MHz;
- If DOCSIS channel is configured as annex b, it needs to configure the interleaving depth parameter "interleave", which can be configured as 128 | 64 | 32 | 16 | 8; if it is configured as annex a, no configuration is required for this parameter.
- If EQAM channel is configured as annex a, it needs to configure the symbol rate parameter "symbolrate", which can be configured as 6952 | 6875 | 6900; if it is configured as annex b, no configuration is required for this parameter.
- The CMTS device supports batch configure the downstream channels annex.
- Switching the channel will result in device restart

Procedure

Step 1 Configure the downstream DOCSIS channel annex of CMTS device by using the command "**cable downstream annex**".

Step 2 View the channel annex of the device by using the command "**show running-config verbose**".

Example

The downstream channel is configured as US standard, the starting frequency is 300 Mhz, the frequency interval of each channel is 6 Mhz and the interleaving depth is 16.

```
BT(config-if-cmts-1)# cable downstream annex b start-freq 300000000 width-offset
6000000 interleave 16
Annex type change will request system reboot,continue?(y/n) [n]y
Annex change.
starting pid 6693, tty '': '/bin/sh -l -c "bcm_boot_launcher stop"'
Stopping CMS smd...
smd received Terminate msg!! Terminate all apps and then exit.
Unmounting filesystems...
Sent SIGTERM to all processes
Sent SIGKILL to all processes
Requesting system reboot
```

Related Operations

Table 11-8 Related Operations of Downstream Channel annex

Operation	Command	Remarks
Set the EQAM channel system	**cable downstream eqam annex**	Specific command:**cable downstream** *channel-list* **eqam annex a symbolrate (6952 | 6875 | 6900)** **cable downstream** *channel-list* **eqam annex b**
Set the downstream channel as EQAM channel	**cable downstream frequency modulation annex power-level**	Specific command:**cable downstream** *channel-id* **frequency** *frequency* **modulation (qam64 | qam256 | qam1024) annex a power-level** *power* **cable downstream** *channel-id* **frequency** *frequency* **modulation (qam64 | qam256 | qam1024) annex b power-level** *power* **interleave** *interleave*

11.1.3.5 Configure Downstream SC Channel Modulation Mode

Context

- The downstream channel modulation mode supports qam64 | qam256 | qam1024. The larger the value of modulation mode is, the greater bandwidth for channel transmission is used, but the lower the interference capability is. It needs to be configured according to the actual line.
- If it is not configured, for the default downstream channel modulation mode is qam256.
- The CMTS device supports batch configure the downstream channels modulation mode.

Procedure

Step 1 Configure the channel modulation mode of CMTS device by using the command "**cable downstream modulation**".

Step 2 View the configurations of the device by using the command "**show running-config verbose**".

Example

Configure the modulation mode of channel 3 as qam256.

```
BT(config-if-cmts-1)# cable downstream 3 modulation qam256
It will take some time with a large number of CMs,please wait a moment.
BT(config-if-cmts-1)# show running-config verbose | include downstream 3
 no cable downstream 3 shutdown
 cable downstream 3 docsis
 cable downstream 3 frequency 456000000 modulation qam256 annex a power-level 45.0
 no cable downstream 3 primary
 cable downstream 3 prov-attr-mask 00000000
```

Related Operations

Table 11-9 Related Operations of Downstream Channel Modulation Mode

Operation	Command	Remarks
Configure the downstream channel modulation mode	**cable downstream frequency modulation (qam64 | qam256 | qam1024) annex a power-level** **cable downstream frequency modulation (qam64 | qam256 | qam1024) annex b power-level interleave**	Specific command: **cable downstream** *channel-id* **frequency** *frequency* **modulation (qam64 | qam256 | qam1024) annex a power-level** *power* **cable downstream** *channel-id* **frequency** *frequency* **modulation (qam64 | qam256 | qam1024) annex b power-level** *power* **interleave** *interleave*

11.1.3.6 Configure Downstream SC Channel Sending Power Level

Context

Configure the range of downstream channel sending power level by using the command "**cable downstream power-level**".

View the configurable range of the maximum downstream channel sending power level and the number of the channels by using the command "**show cable downstream max-power-level**".

View the configurable range of the minimum downstream channel sending power level by using the command "**show cable downstream min-power-level**".

- If it is not configured, for the default downstream channel sending power level is 45 dBmV.
- The CMTS device supports batch configure the downstream channels sending power level.

Procedure

Step 1 Configure the downstream sending power level of CMTS device by using the command "**cable downstream power-level**".

Step 2 View the configurations of the device by using the command "**show running-config**".

Example

Configure the power level of downstream channel 4 as 43 dBmV.

```
BT(config-if-cmts-1)# cable downstream 4 power-level 43
It will take some time with a large number of CMs,please wait a moment.
BT(config-if-cmts-1)# show running-config | include downstream 4
 cable downstream 4 frequency 464000000 modulation qam256 annex a power-level 43.0
```

Related Operations

Table 11-10 Related Operations of Downstream Channel Modulation Sending Power level

Operation	Command	Remarks
Configure the downstream SC channel center frequency, modulation and power level parameters	**cable downstream frequency modulation (qam64 | qam256 | qam1024) annex a power-level** **cable downstream frequency modulation (qam64 | qam256 | qam1024) annex b power-level**	Specific command: **cable downstream** *channel-id* **frequency** *frequency* **modulation (qam64 | qam256 | qam1024) annex a power-level** *power* **cable downstream** *channel-id* **frequency** *frequency* **modulation (qam64 | qam256 | qam1024) annex b power-level** *power* **interleave** *interleave*

Note:

The downstream circuit attenuation of CC8800-C-P2 equipment is pluggable adjustment. When the maximum output level is set by DOCSIS motherboard module, the pluggable attenuation value of the whole downstream circuit needs to be ⩾ 4dB.

11.1.3.7 Configure Primary Downstream SC Channel

Context

- Configure the primary downstream channel by using the command "**cable downstream primary**".
- In devices, all downstream channels default to the primary channel.
- CM needs to synchronize time in the main channel and receive MDD messages before registering; after

registering, it needs to synchronize time in the main channel.

Procedure

Step 1 Configure the primary downstream of CMTS device by using the command "**cable downstream primary**".

Step 2 View the configurations of the primary downstream channel by using the command "**show running-config**".

Example

Configure the downstream channel 4 as primary channel.

```
BT(config-if-cmts-1)# cable downstream 4 primary
BT(config-if-cmts-1)# show running-config verbose | include cable downstream4
 cable downstream 4 primary
```

Related Operations

Table 11-11 Related Operations of Primary Downstream Channe

Operation	Command	Remarks
Cancel set a single or multiple downstream channels as the primary channels	**no cable downstream primary**	

11.1.4 Configuring an EQAM channel

Integrating the EQAM function in the CMTS device can make full use of the frequency resource of the CMTS device. When the DOCSIS traffic is insufficient to occupy the entire frequency domain, the remaining frequency resources can be used to spread the TV service, which has flexibility. Therefore, CMTS supporting EQAM has become the best choice for HFC network transformation.

11.1.4.1 Example of EQAM Configuration

Data Planning

Multiple STBs are accessed under one CMTS. The EQAM TS stream is pushed to the IP interface 172.16.50.177 of the CMTS. The service mode is VOD on demand. Only two programs are pushed. The two programs are distinguished by different destination UDP ports. The destination UDP ports are 10000 and 10001 respectively. The type of stream is spts.

Table 11-1 Configure EQAM Data Planning

Item	Data
EQAM channel	Channel 32, frequency: 203M Symbol rate: 6875 Transmitting level: 45.0 dBmv, on
EQAM template ID	1

Item	Data
EQAM service IP	172.16.50.177
EQAM service VLAN	0
EQAM service tsid-base value	0
EQAM template internal channel configuration	Channel 32, TSID offset: 1000, QAM manager: VOD
EQAM program stream mapping destination UDP port	program stream 1: 10000 ; program stream 2: 10001
EQAM program stream mapping stream type	spts
EQAM program stream mapping input program number	0
EQAM program stream map output program number	program stream 1:1, program stream 2:2
EQAM program stream mapping PMV	program stream 1:1, program stream 2:2

Context

- Network equipment and lines are normal.

Configuration flowchart

The EQAM process is configured as shown in the following figure.

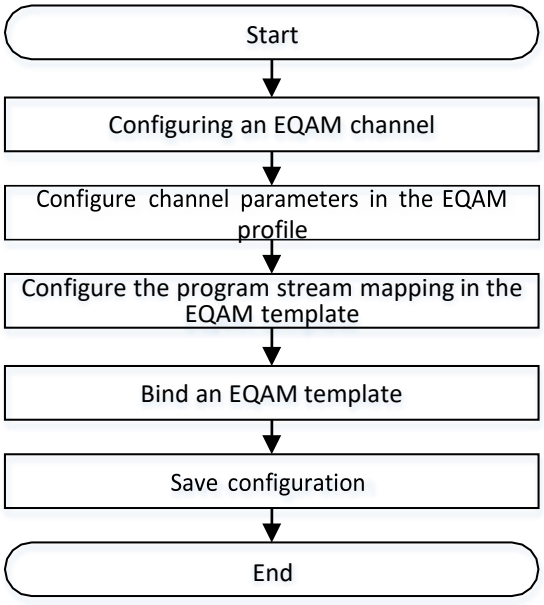

Figure 11-1 Configure the Signal quality monitoring Flowchart of the Uplink Channel

Procedure

Step 1 Configuring an EQAM channel.

1. Configure the download channel 32 to use a frequency of 203 MHz, a modulation scheme of QAM256, and a transmission level of 45 dBmv.

```
BT(config-if-cmts-1)# cable downstream 32 frequency
203000000 modulation qam256 annex a power-level 45.0
It will take some time with a large number of CMs,please wait a
moment.
Modulation, annex, symbolrate and interleave on a group changed!
```

2. The download channel 32 s configured as an EQAM channel, and the standard is the European standard, and the symbol rate is 6875.

```
BT(config-if-cmts-1)# cable downstream 32 eqam annex a
symbolrate 6875
It will take some time with a large number of CMs, please wait
amoment.
```

3. Open the downstream channel 32.

```
BT(config-if-cmts-1)# no cable downstream 32 shutdown It will
take some time with a large number of CMs,please wait amoment.
```

Step 2 Configure the channel parameters in the EQAM profile. The QAM manager is VOD, the TSID offset is 1000, and the rest of the parameters are configured by default.

```
BT(config-if-eqam-template-1)# eqam channel 32 tsid-offset 1000
qam-group-name Beijing-haidian qam-manager vod original- network-
id 32 pat-interval 100 pmt-interval 100 sdv-switch disable
sdv-port-start 1
```

Step 3 Configure the program stream mapping in the EQAM template.

1. Configure program stream 1 to configure the destination UDP port to be 10000, the stream type to spts, the output program number to 1, the PMV to 1, and the rest of the parameters to use the default values.

```
BT(config-if-eqam-template-1)# eqam channel 32 mapping 1
stream-type spts udp 10000 out-pn 1 pmv 1
```

2. Configure program stream 2 to configure the destination UDP port to be 10001, the stream type to spts, the output program number to 2, and the PMV to 2. The remaining parameters are default values.

```
BT(config-if-eqam-template-1)# eqam channel 32 mapping 2
stream-type spts udp 10001 out-pn 2 pmv 2
```

Step 4 Bind an EQAM template.

1. Exit the eqam template view.

```
BT(config-if-eqam-template-1)# exit
```

2. Enter cmts view.

```
BT(config)# interface cmts 1
```

3. Bind an EQAM template.

```
BT(config-if-cmts-1)# eqam bind eqam-template 1 service-ip
172.16.50.177 tsid-base 0
```

Step 5 Save configuration

```
BT(config)# end
BT# copy running-config startup-config
This will save the configuration to the flash memory.
Are you sure?(y/n) [n]y
Building configuration.....
Configuration saved successfully.
```

---- The end

Result

After the configuration is completed, the server pushes the program stream. The destination IP of the program stream is 172.16.50.177, the destination UDP port number of program stream 1 is 10000, and the destination UDP port number of program stream 2 is 10001. At this point, the user can use the set-top box to normally order the program.

11.1.4.2 Configure an EQAM template

Context

Configuration within the EQAM template includes program stream mapping configuration and channel parameter configuration

- The program stream mapping supports mapping to source IP address, destination IP address, UDP port, stream-type, in-pn, and out-pn parameters.
- Channel parameter configuration supports tsid-offset, qam-group-name, qam-manage, original-network-id, pat-interval, pmt-interval, sdv-switch, sdv-port-start parameters

Procedure

Step 1 Use the "**eqam channel original-network-id**" command to configure the initial network ID of the EQAM profile (see related operations for other parameters) or use the "**eqam batch-mapping channel mapping-start**" command to configure the mapping (see related operations for other parameters).

Step 2 Use the "**show running-config**" command to view the configuration of the device.

---- The end

Example

Set the initial network ID in the EQAM profile to 1000.

```
BT(config-if-eqam-template-1)# eqam channel 32 original-network-id 1000 BT(config-if-eqam-template-1)# show running-config | include original-network-id
```

```
eqam channel 32 tsid-offset 1000 qam-group-name "BEIJING-HAIDIAN" qam-manager vod
original-network-id 1000 pat-interval 100 pmt-interval 100 sdv-switch disable sdv-
port-start 1
```

Related Operations

Table 11-2 Related Operations for the EQAM Template Configuration

Operation	Command	Remarks
Configure the EQAM channel-level service-related configuration in the EQAM profile view.	**eqam channel tsid-offset qam-group-name qam-manager original-network-id pat-interval pmt-interval sdv-switch sdv-port-start**	The specified command is: **eqam channel** *channel-list* **tsid-offset** *tsid-offset* **qam-group-name** *gpnm* **qam-manager (vod | svod | broadcast) original-network-id** *network-id* **pat-interval** *pat-interval* **pmt-interval** *pmt-interval* **sdv-switch (enable | disable) sdv-port-start** *sdv-port-start*
Configure the PAT table sending interval.	**eqam channel pat-interval**	
Configure the PMT table sending interval.	**eqam channel pmt-interval**	
Configure the QAM group name.	**eqam channel qam-group-name**	
Configuring the QAM manager type	**eqam channel qam-manager**	
Configure the SDV port start value.	**eqam channel sdv-port-start**	
Configure SDV function management status	**eqam channel sdv-switch**	
Configure the TSID offset value	**eqam channel tsid-offset**	
Configure the TSID offset value to modify the start value and TSID offset value in batches.	**eqam tsid-start tsid-step**	
Create program stream maps in batches based on specified channels	**eqam batch-mapping channel**	The specified command is: **eqam batch-mapping channel** *channel-id* **mapping-start** *mapping-id-start* **mapping-num** *mapping-num* **src-ip-start** *src-ipv4-start* **src-ip-step** *src-ipv4-step* **dst-ip-start** *dst-ipv4-start* **dst-ip-step** *dst-ipv4-step* **udp-start**

Operation	Command	Remarks
		dst-port-start **udp-step** *dst-port-step* **stream-type (mpts | data)** **eqam batch-mapping channel** *channel-id* **mapping-start** *mapping-id-start* **mapping-num** *mapping-num* **src-ip-start** *src-ipv4-start* **src-ip-step** *src-ipv4-step* **dst-ip-start** *dst-ipv4-start* **dst-ip-step** *dst-ipv4-step* **udp-start** *dst-port-start* **udp-step** *dst-port-step* **stream-type (spts | datar) in-pn-start** *in-program-no-start* **in-pn-step** *in-program-no-step* **out-pn-start** *out-program-no-start* **out-pn-step** *out-program-no-step* **pmv-start** *pmv-start* **pmv-step** *pmv-step*
Delete program stream mapping configuration	**no eqam mapping**	

11.1.4.3 Apply an EQAM template to the CMTS device.

Context

After the EQAM template is configured, you can apply the template on the CMTS.

- When applied to a template, you can configure the service IP address, service VLAN, and TSID base value.
- The EQAM profile has been applied to the CMTS. If you need to adjust the service IP address, service VLAN, and TSID base value, you can reconfigure it through a separate command without releasing the application.

Procedure

Step 1 Use the "**eqam bind eqam-template service-ip tsid-base**" command to configure the application of the EQAM profile on the CMTS.

Step 2 Use the "**show running-config**" command to view the configuration of the device.

---- The end

Example

Applies EQAM profile 1 on CMTS 1, and the service IP address is 172.16.50.177, the TSID base value is10000, and the service VLAN is 20.

```
BT(config-if-cmts-1)# eqam bind eqam-template 1 service-ip 172.16.50.177tsid-
base 10000 vlan 20
BT(config-if-cmts-1)# show running-config | include eqam bind
 eqam bind eqam-template 1 service-ip 172.16.50.177 tsid-base 10000 vlan 20
```

Related Operations

Table 11-3 Related Operations for Applying EQAM Template in CMTS

Operation	Command	Remarks
Release CMTS application EQAM	**no eqam bind**	
Adjust business IP	**eqam service-ip**	The specified command is: **eqam service-ip** *service-ipv4* **[vlan** *vlan-id***]**
Adjust the TSID base value	**eqam tsid-base**	

11.2 Channel Quality Monitoring

Upstream noise interferes with signal transmission of upstream channels and affects the quality of the user data service, voice service, and other services.

This section describes the basic channel quality management of the CMTS. When the channel quality deteriorates, the CMTS generates an alarm and notifies users in time for troubleshooting and service adjustment. The next section describes the automatic frequency hopping function.

11.2.1 Configure the Example of Upstream Channel Signal Quality Monitoring

Data Planning

The data planning for configuring the example of upstream channel signal quality monitoring is shown as follows.

Table 11-12 Data Planning for Configuring the Example of Upstream Channel Signal Quality Monitoring

Item	Data
The function of upstream channel signal quality monitoring	Enabled
Polling cycle of upstream channel signal quality monitoring	100 seconds
Recording of upstream channel signal quality parameters	Enabled
SNR warning threshold	21.0
SNR recovery threshold	28.0
Error-correctable code waring threshold	200
Error-correctable code recovery threshold	100
Error-correctable code waring threshold	180
Error-correctable code recovery threshold	120

Context

Network devices and lines must be in the normal state.

Configuration flowchart

The process for configuring the spectrum noise monitoring is shown as follows.

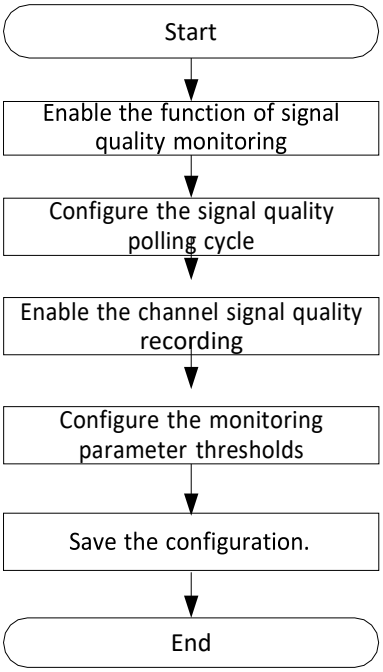

Figure 11-2 Flowchart for Configuring the Upstream Channel Signal Quality Monitoring

Procedure

Step 1 Enable real-time upstream channel signal acquisition function of CMTS device.

```
BT(config)# cable upstream signal-quality real-time snmp-data
```

Step 2 Configure the signal quality polling cycle as 100s.

```
BT(config)# cable upstream signal-quality query-period 100
```

Step 3 Enable the function of signal quality recording.

```
BT(config)# cable upstream signal-quality record
```

Step 4 Configure the monitoring parameter thresholds.

1. Configure SNR warning threshold as 21.0 and recovery threshold as 28.0.

   ```
   BT(config)# cable upstream snr threshold-warning 21.0
   threshold-recovery 28.0
   ```

2. Configure the error-correctable code warning threshold as 200 and recovery threshold as 100.

   ```
   BT(config)# cable upstream correcteds threshold-warning
   200 threshold-recovery 100
   ```

3. Configure the error-uncorrectable code warning threshold as 180 and recovery threshold as 120.

   ```
   BT(config)# cable upstream uncorrectable threshold-warning
   180 threshold-recovery 120
   ```

Step 5 Save the configurations.

```
BT(config)# end
BT# copy running-config startup-config
This will save the configuration to the flash memory.
Are you sure?(y/n) [n]y
Building configuration.....
Configuration saved successfully.
```

Result

After finishing the configuration, CMTS will monitor the signal quality according to the configured monitoring cycle and frequency interval. If the acquired data exceeds the configured threshold, an alarm will be triggered.

11.2.2 Enable the Upstream Signal Quality Monitoring

Context

- CMTS device supports real-time upstream signal acquisition via SNMP.
- If it is not configured, by default, the function is enabled.

Procedure

Step 1 Enable the upstream channel spectrum noise monitoring of CMTS device by using the command "**cable upstream signal-quality real-time snmp-data**".

Step 2 View the real-time upstream signal acquisition function of the device by using the command "**show running-config verbose**".

Example

Enable the upstream channel spectrum noise monitoring.

```
BT(config)# cable upstream signal-quality real-time snmp-data
BT(config)# show running-config verbose | include snmp-data
 cable upstream signal-quality real-time snmp-data
```

Related Operations

Table 11-13 Related Operations of Upstream Signal Quality Monitoring

Operation	Command	Remarks
Disable the real-time upstream signal acquisition function	**no cable upstream signal-quality real-time snmp-data**	

11.2.3 Enable the Polling Cycle of Upstream Quality Monitoring

Context

- Before setting the polling cycle of quality monitoring, CMTS device shall enable its upstream channel quality monitoring function.
- If it is not configured, the default cycle is 180s.

Procedure

Step 1 Configure the polling cycle of upstream channel quality monitoring of CMTS device by using the command "**cable upstream signal-quality query-period**".

Step 2 View the polling cycle of upstream channel quality monitoring of the device by using the command "**show running-config verbose**".

Example

Enable the upstream channel spectrum noise monitoring.

```
BT(config)# cable upstream signal-quality query-period 100
BT(config)# show running-config verbose | include query-periodcable
upstream signal-quality query-period 100
```

Related Operations

Table 11-14 Related Operations of Upstream Signal Quality Monitoring

Operation	Command	Remarks
Restore the default polling cycle against channel quality parameters	**no cable upstream signal-quality query-period**	

11.2.4 Enable the Upstream Signal Quality Recording

Context

- CMTS device supports the function of upstream channel quality history. After this function is enabled, the device will record the upstream channel data in the memory.
- If it is not configured, by default, the function is disabled.

Procedure

Step 1 Enable the function of upstream channel quality recording of CMTS device by using the command "**cable upstream signal-quality record**".

Step 2 View the function of real-time upstream signal acquisition by using the command "**show running-config**".

Example

Enable the function of upstream channel quality history.

```
BT(config-if-cmts-1)# cable upstream signal-quality record
BT(config-if-cmts-1)# show running-config | include signal-quality
 cable upstream signal-quality record
```

Related Operations

Table 11-15 Related Operations of Upstream Channel Quality Parameter History

Operation	Command	Remarks
Disable the upstream channel quality history of the device	**no cable upstream signal-quality record**	
Clear the upstream channel quality history of the device	**clear cable upstream signal-quality record**	

11.2.5 Configure the Upstream Signal Quality Monitoring Threshold

Context

- When configuring this item, it requires enabling the upstream signal quality monitoring first.
- The upstream signal quality monitoring includes SNR monitoring, error-correctable code monitoring and error-uncorrectable code monitoring.
- If it is not configured, the default SNR threshold is 26.0 and recovery threshold is 27.0; the default error-correctable and error-uncorrectable code threshold is 150 and recovery threshold is 100.

Procedure

Step 1 Configure the upstream SNR warning threshold and recovery threshold of CMTS device by using the command "**cable upstream snr threshold-warning threshold-recovery**".

Step 2 Configure the upstream error-correctable code warning threshold and recovery threshold of CMTS device by using the command "**cable upstream correcteds threshold-warning threshold-recovery**".

Step 3 Configure the upstream error-uncorrectable code warning threshold and recovery threshold of CMTS device by using the command "**cable upstream uncorrectables threshold-warning threshold-recovery**".

Step 4 View the configuration of upstream signal monitoring threshold by using the command "**show running-config verbose**".

Example

Configure the SNR warning threshold as 21.0 and recovery threshold as 28.0; configure the error-correctable code warning threshold as 200 and recovery threshold as 100; configure the error-uncorrectable code warning threshold as 180 and recovery threshold as 120.

```
BT(config-if-cmts-1)# cable upstream snr threshold-warning 21.0 threshold-recovery 28.0
BT(config-if-cmts-1)# cable upstream correcteds threshold-warning 200 threshold-recovery 100
BT(config-if-cmts-1)# cable upstream uncorrectable threshold-warning 180 threshold-recovery 120
BT(config-if-cmts-1)# show running-config | include threshold-warning
 cable upstream snr threshold-warning 21.0 threshold-recovery 28.0
 cable upstream correcteds threshold-warning 200 threshold-recovery 100
 cable upstream uncorrectables threshold-warning 180 threshold-recovery 120
```

11.2.6 Display the Noise Information of the Upstream Spectrum

Context

CMTS upstream data transmission is vulnerable to external noise interference. The user can view the noise information of the upstream spectrum to analyze the noise levels on the spectrum spatial signal and the upstream channel. This device supports to display the upstream noise spectrum at specific frequency intervals.

Procedure

Step 1 Enter the cmts view by using the command "**interface cmts 1**".

Step 2 Display the noise information of the upstream spectrum by using the command "**show cable scqam upstream-spectrum (channel-width-1.6M | channel-width-3.2M | channel-width-6.4M)**".

Example

Display noise information of the upstream spectrum.

```
BT(config)# interface cmts 1
BT(config-if-cmts-1)# show cable scqam upstream-spectrum channel-width-6.4M
FREQUENCY  NOISE-LEVEL at channel-width 6400000
CenterFreq(Hz)  AVG(dBmV)   MIN(dBmV/Hz)        MAX(dBmV/Hz)
5000000         -54.9       -60.7/8160000       -42.1/5220000
11400000        -55.8       -61.0/9620000       -45.5/12260000
17800000        -58.3       -61.0/15220000      -47.1/20920000
24200000        -48.4       -61.0/21380000      -37.9/25520000
30600000        -51.0       -61.0/33400000      -38.0/28100000
```

37000000	-54.5	-60.8/35820000	-45.1/38120000
43400000	-59.0	-61.0/43040000	-49.0/40480000
49800000	-59.6	-61.0/46920000	-53.8/52600000
56200000	-59.2	-61.0/53240000	-52.7/55480000
62600000	-59.9	-61.0/60240000	-57.3/61840000
69000000	-60.0	-61.0/66980000	-57.0/70180000
75400000	-60.0	-61.0/72300000	-59.0/72940000
81800000	-59.9	-61.0/82160000	-59.0/78920000

Related Operations

Table 11-16 Related Operations of Noise Information of the Upstream Spectrum

Operation	Command	Remarks
Display the noise information of the upstream spectrum	**show cable scqam upstream-spectrum** *freq-begin freq-end freq-interval*	

11.3 Spectrum (Automatic Frequency-Hopping) Management

When the quality of upstream channel between CMTS and CM deteriorates, such as too heavy upstream channel noise, too heavy downstream channel noise, and other factors causing the increased packet loss and bad packets, normal data communication between CMTS and CM will be affected. Spectrum function can achieve automatic recovery in case of upstream channel quality deterioration, and automatic recovery and location of .network faults, thus avoiding the situation that the users are not served for a long period due to channel quality deterioration.

The principle for spectrum realization is as follows: read periodically the upstream channel quality parameter, and compare it with the pre-set threshold parameter. When the recovery threshold is met for three consecutive cycles, and the delay to the previous hop reaches at least 600s, it will be recovered to a better modulation mode.

Three conditions must be satisfied simultaneously for triggering the frequency-hop check:

- Global spectrum function is enabled;
- Spectrum group function is enabled;
- Apply the spectrum group on the channel.

When the frequency-hop check is triggered, the parameters cannot be modified. To configure parameters of spectrum group, it requires disabling the frequency-hop check first, that is, just have any of the above-mentioned three conditions not satisfied.

The configuration of spectrum function includes three aspects: global configuration, spectrum group-based configuration, and channel-based spectrum application configuration. In the following, these three aspects will be described respectively.

11.3.1 Example of Spectrum Configuration

In existing network, CMTS may suffer from unstable channel frequency quality. Appropriate recovery and adjustment are expected when the channel quality deteriorates. It is expected to try the modulation mode with better fault tolerance first, then reduce the bandwidth of original frequency and finally try a new central frequency when the original channel frequency quality deteriorates.

Data Planning

The data planning for configuring the upstream channel spectrum example is shown as follows.

Table 11-17 Data Planning for Configuring the Mode Example

Item	Data
Global frequency-hop function	Enabled
Cycle of Channel quality polling	100s
Max. number of spectrum history	20
Spectrum-group ID	1
Spectrum-group state	enable
Spectrum-group policy	modulation
Spectrum-group mode	SNR
SNR threshold 1	25
SNR threshold 2	20
FEC recovery threshold 1	0
FEC recovery threshold 2	0
FEC irreparability threshold 1	0
FEC irreparability threshold 2	0
Spectrum group-based number of frequency-hop per channel	100
Channel modulation mode	atdma qam16 qpsk
Channel ID applied to spectrum group	1

Context

Network devices and lines must be in the normal state.

Configuration flowchart

The process for configuring the spectrum is shown as follows.

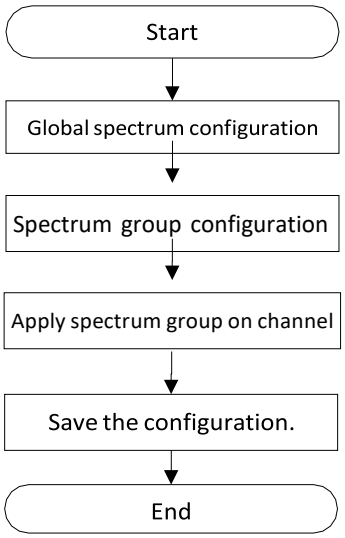

Figure 11-3 Flowchart for Configuring the Spectrum

Procedure

Step 1 Global spectrum configurations.

1. Enable the spectrum function globally.

   `BT(config)# cable spectrum-group enable`

2. Configure the polling cycle of channel quality monitoring as 100s. `BT(config)# cable upstream signal-quality query-period100`

3. Configure the max. number of spectrum data history as 20.

   `BT(config)# cable spectrum-group max-history 20`

Step 2 Spectrum group configurations.

1. Create spectrum group 1.

   `BT(config)# cable spectrum-group 1`

2. Enable spectrum group 1.

   `BT(config)# cable spectrum-group 1 enable`

3. Configure spectrum group policy as width mode.

   `BT(config)# cable spectrum-group 1 policy modulation`

4. Configure the frequency-hop mode as SNR threshold. `BT(config)# cable spectrum-group 1 method snr`Configure SNR warning

5. threshold 1 as 25 and SNR warning threshold 2 as 20.

   `BT(config)# cable spectrum-group 1 threshold snr 25 20`

6. Configure not supporting the FEC correctable code-based frequency hop. `BT(config)# cable spectrum-group 1 threshold fec correct0 0`

7. Configure not supporting the FEC uncorrectable code-based frequency hop.

   `BT(config)# cable spectrum-group 1 threshold fec uncorrect 0 0`

Step 3 Configure the channel-based application of spectrum group.

1. Configure the frequency-hop limit of the channel applying spectrum group as 100.

```
BT(config)# cable spectrum-group 1 limit 100
```

2. Enter the cmts view.

```
BT(config)# interface cmts 1
```

3. Configure the backup modulation mode of upstream channel 1 as atdma qam16 qpsk.

```
BT(config-if-cmts-1)# cable upstream 1 spectrum-groupprofile
atdma qam16 qpsk
```

4. Configure applying applying the spectrum group 1 to upstream channel 1.

```
BT(config-if-cmts-1)# cable upstream 1 spectrum-group 1
```

Step 4 Save the configurations.

```
BT(config)# end
BT# copy running-config startup-config
This will save the configuration to the flash memory.
Are you sure?(y/n) [n]y
Building configuration.....
Configuration saved successfully.
```

Result

After finishing the configurations, CMTS executes the frequency hop by the configured frequency-hop policy, mode and threshold. When the real-time data reaches the threshold, the frequency-hop will be triggered.

11.3.2 Global Spectrum Configuration

Context

Global spectrum configuration includes: global state of spectrum function, cycle of upstream channel quality query and the maximum number of upstream channel spectrum history.

- The global state of spectrum function determines the effectiveness of spectrum function of the device. When the management state is “enable”, the spectrum function may take effect, which may also depend on other configurations. When the management state is “disable”, the spectrum function will not take effect. By default, it is disabled.
- The query cycle of upstream channel quality parameter determines the spectrum responsiveness. The system will depend on the channel quality parameter in three consecutive cycles to determine whether to conduct the frequency-hop. To make the spectrum responsive, it requires setting the cycle to be a smaller value, but taking into comprehensive account the load capability of the system. It is recommended to configure this parameter on a reasonable manner. The default value of this parameter is 180s.

- In the process of frequency-hop by the upstream channel, the system will record the frequency-hop history by channel, and allows to configure the channel-based maximum number of history. If exceeding this number, new frequency-hop event will cover the old one. The default value of this parameter is 16.

Procedure

Step 1 Configure enabling the spectrum group globally by using the command "**cable spectrum-group enable**".

Step 2 View the configurations of global spectrum of the device by using the command "**show cable spectrum-group**".

Example

Set enabling the frequency-hop function globally.

```
BT(config)# cable spectrum-group enable
BT(config)# show cable spectrum-group spectrum
group global configuration:
------------------------------------------------------------------------
 administration status: enable
 maximum hop history record: 20
 hop recover time limit: 1800s
 Created spectrum group: 1
```

Related Operations

Table 11-18 Related Operations of Global Spectrum

Operation	Command	Remarks
Configure the polling cycle of channel signal quality	**cable upstream signal-quality query-period**	
Configure the max number of frequency-hop history	**cable spectrum-group max-history**	

11.3.3 Spectrum Group Configuration

The system supports at most 32 spectrum groups. Each spectrum group can configure different frequency-hop policy. CMTS can execute the frequency-hop by such policies, to avoid channel quality deterioration.

11.3.3.1 Create and Enable A Spectrum Group

Context

The system supports at most 32 spectrum groups. The successfully-create spectrum groups can be applied to any upstream channel of CMTS. Each channel can only apply one spectrum group.

Procedure

Step 1 Create a spectrum group by using the command "**cable spectrum-group** *group-id*".

Step 2 Configure enabling the spectrum group by using the command "**cable spectrum-group** *group-id* **enable**".

Step 3 Configure parameters of the spectrum group.

Step 4 View specified spectrum group configuration by using the command "**show cable spectrum-group** *group-id*".

Example

Set enabling spectrum group 1, with the maximum number of channel frequency-hop as 20 via SNR.

```
BT(config)# cable spectrum-group 1 BT(config)# cable
spectrum-group 1 enable BT(config)# cable spectrum-group 1
limit 20 BT(config)# cable spectrum-group 1 method snr
BT(config)# cable spectrum-group 1 min-interval 35
BT(config)# cable spectrum-group 1 policy frequency
BT(config)# cable spectrum-group 1 threshold snr 25 20
BT(config)# cable spectrum-group 1 threshold fec correct 0 0
BT(config)# cable spectrum-group 1 threshold fec uncorrect 0 0
BT(config)# cable spectrum-group 1 frequency 3 47800000 width 6.4M 11
BT(config)# show cable spectrum-group 1
spectrum group 1 config:
-----------------------------------------------------------------------------------------
 administration status: enable
 hop method: snr
 hop minimum interval: 35s
 channel snr threshold(1,2): 25.0dB,20.0dB
 channel fec corretable threshold(1,2): 0%,0%
 channel fec uncorretable threshold(1,2): 0%,0%
 channel range-loss threshold: 20
 hop policy: frequency
 hop limit: 20
spectrum group 1 member frequency:
Index     frequency     maxWidth     power
-------------------------------------------------------------
3         47800000      6.4M         11.0
spectrum group 1 application info:
cmts                     upstream channels
-------------------------------------------------------------
```

Related Operations

Table 11-19 Related Operations for Creating and Enabling the Spectrum Group

Operation	Command	Remarks
Delete the spectrum group	**no cable spectrum-group group-id**	
Disable the spectrum group	**cable spectrum-group group-id disable**	

11.3.3.2 Frequency-hop Policy for Spectrum Group

Context

- The spectrum group policy includes: frequency | width | modulation | freq-width.
- When configuring the frequency-hop policy, the frequency-hop check shall be disabled. For conditions for triggering the frequency-hop check, refer to the section "Create and Enabling the Spectrum Group".
- The default spectrum group is "modulation".

Procedure

Step 1 Configure the spectrum group policy by using the command "**cable spectrum-group policy**".

Step 2 View the spectrum group policy by using the command "**show cable spectrum-group group-id**".

Example

Set the policy for enabling the spectrum group 1 as width.

```
BT(config)# cable spectrum-group 1 policy width
BT(config)# show cable spectrum-group 1 spectrum group
1 config:
--------------------------------------------------------------------------------------------
 administration status: enable
 hop method: snr
 hop minimum interval: 600s
 channel snr threshold(1,2): 20.0dB,15.0dB
 channel fec correctable threshold(1,2): 0%,0%
 channel fec uncorrectable threshold(1,2): 0%,0%
 channel range-loss threshold: 20
 hop policy: width
 hop limit: unlimited
spectrum group 1 member frequency:
Index     frequency     maxWidth      power
-----------------------------------------------------------------
spectrum group 1 application info:
cmts          upstream channels
-----------------------------------------------------------------
```

Related Operations

Table 11-20 Related Operations of Spectrum Policy

Operation	Command	Remarks
Restore the default spectrum group policy	**no cable spectrum-group** *group-id* **policy**	

11.3.3.3 Frequency-hop Mode of Spectrum Group

Context

- The spectrum group mode: snr.
- Currently the frequency-hop mode only supports SNR.
- When configuring the spectrum group mode, the frequency-hop check shall be disabled. For conditions for triggering the frequency-hop check, refer to the section "Create and Enable the Spectrum Group".
- The default frequency-hop mode is snr.

Procedure

Step 1 Configure the spectrum group policy by using the command "**cable spectrum-group method**".

Step 2 View the spectrum mode by using the command "**show cable spectrum-group** *group-id*".

Example

Set the spectrum mode as SNR.

```
BT(config)# cable spectrum-group 1 method snr
BT(config)# show running-config verbose | include method snr
 cable spectrum-group 1 method snr BT(config)#
show cable spectrum-group 1spectrum group 1
config:
--------------------------------------------------------------------------------------------
 administration status: enable
 hop method: snr
 hop minimum interval: 600s
 channel snr  threshold(1,2):  20.0dB,15.0dB
 channel fec correctable threshold(1,2): 12%,20%
 channel fec uncorrectable threshold(1,2): 15%,20%
 channel range-loss threshold: 20
 hop policy: modulation
 hop limit: 100
spectrum group 1 member frequency:
Index     frequency     maxWidth      power
------------------------------------------------------------
```

```
spectrum group 1 application info:
cmts                        upstream channels
------------------------------------------------------------------
```

Related Operations

Table 11-21 Related Operations of Spectrum Mode

Operation	Command	Remarks
Restore the default spectrum mode.	**no cable spectrum-group** *group-id* **policy**	

11.3.3.4 Frequency-hop Threshold of Spectrum Group

Context

The spectrum group threshold includes SNR threshold and FEC threshold.

The parameters of upstream channel quality include: SNR, correctable FEC and uncorrectable FEC. FEC threshold parameter is allowed to be set as 0, i.e., this parameter is not taken into account, but just take SNR as the threshold parameter.

The channel quality deterioration threshold can be determined if the following two conditions are satisfied simultaneously:

- SNR <= SNR threshold.
- The correctable FEC ≥ correctable threshold, or the uncorrectable CodeWord ≥ uncorrectable threshold.

The channel quality recovery threshold can be determined if any of the following two conditions is satisfied:

- SNR>SNR threshold.
- When threshold is not 0: The correctable FEC < correctable threshold; When threshold is 0: Ignore this condition.
- When threshold is not 0: The uncorrectable FEC < uncorrectable threshold; When threshold is 0: Ignore this condition.

Procedure

Step 1 Configure the frequency-hop threshold by using the command "**cable spectrum-group threshold**".

Step 2 View the spectrum mode by using the command "**show cable spectrum-group** *group-id*".

Example

Set the SNR threshold of spectrum group 1 as 25.1 19.1.

```
BT(config)# cable spectrum-group 1 method snr
```

```
BT(config)# cable spectrum-group 1 threshold snr 25.1 19.1
BT(config)# cable spectrum-group 1 threshold fec correct 0 0
BT(config)# cable spectrum-group 1 threshold fec uncorrect 0 0
BT(config)# show running-config verbose | include method snr
 cable spectrum-group 1 method snr BT(config)#
show cable spectrum-group 1spectrum group 1
config:
--------------------------------------------------------------------------------------------
 administration status: enable
 hop method: snr
 hop minimum interval: 600s
 channel snr threshold(1,2): 25.1dB,19.1dB
 channel fec correctable threshold(1,2): 0%,0%
 channel fec uncorrectable threshold(1,2): 0%,0%
 channel range-loss threshold: 20
 hop policy: modulation
 hop limit: 100
spectrum group 1 member frequency:
Index     frequency     maxWidth      power
------------------------------------------------------------
spectrum group 1 application info:
cmts                      upstream channels
------------------------------------------------------------
```

Related Operations

Table 11-22 Related Operations of Spectrum Threshold

Operation	Command	Remarks
Restore the default SNR threshold of spectrum group	**no cable spectrum-group** *group-id* **threshold snr**	
Restore the default FEC threshold of spectrum group	**no cable spectrum-group** *group-id* **threshold fec (correct | uncorrect)**	

11.3.4 Channel-based Spectrum Configuration

Context

To apply the spectrum function on CMTS device, it needs to apply the spectrum group on the channel. One channel can apply exclusively one spectrum group. The following spectrum parameters can be configured on the channel:

- Configure the limit number of frequency hop each channel in the spectrum group;
- Configure the standby modulation mode on the channel;

- Apply the spectrum group on the channel.

There's interval limit between two frequency hops on the channel. The interval parameter can be configured. When the conditions for frequency hop are satisfied, but the minimum interval is not satisfied, the frequency-hop event will not be triggered until the minimum interval reaches. Appropriate configuration of the minimum interval for frequency hop can effectively improve the responsiveness of channel parameters for fast implementation of frequency hop.

Procedure

Step 1 Configure the limit number of upstream channel frequency-hop by using the command "**cable spectrum-group limit**".

Step 2 Configure the upstream channel modulation mode by using the command "**cable upstream spectrum-group profile**".

Step 3 Apply the spectrum group to the upstream channel by using the command "**cable upstream spectrum-group**".

Step 4 Display the spectrum configurations of special upstream channel by using the command "**show cable upstream spectrum-group**".

Example

Set the number of channel frequency-hop as 100; then set the channel modulation mode as ATDMAQAM16 QPSK; and apply the spectrum group 1 to the upstream channel 1 in the end.

```
BT(config)# cable spectrum-group 1 limit 100
BT(config)# interface cmts 1
BT(config-if-cmts-1)# cable upstream 1 spectrum-group profile atdma qam16qpsk
BT(config-if-cmts-1)# cable upstream 1 spectrum-group 1 BT(config-
if-cmts-1)# show cable upstream 1 spectrum-groupchannel's spectrum
group configuration:
--------------------------------------------------------------------------
 spectrum group id: 1
 spectrum group backup profile-type:qam64 qpsk
 channel's spectrum group status information:
--------------------------------------------------------------------------
 current center frequency: 10000000 Hz
 current width: 3.2MHz
 current modulation: qam256
 current receive power: 10.0 dBmV
 current channel snr: ---
 current channel correctable code rate: ---
 current channel uncorrectable code rate: ---
 current channel range-loss: 0 %
```

```
current channel good count: 0
current channel bad count: 0
total hop count: 0
current used member frequency:
last hop time: ---
last recovery hop time: ---
```

Related Operations

Table 11-23 Related Operations of Automatic Frequency Hopping Based on Channel

Operation	Command	Remarks
Set not to limit the number of channel frequency hop	**cable spectrum-group** *group-id* **limit unlimited**	
Restore the default total number of spectrum(not to limit the number of channel frequency hop)	**no cable spectrum-group** *group-id* **limit**	
Delete the backup spectrum modulation mode	**no cable upstream** *channel-id* **spectrum-group profile**	
Delete the channel spectrum group	**no cable upstream** *channel-id* **spectrum-group**	
Clear the channel spectrum group application on all channels	**clear cable spectrum-group** *group-id* **apply**	

11.4 RCC Template Configuration

When a CM goes online, it sends its rcp-id to the CMTS to indicate its receiving capability. The RCC template automatically compares its rcp-id with that sent by the CM when the CM goes online. If the two rcp-ids are consistent, the CMTS initializes the CM by using the receive module and receive channel information configured in the template. If the two rcp-ids are inconsistent, the CMTS uses the built-in RCC template to initialize the CM.

The RCC configuration includes the receive module and receive channel:

- Receive module: It specifies the number of receive modules available to the CM, start frequency, end frequency, and associated receive modules. A single template supports at most 6 receive modules.
- Receive channel: It specifies the number of channels on each receive module corresponding to the CM, and related frequencies. An RCC template supports at most 10 receive channels.

11.4.1 RCC Template Configuration Example

The CMTS is connected to CMs provided by different vendors. With the RCC template, different CMs can go online on different channels.

Data Planning

The following table provides data planning for the RCC template configuration example.

The CMTS is connected to CMs provided by different vendors. The rcp-id for one CM type is 00 10 00 00 08, and the rcp-id for another CM type is 00 20 00 00 08. The CMs of the first type must go online on channel 1, and the CMs of the second type must go online on channel 2.

Table 11-24 Data planning for the RCC template configuration example

Item	Data
CM 1 rcp-id	00 10 00 00 08
CM 2 rcp-id	00 20 00 00 08
Receiving module 1 corresponding to CM 1	Channel 1 frequency : 440000000
Receiving module 1 corresponding to CM 2	Channel 1 frequency : 512000000
CM 1 Corresponding Receiving Channel 1	Central frequency : 440000000, connect receiving module 1
CM 2 Corresponding Receiving Channel 1	Central frequency : 512000000, connect receiving module 1

Background Information

- Network devices and lines are both normal.

Configuration Flow

The following figure shows the RCC template configuration flow.

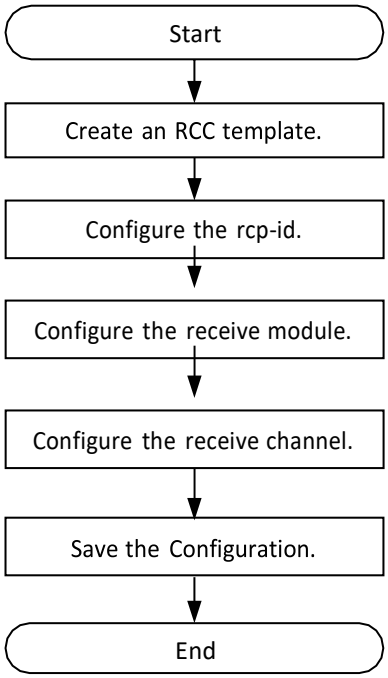

Figure 11-4 Flowchart for Configuration the Parameters of RCC template

Operation Procedures

RCC template configuration for the first type of CM:

Step 1 Create an RCC template.

```
BT(config)# cable rcc-template 1
```

Step 2 Configure the rcp-id in the RCC template.

```
BT(config-rcc-template1)# rcp-id 00 10 00 00 08
```

Step 3 Configure the receive module in the RCC template.

```
BT(config-rcc-template1)# receive-module 1 first-channel-center-frequency 440000000
```

Step 4 Configure the receive channel in the RCC template.

```
BT(config-rcc-template1)# receive-channel 1 center-frequency 440000000 connected-receive-module 1
BT(config-rcc-template1)# exit
```

RCC template configuration for the second type of CM:

Step 1 Create an RCC template.

```
BT(config)# cable rcc-template 2
```

Step 2 Configure the rcp-id in the RCC template.

```
BT(config-rcc-template2)# rcp-id 00 20 00 00 08
```

Step 3 Configure the receive module in the RCC template.

```
BT(config-rcc-template2)# receive-module 2 first-channel-center-frequency 512000000
```

Step 4 Configure the receive channel in the RCC template.

```
BT(config-rcc-template2)# receive-channel 2 center-frequency 512000000 connected-receive-module 2
```

Step 5 Save the configuration.

```
BT(config-rcc-template2)# end
BT# copy running-config startup-config
This will save the configuration to the flash memory.
Are you sure?(y/n) [n]y
Building configuration.....
Configuration saved successfully.
```

Operational Result

After configuration is completed, the CMTS is connected to CMs provided by different vendors, and CMs of different vendors go online on different channels.

11.4.2 Configure RCC receive channel parameters

Context

The configuration of RCC receiving parameters includes: receiving channel index, receiving channel center frequency, receiving module index and whether or not the main channel.

Procedure

Step 1 Use the "**receive-channel** *channel-id* **center-frequency** *frequency* **connected-receive-module** *connect-module-id* **[primary]**" command to configure RCC receive channel parameters.

Step 2 Use the "**show running-config**" command to see the RCC receive channel parameters.

Example

$Configuring receive channel parameters.

```
BT(config-rcc-template1)# receive-channel 1 center-frequency 560000000
connected-receive-module 1 primary
BT(config-rcc-template1)# show running-config
rcp-id 0x00 0x00 0x00 0x00 0x00
 receive-module 1 channel-center-frequency 560000000 connected-receive-module 1
```

Related Operations

Table 11-4 Related Operations for Receiving Channel Parameters

Operation	Command	Remarks
Delete receive channel	**no receive-channel** *channel-id*	

11.4.3 Configuring RCC receiver module

Context

The configuration of RCC receiving module includes: the index of receiving module, the central frequency of the first channel of receiving module, the index signal of receiving channel, whether it is configured as the main channel, etc.

Procedure

Step 1 configures the RCC receiving module using the "**receive-module** *module-id* **first-channel-center-frequency** *frequency* **[connected-receive-module** *connect-module-id***]**" command.

Step 2 uses the "**show running-config**" command to view the RCC receiving module.

Example

Configure receive module.

```
BT(config-rcc-template1)# receive-module 1 first-channel-center-frequency
440000000
BT(config-rcc-template1)# show running-config
receive-module 1 first-channel-center-frequency 440000000
```

Related Operations

Table 11-5 Related Operations for Configure Receive Module

Operation	Command	Remarks
Delete receive channel	`no receive-channel`	

11.5 Modulation Template Management

CM will select the corresponding modulation template for different services. CM sends different types of data to the upstream. The system supports 18 default modulation templates.

Added system-supported modulation templates (tabular form)

When the default modulation template can not meet the actual deployment of customers, we can meet business needs by customizing the modulation template (adjusting DOCSIS signal debugging parameters). The system supports 36 customized modulation templates. DOCSIS's modulation parameters are very professional and need to have professional staffing. Otherwise, it may have an impact on the business.

11.5.1 Example of Create and Refer to ATDMA Modulation Template

Networking Diagram

Through this example, an ATDMA mode modulation template can be created and referenced by the upstream channel. The requirements are as follows:

Data Planning

In this example, the index ID of the extended modulation template is 20, the channel mode is ATDMA, and the modulation mode is QAM64, which enables FEC to correct errors.

The upstream channel UCD type is 29.

Each IUC data plan is shown below.

Table 11-6 Data Planning for Configuration of ATDMA QAM64 Modulation Template

IUC / Item	Request	Initial	Station	Adv Short	Adv Long	Adv UGS
fecT	0	5	5	12	16	8
fecK	16	34	34	75	223	76
Maximum mini-slot in burst	1	0	6	11	0	0
Sudden intervals	8	48	48	8	8	8
modulation mode	QPSK	QPSK	QPSK	QAM64	QAM64	QAM16
Scrambling switch	Enable	Enable	Enable	Enable	Enable	Enable
Scrambling polynomial factor	338	338	338	338	338	338

IUC / Item	Request	Initial	Station	Adv Short	Adv Long	Adv UGS
Differential Coding Switch	Shut	Shut	Shut	Shut	Shut	Shut
preamble size	56	384	384	68	76	76
Whether the FEC codeword is truncated at last	Fixed	Fixed	Fixed	Shortened	Shortened	Shortened
Preamble type	QPSK1	QPSK1	QPSK1	QPSK1	QPSK1	QPSK1
RS Coding Interleaving Depth	1	1	1	1	0	1
RS coded interleaving block size	1536	1536	1536	1536	1536	1536

Prerequisite

- CMTS and CM terminals are properly configured

Configuration flowchart

The process of configuring a modulation template that creates and references ATDMA mode is illustrated below.

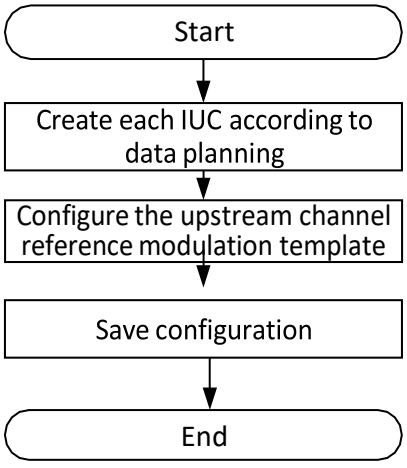

Figure 11-5 Flowchart for Create ATDMA Modulation Template and Reference it

Procedure

Step 1 Create each IUC configuration in the modulation template.

```
BT(config)# cable modulation-profile 20 requestqpsk    0 16 1 8
scrambler 338 no-diff 56 fixed qpsk1 1 1536
BT(config)# cable modulation-profile 20 initial        5 34 0 48
qpsk scrambler 338 no-diff 384 fixed qpsk1 1 1536
BT(config)# cable modulation-profile 20 station        5 34 6 48
qpsk scrambler 338 no-diff 384 fixed qpsk1 1 1536
```

```
BT(config)# cable modulation-profile 20 a-short 12 75 11 8
qam64 scrambler 338 no-diff 68 shortened qpsk1 1 1536
BT(config)# cable modulation-profile 20 a-long 16 223 0 8
qam64 scrambler 338 no-diff 76 shortened qpsk1 0 1536
BT(config)# cable modulation-profile 20 a-ugs 8 76 0 8 qam16
scrambler 338 no-diff 76 shortened qpsk1 1 1536
```

Step 2 Enter the CMTS view and configure the upstream channel 2 reference to the extended template.

```
BT(config-if-cmts-1)# cable upstream 2 frequency 15400000channel-
width 3.2M modulation-profile 20 channel-mode v2.0
```

Step 3 Save configuration.

```
BT(config)# end
BT# copy running-config startup-config
This will save the configuration to the flash memory.
Are you sure?(y/n) [n]y
Building configuration.....
Configuration saved successfully.
```

Result

After configuration is completed, CMTS device can create a modulation template of ATDMA mode and let the upstream channel reference.

11.6 Configure Basic Parameters of OFDM Downstream Channel

The basic parameters of the downstream OFDM channel include the following. Different parameters are configured with different functions. For details, please refer to the specific configuration section of each parameter:

- ID of downstream channel
- Downstream start and end frequency
- Frequency point of downstream PLC
- NCP modulation mode
- Cycle prefix length
- Roll off interval
- Time domain interleaving depth
- Transmission level
- Management status

- Excluded bandwidth
- Profile configuration
- Subcarrier spacing of downstream channel
- Frequency point 0 of downstream channel subcarrier
- Downstream main channel capacity

11.6.1 Configure OFDM Downstream Channel State

Context

- The range of the OFDM downstream channel ID is 193-193.
- By default, the OFDM downstream channel is disabled.
- After CMTS is online for the first time, it requires manually enabling the OFDM downstream channel to be used, and save it as the startup configuration.
- The CMTS device supports batch change the OFDM downstream channels state.

Procedure

Step 1 Disable the OFDM downstream channels by using the command "**cable ofdm-downstream shutdown**" or enable the OFDM downstream channels by using the command "**no cable ofdm-downstream shutdown**".

Step 2 View the channel state of the device by using the command "**show cable ofdm-downstream config**".

Example

Enable the first OFDM downstream channel of CMTS:

```
BT(config-if-cmts-1)#  no  cable  ofdm-downstream  193  shutdown
BT(config-if-cmts-1)# show cable ofdm-downstream 193 configChannel
ID                              : 193
Admin Status                    : enable
Lower Edge Frequency(Hz)        : 660000000
Upper Edge Frequency(Hz)        : 684000000
PLC Frequency(Hz)               : 666000000
Subcarrier Zero Frequency(Hz)  : 650000000
Subcarrier Spacing Type         : 50k
Cyclic Prefix                   : 256tsu
Rolloff Period                  : 64tsu
Time Interleave Depth           : 16
Ncp Modulation Type             : qam16
```

```
Output power(dBmV)              : 20.0
Profile List                    : 0-1
Is primary channel              : Yes
```

Related Operations

N/A

11.6.2 Configure Lower Frequency and Upper Frequency of OFDM Downstream Channel

Context

- The range of the lower frequency and upper frequency is 258MHz - 1218MHz.
- The bandwidth of the channel is 22MHz - 190MHz
- The lower frequency and upper frequency must be a multiple of the carrier interval.
- The lower frequency must be greater than subcarrier zero frequency + 6.4MHz.

Procedure

Step 1 Disable the OFDM downstream channels by using the command "**cable ofdm-downstream shutdown**".

Step 2 Configure the lower frequency and upper frequency OFDM downstream channels by using the command "**cable ofdm-downstream lower-frequency upper-frequency**".

Step 3 View the lower frequency and upper frequency by using the command "**show cable ofdm-downstream config**".

Example

Configure the lower frequency as 662000000 Hz and upper frequency as 690000000 Hz:

```
BT(config-if-cmts-1)# cable ofdm-downstream 193 shutdown
BT(config-if-cmts-1)# cable ofdm-downstream 193 lower-frequency 662000000
upper-frequency 690000000
BT(config-if-cmts-1)# show cable ofdm-downstream 193 config
Channel ID                      : 193
Admin Status                    : disable
Lower Edge Frequency(Hz)        : 662000000
Upper Edge Frequency(Hz)        : 690000000
PLC Frequency(Hz)               : 666000000
Subcarrier Zero Frequency(Hz)   : 650000000
Subcarrier Spacing Type         : 50k
Cyclic Prefix                   : 256tsu
```

```
Rolloff Period                : 64tsu
Time Interleave Depth         : 16
Ncp Modulation Type           : qam16
Output power(dBmV)            : 20.0
Profile List                  : 0
Is primary channel            : Yes
```

Related Operations

N/A

11.6.3 Configure NCP Modulation of OFDM Downstream Channel

Context

- The range of the NCP (Next Codeword Pointer) modulation is QPSK, QAM16 and QAM64.

Procedure

Step 1 Configure the NCP modulation of OFDM downstream channels by using the command "**cable ofdm-downstream ncp-modulation**".

Step 2 View the NCP modulation by using the command "**show running-config verbose**".

Example

Configure the NCP modulation of OFDM downstream channels as QAM64:

```
BT(config-if-cmts-1)# cable ofdm-downstream 193 ncp-modulation qam16
BT(config-if-cmts-1)# show cable ofdm-downstream 193 config
Channel ID                        : 193
Admin Status                      : enable
Lower Edge Frequency(Hz)          : 198000000
Upper Edge Frequency(Hz)          : 258000000
PLC Frequency(Hz)                 : 214000000
Subcarrier Zero Frequency(Hz)  :  191600000
Subcarrier Spacing Type  : 50k
Cyclic Prefix                     : 512tsd
Rolloff Period                    : 128tsd
Time Interleave Depth             : 16
Ncp Modulation Type               : qam16
Output power(dBmV)                : 45.0
Profile List                      :
Is primary channel                : Yes
```

Related Operations

N/A

11.6.4 Configure Cyclic Prefix and Rolloff Period of OFDM Downstream Channel

Context

- If it is not configured, for the default cyclic prefix as 512tsd. The range as follows:
  - 192tsd
  - 256tsd
  - 512tsd
  - 768tsd
  - 1024tsd
- If it is not configured, for the default rolloff period as 128tsd. The range as follows:
  - 0tsd
  - 64tsd
  - 128tsd
  - 192tsd
  - 256tsd
- The value of rolloff period must be less than half the cyclic prefix.

Procedure

Step 1 Disable the OFDM downstream channels by using the command "**cable ofdm-downstream shutdown**".

Step 2 Configure the cyclic prefix and rolloff period of OFDM downstream channel by using the command "**cable ofdm-downstream cyclic-prefix rolloff-period**".

Step 3 View the configured the cyclic prefix and rolloff period by using the command "**show cable ofdm-downstream config**".

Example

Configure the the cyclic prefix as 192tsd and rolloff period as 64tsd:

```
BT(config-if-cmts-1)# cable ofdm-downstream 193 shutdown
BT(config-if-cmts-1)# cable ofdm-downstream 193 cyclic-prefix 192tsd rolloff-period
64tsd
BT(config-if-cmts-1)# show cable ofdm-downstream 193 config
Channel ID                      : 193
Admin Status                    : disable
```

```
Lower Edge Frequency(Hz)    : 662000000 Upper
Edge  Frequency(Hz)         :  690000000  PLC
Frequency(Hz)                    : 668000000
Subcarrier  Zero  Frequency(Hz)  :  652000000
Subcarrier Spacing Type  : 25k
Cyclic Prefix                    : 192tsd
Rolloff Period                   : 64tsd
Time Interleave Depth            : 16
Ncp Modulation Type              : qam16
Output power(dBmV)               : 20.0
Profile List                     : 0
Is primary channel               : Yes
```

Related Operations

N/A

11.6.5 Configure Time Interleave of OFDM Downstream Channel

Context

- Time interleave is a method to transform the sequence of data.
- When the carrier is 25KHz, the range of time interleave is 1-16.
- When the carrier is 50KHz, the range of time interleave is 1-32.

Procedure

Step 1 Disable the OFDM downstream channels by using the command "**cable ofdm-downstream shutdown**".

Step 2 Configure the time interleave of the OFDM downstream channel by using the command "**cable ofdm-downstream time-interleave**".

Step 3 View the channel annex of the device by using the command "**show cable ofdm-downstream config**".

Example

Configure the time interleave of the OFDM downstream channel as 10:

```
BT(config-if-cmts-1)# cable ofdm-downstream 193 shutdown BT(config-if-
cmts-1)# cable ofdm-downstream 193 time-interleave 10BT(config-if-cmts-1)#
show cable ofdm-downstream 193 config
Channel ID                       : 193
Admin Status                     : disable
Lower Edge Frequency(Hz)         : 662000000
Upper Edge Frequency(Hz)         : 690000000
```

```
PLC Frequency(Hz)                : 668000000
Subcarrier Zero Frequency(Hz)  : 652000000
Subcarrier Spacing Type   : 25k
Cyclic Prefix                    : 96tsu
Rolloff Period                   : 32tsu
Time Interleave Depth            : 10
Ncp Modulation Type              : qam16
Output power(dBmV)               : 20.0
Profile List                     : 0
Is primary channel               : Yes
```

Related Operations

N/A

11.6.6 Configure PLC Frequency of OFDM Downstream Channel

Context

- The range of PLC (PHY Link Channel) frequency must be within the range of the channel's effective spectral.
- The start frequency of the PLC must be an integer multiple of 1MHz

Procedure

Step 1 Disable the OFDM downstream channels by using the command "**cable ofdm-downstream shutdown**".

Step 2 Configure the PLC frequency of the OFDM downstream channel by using the command "**cable ofdm-downstream plc-frequency**".

Step 3 View the PLC frequency by using the command "**show cable ofdm-downstream config**".

Example

Configure the PLC frequency of the OFDM downstream channel as 668000000 Hz:

```
BT(config-if-cmts-1)# cable ofdm-downstream 193 shutdown BT(config-if-cmts-1)#
cable ofdm-downstream 193 plc-frequency 668000000BT(config-if-cmts-1)# show
cable ofdm-downstream 193 config
Channel ID                       : 193
Admin Status                     : disable
Lower Edge Frequency(Hz)         : 662000000
Upper Edge Frequency(Hz)         : 690000000
PLC Frequency(Hz)                : 668000000
Subcarrier Zero Frequency(Hz)  : 652000000
Subcarrier Spacing Type          : 25k
```

```
Cyclic Prefix                  : 96tsu
Rolloff Period                 : 32tsu
Time Interleave Depth          : 10
Ncp Modulation Type            : qam16
Output power(dBmV)             : 20.0
Profile List                   : 0
Is primary channel             : Yes
```

Related Operations

N/A

11.6.7 Configure Sending Power Level of OFDM Downstream Channel

Context

- The transmission level support range is 17-60 dBmv.

Procedure

Step 1 Disable the OFDM downstream channels by using the command "**cable ofdm-downstream shutdown**".

Step 2 Configure the downstream sending power level of CMTS device by using the command "**cable ofdm-downstream power-level**".

Step 3 View the sending power level of the device by using the command "**show cable ofdm-downstream config**".

Example

Configure the power level of OFDM downstream channel 193 as 25 dBmV:

```
BT(config-if-cmts-1)# cable ofdm-downstream 193 shutdown BT(config-if-
cmts-1)# cable ofdm-downstream 193 power-level 25BT(config-if-cmts-1)#
show cable ofdm-downstream 193 config Channel ID      : 193
Admin Status                   : disable
Lower Edge Frequency(Hz)       : 662000000
Upper Edge Frequency(Hz)       : 690000000
PLC Frequency(Hz)              : 668000000
Subcarrier Zero Frequency(Hz) : 652000000
Subcarrier Spacing Type        : 25k
Cyclic Prefix                  : 96tsu
Rolloff Period                 : 32tsu
Time Interleave Depth          : 10
Ncp Modulation Type            : qam16
Output power(dBmV)             : 25.0
```

```
Profile List                    : 0
Is primary channel              : Yes
```

Related Operations

N/A

11.6.8 Configure Exclusion Band of OFDM Downstream Channel

Context

- OFDM downstream channel allows the partial spectrum bandwidth to be set to exclude. That is, to allow a part of the OFDM channel spectrum to be reserved for other services, to avoid interference with the spectrum.
- The start frequency and the end frequency must be an integer multiple of the subcarrier spacing.
- The start frequency and the end frequency must be within the OFDM channel spectrum (lowerFreq+1M, upperFreq-1M).
- The start frequency is less than the end frequency.
- At least one continuous 22M wide continuous modulation bandwidth.
- The minimum continuous modulation bandwidth is 2M.
- Excluded band is at least 1M, and the granularity is an integer multiple of the subcarrier width.
- The PLC frequency (6MHz) spectrum bandwidth can not include the excluded bandwidth.
- Different excluded bandwidth can not overlap.

Procedure

Step 1 Disable the OFDM downstream channels by using the command "**cable ofdm-downstream shutdown**".

Step 2 Configure the exclusion band of OFDM downstream channels by using the command "**ofdm-downstream exclude-band**".

Step 3 View the configurations of the device by using the command "**show cable ofdm-downstream exclusion-band**".

Example

Configure the exclusion band of OFDM downstream channel 193 as 25 dBmV:

```
BT(config-if-cmts-1)# cable ofdm-downstream 193 shutdown
BT(config-if-cmts-1)# cable ofdm-downstream 193 exclusion-band 662000000
664000000
BT(config-if-cmts-1)# show cable ofdm-downstream 193 exclusion-band
Channel ID              : 193
```

```
Start Frequency(Hz)    : 662000000
End Frequency (Hz)     : 664000000
```

Related Operations

N/A

11.6.9 Configure Profile Defalt Modulation of OFDM Downstream Channel

Context

- Each OFDM downstream channel supports several profiles for data transmission.
- The range of profile ID is 0-15, that is Profile A, Profile B …Profile P. Profile A is a general profile
- By default, only Profile A configuration exists on the channel, which supports dynamic creation of Profile B-P, and Profile A does not support deletion
- Default modulation mode of Profile A 1024qam

Procedure

Step 1 Configure the profile default modulation of the OFDM downstream channels by using the command "**cable ofdm-dowstream profile default-modulation**".

Step 2 View the configurations of the device by using the command "**show cable ofdm-downstream profile**".

Example

$ Set the modulation profile 0 of OFDM downstream channel 193 as qam64:

```
BT(config-if-cmts-1)# cable ofdm-downstream 193 profile 0 default-modulationqam64
BT(config-if-cmts-1)# show cable ofdm-downstream 193 profile 0
Channel ID                  : 193
Profile ID                  : 0
Default Modulation Type     : qam64
```

Related Operations

N/A

11.6.10 Configure Modulation Mode by Frequency Range of OFDM Downstream Channel

Context

- Each profile supports specifying the modulation mode according to the frequency.
- Both the start frequency and the end frequency are within the normal spectral range of the channel and must be an integer multiple of the subcarrier type.
- The start frequency needs to be less than the end frequency.
- The input start frequency and end frequency must be within the OFDM channel spectrum(subcarrier 0 frequency + 7.4MHz, subcarrier 0 frequency + 197.4MHz).

Procedure

Step 1 Configure the modulation mode by frequency range by using the command "**cable ofdm-downstream profile subcarrier**".

Step 2 View the configurations of the device by using the command "**show cable ofdm-downstream profile**".

Example

Configure the modulation mode as qam512 by frequency 210000000-220000000:

```
BT(config-if-cmts-1)# cable ofdm-downstream 193 profile 0 subcarrier
210000000 220000000 qam512
BT(config-if-cmts-1)# show cable ofdm-downstream 193 profile 0
Channel ID                        : 193
Profile ID                        : 0
Default Modulation Type           : qam256
Start Subcarrier Frequency(Hz)    : 210000000
End Subcarrier Frequency(Hz)      : 220000000
Modulation Type                   : qam512
```

Related Operations

N/A

11.6.11 Configure Subcarrier Zero Frequency of OFDM Downstream Channel

Context

- The range of subcarrier zero frequency is 258-1218MHz.
- Both the start frequency and the end frequency are within the normal spectral range of the channel and must be an integer multiple of the subcarrier type.
- The frequency of subcarrier 0 is less than or equal to the starting frequency of -6.4MHz.

Procedure

Step 1 Disable the OFDM downstream channels by using the command "**cable ofdm-downstream shutdown**".

Step 2 Configure the subcarrier zero frequency of the channel by using the command "**cable ofdm-downstream subcarrier-zero-frequency**".

Step 3 View the configurations of the device by using the command "**show cable ofdm-downstream config**".

Example

Configure the subcarrier zero frequency of OFDM downstream channel 193 as 652000000Hz:

```
BT(config-if-cmts-1)# cable ofdm-downstream 193 shutdown
BT(config-if-cmts-1)# cable ofdm-downstream 193 subcarrier-zero-frequency
652000000
BT(config-if-cmts-1)# show cable ofdm-downstream 193 config
Channel ID                      : 193
Admin Status                    : disable
Lower Edge Frequency(Hz)        : 662000000
Upper Edge Frequency(Hz)        : 690000000
PLC Frequency(Hz)               : 668000000
Subcarrier Zero Frequency(Hz)  : 652000000
Subcarrier Spacing Type         : 25k
Cyclic Prefix                   : 256tsu
Rolloff Period                  : 64tsu
Time Interleave Depth           : 16
Ncp Modulation Type             : qam16
Output power(dBmV)              : 20.0
Profile List                    : 0
Is primary channel              : Yes
```

Related Operations

N/A

11.6.12 Configure Subcarrier Spacing of OFDM Downstream Channel

Context

- Carrier spacing supports 25KHz and 50KHz.
- The default is 50KHz.

Procedure

Step 1 Disable the OFDM downstream channels by using the command "**cable ofdm-downstream shutdown**".

Step 2 Configure the subcarrier spacing of the channel by using the command "**cable ofdm-downstream subcarrier-spacing**".

Step 3 View the configurations of the device by using the command "**show cable ofdm-downstream config**".

Example

Configure the subcarrier spacing of OFDM downstream channel 193 as 25KHz:

```
BT(config-if-cmts-1)# cable ofdm-downstream 193 shutdown BT(config-if-cmts-1)#
cable ofdm-downstream 193 subcarrier-spacing 25kBT(config-if-cmts-1)# show
cable ofdm-downstream 193 config
Channel ID                      : 193
Admin Status                    : disable
Lower Edge Frequency(Hz)        : 662000000
Upper Edge Frequency(Hz)        : 690000000
PLC Frequency(Hz)               : 668000000
Subcarrier Zero Frequency(Hz) : 652000000
Subcarrier Spacing Type         : 25k
Cyclic Prefix                   : 256tsu
Rolloff Period                  : 64tsu
Time Interleave Depth           : 16
Ncp Modulation Type             : qam16
Output power(dBmV)              : 20.0
Profile List                    : 0
Is primary channel              : Yes
```

Related Operations

N/A

11.6.13 Configure Downstream OFDM Main Channel Capability

Context

When a downstream channel has enabled the main channel capability, it means that CM can go online from the channel. In order to ensure the normal online of CM, it is necessary to ensure that at least one downstream channel has enabled the main channel capability.

Procedure

Step 1 Enable the downstream OFDM channel to be configured by using the command "**no cable ofdm-downstream shutdown**"

Step 2 Enabled the main channel capability by using the command "**cable ofdm-downstream**

primary"

Step 2

Step 3 View information about the devic by using the command "**show cable ofdm-downstream config**"

Example

Enable the main channel capability of downstream OFDM channel 193:

```
BT(config-if-cmts-1)# no cable ofdm-downstream 193 shutdown
Power-level which is out range of 18.5-48.4 dBmv was truncated.
BT(config-if-cmts-1)# cable ofdm-downstream 193 primary BT(config-
if-cmts-1)# show cable ofdm-downstream 193 configChannel ID : 193
Admin Status                        : enable
Lower Edge Frequency(Hz)            : 198000000
Upper Edge Frequency(Hz)           : 258000000
PLC Frequency(Hz)                   : 214000000
Subcarrier Zero Frequency(Hz)  :  191600000
Subcarrier Spacing Type  : 50k
Cyclic Prefix                       : 512tsd
Rolloff Period                      : 128tsd
Time Interleave Depth               : 16
Ncp Modulation Type                 : qam16
Output power(dBmV)                  : 45.0
Profile List                        : 0-1
Is primary channel                  : Yes
```

Related Operations

N/A

11.7 Overview of CM OFDM Multi-profile

11.7.1.1 Overview of CM OFDM Multi-profile

The multi profile function of DOCSIS 3.1 CM OFDM channel enables the device to dynamically adjust the profile according to the downstream signal quality of CM side during operation, which is used to ensure the maximum data bandwidth under the premise of proper transmission quality.

11.7.1.2 Example of Configure CM OFDM Multi-profile

Through this task, the CM OFDM multi profile function configuration of CMTS device is realized.

Data Planning

The data plan of CM OFDM multi profile configuration instance is shown in the table below.

Table 11.7-1 Data Planning for CM OFDM Multi-profile

Item	Data
multi-profile management status	Enable
Downgrade management status	Enable
protect-power	1.5
recommand-age	600
unfit-age	1800
qam-threshold	qam16:16 dB, qam64:21 dB, qam128:24 dB, qam256:27 dB, qam512:30.5dB, qam1024:34 dB qam2048:37 dB, qam4096:41 dB.
OFDM channel	193
Profile of OFDM channel	0 1 2 3
DATA profile-list of OFDM channel	0-3

Prerequisite

N/A

Configuration flowchart

The process of configuring CM OFDM multi profile is as follows:

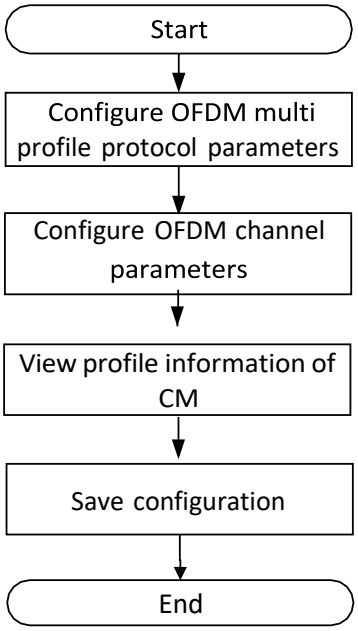

图 11.7-1 Configure CM OFDM multi profile flowchart

Procedure

Step 1 Configure CMTS OFDM multi profile protocol parameters:

```
BT(config-if-cmts-1)# cable ofdm-downstream multi-profileenable
BT(config-if-cmts-1)# cable ofdm-downstream multi-profile
downgrade enable
```

```
BT(config-if-cmts-1)# cable ofdm-downstream multi-profileprotect-power 1.5
BT(config-if-cmts-1)# cable ofdm-downstream multi-profile recommand-age 600
BT(config-if-cmts-1)# cable ofdm-downstream multi-profileunfit-age 1800
BT(config-if-cmts-1)# cable ofdm-downstream multi-profileqam-threshold qam16 16
BT(config-if-cmts-1)# show running-config verbose | includemulti-profile
 cable ofdm-downstream multi-profile protect-power 1.5
 cable ofdm-downstream multi-profile recommand-age 600
 cable ofdm-downstream multi-profile unfit-age 1800
 cable ofdm-downstream multi-profile downgrade enable
 cable ofdm-downstream multi-profile enable
 cable ofdm-downstream multi-profile qam-threshold qam16 16.0
 cable ofdm-downstream multi-profile qam-threshold qam64 21.0
 cable ofdm-downstream multi-profile qam-threshold qam128 24.0
 cable ofdm-downstream multi-profile qam-threshold qam256 27.0
 cable ofdm-downstream multi-profile qam-threshold qam512 30.5
 cable ofdm-downstream multi-profile qam-threshold qam1024 34.0
 cable ofdm-downstream multi-profile qam-threshold qam2048 37.0
 cable ofdm-downstream multi-profile qam-threshold qam4096 41.0
Topvision(config-if-ccmts-1)#
```

Step 2 Configure CMTS OFDM channel parameters:

```
Topvision(config-if-ccmts-1)# cable ofdm-downstream 193 profile 0 default-modulation qam16
Topvision(config-if-ccmts-1)# cable ofdm-downstream 193 profile 1 default-modulation qam64
Topvision(config-if-ccmts-1)# cable ofdm-downstream 193 profile 2 default-modulation qam128
Topvision(config-if-ccmts-1)# cable ofdm-downstream 193 profile 3 default-modulation qam256
Topvision(config-if-ccmts-1)# cable ofdm-downstream 193 profile-list 0-3
BT(config-if-cmts-1)#  no  cable  ofdm-downstream  193  shutdown
BT(config-if-cmts-1)# show running-config verbose | includeofdm-downstream 193
 cable ofdm-downstream 193 subcarrier-spacing 50k
```

```
 cable ofdm-downstream 193 subcarrier-zero-frequency 191600000
lower-frequency 198000000 upper-frequency 258000000 plc-frequency
214000000
 cable ofdm-downstream 193 cyclic-prefix 512tsd rolloff-period
128tsd
 cable ofdm-downstream 193 time-interleave 16
 cable ofdm-downstream 193 ncp-modulation qam16
 cable ofdm-downstream 193 power-level 45.0
 cable ofdm-downstream 193 primary
 cable ofdm-downstream 193 profile 0 default-modulation qam16
 cable ofdm-downstream 193 profile 1 default-modulation qam64
 cable ofdm-downstream 193 profile 2 default-modulation qam128
 cable ofdm-downstream 193 profile 3 default-modulation qam256
 cable ofdm-downstream 193 profile-list 0-3
 no cable ofdm-downstream 193 shutdown
 cable ofdm-downstream 193 prov-attr-mask 00000000
BT(config-if-cmts-1)#
```

Step 3 View profile information of CM:

```
BT(config-if-cmts-1)# show cable modem 0010.18de.ad01 prof-mgmt
downstream
MAC Address : 0010.18de.ad01
IPv4 Address : 110.33.33.11
IPv6 Address : --
RxMer Exempt Percent : 0
RxMer Margin qDB : 0
Automatic Prof Downgrade : Inactive
DCID : 193
Configured Profile(s) : 0-3
Profile(s) in REG-RSP-MP : 0-3
 Profile(s) in DBC-REQ : 0-3
 Current profile : 0
 Percentages of ideal BL vs Curr Prof : N/A
 Downgrade profile : 0
 Recommend profile : 1
 Unfit profile(s) : N/A
 Recommend profile (Expired) : N/A
 Unfit profile(s) (Expired) : N/A
Number of SubCarrier : 4096
1st Active SubCarrier : 148
# of Active SubCarrier : 3148
```

```
Tx Timer : 0h:1m:14s ago
Rx Timer : 0h:1m:8s ago
OFDM Profile Failure Rx : 0
MER Poll Period (s) : 10
Recommend Timeout (s) : 600
Unfit Timeout (s) : 300
Average RxMer(dbmv) : 41.0
Source : OPT
Sub-Carrier RxMER
0x0000 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0
0x0010 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0
0x0020 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0
0x0030 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0
0x0FF0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0
```

Step 4 Save the configuration:

```
BT# copy running-config startup-config
This will save the configuration to the flash memory.
Are you sure?(y/n) [n]y
Building configuration.....
Configuration saved successfully.
BT#
```

Result

According to the above configuration, after DOCSIS 3.1 CM goes online, it can dynamically adjust the appropriate profile according to the real-time RxMER value.

11.8 ERM Management

EQAM registers its own resources to the ERM system through the edge resource registration interface (D6), which enables ERM to synchronize the status and faults of EQAM. The resource application and release interface (R6) is used to pre-distribute, distribute and recycle edge resources, and report the related errors and abnormal states.

11.8.1 Example of ERM Configuration

Through this task, EQAM status and failure information will be reported to the server.

Data Planning

Configure the ERM instance data plan as shown in the following table.

Table 11-2 Data Planning for Configure the ERM Instance DATA

Item	Data
ERM state	Enable
ERM IP address	192.165.152.89
ERM TCP port number	6069
EQAM name	EQAM1
Stream area	BeiJing.HaiDian
Update bandwidth threshold	100
Routing overhead	15
RTSP port	554
ERM alivetime	30
Connection retry time	10
Maintenance time	90

Context

- Network equipment and lines are normal.
- Equipment supports D6/R6 protocol.

Configuration flowchart

The ERM configuration process is shown in the following figure.

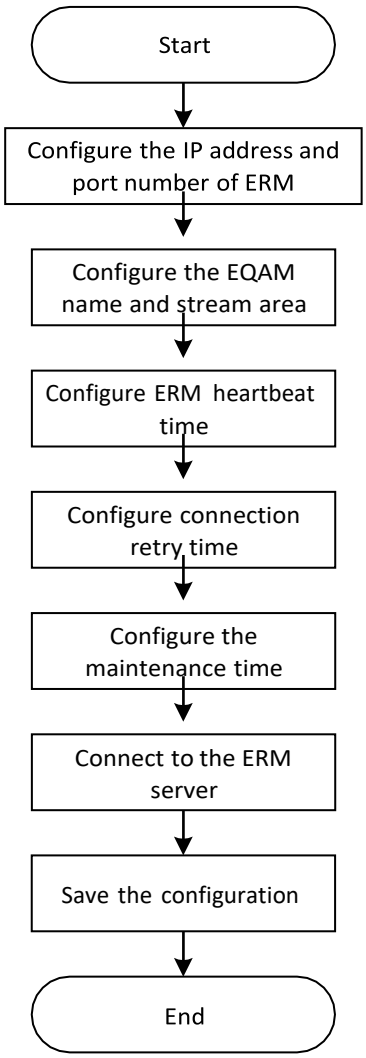

Figure 11-6 ERM configuration flow chart

Procedure

Step 1 Configure the IP address and port number of ERM

```
BT(config-if-eqam-template-1)# eqam erm erm-ip
192.165.152.89 port 6069
```

Step 2 Configure EQAM names and streams area

```
BT(config-if-eqam-template-1)# eqam erm qam-name EQAM1
streamzone BeiJing.HaiDian
```

Step 3 Configure ERM alivetime

```
BT(config-if-eqam-template-1)# eqam erm alivetime 30
```

Step 4 Configure the ERM connection retry time

```
BT(config-if-eqam-template-1)# eqam erm retrytime 10
```

Step 5 Configure the ERM maintenance time

```
BT(config-if-eqam-template-1)# eqam erm holdtime 90
```

Step 6 Connect to ERM Server

```
BT(config-if-eqam-template-1)# eqam erm enable
```

Step 7 Save configuration

```
BT(config-if-eqam-template-1)# end
BT# copy running-config startup-config
This will save the configuration to the flash memory.
Are you sure?(y/n) [n]y
Building configuration.....
Configuration saved successfully.
```

Result

When the ERM server is successfully connected, the status and failure of EQAM will be reported to the server.

11.8.2 ERM Configuration

Context

EQAM registers its own resources to the ERM system through the edge resource registration interface (D6), which enables ERM to synchronize the status and faults of EQAM.

ERM must configure the ERM IP address and ERM TCP port number. Other parameters are optional.

Procedure

Step 1 Use the "**eqam erm erm-ip** *ipv4-address* **port** *erm-port"* command to configure the IP address and port number of the ERM server.

Step 2 Use the "**eqam erm qam-name** *QAMNAME* **streamzone** *STREAMZONE"* command to configure EQAM names and streams area.

Step 3 Use the "**eqam erm alivetime** *alive-time"* command to configure the alivetime of ERM and send the alivetime cycle.

Step 4 Use the "**eqam erm retrytime** *retry-time"* command to configure connection retry time

Step 5 Use the "**eqam erm holdtime** *hold-time"* command to configure the maintenance time

Step 6 Use the "**eqam erm (enable|disable)***"* command to connect to the ERM server

Example

ERM configuration

```
BT(config-if-eqam-template-1)# eqam erm erm-ip 192.165.152.89 port 6069
BT(config-if-eqam-template-1)# eqam erm qam-name EQAM1 streamzone
BeiJing.HaiDian
BT(config-if-eqam-template-1)# eqam erm alivetime 30
BT(config-if-eqam-template-1)# eqam erm retrytime 10
```

```
BT(config-if-eqam-template-1)# eqam erm holdtime 90
BT(config-if-eqam-template-1)# eqam erm enable
```

Related Operations

N/A

11.8.3 View ERM Status

Context

Users can check the status of the ERM to confirm whether the configuration parameters are correct and whether the ERM server is connected properly.

Procedure

Step 1 Use the "**show eqam erm status**" command to view the ERM status.

Example

View ERM configuration information and connection status:

```
BT(config-if-cmts-1)# show eqam erm status
erm-switch:             disable
link-status:            unconnected
Erm-IP:                 192.165.152.89
port:                   6069
qam-name:               EQAM1
stream-zone:            BeiJing.HaiDian
Bandwidth-Update(kbps): 100
Routing-Cost:           15
RTSP-Port:              554
Keep-Alive(s):          30
Connection-Retry(s):    10
Hold-Time(s):           90
```

Related Operations

N/A

Chapter 12 CMTS DOCSIS Configuration Management

12.1 CMTS DOCSIS Overview

The management of CMTS DOCSIS includes the configuration of upstream scheduling parameters, the configuration of MDD message sending time interval, the configuration of CM for downstream multicast message forwarding, the configuration of CMTS shared key, the configuration of piggyback function, the configuration of UDC function, the configuration of CM IP initialization mode and the initialization of ranging interval.

12.2 Configuration of Upstream Dispatching Parameters

CMTS models the upstream channel into numerous mini-slots. CMTS uses MAP messages to control the use of these mini-slots. When CM has upstream data to transmit, it must request the transmission bandwidth (how many mini-slots) from CMTS. After receiving the request, CMTS will allocate the mini-slot to CM through MAP message. Because network delay and signal processing need a certain time, CMTS must transmit a MAP message earlier than the actual effective time of a MAP message, so that CM can receive the MAP message and process it, and then transmit data within the effective time allocated by MAP. The schematic diagram of CMTS transmitting MAP message is as follows:

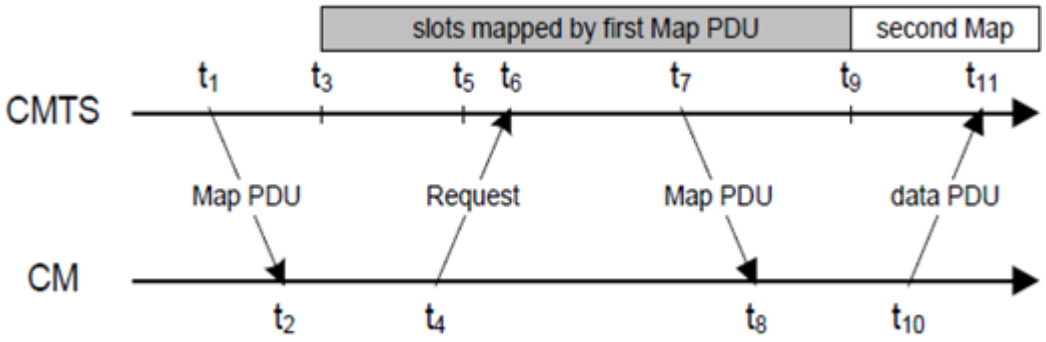

Figure 12-1 Schematic diagram of CMTS transmitting MAP message

In the figure above, CMTS transmits a MAP message at t1, and the actual effective time of the MAP message starts from t3. The difference between t1 and t3 is a pre time reserved to compensate the delay of network transmission and signal processing. The difference between t3 and t9 is the amount of time taken by the MAP message.

CM must request a transfer opportunity (transfer bandwidth) from CMTS before transferring upstream data. CM must send a request to CMTS to request upstream transmission bandwidth. CMTS allocates bandwidth to CM through MAP message. CM requests bandwidth from CMTS through request frame to transmit upstream data. The request frame format is divided into two types according to the upstream bandwidth request mechanism.

For CM below DOCSIS 3.0, the bandwidth request mechanism based on mini-slot is used. The feature of this mechanism is to use the number of mini-slots to represent the bandwidth required by C M. CM calculates the bandwidth required by the data to be transmitted in the upstream service flow queue, and converts it into the number of mini-slots to send requests to CMTS. The format of the request frame used by this request mechanism is as follows:

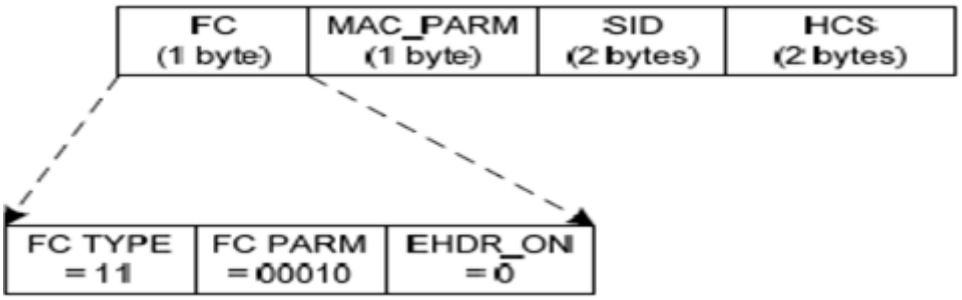

Figure 12-2 CMTS Request Frame Format Based on mini-slot Request Mechanism

The meaning of each field of Request Frame is shown in the table:

Field	Usage	Size
FC	FC_TYPE = 11; MAC-Specific Header FC_PARM[4:0] = 00010; MAC Header only; no data PDU following EHDR_ON = 0; No EHDR allowed	8 bits
MAC_PARM	REQ, total number of mini-slots requested	8 bits
SID	Service ID used for requesting bandwidth. For valid SID ranges, see Section 7.2.1.2.	16 bits
EHDR	Extended MAC Header not allowed	0 bytes
HCS	MAC Header Check Sequence	2 bytes
	Length of a REQ MAC Header	6 bytes

Figure 12-3 Field Description of Request Frame Based on mini-slot Request Mechanism

The Request Frame based on mini-slot must contain the following two parameters:

- SID for bandwidth request
- Number of mini-slots to be requested

For DOCSIS 3.0 and advanced versions of CM, a bandwidth request mechanism based on queue depth is used. The feature of this mechanism is to use the number of bytes to represent the bandwidth that CM needs to request. CM calculates the number of bytes that need to be transmitted in the upstream service flow queue, and uses it directly to represent the bandwidth that needs to be requested, instead of converting it to the number of mini-slots, and then sends a request to CMTS. The request frame format of this request mechanism is as follows:

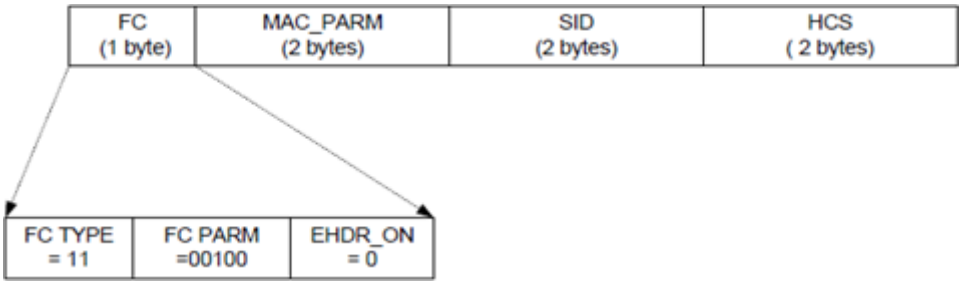

Figure 12-4 Request Frame Format Based on Queue Depth Request Mechanism

The meaning of each field of Request Frame is shown in the table:

Field	Usage	Size
FC	FC_TYPE = 11; MAC-Specific Header FC_PARM[4:0] = 00100; MAC Header only; no data PDU following EHDR_ON = 0; No EHDR allowed	1 byte
MAC_PARM	Total number of bytes requested in units of N bytes, where N is a parameter of the service flow for which this request is being made	2 bytes
SID	Service ID (0...0x3DFF)	2 bytes
EHDR	Extended MAC Header not allowed	0 bytes
HCS	MAC Header Check Sequence	2 bytes
	Length of a Queue-depth Based REQ MAC Header	7 bytes

Figure 12-5 Description of Request Frame Field Based on Queue Depth Request Mechanism

The request frame based on the queue depth must contain the following two parameters:

- Sid for bandwidth request
- Number of bytes to be requested, in N bytes, N is a parameter of service flow

The SID here is the Service ID. For CM lower than DOCSIS 3.0, the upstream service flow is based on a single channel. The upstream service flow of each activity has a SID associated with it. When CM requests bandwidth for the upstream service flow, it must include the SID of the upstream service flow.

For DOCSIS 3.0 and advanced CM versions, the upstream service flow is based on an upstream channel binding group. In order that CM can request bandwidth for each upstream service flow on multiple upstream channels, a new concept called SID Cluster is introduced into DOCSIS 3.0 protocol. SID Cluster contains a set of SIDS. Each SID in this group corresponds to a unique upstream channel in the upstream binding group. For example, the following figure is an example of SID Cluster.

SID Cluster	US#1 SID	US#2 SID	US#3 SID	US#4 SID
Cluster_0	58	479	85	1001

Figure 12-6 Description of Request Frame Field Based on Queue Depth Request Mechanism

A Service Flow must have at least one SID Cluster or multiple SID Clusters. Because each Service Flow allows multiple outstanding Request at the same time, and allows CMTS to Grant a Request multiple times, in addition, it also allows CM to initiate another Request for the part of the previous Request that did not receive

Grant. When some requests or grant are lost, there will be a mismatch between request size and grant size. But

this mismatch is temporary and will eventually return to normal. But this recovery process is an additional delay for CM. In order to reduce this delay, you need to use another SID Cluster. When a SID Cluster is in the process of unmatched recovery, CM can use another SID Cluster to initiate a request. CM can determine when to switch to a new SID Cluster by judging certain conditions. For example, it can determine the number of outstanding bytes of the current SID Cluster. When the number reaches a certain value, a new SID Cluster will be used for request. And more SID Clusters can better control the unmatched recovery process. We call all SID Clusters associated with the Service Flow a SID Cluster group.

12.2.1 Example of Configure Upstream Scheduling Parameters

Through this task, the configuration of upstream scheduling parameters is realized to ensure large upstream bandwidth and low transmission delay.

Data Planning

The configuration data plan of upstream dispatching parameters of CMTS equipment is shown in the table below.

Table 12-1 Data Planning for Configure the Upstream Scheduling Parameters of the CMTS Device

Item	Data
Number of service flow Sid clusters	2
Multiplier of the number of request bytes for a single request	4
The maximum number of requests for Sid cluster	8
The maximum number of outstanding requests for Sid cluster	1000000
The maximum total number of requests for Sid cluster	500000
The maximum time Sid cluster requests bandwidth	5000
The maximum interval between CMTS devices sending map messages	5000
The minimum interval between CMTS devices sending map messages	2500
The relative lead time for CMTS devices to send map messages	1000

Prerequisite

CMTS device is online normally.

Configuration Flow

The configuration process of upstream scheduling parameters is shown in the figure below:

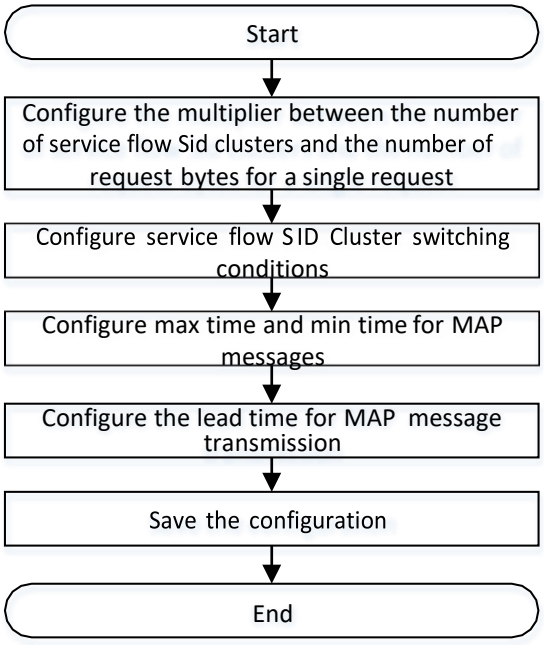

Figure 12-7 Flowchart for Configuration of Upstream Scheduling Parameters

Procedure

Step 1 Configure the multiplier for the number of Service Flow SID Cluster and the number of Request bytes for a single request.

```
BT(config-if-cmts-1)# cable sid-cluster-group num-of-cluster2
BT(config-if-cmts-1)# cable sid-cluster-group req-multiplier4
```

Step 2 Configure switching conditions for Service Flow SID Clusters.

```
BT(config-if-cmts-1)# cable sid-cluster-switching max-request
8
BT(config-if-cmts-1)# cable sid-cluster-switching max-
outstanding-byte 1000000
BT(config-if-cmts-1)# cable sid-cluster-switching max-total-byte
500000
BT(config-if-cmts-1)# cable sid-cluster-switching max-time5000
```

Step 3 Configure max time and min time for MAP messages.

```
BT(config-if-cmts-1)# cable map max-time 5000
BT(config-if-cmts-1)# cable map min-time 2500
```

Step 4 Configure the lead time for MAP message transmission.

```
BT(config-if-cmts-1)# cable map lead-time 1000
```

Step 5 Save the configuration.

```
BT(config-if-cmts-1)# end
```

```
BT# copy running-config startup-config
This will save the configuration to the flash memory.
Are you sure?(y/n) [n]y
Building configuration.....
Configuration saved successfully.
```

Result

According to the above configuration of upstream channel parameters of CMTS equipment, the configuration of upstream scheduling parameters is realized by using channel frequency and frequency width and other parameters of configured channel on-line CM, so as to ensure large upstream bandwidth and low transmission delay.

12.3 Configure the Operating Mode of CM

Configure the operating mode of CM through this configuration task.

Context

CMTS will send periodically the MDD(MAC Domain Descriptor) information to ensure normal registration of 3.0 CM (i.e., CM supporting DOCSIS 3.0). If 3.0 CM fails to receive MDD information sent by CMTS, it will be registered as DOCSIS 2.0 mode.

Note:

This configuration task is valid only for 3.0 CM.

Procedure

Step 1 Enter the cmts view by using the command "**interface cmts**".

Step 2 Configure the interval for CMTS to send MDD information by using the command "**cable mdd-interval**".

By default, the interval for CMTS to send MDD information is 1, 500ms.

Example

Configure the operating mode of 3.0 CM under CMTS as DOCSIS 2.0.

```
BT(config)# interface cmts 1
BT(config-if-cmts-1)# cable mdd-interval 0
BT(config-if-cmts-1)# show running-config verbose | include mdd
 cable mdd-interval 0
```

Related Operations

N/A

12.4 Configure the Forwarding Mode of CM Multicast Management Packet

Configure the forwarding mode of CM multicast management packet through this task.

Context

Configure whether to enable the MDF (Multicast DSID Forwarding) function of CMTS to control the forwarding mode of CM multicast management packet, with specific ways as follows:

- When enabling the MDF function, CM adopts a CMTS control-based mode to inform CM of multicast forwarding through DSID.
- When disabling the MDF function, CM adopts the IGMP Snooping mode for multicast forwarding.

Note:

It requires making CM work in DOCSIS3.0 mode before configuring the forwarding mode of CM multicast management packet.

Procedure

Step 1 Enter the cmts view by using the command "**`interface cmts`**".

Step 2 Configure the state of CMTS MDF function by using the command "**`cable multicast mdf (enable | disable)`**".

By default, CMTS MDF function is enabled.

Example

Configure multicast forwarding of CM multicast management packet through IGMP Snooping.

```
BT(config)# interface cmts 1
BT(config-if-cmts-1)# cable multicast mdf disable
BT(config-if-cmts-1)# show running-config verbose | include mdf
 cable multicast mdf disable
```

Related Operations

N/A

12.5 Configure CM Online Authentication by CMTS

Configure the CM online authentication by CMTS through this task.

Context

CMTS will check the validity of CM configuration file by configuring the MIC (Message Integrity Check) function. Only when the configuration fie is valid, can CM be allowed to be online.

In the process of CM registration, CMTS will calculate CMTS MIC according to the configuration information in the REG-REQ/REG-REQ-MP massage sent by CM and the shared key. Then compare CMTS with CMTS MIC in the REG-REQ/REG-REQ-MP message. If they are the same, this CM is allowed to be online.

Procedure

Step 1 Enter the cmts view by using the command "**interface cmts**".

Step 2 Configure the shared key by using the command "**cable shared-secret [0 | 7]** *text*". By default, CMTS doesn't configure the MIC function, that is, all CMs can be online.

Step 3 View the configuration information of the shared key by using the command "**show cable shared-secret**".

Example

Configure the shared key for CM to be online as secretkey-cm.

```
BT(config)# interface cmts 1
BT(config-if-cmts-1)# cable shared-secret secretkey-cm
BT(config-if-cmts-1)# show cable shared-secretThe
shared-secret is unencrypted,information is:
Plaintext :secretkey-cm
   Cipher : f1dd20390fdf017a51905d6eac9d36c8
```

Related Operations

Table 12.5-1 Related Operations for Configuring CM Online Authentication by CMTS

Operation	Command	Remarks
Configure CMTS not to perform the CM online authentication	**no cable shared-secret**	

12.6 Configure Multi-channel Data Transmission of CM

Configure the multi-channel data transmission of CM through this task.

Context

After this task is configured, CM can bind multiple upstream channels for data transmission, and multiple downstream channels for receiving data.

Note:

It requires making CM work in DOCSIS3.0 mode before configuring the multi-channel data transmission of CM.

Procedure

Step 1 Enter the cmts view by using the command "**interface cmts**".

Step 2 Configure the multi-channel data transmission of CM by using the following commands.

Configure CM to bind multiple downstream channels for data transmission by using the command "**cable mrc-mode**".

Configure CM to bind multiple upstream channels for data transmission by using the command "**cable mtc-mode**".

Example

Configure CM to bind multiple upstream channels for data transmission.

```
BT(config)# interface cmts 1
BT(config-if-cmts-1)# cable mtc-mode
BT(config-if-cmts-1)# show running-config verbose | include mtc
 cable mtc-mode
```

Related Operations

Table 12.6-1 Related Operations for Configuring the Multi-channel Data Transmission by CM

Operation	Command	Remarks
Configure the data transmission of CM on one upstream channel	**no cable mtc-mode**	
Configure the data transmission of CM on one downstream channel	**no cable mrc-mode**	

12.7 Disable the piggyback Function

Disable the piggyback function through this task.

Context

When there are more than one 3.0 CM under CMTS, and such 3.0 CM have their upstream traffic reach the maximum bandwidth, there may be a case that some a 3.0 CM has very high traffic, but others have very low traffic. Now disable the piggyback function to ensure such 3.0 CM evenly share the bandwidth of upstream channel.

Note:

1. It requires making CM work in DOCSIS 3.0 mode before disabling the piggyback function.

2. Configuration of the state of piggyback function is only valid for the online CM after the configuration. To make it valid for all CMs, it further needs to restart all CMs.

Procedure

Step 1 Enter the cmts view by using the command "**interface cmts**".

Step 2 Disable the piggyback function by using the command "**no cable piggyback-allowed**". By default, the piggyback function is disabled.

Example

$Disable the piggyback function.

```
BT(config)# interface cmts 1
BT(config-if-cmts-1)# no cable piggyback-allowed
BT(config-if-cmts-1)# show running-config verbose | include piggyback
 no cable piggyback-allowed
```

Related Operations

Table 12.7-1 Related Operations for Disabling piggyback Functions

Operation	Command	Remarks
Enable the piggyback function	**cable piggyback-allowed**	

12.8 Enable the UDC Function

Enable the UDC function through this task.

Context

When enabling the UDC (Upstream Drop Classifier) function of CMTS, it also requires the configuration of QoS classifier in the CM configuration file. Then 3.0 CM under CMTS will filter traffic by QoS policy in the configuration file.

Since the UDC (Upstream Drop Classifier) function conflicts with IP_Filter function, users can disable the UDC function to filter traffic by adopting IP_Filter function.

⚠ Warning:

It requires making CM work in DOCSIS3.0 mode before disabling the UDC function.

Procedure

Step 1 Enter the cmts view by using the command "**interface cmts**".

Step 2 Enable the UDC function by using the command "**cable udc enable**"

Step 3 By default, the UDC function is not enabled.

Example

Enable the UDC function.

```
BT(config)# interface cmts 1 BT(config-if-cmts-1)#
cable udc enable Please reset all the online 3.0
CMs to take effect!
```

Related Operations

Table 12.8-1 Related Operations for Enabling UDC Function

Operation	Command	Remarks
Disable the UDC function	**cable udc disable**	

12.9 Configure the IP Provisioning Mode of CM

Configure the IP provisioning mode in the MDD messages which is used to communicate to the CM certain parameters related to the initialization of the CM's IP layer services.

Context

The CM performs IP initialization provisioning in one of four modes:

1. IPv4 Only: The CM is allowed to obtain an IPv4 address only.
2. IPv6 Only: The CM is allowed to obtain an IPv6 address only.
3. Alternate Provisioning Mode (APM): The CM is allowed to obtain an IPv4 address or IPv6 address only. In this mode, the CM tries to provision using IPv6 first. If IPv6 provisioning is unsuccessful, the CM will attempt provisioning using IPv4.
4. Dual-stack Provisioning Mode (DPM): The CM is allowed to obtain both an IPv4 address and IPv6 address. In this mode, the CM uses IPv6 address to acquire TOD and download the configuration file. If the CM cannot obtain an IPv6 address, or if it cannot download a configuration file using IPv6, it tries downloading the configuration file using IPv4.

Note:

This configuration only apply to the DOCSIS3.0 CM.

Procedure

Step 1 Enter the cmts view by using the command "**interface cmts**".

Step 2 Configure the IP provisioning mode of CM by using the command "**cable ip-init (alternate | dual-stack | ipv4 | ipv6)**".

By default, the CM performs the IP initialization in IPv4 only.

Example

Configure the IP provisioning mode to dual-stack.

```
BT(config)# interface cmts 1
BT(config-if-cmts-1)# cable ip-init dual-stack
The IP provisioning process begins after the completion of ranging, or EAE if
enabled.
Please reset CM to take effect!
BT(config-if-cmts-1)# show running-config verbose | include ip-init
 cable ip-init dual-stack
```

Related Operations

Table 12.9-1 Related Operations for Configuring IP Provisioning Mode of CM

Operation	Command	Remarks
Configure the forwarding mode of the DHCP packets	**cable (dhcp-mode | dhcpv6-mode) (cm|host|mta|stb |***device***) (snooping | l2-relay | l3-relay)**	

12.10 Configure Initial-Maintenance

Use this configuration task to configure the interval for the periodic ranging sent by the CMTS.

Context

The periodicity of the CMTS equipment (the interval for sending periodic ranging is the configuration value for Initial-Maintenance), is the time slot used to distribute the initialization request for ranging to the CMs. This time slot will be broadcast to all CMs, and the CMs will compete to use that time slot. However, if at the same time, there are two CMs, such as CM A and CM B, only one CM (either CM A or CM B) can obtain the time slot to send the message for ranging initialization, otherwise, it will lead to a collision. Collision will cause the CMTS parse message to fail, and the CMTS will eventually fail to reply to the RNG-RSP message.

Note:

The default value is 100ms. If the number of CMs is larger (for example, 500), it is recommended to set the value to 2,000ms. Execute the no cable insertion-interval command to restore the default settings.

Procedure

Step 1 Use the "**interface cmts**" command to enter the cmts view.

Step 2 Use the "**cable insertion-interval**" command to configure the interval for the periodic ranging sent by the CMTS equipment.

By default, the interval for periodic ranging sent by the CMTS equipment is 100 ms.

Example

Configure the interval for the periodic ranging sent by the CMTS equipment to 200.

```
BT(config-if-cmts-1)# cable insertion-interval 200
BT(config-if-cmts-1)# show running-config verbose | include insertion-interval
cable insertion-interval 200
```

Related Operations

N/A

Chapter 13 Terminal Configuration Management

Terminal configuration management includes basic configuration of CM, CM Remote Query function and CPE management.

13.1 Configure Basic Management of CM

Ensure basic management of CM by users through this task.

13.1.1 Configure the Maximum Number of Downstream CM Connected to CMTS

Configure the maximum number of downstream CM connected to CMTS through this task.

Context

Control the maximum number of downstream CM connected to CMTS to guarantee the quality of current network.

Procedure

Step 1 Enter the cmts view by using the command "**`interface cmts`**".

Step 2 Configure the maximum number of downstream CM connected to CMTS by using the command "**`cable modem max-number`** *`max-number`*".

Example

Configure the maximum number of CM connected to CMTS as 200.

```
BT(config)# interface cmts 1
BT(config-if-cmts-1)# cable modem max-number 200
```

13.1.2 Configure the Corresponding Relationship between CM Service Type and Downstream Frequency

Configure the corresponding relationship between CM service type and downstream frequency through this task.

Context

After configuring the corresponding relationship between CM service type and downstream frequency, upon the receipt of registration request containing such service type from CM, CMTS will scan the downstream frequency corresponding to such service type.

Procedure

Step 1 Configure the corresponding relationship between CM service type and downstream frequency by using the command "**cable service type** *service-type* **ds-frequency** *frequency*".

Example

Configure the downstream frequency corresponding to CM whose service type is commercial as 550000000 Hz.

```
BT(config)# cable service type commercial ds-frequency 550000000
BT(config)# show cable modem service-type-id
MAC Address       IP Address      I/F     MAC      Primary  Service-type-id
                                          State    Sid
0026.5ba6.4779  192.168.2.167   C1/U1   online   1          commercial
```

Related Operations

Table 13-1 Related Operations for the Corresponding Relationship between CM Service Type and Downstream Frequency

Operation	Command	Remarks
Delete the corresponding relationship between CM service type and CMTS downstream frequency	**no cable service type** *service-type*	
View information of CM service type	**show cable modem service-type-id** [*service-type-id*]	
Clear information of CM service type	**clear cable modem** *(ip-address | mac-address)* **service-type-id**	

13.1.3 Configure CM Status Global Polling Cycle

Context

Configure the CM status global polling cycle, so that the SNMP table related to the CM Status can collect the polling data. Polling data can significantly improve the collection efficiency and save time. However, due to the fact that such data is not real-time data, the data timeliness is not as good as that of real-time data collection.

- Configure the global polling cycle as zero, then the response will be slower when the SNMP table related to the CM Status collects real-time data;
- Configure the global polling cycle as nonzero, then the response will be faster when the SNMP table related to the CM Status collects real-time data;

Procedure

Step 1 Enter the config view by using the command "**configure terminal**".

Step 2 Configure the CM status global polling cycle by using the command "**cable modem polling-period**".

Example

Configure the CM status global polling cycle as 60 s.

```
BT# configure terminal
BT(config)# cable modem polling-period 60
```

Related Operations

Table 13-2 Related Operations for the CM Status Global Polling Cycle

Operation	Command	Remarks
Display the CM status global polling cycle	**show cable modem polling-period**	

13.1.4 Configure CM Data Backoff Window

Context

When multiple CMs send the upstream data request or start the ranging simultaneously, there may be conflicts. Configuring the data backoff window can reduce the conflicts to avoid data congestion.

Procedure

Step 1 Enter the cmts view by using the command "**interface cmts**".

Step 2 Configure CM data backoff window by using the following commands.

- Configure the data backoff window for use at the time when CM sends the upstream data request by using the command "**cable upstream data-backoff** *backoff-begin backoff-end*".
- Configure the data backoff window for use at the time when CM starts ranging by using the command "**cable upstream range-backoff** *backoff-begin backoff-end*".

Example

Configure the start value of data backoff window for use at the time when CM sends the upstream data request as 4 and the end value as 5.

```
BT(config)# interface cmts 1
BT(config-if-cmts-1)# cable upstream 1 data-backoff 4 5
BT(config-if-cmts-1)# show running-config verbose | include data-backoff
 cable upstream 1 data-backoff 4 5
```

Related Operations

Table 13-3 Related Operations for the CM Data Backoff Window

Operation	Command	Remarks
Restore the default value of CM data backoff.	**no cable upstream data-backoff** **no cable upstream range-backoff**	

13.1.5 Restart CM

Restart CM under CMTS through this task.

Context

In case of any abnormity of CM, change in service or topology, users can restart CM through this task.

CM can be restarted by the following four ways:

- Restart all CMs under CMTS by using the command "**clear cable modem all reset**".
- Restart the specified CM unser CMTS by using the command "**clear cable modem** (*ip-address* | *mac-address*) **reset**".
- Restart all CMs under CMTS and delete their record information by using the command "**clear cable modem all delete**".
- Restart the specified CM under CMTS and delete its record information by using the command "**clear cable modem** (*ip-address* | *mac-address*) **delete**".

Warning:

Restarting CM will cause service interruption. Please confirm carefully before restarting.

Procedure

Step 1 Restart all CMs under CMTS by using the command "**clear cable modem all reset**".

Example

$Restart all CMs under CMTS.

```
BT(config)# clear cable modem all reset
```

Related Operations

N/A

13.1.6 Clear the Record Information of Offline CM

Users can clear the record information of offline CM through this task.

Context

The record information of offline CM can be cleared by the following two ways:

- Clear manually the record information of all or the specified offline CM by using the command "**clear cable modem offline** (**all** | *mac-address*)".
- With the configurations to achieve automatic clearing offline CMs recording, configuration steps are as follows:
  - We configure offline CM aging time threshold by the command "**cable modem offline age-time** *age-time*". When CM offline time is reached the threshold. The CMTS device will clear the CMs records based the CM aging mode.
  - We configure offline CM aging mode by the command "**cable modem offline age-mode (polling | timing)**". The CMTS device clear the CMs records based the CM aging mode.
  - When the command "**cable modem offline age-mode (polling | timing)**" is configured for timing mode. It need to set the clear time by the command "**cable modem offline age-clock** *time*", To achieve clearing the CMs records which the CM offline time reached the threshold.

Procedure

Step 1 Clear manually the record information of all offline CMs by using the command "**clear cable modem offline all**".

Step 2 View the information of CM by using the command "**show cable modem**".

Example

$Clear the record information of all offline CMs.

```
BT(config)# show cable modem
MAC Address    IP Address I/F    MAC      Primary RxPwr Timing  Number BPI    Online
                                 State    Sid     (dBmV) Offset CPE    Enabled Time
001c.1df5.7306 --         C1/U3  offline 72       10.0    0      0      no      0d0h0m
BT(config)# clear cable modem offline all
BT(config)# show cable modem
MAC Address IP Address I/F  MAC     Primary RxPwr  Timing  Number BPI      Online
                            State   Sid     (dBmV)  Offset CPE    Enabled  Time
```

Related Operations

N/A

13.2 Configure CM Remote Query Function

13.2.1 CM Remote Query Function Overview

Remote Query function is used for CMTS to acquire specific SNMP information of online CM through SNMP protocol. With this function, users can monitor CM to some extent.

13.2.2 Configure the Example of CM Remote Query Function

Through this example, CMTS can acquire the information of CM via Remote Query function.

Data Planning

The planning for Remote Query function is shown as follows.

Table 13-4 Data Planning for CM Remote Query

Item	Data
Remote Query community name	public
Remote Query polling interval	5s
Remote Query local IP address	The configured and available IP address in CMTS

Prerequisite

The network CMTS, CM and lines are normal.

Configuration flowchart

The process for configuring the regular load balance is shown as follows.

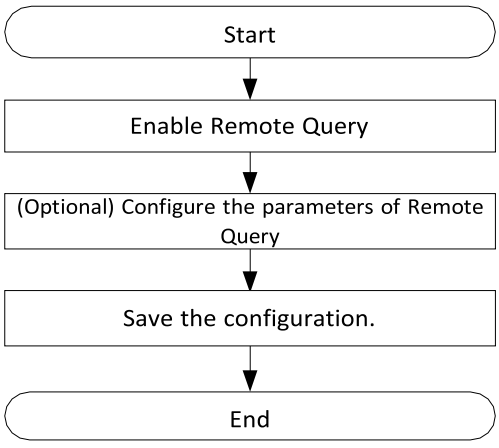

Figure 13-1 Flowchart for Configuring the Remote Query Function

Procedure

Step 1 Enable Remote Query.

```
BT(config)# interface cmts 1
BT(config-if-cmts-1)# cable modem remote-query
```

Step 2 (Optional) Configure the parameters of Remote Query.

In this example, the parameters of Remote Query are the default values. If configuration is required, refer to "13.2.4 Configure the Operating Parameters of Remote Query Function".

Step 3 Save the configurations.

```
BT(config)# exit
BT# copy running-config startup-config
This will save the configuration to the flash memory.
Are you sure?(y/n) [n]y
Building configuration.....
Configuration saved successfully.
```

Result

According to the above configurations, Remote Query function can ensure normal acquisition of the information of online CM.

13.2.3 Enable the Remote Query Function of CMTS

Users can enable the Remote Query of CMTS through this task.

Context

Only when the Remote Query function of CMTS is enabled, can other configured parameters of Remote Query take effect.

Procedure

Step 1 Enter the cmts view by using the command "**interface cmts**".

Step 2 Enable the Remote Query function of CMTS by using the command "**cable modem remote-query**".

Step 3 Return to the config view by using the command "**exit**".

Step 4 View the configuration information of Remote Query function by using the command "**show cable modem remote-query config**".

Example

Enable the Remote Query function of CMTS.

```
BT(config)# interface cmts 1
BT(config-if-cmts-1)# cable modem remote-query
BT(config-if-cmts-1)# exit
BT(config)# show cable modem remote-query config
cmts remote query status:
```

```
Interface      Status         Interval(s)    Src-ip         Community
C1             enable         5              0.0.0.0        public
```

Related Operations

Table 13-5 Related Operations for Enabling Remote Query Function of CMTS

Operation	Command	Remarks
Disable the Remote-Query function of CMTS	**no cable modem remote-query**	

13.2.4 Configure the Operating Parameters of Remote Query Function

Users can configure the operating parameters of Remote Query function through this task.

Context

Configuration of the operating parameters of Remote Query function is shown as follows:

Table 13-6 Descriptions on Parameter Configuration of Remote Query Function

Configuration parameter	Description
Configure Remote Query community name	Remote Query will take the configured community name as the authentication community name for use at the time of SNMP communication between CMTS and CM.
Configure the polling interval of Remote Query	The polling interval refers to the interval between the end of a complete polling of Remote Query function and the start of the next polling. A complete polling refers to making CMTS with enabled Remote Query function entirely finish the polling against all its CMs.
Configure local address of Remote Query	Remote Query specifies CMTS for SNMP communication with CM via this IP address. The configured local IP address must be the IP address that has been configured by CMTS and can achieve communication with CM.

Procedure

Step 1 Configure the operating parameters of Remote Query function by using the following commands.

- Configure the Remote Query community name by using the command "**cable modem remote-query community-string** *community-string*".
- Configure the polling interval of Remote Query by using the command "**cable modem remote-query interval** *interval*".
- Configure local IP address of Remote Query by using the command "**cable modem remote-query src-ip** *ip-address*".

Step 2 View the configuration information of Remote Query by using the command "**show cable modem remote-query config**".

Example

Configure the community name of Remote Query as community-name, the polling interval as 30 minutes and local IP address as 1.1.1.1.

```
BT(config-if-cmts-1)# cable modem remote-query community-string community-name
BT(config-if-cmts-1)# cable modem remote-query interval 1800
BT(config-if-cmts-1)# cable modem remote-query src-ip 1.1.1.1
BT(config-if-cmts-1)# show cable modem remote-query config
cmts remote query status:
 Interface     Status     Interval(s)   Src-ip     Community
 C1            enable     1800          1.1.1.1    community-name
```

Related Operations

Table 13-7 Related Operations for Configuring the Running Parameters for Remote Query Function

Operation	Command	Remarks
Restore the default local IP address of Remote Query function	**no cable modem remote-query src-ip**	

13.3 View QoS Configuration Information

Context

Quality of Service (QOS) refers to the performance of data flow through the network. Through a series of metrics, such as service availability, throughput, delay/jitter, packet loss rate, QoS provides end-to-end quality assurance for user services.

- DOCSIS network provides different services with different quality of service through the mechanism of service flow.
- Upstream message matches CM's upstream classifier to classify services into different upstream service flows. The downstream message matches CMTS downstream classifier to classify services into different downstream service flows.
- Service flow types can view CM's service flow information through commands. There are several classifier types that support viewing CM:
- CM's service flow and classifier information are specified in the CM configuration file, and the first service flow configured in the CM configuration file is the default service flow. In addition to the default service flow, other service flows must have classifier correspondences. CM can trigger the creation of dynamic service flows according to business needs. The command can query the relevant information of QoS on CMTS device.

The service flow and classifier are configured in the CM configuration file. The service flow parameters and classifier types supported are as follows:

- The service flow supports the following parameters for dispatching different services.
  - Service flow reference
  - Service Class Name
  - Type of QoS parameter settings
  - Transport priority
  - Maximum stable transmission speed
  - Maximum burst rate
  - Maximum cascade burst rate
  - Minimum Reserved Packet Size
  - Scheduling type of service flow
  - Request/Transfer Policy
- The classifier supports the following types to classify business into different service flows.
  - Source IP address
  - Destination IP Address
  - Source port number
  - Destination port number
  - IP Protocol
  - Ethernet Protocol Type

Procedure

Step 1 Query relevant configuration information of QoS by using the command "**`show cable modem qos`**".

Example

Query relevant configuration information of CMTS QoS.

```
BT(config)# show cable modem a4a8.0fa9.607c qos
Qos informations of CM a4a8.0fa9.607c are as follows:
SFID    SF   Dir Curr     Sid    Sched   Prio  MaxSusRate MaxBurst MinRate PeakRate Flags
        Ref      State                    Type
2       1    US  active   2      BE(Y)   0(Y)  0(N)         6400(Y)  0(N)    0(N)     static
1024    2    US  active   1024   BE(Y)   1(Y)  0(N)         6400(Y)  0(N)    0(N)     static
1025    3    US  active   1025   BE(Y)   2(Y)  0(N)         6400(Y)  0(N)    0(N)     static
1026    4    US  active   1026   BE(Y)   3(Y)  0(N)         6400(Y)  0(N)    0(N)     static
1027    5    US  active   1027   BE(Y)   4(Y)  0(N)         6400(Y)  0(N)    0(N)     static
```

```
1028    6    US   active  1028   BE(Y)  5(Y)   0(N)          6400(Y)  0(N)   0(N)    static
1029    7    US   active  1029   BE(Y)  6(Y)   0(N)          6400(Y)  0(N)   0(N)    static
1030    8    US   active  1030   BE(Y)  7(Y)   0(N)          6400(Y)  0(N)   0(N)    static
65538   21   DS   active  N/A    BE(N)  0(Y)   0(N)          6400(Y)  0(N)   0(N)    static
66562   22   DS   active  N/A    BE(N)  1(Y)   60000007(Y)   6400(Y)  0(N)   0(N)    static
67586   28   DS   active  N/A    BE(N)  7(Y)   8000005(Y)    6000000(Y) 0(N)  0(N)    static
68610   24   DS   active  N/A    BE(N)  2(Y)   60000005(Y)   3044(N)  0(N)   0(N)    static
69634   25   DS   active  N/A    BE(N)  6(Y)   60000005(Y)   3044(N)  0(N)   0(N)    static
70658   23   DS   active  N/A    BE(N)  3(Y)   60000006(Y)   3044(N)  0(N)   0(N)    static
71682   26   DS   active  N/A    BE(N)  7(Y)   60000005(Y)   3044(N)  0(N)   0(N)    static
72706   27   DS   active  N/A    BE(N)  7(Y)   60000005(Y)   3044(N)  0(N)   0(N)    static
```

Related Operations

Table 13-8 Related Operations for Query about QoS configurations

Operation	Command	Remarks
Query QoS information of the specified CM	**show cable modem qos verbose**	
Query the classifier information of the specified CM	**show cable modem classifiers [verbose]**	
Query the service flow information of the specified CM	**show cable modem service-flow**	

13.4 Cable Access List Management

Through this task, users can disable or permit specific CMs from accessing the network. The priority of a black list is higher than that of a white list. CMs added to a black list will be rejected in the phase of ranging. If CM has accessed a network, after being added to the network, the CM will become off line. If CM has not accessed a network, its status will not be displayed. Users can also permit specific CMs from accessing the network.

13.4.1 Configuring Black List Switch

Context

Through this task, users can enable or disable a black list. Only when the black list is enabled, the contents set by blacklist can be validate and the access of CMs lists in it to the network will be rejected. By default, the black list function is disabled.

Procedure

Step 1 Enter the cmts iew and use the "**cable access black-list (enable|disable)**" to enable/disable the black list.

Step 2 Use the" **show cable access black-list**" command to view the result.

Example

$ Enable black list.

```
BT(config-if-cmts-1)# cable access black-list enable
BT(config-if-cmts-1)# show cable access black-list
 cable access black-list enable
 the total number of CM is 0
!
```

13.4.2 Setting the Black List

Context

Through this task, users can add a CM MAC address segment of the specified CM to the black list. A black list can be configured with up to 1000 black list rules.

Procedure

Step 1 Use the "**cable access black-list** *mac-begin* [*mac-end*]" command to add MAC address to a black list.

Step 2 Use the command to view the result of the "**show cable access black-list**" command.

Example

Add a single MAC address to a black list.

```
BT(config-if-cmts-1)# cable access black-list 2476.7d06.bd9a
```

Add a MAC address segment to a black list.

```
BT(config-if-cmts-1)# cable access black-list 4432.c83c.0000 4432.c83c.0009
BT(config-if-cmts-1)# show cable access black-list
 cable access black-list disable
 cable access black-list 2476.7d06.bd9a
 cable access black-list 4432.c83c.0000 4432.c83c.0009
 the total number of CM is 11
!
```

13.4.3 Delete the Black List

Through this task, users can delete specified MAC address or MAC address segment from the black list or delete the entire list. The MAC address cannot be FFFF.FFFF.FFFF.

Context

N/A

Procedure

Step 1 Enter the cmts view.

Step 2 Use the "**no cable access black-list** (*mac-begin* | **all**)" command to delete MAC addresses from the black list.

Step 3 Use the "**show cable access black-list**" command to view if it is deleted.

Example

Delete MAC addresses from the black list.

```
BT(config-if-cmts-1)# show cable access black-list
 cable access black-list disable
 cable access black-list 2222.2222.2222
 cable access black-list 2476.7d06.bd9a
 cable access black-list 4432.c83c.0000 4432.c83c.0009
 the total number of CM is 12
!
```

When deleting a MAC address segment, enter only the start address of the MAC segment.

```
BT(config-if-cmts-1)# no cable access black-list 4432.c83c.0000
BT(config-if-cmts-1)# show cable access black-list
 cable access black-list disable
 cable access black list 2222.2222.2222
 cable access black list 2476.7d06.bd9a
 the total number of CM is 2
!
BT(config-if-cmts-1)# no cable access black-list all
BT(config-if-cmts-1)# show cable access black-list
 cable access black-list disable
 the total number of CM is 0
!
```

13.4.4 View the Black List

Through this task, users can view if the black list is enabled and list of devices in the current black list.

Context

N/A

Procedure

Step 1 Enter the cmts view.

Step 2 Use the "**show cable access black-list**" command to view the configuration of the black list.

Example

View the black list.

```
BT(config-if-cmts-1)# show cable access black-list
 cable access black-list disable
 cable access black-list 2476.7d06.bd9a
 the total number of CM is 1
!
```

13.4.5 Configuring White List Switch

Through this task, users can enable or disable a white list; only when it is enabled, the setting of the white list can be valid. By default, white list is disabled.

Context

N/A

Procedure

Step 1 Enable the white list use the command "**cable access white-list (enable|disable)**" to enable/disable the black list.

Step 2 Use the command "**show cable access white-list**" to view the result.

Example

Enable the white list.

```
BT(config-if-cmts-1)# cable access white-list enable
BT(config-if-cmts-1)# show cable access white-list
 cable access white-list enable
 the total number of CM is 0
!
```

13.4.6 Setting the White List

Through this task, users can add a CM MAC or CM MAC address segment to a white list. A white list can be configured with up to 1000 white list rules.

Context

N/A

Procedure

Step 1 Use the "**cable access white-list** *mac-begin [mac-end]*" command to add MAC address to a white list.

Step 2 Use the "**show cable access black-list**" command to view the result.

Example

Add a single MAC address to the white list.

```
BT(config-if-cmts-1)# cable access white-list 2476.7d06.bd9a
```

Add a MAC address segment to the white list.

```
BT(config-if-cmts-1)# cable access white-list 4432.c83c.0000 4432.c83c.0009
BT(config-if-cmts-1)# show cable access white-list
 cable access white-list disable
 cable access white-list 2476.7d06.bd9a
 cable access white-list 4432.c83c.0000 4432.c83c.0009
 the total number of CM is 11
!
```

13.4.7 Deleting the White List

Through this task, users can delete specified MAC address or MAC address segment from the white list, or delete the entire list contents. The specified MAC address cannot be FFFF.FFFF.FFFF.

Context

N/A

Procedure

Step 1 Enter the cmts view.

Step 2 Use the "**no cable access white-list** (*mac-begin* | **all**)" command to delete MAC addresses from the white list.

Step 3 Use the "**show cable access white-list**" command to view if it is deleted.

Example

Delete MAC address from the white list.

```
BT(config-if-cmts-1)# show cable access white-list
 cable access white-list disable
 cable access white-list 2222.2222.2222
 cable access white-list 2476.7d06.bd9a
 cable access white-list 4432.c83c.0000 4432.c83c.0009
 the total number of CM is 12
!
```

$ When deleting a MAC address segment, enter only the start address of the MAC segment.

```
BT(config-if-cmts-1)# no cable access white-list 4432.c83c.0000
BT(config-if-cmts-1)# show cable access white-list
```

```
 cable access white-list disable
 cable access white-list 2222.2222.2222
 cable access white-list 2476.7d06.bd9a
 the total number of CM is 2
!
BT(config-if-cmts-1)# no cable access white-list all
BT(config-if-cmts-1)# show cable access white-list
 cable access white-list disable
 the total number of CM is 0
!
```

13.4.8 View the White List

Through this task, users can view the switch status of the white list and device MAC addresses added to the white list.

Context

N/A

Procedure

Step 1 Enter the cmts view.

Step 2 Use the "**show cable access white-list**" command to view the configuration information of the white list.

Example

View the white list.

```
BT(config-if-cmts-1)# show cable access white-list
 cable access white-list disable
 cable access white-list 2476.7d06.bd9a
 the total number of CM is 1
!
```

13.5 Managing CM Upgrades

13.5.1 Overview

This section mainly describes how the CMTS manages CM upgrades. Users can refer to this section to manually upgrade a specific CM to the designated software version or configure the CM to carry out automatic batch upgrades.

13.5.2 Upload/Download CM Image File

Users can refer to this section to understand how to download the CM image file to the CMTS or upload the CM image file in the CMTS to the PC.

Use either the FTP or TFTP protocol to download the CM image file to the specified folder from the FTP and TFTP server respectively. The filename of the CM image file downloaded to the device can be modified according to the user configuration. The default is to retain the original filename.

Operation Procedures

Step 1 Determine if FTP or TFTP will be used to download the file. Prepare the CM image file on the server, and build the connection to make sure that the device can communicate with the server network.

Step 2 In the enable view, use the command "**load cm-class-image**" to upload to the server or download from the server.

Task Example

Download CM image file, SC011_Tv_151128.bin, from FTP server 192.168.0.232 to device and store as SC012_Tv.bin

```
BT# load cm-class-image ftp 192.168.0.232 mpu mpu SC011_Tv_151128.bin
SC012_Tv.bin
File saved successfully!
```

Related Operations

Table 13-9 Related operations to download the CM image file to the device using FTP

Operation	Command	Remark
Upload CM image file to a PC using FTP/TFTP	**upload cm-class-image (ftp | tftp)**	Get the CM image file from the /app/cmImage/ directory
Use TFTP to download the CM image file to the device	**load cm-class-image tftp**	Save the CM image file to /app/cmImage/

13.5.3 Manually Upgrade Specific CM

Users can refer to this section to manually upgrade the software version for specific CM.

Operation Procedures

Step 1 Download the CM image file to the file system in the CMTS.

Step 2 Use the "**upgrade cable modem**" command to use the designated CM image file to upgrade the CM.

Step 3 Use the "**show cable modem upgrade status**" to check if the CM upgrade is successful.

Task Example

Manually upgrade specific CM.

```
BT# upgrade cable modem 001c.1df5.72e1 SC011_Tv_151128.bin
BT# show cable modem all upgrade status
MAC Address      Last-Sw-Vers    Curr-Sw-Vers    Upgrade Status Begin Time
End Time         File Name
001c.1df5.72e1 SC011_Tv_151128 SC011_Tv_151128 upgrading      1970/01/01 06:53 ----/--
/-- --:--       SC011_Tv_151128.bin
```

Related Operations

N/A

13.5.4 CM Automatic Batch Upgrade

Users can refer to this section to configure automatic batch upgrade for the CMs.

Operation Procedures

Step 1 Download the CM image file to the file system in the CMTS.

Step 2 In the config view, use the command "**cable modem auto-upgrade**" to specify the upgrade image file that CM of specific model number should use if the designated software version has not been applied to the CM.

Step 3 In the config view, enable automatic batch upgrade for the CM.

Step 4 Restart the CM.

Step 5 Check the CM upgrade status immediately once the CM is online.

Task Example

Automatic upgrade when the CM is online.

```
BT(config)# show cable modem
MAC Address      IP Address I/F   MAC      Primary RxPwr Timing  Number BPI     Online
                                  State    Sid     (dBmV) Offset CPE    Enabled Time
001c.1df5.72e1 6.6.6.1    C1/U2 w-online 16.0     685    0              no    0d15h24m
Total CM:1
BT(config)# cable modem auto-upgrade BCM93383DCM SC011_Tv_151123
SC011_Tv_151128.bin
Warning:If the configured software version does not match the software version parsed
from the image file,the CM will repeatedly upgrade and reboot.
BT(config)# cable modem auto-upgrade BT(config)# clear
cable modem all reset BT(config)# show cable modem all
upgrade status
MAC Address      Last-Sw-Vers     Curr-Sw-Vers     Upgrade Status Begin Time
End Time            File Name
```

```
001c.1df5.72e1    SC011_Tv_151128 SC011_Tv_151128 upgrading       1970/01/01 22:23
----/--/ ---------SC011_Tv_151128.bin
```

Related Operations

N/A

13.6 Configure CPE Management

Users can manage CPE(Customer Premise Equipment) through this task.

13.6.1 View CPE Information

Users can view the CPE information through this task.

Context

It is allowed to use the following commands to view CPE information for CPE monitoring.

- View the information of CPE under the specified CM by using the command "**show cable modem** (*ip-address* | *mac-address*) **cpe**".
- View the information of all CPEs by using the command "**show cpe all**".
- View the information of the specified CPE by using the command "**show cpe** (*ip-address* | mac *mac-address*)".
- View the number of all types of CPE by using the command "**show cpe summary**".

Procedure

Step 1 View the information of all CPEs by using the command "**show cpe all**".

Example

View the information of all CPEs.

```
BT(config)# show cpe all
MAC               CMC Index  CM MAC            IP Address            Dual IP   CPE
Type  Lease Time
0003.c83c.88e5  C1           4432.c83c.88e5  2000::1:2303:6789:abcc  N          Host
600000s
Host count             :   1
MTA count              :   0
STB count              :   0
Extension device count :   0
IAPD count             :   0
Total count            :   1
```

Related Operations

N/A

13.6.2 Clear CPE Entries

Users can clear CPE entries through this task.

Context

After the specified CPE in the CPE entries is cleared, this CPE is refused to access to the network immediately.

Procedure

Step 1 Clear the CPE entries by using the command "**clear cpe** *mac-address*".

Example

Clear the entries of CPE whose MAC address as 60eb.69e2.d21d.

```
BT(config)# show cpe all
MAC               CMC Index  CM MAC            IP Address               Dual IP   CPE
Type  Lease Time
60eb.69e2.d21d  C1          a4a8.0fa9.607c  10.10.28.239             N          Host
604800s
0003.c83c.88e5  C1          4432.c83c.88e5  2000::1:2303:6789:abcc  N          Host
600000s
Host count              :   2
MTA count               :   0
STB count               :   0
Extension device count  :   0
IAPD count              :   0
Total count             :   2
Topvision(config)# clear cpe 60eb.69e2.d21d
Topvision(config)# show cpe all
MAC            CMC Index  CM MAC        IP Address             Dual IP   CPE Type
Lease Time
0003.c83c.88e5 C1       4432.c83c.88e5 2000::1:2303:6789:abcc  N          Host
600000s
Host count              :   1
MTA count               :   0
STB count               :   0
Extension device count  :   0
IAPD count              :   0
Total count             :   1
```

13.7 CM-based Downstream Frequency Shift

You can perform this task to shift the downstream frequency of the CM. Two methods are available to configure the CM downstream frequency shift:

- Modify the CM downstream frequency based on the CM MAC address: Specify the CM MAC address, and change the downstream frequency of a specified CM to the downstream channel frequency.
- Modify the CM downstream frequency based on the CM service type ID: Specify the CM service type ID, and change the downstream frequency of all CMs carrying this CM service type ID to the downstream channel frequency.

13.7.1 Modifying the CM Downstream Frequency Based on the CM MAC Address

Background Information

When a user requires a specified service, you need to configure a specified downstream frequency for a specified CM.

When modifying the CM downstream frequency based on the CM MAC address, you must specify the frequency shift timeout for the CM. If the CM does not go online using the specified downstream frequency before timeout, the downstream frequency of the CM is no longer restricted, and the CM can use any frequency to go online. The timeout ranges from 60 to 1800 seconds. The default timeout is 720 seconds.

Note:

When the CM downstream frequency is modified based on the CM MAC address, the specified CM must be in a state other than the offline state. At this time, the CM goes offline, the distance is measured again, and then the CM goes online again.

Procedure

Step 1 Run **`cable modem ds-frequency`** to modify the downstream frequency of the specified CM.

Step 2 Run **`cable modem ds-frequency-timeout`** to modify the CM downstream frequency shift timeout.

Step 3 Run **`show cable modem ds-frequency-timeout`** to view the CM downstream frequency shift timeout.

Example

Change the downstream frequency of the CM with the MAC address e889.2c97.de83 to the central frequency 472000000 Hz, and set the timeout to 180 seconds.

```
BT(config)# cable modem e889.2c97.de83 ds-frequency 472000000
BT(config)# cable modem ds-frequency-timeout 180
```

```
BT(config)# show cable modem ds-frequency-timeout
cable modem ds-frequency-timeout: 180s
```

Related Operations

N/A

13.7.2 Modifying the CM Downstream Frequency Based on the CM Service Type ID

Background Information

When a user requires a specified service, you need to configure a specified downstream frequency for a specified CM.

The CMTS supports modification of the CM downstream frequency based on the CM service type ID. The CM service type ID can be specified in the CM configuration file. All CMs obtaining this CM configuration file must go online using the specified frequency. No timeout is configured when the CM downstream frequency is modified based on the CM service type ID. The specified CM must go online using the specified frequency.

Procedure

Step 1 Run **cable service type ds-frequency** to modify the downstream frequency of the specified CM.

Step 2 Run **show cable modem service-type-id** to view the CM downstream frequency shift timeout.

Example

Change the downstream frequency of all CMs using the same CM service type ID "commercial" to550000000 Hz.

```
BT(config)# cable service type commercial ds-frequency 550000000
BT(config)# show cable modem service-type-id
MAC Address      IP Address      I/F     MAC       Primary   Service-type-id
                                         State     Sid
a4a8.0fa9.607c   10.10.28.118    C1/U3   online    13        commercial
Total CM:1
```

Related Operations

Table 13-10 Related operations to modifying the CM downstream frequency based on the CM service type ID

Operation	Command	Remark
Delete the CM service type ID.	**clear cable modem service-type-id**	

Chapter 14 Load Balance Configuration Management

14.1 Load Balance Overview

Load balancing aims to evenly distribute the load to available resources and improve the resource utilization efficiency. When or after a CM goes online, the CMTS periodically checks the loads of channels to determine whether the load balancing conditions are met. If the conditions are met, the CMTS instructs the CM to move to a specified channel through DCC or DBC to improve the throughput of the CMTS.

Load Balancing Group

CMTS load balancing is applied to the load balancing groups. In order to achieve different load balancing policies, the CMTS device supports two types of load balancing groups, namely, common load balancing groups and restricted load balancing groups.

- Common load balancing group: It is the load balancing group created by the CMTS by default. This load balancing group is available to all the downstream channel and upstream channel RF interfaces of the CMTS device, and all the channel resources can be shared. Common load balancing groups are mainly used to provide services to ordinary users.
- Restricted load balancing group: Carriers can configure restricted load balancing groups. Corresponding downstream channels and upstream channels as well as included CMs can be added to this type of group. Restricted load balancing groups are primarily used for providing services to VIP users to ensure that these users can exclusively use channels. You can add restricted CMs to a restricted load balancing group using the following methods:
  - Directly add the CM MAC address segments. Run "**cable load-balance restrict modem**" in the config view to directly add the CM MAC address segments.
  - Add the CM MAC address segments through calculation. The CMTS allows you to run "**exclude modem**" and "**include all cm**" in the cmts-lb-group view to add the CM MAC address segments. The actual address segment is the calculation result of "**exclude modem**" and "**include all**" cm.
  - Add the restricted CMs based on the DOCSIS types supported by CMs. The CTMS supports DOCSIS2.0 CM and DOCSIS3.0 CM.

Note:

1. In a restricted load balancing group, the above three methods cannot be configured at the same time.

---

2. It is prohibited to configure overlapping MAC address segments in two or more restricted load balancing groups.
3. It is prohibited to configure the same DOCSIS version types in two or more restricted load balancing groups.

Load Balancing Method

The method of CMTS load balance. It can be classified in three ways:

- Real-time flow based load balance: This load balancing method is suitable for scenarios where the requirement for equalization is high and the network is under real-time load.
- Active service flow based load balance: This load balancing method is suitable for use when the service scenario is complex. Under normal circumstances, the service bandwidth of each CM is not balanced and needs to be finely divided according to the service flow bandwidth.
- CM number based load balance: This load balancing method is suitable for use when the service scenario is relatively simple. Under normal circumstances, the service bandwidth of each CM is relatively balanced and can be divided directly by the number of CMs.

 Note:

1. To implement load balancing, the CMTS allows you to use command lines to move particular CMs to specified upstream or downstream channels, which can be either a single channel or a set of multiple upstream or downstream channels.
2. For 2.0 CM, it will only work in a single upstream channel and downstream channel, at this time the CMTS device calculate the load as an upstream channel load and a downward channel load.
3. For 3.0 CM, it can work in a number of upstream channels and downstream channels, at this time the CMTS device calculate the load for each of the upstream channel and downstream channel a load.

14.2 Example of Configuration of load balancing instance based on CM

Through this example, the load balancing function of CMTS device based on CM quantity can be realized.

- The requirements are as follows: Load balancing is enabled.
- When the number of CMs between channels exceeds 10, the number of CMs is 16.
- Other load balancing parameters use default values, as shown in 14.6

Data Planning

Load balancing planning is shown below.

Table 14-1 Data Planning forLoad balancing based on CM quantity

Item	Data
Load balancing mode	modem
High flow switch	enable
Maximum number of CM moves per load balancing	16
Minimum difference of CM number between channels	10

Prerequisite

Network CMTS equipment, CM and line are normal.

Configuration flowchart

The load balancing configuration process is shown below.

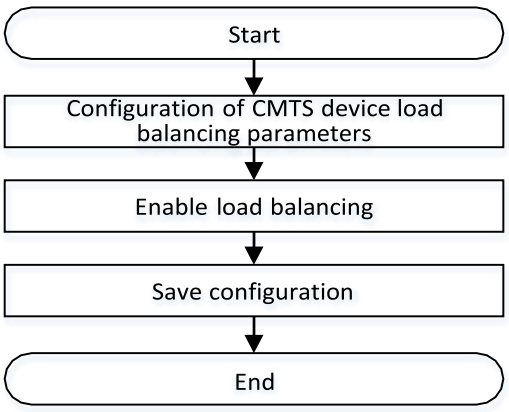

Figure 14-1 Flowchart forLoad balancing configuration based on CM

Procedure

Step 1 Configure CMTS device load balancing parameters

1. Enter the CMTS view

   ```
   BT(config)# interface cmts 1
   ```

2. Configuring load balancing mode is to balance the load according to the number of CM

   ```
   BT(config-if-cmts-1)# cable load-balance method modem
   ```
   The

3. minimum difference of the number of CM channels is 10.

   ```
   BT(config-if-cmts-1)# cable load-balance threshold loadminimum 10
   ```

4. The maximum number of CMs per mobile is 16

   ```
   BT(config-if-cmts-1)# cable load-balance modem-moved 16
   ```

Step 2 Enable load balancing.

1. Exit the CMTS view

   ```
   BT(config-if-cmts-1)# exit
   ```

2. Enable load balancing

   ```
   BT(config)# cable load-balance enable
   ```

Step 3 Save configuration

```
BT(config)# exit
BT# copy running-config startup-config
This will save the configuration to the flash memory.
Are you sure?(y/n) [n]y
Building configuration.....
Configuration saved successfully.
```

Result

According to the above configuration, the CMTS device has normal load balancing function based on the number of CM, and it can move CM normally when the number of CM distributed on the channel reaches the mobile condition.

14.3 Example of Configuration is Based on CM MAC Address Load Balancing Group

Through this example, a CM device with a specified MAC address segment can achieve load balancing in a restricted load balancing group. The requirements are as follows:

- The CM in the MAC address range from 0025.f102.0000 to 0025.f102.ffff balances the load in the restricted load balancing group 1, and the bound upstream and downstream channels are 1-4 and 1-8, respectively.
- CM within the MAC address range of 0025.f105.0000 - 0025.f105.ffff performs load balancing in the restricted load balancing group 2, and the bound upstream and downstream channels are 5-8 and 9-16, respectively.

Data Planning

Load balancing planning is shown below.

Table 14-2 Data Planning forLimited Load Balancing Based on CMMAC Address

Item	Data
Load balancing group	1, 2
Upstream channel in load balancing group 1	1-4
Downstream channel in load balancing group 1	1-8
CM MAC address range in load balancing group 1	0025.f102.0000 - 0025.f102.ffff
Upstream channel in load balancing group 2	5-8
Downstream channel in load balancing group 2	9-16
CM MAC address range in load balancing group 2	0025.f105.0000 - 0025.f105.ffff

Prerequisite

Network CMTS equipment, CM and line are normal.

Configuration flowchart

The load balancing configuration process is shown below.

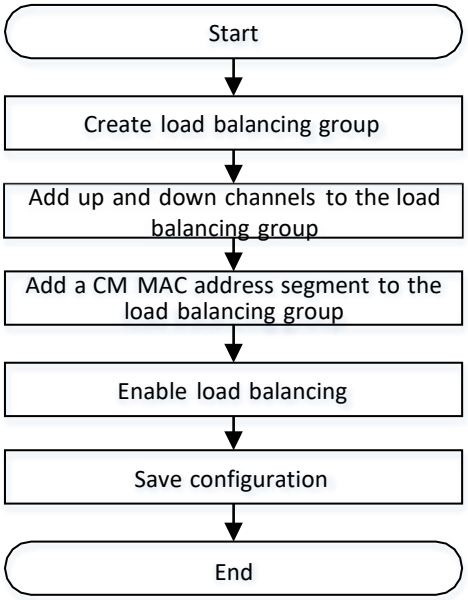

Figure 14-2 Flowchart for CM MAC address-constrained load balancing group configuration

Procedure

Step 1 Create load balancing group 1-2

```
BT(config)# cable load-balance group 1-2 cmts 1
```

Step 2 Add the upstream and downstream channels of the load balancing group

1. Enter load balancing group 1.

   `BT(config)# cable load-balance group 1`Upstream

2. channel 1-4 is added to load balancing group 1 `BT(cmts-lb-group-01)# upstream 1-4` Load balancing group 1 adds

3. downstream channel 1-8 `BT(cmts-lb-group-01)# downstream 1-8` Exit load balancing group 1

4. `BT(cmts-lb-group-01)# exit`

5. Enter load balancing group 2

   `BT(config)# cable load-balance group 2`Upstream

6. channel 5-8 is added to load balancing group 2 `BT(cmts-lb-group-02)# upstream 5-8` Load balancing group 2 adds

7. downstream channel 9-16 `BT(cmts-lb-group-02)# downstream 9-16`Exit load balancing group 2.

8.

```
BT(cmts-lb-group-02)# exit
```

Step 3 Add CM MAC address segment to load balancing group

1. CM MAC address segment 0025.f102.0000-0025.f102.ffff is added to load balancing group 1

```
BT(config)# cable load-balance restrict modem 0025.f102.0000
ffff.ffff.0000 group 1
```

2. CM MAC address segment 0025.f105.0000-0025.f105.ffff was added in load balancing group 2

```
BT(config)# cable load-balance restrict modem
0025.f102.0000 ffff.ffff.0000 group 2
```

Step 4 Enable load balancing

```
BT(config)# cable load-balance enable
```

Step 5 Save configuration

```
BT(config)# end
BT# copy running-config startup-config
This will save the configuration to the flash memory.
Are you sure?(y/n) [n]y
Building configuration.....
Configuration saved successfully.
```

Result

According to the above configuration, CMTS devices will add CM to the restricted load balancing group according to the MAC address, and CM will do load balancing on the intra-group channel.

Note:

Using MAC address to add restricted CM in restricted load balancing group conflicts with the following functions:

1. Adding restricted CM based on CM DOCSIS version type: Both cannot exist simultaneously in the same CMTS device.

2. Exclusion of CM within a group: Both cannot exist simultaneously in the same group of CMTS.

14.4 Example of Configuration is Based on CM Version Load Balancing Group

When the environment needs different DOCSIS versions of CM for different load balancing, different restricted load balancing groups need to be set up to bind different versions of CM to different balancing groups. Through this example, CM can achieve load balancing in restricted load balancing group based on DOCSIS version type. The requirements are as follows:

- DOCSIS version 2.0 CM performs load balancing in the restricted load balancing group 1, and the bound upstream and downstream channels are 1-2 and 1-3, respectively.
- DOCSIS version 3.0 CM performs load balancing in restricted load balancing group 2, and the bound upstream and downstream channels are 3-5 and 4-8, respectively.

Data Planning

Load balancing planning is shown below.

Table 14-3 Data Planning forRestricted Load Balancing Based on CM Version Type

Item	Data
Load balancing group	1, 2, 3
Upstream channel in load balancing group 1	1-2
Downstream channel in load balancing group 1	1-3
CM version type supported by oad balancing group 1	DOCSIS 2.0
Upstream channel in load balancing group 2	3-5
Downstream channel in load balancing group 2	4-8
CM version type supported by oad balancing group 2	DOCSIS 3.0

Prerequisite

Network CMTS equipment, CM and line are normal, CMTS does not exist load balancing group with configuration conflict.

Configuration flowchart

The configuring process of restricted load balancing group based on CM version number is as follows.

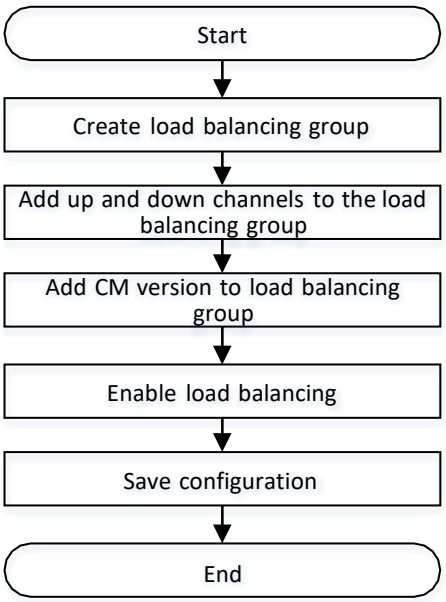

Figure 14-3 Flowchart for CM Version Constrained Load Balancing Group Configuration

Procedure

➢ Configure load balancing group 1:

Step 1 Create load balancing group 1

```
BT(config)# cable load-balance group 1 cmts 1
```

Step 2 Upstream and downstream channels are added to the load balancing group.

1. Upstream channel 1-2 is added to load balancing group 1

   `BT(cmts-lb-group-1)# upstream 1-2` Load

2. balancing group 1 adds downstream channel 1-3 `BT(cmts-lb-group-1)# downstream 1-3`

Step 3 Add CM version number DOCSIS 2.0 in load balancing group 1

```
BT(cmts-lb-group-1)# cm-type d20 BT(cmts-lb-group-1)# exit
```

➢ Configure load balancing group 2:

Step 1 Create load balancing group 2

```
BT(config)# cable load-balance group 2 cmts 1
```

Step 2 Upstream and downstream channels are added to the load balancing group

1. Upstream channel 3-5 is added in load balancing group 2 `BT(cmts-lb-group-2)# upstream 3-5`
2. Load balancing group 2 adds downstream channel 4-8

   `BT(cmts-lb-group-2)# downstream 4-8`

Step 3 Add CM version number DOCSIS 3.0 in load balancing group 2.

```
BT(cmts-lb-group-2)# cm-type d30
BT(cmts-lb-group-2)# exit
```

Step 4 Enable load balancing

```
BT(config)# cable load-balance enable
```

Step 5 Save configuration

```
BT(config)# end
BT# copy running-config startup-config
This will save the configuration to the flash memory.
Are you sure?(y/n) [n]y
Building configuration.....
Configuration saved successfully.
```

Result

According to the above configuration, CMTS device will add CM to the restricted load balancing group according to CM registered version, CM will do load balancing on the intra-group channel.

14.5 Configuring a Load Balancing Group

In order to achieve different load balancing policies, the CMTS device supports two types of load balancing groups, namely, common load balancing groups and restricted load balancing groups.

- Common load balancing group: It is the load balancing group created by the CMTS by default. This load balancing group is available to all the downstream channel and upstream channel RF interfaces of the CMTS device, and all the channel interface resources can be shared. A CMTS device supports only one common load balancing group, and it is primarily used for providing services to ordinary users.
- Restricted load balancing group: Carriers can flexibly create and configure restricted load balancing groups. Corresponding downstream channels and upstream channels as well as included CMs can be added to this type of group. The CMTS device can support several restricted load balancing groups, and they are primarily used for providing services to VIP users. By configuring a restricted load balancing group, you can specify the upstream channels and downstream channels used for load balancing in the group, as well as the CMs participating in load balancing.

After load balancing is enabled, CMs can be added to only one load balancing group. They are preferentially added to a restricted load balancing group. If CMs do not meet conditions for adding to a restricted load balancing group, they are added to a common load balancing group.

14.5.1 Configure the General Load-Balance Group

Users can configure the general load-balance group through this task.

Context

The CMTS allows you to configure a general load balancing group. Configuration of a general load balancing group includes:

- Enabling and disabling of the general load balancing group.
- Initialization technology of the general load balancing group. For details, see Configure the Initialization Technology of Load Balance.
- Policies of the general load balancing group. For details about the policy and rule association modes, see Configure the Load-Balance Time Policy.

Procedure

Step 1 In the cmts view, configure the status of the general load balancing group by using the command "**`cable load-balance general group (disable | enable)`**".

Step 2 Configure the initialization technology of the general load-balance group by using the command "**`init-tech`**".

Step 3 Configure the policy of the general load-balance group by using the command "**`policy`**".

Step 4 Query the information of restricted load-balance group by using the command "**`show running-config`**".

Example

Configure the general load balancing group.

```
BT(config)# interface cmts 1
BT(config-if-cmts-1)# cable load-balance general group enable
BT(config-if-cmts-1)# init-tech 0-3
BT(config-if-cmts-1)# policy 1
BT(config-if-cmts-1)# show running-config verbose | include general groupenable
cable load-balance general group enable
BT(config-if-cmts-1)# show running-config | include init-tech
init-tech 0-3
BT(config-if-cmts-1)# show running-config | include policy
policy 1
```

Related Operations

Table 14-1 Related Operations for Configuring the Restricted Load-balance Group

Operation	Command	Remarks
Restore the default initialization technology of the restricted load balancing group.	`no init-tech`	
Delete the policy of the restricted load balancing group.	`no policy`	

14.5.2 Configure the Restricted Load-Balance Group

Users can configure the restricted load-balance group through this task.

Context

The CMTS supports a maximum of 512 restricted load balancing groups. You can specify the upstream channels and downstream channels used for load balancing in a restricted load balancing group, as well as the CMs participating in load balancing.

- Status of the restricted load balancing group.
- Initialization technology of the restricted load balancing group. For details, see Configure the Initialization Technology of Load Balance.
- Policies of the restricted load balancing group. For details about the policy and rule association modes, see Configure the Load-Balance Time Policy.
- Upstream and downstream channels. A restricted load balancing group supports one or more upstream and downstream channels. The load of restricted CMs in the group are strictly balanced on channels in the same group.

- You can add CMs to a restricted load balancing group using the following methods:
  - Directly add the CM MAC address segments. Run cable load-balance restrict modem in the config view to directly add the CM MAC address segments.
  - Add the CM MAC address segments through calculation. The CMTS allows you to run exclude modem and include all cm in the cmts-lb-group view to add the CM MAC address segments. The actual address segment is the calculation result of exclude modem and include all cm.
  - Add the restricted CMs based on the DOCSIS types supported by CMs. The CTMS supports DOCSIS2.0 CM and DOCSIS3.0 CM.

Procedure

Step 1 In the config view, create a restricted load balancing group by using the command "**cable load-balance group** *group-list* **cmts** *cmts-id*".

Note:

1. If *group-list* is set to a single ID, one restricted load balancing group is created and the system automatically enters the cmts-lb-group view.

2. If *group-list* is set to multiple IDs, multiple restricted load balancing groups are created and the system does not enter the cmts-lb-group view.

Step 2 In the cmts-lb-group view, configure the initialization technology of the restricted load-balancegroup by using the command "**init-tech**".

Step 3 In the cmts-lb-group view, configure the policy of the restricted load-balance group by using the command "**policy**".

Step 4 In the cmts-lb-group view, configure the upstream channels of the restricted load-balance group by using the command "**upstream**", configure the downstream channels of the restricted load-balance group by using the command "**downstream**".

Step 5 In the cmts-lb-group view, add CMs of the restricted load-balance group by using the command "**cable load-balance restrict modem**". In the cmts-lb-group view, add CM address segments of the restricted load-balance group by using the command "**include all cm**" and "**exclude modem**". In the cmts-lb-group view, add CMs based on the supported DOCSIS versionsof the restricted load-balance group by using the command "**cm-type**".

Step 6 Query the information of restricted load-balance group by using the following commands.

- Query the configuration information of restricted load-balance group by using the command "**show cable load-balance group**".
- Query the information of valid CM in the specified restricted load-balance group by using the command "**show cable load-balance group** *group-id* **active cm**".

Example

Configure the preferred load-balance group 1, including upstream channel 1 and 2, downstream channel 1, 3, 4, 5 and 7, and the MAC address of the specified CM to be added to the group as 0026.5ba6.4779-0026.5ba6.4789.

```
BT(config)# cable load-balance group 1 cmts 1
BT(cmts-1-lb-group-1)# init-tech 1-4
BT(cmts-1-lb-group-1)# policy 2
BT(cmts-1-lb-group-1)# upstream 1-3
BT(cmts-1-lb-group-1)# downstream 1-16 BT(cmts-1-
lb-group-1)# cm-type d30 BT(cmts-1-lb-group-1)#
show running-config
 init-tech 1,2,3,4
 policy 2
 upstream 1-3
 downstream 1-16
 cm-type d30
```

Related Operations

Table 14-2 Related Operations for Configuring the Restricted Load-balance Group

Operation	Command	Remarks
Restore the default initialization technology of the restricted load balancing group.	**no init-tech**	
Delete the policy of the restricted load balancing group.	**no policy**	
Delete upstream channels in the restricted load balancing group.	**no upstream** *upstream-list*	
Delete downstream channels in the restricted load balancing group.	**no downstream** *downstream-list*	
Delete restricted CMs in the group.	**no cable load-balance restrict modem** *index* **(group** *group-id* **| service-type-id** *service-type-id***)** **no cable load-balance restrict modem (***index-list* **| all) cmts** *cmts-id*	
Delete the excluded restricted CMs in the group.	**no exclude modem (***index-list* **| all)**	
Delete the supported DOCSIS versions in the group.	**no cm-type (d20 | d30)**	

Operation	Command	Remarks
Delete the restricted load balancing group.	**no cable load-balance group** (*group-list* **| all) cmts** *cmts-id*	When a restricted load balancing group is deleted, all configurations in the group are deleted as well.

14.6 Configure the Parameters of Load Balance

14.6.1 Configure the Method of Load Balance

Context

CMTS load balance can be classified in three ways:

- utilization: Real-time flow based load balance
- service-flows: Active service flow based load balance
- modem: CM number based load balance

Procedure

Step 1 Enter the cmts view by using the command "**interface cmts**".

Step 2 Configure the method of load balance by using the command "**cable load-balance method (utilization | service-flows | modem)**". Or configure the method of load balance by using the command "**cable load-balance method upstream (modem | service-flows | utilization) downstream (modem | service-flows | utilization)**"

By default, CMTS executes the load balance based on the channel utilization.

Example

Configure CMTS to execute the active service flow based load balance.

```
BT(config)# interface cmts 1
BT(config-if-cmts-1)# cable load-balance method service-flow
```

Related Operations

N/A

14.6.2 Configure the Heavy/Light-Traffic Thresholds of Load Balance

Users can configure the heavy/light-traffic thresholds of load balance through this task.

Context

- The function will be effective when the load balance methed is utilization.
- When the channel utilization is increasing, CMTS will change the operating mode of load balance to the channel utilization load balance after the channel utilization exceeds the heavy-traffic threshold.
- When the channel utilization is decreasing, CMTS will change the operating mode of load balance to the channel CM number load balance after the channel utilization is lower than the light-traffic threshold.

Procedure

Step 1 Enter the cmts view by using the command "**interface cmts**".

Step 2 Configure the heavy-traffic threshold of load balance by using the command "**cable load-balance system threshold** *threshold-low threshold-high*".
By default, the light-traffic threshold of load balance is 0%, and the heavy-traffic threshold is 0%.

Example

Configure the light-traffic threshold of load balance as 15%, and the heavy-traffic threshold as 25%.

```
BT(config)# interface cmts 1
BT(config-if-cmts-1)# cable load-balance system threshold 15 25
```

Related Operations

N/A

14.6.3 Configure the Execution Cycle of Load Balance

Users can configure the cycle of load balance through this task.

Context

The cycles configured in different operating mode may differ:

- Active service flow based and CM number based load balance: in this mode, only the configuration of execution cycle is valid, which means the main thread for DOCSIS will balance the load of each channel once every cycle.
- Real-time flow based load balance: in this mode, the configurations of both execution cycle and the number of cycle for calculating the average weighted channel load are valid, which means that MAC address statistics thread will update the dynamic load of upstream/downstream channels once every a cycle. The dynamic load will be calculated by the following means: assign a weight to the real-time load in previous N cycles (including the current cycle), and then calculate the weighted load, which is the dynamic load of the channel.

Procedure

Step 1 Enter the cmts view by using the command "**interface cmts**".

Step 2 Configure the cycle of load balance by using the command "**cable load-balance period** *period* **number (1 | 2 | 4)**".

Example

Configure the execution cycle of CMTS load balance as 70s, and the number of cycle for calculating the average weighted channel load as 2.

```
BT(config)# interface cmts 1
BT(config-if-cmts-1)# cable load-balance period 70 number 2
```

Related Operations

Table 14-3 Related Operations for Configuring the Load-balance Mode

Operation	Command	Remarks
Configure the operating mode of load balance	**cable load-balance method**	

14.6.4 Configure the Channel Overload Threshold and Difference Threshold

Users can configure the channel overload threshold and difference threshold through this task.

Context

Only when the following two conditions are met at the same time can CMTS be ready to move CM on this channel.

- Only when the channel utilization exceeds the channel overload threshold,
- the difference between the source channel utilization and the destination channel utilization exceeds the difference threshold

Procedure

Step 1 Enter the cmts view by using the command "**interface cmts**".

Step 2 Configure the channel overload threshold and the difference threshold between the source channel utilization and the destination channel utilization when moving CM by using the command "**cable load-balance threshold trigger** *trigger* **diff** *diff*".

Example

Configure the channel overload threshold as 65%, and the difference threshold between the source channel utilization and the destination utilization when moving CM as 15%.

```
BT(config)# interface cmts 1
BT(config-if-cmts-1)# cable load-balance threshold trigger 65 diff 15
BT(config-if-cmts-1)# show running-config verbose | include threshold trigger
```

```
cable load-balance threshold trigger 65 diff 15
```

Related Operations

N/A

14.6.5 Configure the Channel Minimum Load Threshold

Context

This function takes effect when the working mode of load balancing is service-flows or modem.

- When the working mode of load balancing is service-flows, and the difference of service flows between CMTS channels exceeds the configured value, the CMTS performs load balancing.
- When the working mode of load balancing is service-flows or modem, and the difference of CM counts between CMTS channels exceeds the configured value, the CMTS performs load balancing.

Procedure

Step 1 Enter the cmts view by using the command "**interface cmts**".

Step 2 Configure the method by using the command "**cable load-balance threshold method (service-flows | modem)**".

Step 3 Configure the minimum load threshold by using the command "**cable load-balance threshold load minimum**".

Step 4 Display the minimum load threshold of special upstream channel by using the command "**show running-config verbose**".

Example

Configure the minimum load threshold as 10.

```
BT(config)# interface cmts 1
BT(config-if-cmts-1)# cable load-balance method modem BT(config-if-cmts-1)#
cable load-balance threshold load minimum 10 BT(config-if-cmts-1)# show
running-config verbose | include minimum
 cable load-balance threshold load minimum 10
```

Related Operations

N/A

14.6.6 Configure Maximum Number of CM to be Moved Each Time

Users can configure the parameters when CMTS moves CM during the load balance through this task.

Context

Configure the maximum number of CM to be moved each time by the upstream and downstream of load balance to adjust the efficiency of load balance. This configuration takes effect for both upstream and downstream.

Procedure

Step 1 Enter the cmts view by using the command "**interface cmts**".

Step 2 Configure the maximum number of CM to be moved each time by the load balance by using the command "**cable load-balance modem-moved** *modem-num*".

Example

Configure the maximum number of CM to be moved each time by the load balance as 20.

```
BT(config)# interface cmts 1
BT(config-if-cmts-1)# cable load-balance modem-moved 20
BT(config-if-cmts-1)# show running-config verbose | include modem-moved
 cable load-balance modem-moved 20
```

Related Operations

N/A

14.6.7 Configure the Minimum Interval for Moving CM

Users can configure the minimum interval for moving CM through this task.

Context

Only when the interval of CM to be moved from the last move exceeds the minimum interval, can CMTS move this CM.

Procedure

Step 1 Enter the cmts view by using the command "**interface cmts**".

Step 2 Configure the minimum interval for moving CM by using the command "**cable load-balance interval** *interval*".

Example

Configure the minimum interval for moving CM as 200s.

```
BT(config)# interface cmts 1
BT(config-if-cmts-1)# cable load-balance interval 200
BT(config-if-cmts-1)# show running-config verbose | include balance interval
 cable load-balance interval 200
```

Related Operations

N/A

14.6.8 Configure the Initialization Technology of Load Balance

Users can configure the initialization technology of load balance through this task.

Context

For different upstream channel multiplexing modes, CMTS may use different initialization technologies.

There are 8 initialization technologies in the DOCSIS standard for selection, which will bring about different degrees of interruption of CM data and the success rate of switching channels. The device supports multiple initialization technologies at the same time. When the configuration is not unique, the use of numerically larger initialization technology is preferred.

When the channel type is SCQAM DCC, the supported initialization technique is 0-4 and the priority is: 4>3>2>1>0.

When the channel type is SCQAM DBC, the supported initialization technique is 1-4 and the priority is: 4>3>2>1.

- Initialization technique 0: The use of initialization technique 0 (reinitialize the MAC), results in the longest interruption of service.
- Initialization technique 1: (All upstream channel types) Perform broadcast initial ranging (IUC3) on new channel before normal operation.
- Initialization technique 2: (S-CDMA and TDMA channels only) Perform unicast ranging (IUC3 or IUC4) on new channel before normal operation.
- Initialization technique 3: (S-CDMA and TDMA channels only) Perform either broadcast (IUC3) or unicast (IUC3 or IUC4) ranging on new channel before normal operation.
- Initialization technique 4: (S-CDMA and TDMA channels only) Use new channel directly without reinitializing or ranging.

Procedure

Step 1 Enter the cmts view by using the command "**interface cmts**".

Step 2 Configure the initialization technique of load balance by using the command "**init-tech**".

Example

Configure the initialization technique of load balance as 1-4.

```
BT(config)# interface cmts 1
BT(config-if-cmts-1)# init-tech 1-4
```

```
BT(config-if-cmts-1)# show running-config verbose | include init-tech
 init-tech 1,2,3,4
```

Related Operations

N/A

14.6.9 Enable the Load-Balance Ranging Override Mode

Users can enable the load-balance ranging override mode through this task.

Context

Configure CMTS to enable the channel reload function for RNG-RSP message before CM is registered.

Procedure

Step 1 Enter the cmts view by using the command "**interface cmts**".

Step 2 Enable the load-balance ranging override mode by using the command "**cable load-balance ranging-override enable**".

Example

Enable the load-balance ranging override mode.

```
BT(config)# interface cmts 1
BT(config-if-cmts-1)# cable load-balance ranging-override enable BT(config-if-cmts-1)# show running-config verbose | include ranging-overridecable load-balance ranging-override enable
```

Related Operations

N/A

14.6.10 Configure the Load-Balance Blacklist

Users can configure the load-balance blacklist through this task.

Context

Configure the load-balance blacklist to make the specified CM not participate in the load balancing.

Procedure

Step 1 Enter the cmts view by using the command "**interface cmts**".

Step 2 Configure the load-balance blacklist by using the command "**cable load-balance exclude modem [***index***] mac** *mac-begin* **[***mac-mask***]**".

Step 3 Query the information of load-balance blacklist by using the command "**show cable load-balance exclude active cm**".

Example

Add the CM with MAC address in the range of 0024.6800.0000-0024.6800.00ff to the load-balanceblacklist.

```
BT(config)# interface cmts 1
BT(config-if-cmts-1)# cable load-balance exclude modem mac 0024.6800.0001
ffff.ffff.ff00
BT(config-if-cmts-1)# show cable load-balance exclude active cm
I/F      CM ID       CM MAC
C1       1           0024.6800.0005
Total CMs : 1
```

Related Operations

Table 14-4 Related Operations for Enabling the Load-balance Function of CMTS

Operation	Command	Remarks
Delete the specified CM from the load-balance blacklist	**no cable load-balance exclude modem**	

14.6.11 Configure the Load-Balance Time Policy

Users can configure the load-balance time policy through this task.

Context

By configuring the time strategy of load balancing, the CMTS device can disable the load balancing function within a specified period of time. Rules and policies are associated in the following ways:

- Equipment supports 200 rules and 100 strategies.
- Each policy can associate one enable or disable rule, and multiple disable-period rules.
- Multiple policies can associate the same rule

Procedure

Step 1 Configure the start/end time for disabling the load balance by using the command "**cable load-balance rule** *rule-id* **disable-period dis-start** *dis-start* **dis-end** *dis-end*".

Step 2 Create the load-balance policy and bind it to the specified rule by using the command "**cable load-balance policy** *policy-id* **rule** *rule-id*".

Step 3 Enter the cmts view by using the command "**interface cmts**".

Step 4 Configure the load-balance time policy by using the command "**policy** *policy-id*".

Step 5 Query the information of load-balance time policy by using the following commands.

- View the configuration information of load-balance time policy by using the command "**show cable load-balance policy**".
- View the configuration information of load-balance rule by using the command "**show cable load-balance rule**".

Example

Configure CMTS to disable the load balance in 1:00a.m.-2:00a.m. every day.

```
BT(config)# cable load-balance rule 1 disable-period dis-start 01:00:00 dis-end
02:00:00
BT(config)# cable load-balance policy 1 rule 1
BT(config)# interface cmts 1 BT(config-if-cmts-
1)# policy 1 BT(config-if-cmts-1)# exit
BT(config)# show cable load-balance rule
cable load-balance rule 1 disable-period dis-start 01:00:00 dis-end 02:00:00
BT(config)# show cable load-balance policy
cable load-balance policy 1 rule 1
```

Related Operations

Table 14-5 Related Operations for Enabling the Load-balance Function of CMTS

Operation	Command	Remarks
Disable the prohibited load-balance rule	**cable load-balance rule** *rule-id* **disable**	
Delete the prohibited load balance rule	**no cable load-balance rule** *rule-id*	
Delete the prohibited binding relationship between load balance rule and policy	**no cable load-balance policy** *policy-id* **rule** *rule-id*	
Delete the load balance policy	**no cable load-balance policy** *policy-id*	

14.7 Configure the Manual Load Balance

Configure the manual load balance through this task.

Context

By configuring the manual load balance, make a CM to be moved to the specified upstream/downstream channel to achieve the purpose of load balancing.

Procedure

Step 1 Enter the cmts view by using the command "**interface cmts**".

Step 2 Configure the manual load balance by the following commands.

- Configure the specified CM to be moved to the specified upstream channel by using the command "**cable move cm** *mac-address* **upstream to** *channel-list* **[init-tech** *init-num***] [sfid** *sfid bdg-id***] [trans-id** *trans-id***]**".
- Configure the specified CM to be moved to the specified downstream channel by using the command "**cable move cm** *mac-address* **downstream to** *channel-list* **[init-tech** *init-tech-list***] [sfid** *sfid bdg-id***][trans-id** *trans-id***]**".
- Configure the 3.0 CM to be moved to the specified downstream channel by using the command "**cable move cm** *mac-address* **rcp-id** *rcp-id* **rcc-id** *rcc-id* **[init-tech** *init-tech-list***] [sfid** *sfid bdg-id***] [trans-id** *trans-id***]**".

Step 3 View the upstream and downstream channels currently used by CM by using the command "**show cable modem primary-channel**".

Example

Move the CM with MAC address as 0010.211a.6f7b to upstream channel 2 and downstream channel 5.

```
BT(config)# interface cmts 1
BT(config-if-cmts-1)# cable move cm 0010.211a.6f7b upstream to 2
BT(config-if-cmts-1)# cable move cm 0010.211a.6f7b downstream to 5
BT(config-if-cmts-1)# show cable modem primary-channel
MAC Address     IP Address    I/F  MAC     Primary Num   Upstream       Downstream
                                   State   Sid     CPE   Primary(list)  Primary(list)
0010.211a.6f7b 10.10.28.129  C1/U1 online  7       0     2                5
```

14.8 View load balancing records

This task allows you to view load balancing records.

Context

CMTS devices support viewing the records and statistics of load balanced mobile CM.

Procedure

Step 1 Use the "**interface cmts**" command to enter the CMTS view

Step 2 Use the "**show cable load-balance dynamic**" command to view load balancing mobile CM records

Example

View the records and statistics of load balancing mobile CM:

```
BT(config)# interface cmts 1
BT(config-if-cmts-1)# show cable load-balance dynamic
MAC Address     Upstream    Downstream    Initialization       Message  Result   Time
                Channel(s)  Channel(s)    Technique            Type
2476.7d06.d4fe  2 -> 4      10 -> 8       reinitialize          dcc     success
1970-01-02 15:48:37
fc94.e349.47e0  2 -> 1      16 -> 7       reinitialize          dcc     success
1970-01-02 15:48:37
001c.1df5.5e68  1-4 -> 1-4  8-15 -> 7-14  broadcastInitRanging  dbc     success
1970-01-01 00:15:06
001c.1df5.5ead  1-4 -> 1-4  8-15 -> 9-16  broadcastInitRanging  dbc     success
1970-01-01 00:15:06
```

Chapter 15 Channel Bonding

15.1 Overview

Channel binding means that data of CM service flows is distributed to multiple channels during transmission of service flows. In this way, data bandwidth of a single CM and stability of CMs are improved, the high bandwidth requirements of users are met.

Note: THIS IS A DEPRECATED PRACTICE AND IS ONLY PRESENTED HERE FOR HISTORICAL PURPOSES.

For CMs that supports channel binding, their service flows can be distributed to a single or multiple upstream or downstream channels. When a service flow is transmitted on multiple channels, this service flow is called bound service flow and channels that carry this service flow form a binding group.

Upstream and downstream channels can be separately bound.

- Upstream channel binding: The CM fragments packets and distributes packet fragments to timeslots allocated by the CMTS to the service flow. Each packet fragment carries the fragment SN. On receiving the packet fragments, the CMTS re-sequences packet fragments based on fragment SNs.
- Downstream channel binding: The CMTS distributes packets to multiple channels. Generally, the DOCSIS MAC header of the downstream channel contains the packet SN. On receiving packets, the CMTS re-sequences packets based on packet SNs.

Channel binding can be classified into static and dynamic binding. In static binding, the CMTS selects a channel set for a CM based on constraints of related fields in the CM registration request. In dynamic binding, the CMTS selects a channel set based on certain rules when these constraint fields are unavailable.

- The following static binding modes are available:
  - Specifying using the configuration file: The CM configuration file specifies the channel (TLV 43.9 CM Attribute Masks) used by the CM. This mode is used when the CM channels must be fixed.
  - Receive Channel Configuration (RCC) template: By matching the RCP ID carried in the CM registration message, the CM can use channels configured in the RCC template. This mode is applicable to downstream channels of DOCSIS3.0 CMs.
  - Restricted load balancing group: It can be used to restrict the binding channels of CMs. CMs can only go online using the specified upstream or downstream channel set.
  - Static binding group: CM service flows select binding groups and use channel in the binding group by matching the service flow mask in the CM configuration file with the pre-allocated mask in the static binding group.
- Dynamic channel binding mode:

  When the above channel binding constraints are absent, the CMTS selects available channels based on the

maximum number of bound channels supported by CMs and dynamically creates a channel binding group

for CMs. The basis for the selection is generally load balancing, for example, when the global load balancing is enabled but the CMs are not added to a restricted load balancing group.

15.2 Bonding Group Function

15.2.1 Overview

Bonding Group is a set of pre-planned channels allocated by users to divide CM of different business types into different binding groups. Each upstream binding group or downstream binding group has two attributes: Provisioned Attribute Mask (Provisioned Attribute Mask) and channel list. CMTS matches the ProvAttrMask of the binding group according to the Required Attribute Mask and Forbidden Attribute Mask parameters in CM's service flow parameters and determines CM's channel set according to the channel set in the binding group. The upstream binding group and the downstream binding group are independent of each other and play their respective roles. They need to be configured separately in planning.

CMTS supports the configuration of ProvAttrMask for separate upstream and downstream channels. Like binding groups, CM service flows can configure the corresponding AttrMask and then bind to separate channels.

Attribute Mask is 32 bits, 0-15 bits are regulated by protocol. At present, only 0-2 bits have been planned, 3-15 bits are reserved for future planning, and 16-31 bits are defined by users independently. An example of the use planning of attribute mask bits is given.

Bit (0): Bonded, denoted as a binding group.

Bit (1): Low Latency, which means that CMTS provides a scheduling method with lower delay than conventional scheduling.

Bit (2): High Availability, which means that there is redundant hardware to administer failed channels.

Other possible uses such as DSG, IPVideo, High Robustness (low packet error rate).

Service flow Attribute Mask and Binding Group/Single Channel ProvAttrMask need to be co-planned to ensure that service flows can match their expected binding group/single channel. The rules for CMTS matching service flow Attribute Mask parameters and binding group/single channel ProvAttrMask are as follows:

- Required Attribute Mask requires a Provisioned Attribute Mask corresponding to 1.
- 1 bit of Forbidden Attribute Mask requires that the corresponding bit of Provisioned Attribute Mask be 0.
- The 0 bits of Required Attribute Mask and Forbidden Attribute Mask do not require the corresponding bits of Provisioned Attribute Mask.
- Required Attribute Mask and Forbidden Attribute Mask match Provisioned Attribute Mask only when the service flow matches the binding group.

Binding groups are related to dynamic service flows required by load balancing and voice services. When CMTS registers or balances load, CMTS allocates binding groups or channels for service flows based on the attribute masks of CM service flows and the pre-configured attribute masks of each binding group. When dynamically creating service flows in voice services, if the parameters of service flows in DSA messages received by CMTS have attribute masks, CMTS allocates binding groups or channels to service flows. If there is no attribute mask, CMTS uses the global attribute mask configuration for voice service flow. In the process of CM service flow creation, if the AttrMask parameter of service flow cannot match any binding group/channel, event reporting will be triggered, and the service flow will be bound to all CM channels.

Both binding group and load balancing constrain the set of channels bound by CM. If CM belongs to a load balancing group, CMTS will move CM to the load balancing group first. When CMTS balances the load within the group, CMTS will first ensure that CM service flows are bound to the matching binding group/channel.

When the CM Attribute Mask parameter is specified in the CM configuration file:

- DOCSIS v3.0 mode, service flow Attribute Mask priority is higher than CM Attribute Mask.
- In DOCSIS v2.0 mode, CM Attribute Mask has higher priority than service flow Attribute Mask, and only single channel binding group is selected in matching process.

15.2.2 Example of Bonding Group Configuration

Via this task, a CM can be set to a particular channel set through a bonding group.

Context

For the bonding group configuration of CMTS, CM obtains a configuration file with service flow AttrMask parameters via the Provisioning system go online.

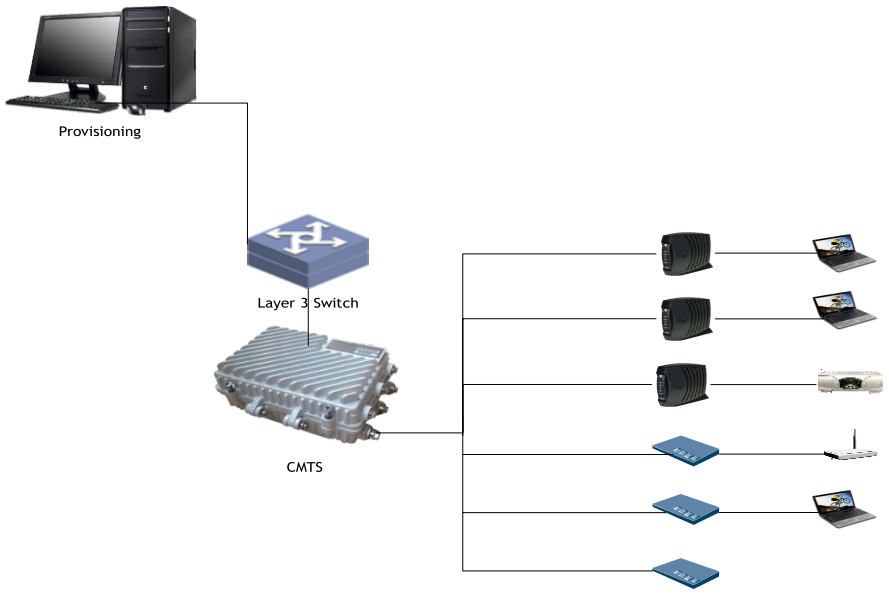

Figure 15-1 Networking Diagram of CMTS Device

Data Planning

In this example, a qualified CM has been set to downstream channel 1, 2, 3, 4, 5, 6, 7 and 8 via downstream bonding group 1 and downstream bonding group 2; of which, bonding group 1 will plan channel 1, 2, 3, and 4 as route 1 data service and configure Provisioned Attribute Mask as bit(0): Bonded(Highest bit is 1), bit(31): Data-1 (the corresponding bit is 1); Bonding group 2 will plan channel 5, 6, 7, and 8 as route 2 data service, and configure Provisioned Attribute Mask as bit(0): Bonded(Highest bit is 1), bit(30): Data-2 (the corresponding bit is Accordingly, the service flow Required Attribute Mask and Forbidden Attribute Mask in the CM configuration file shall be configured so that it matches with its expected bonding group mask. The specific rules have been covered in 15.1. The data planning for bonding group configurations is shown in the table below.

Table 15-1 Data Planning for the Instance for Configuring a Bonding Group

Item	Data
Bonding group 1 ID	1
Bonding group 1 direction	DS
Bonding group 1 ProvAttrMask	80000001
Bonding group 1 channel list	1,2,3,4
Bonding group 2 ID	2
Bonding group 2 direction	DS
Bonding group 2 ProvAttrMask	80000002
Bonding group 2 channel list	5,6,7,8
downstream service flow 1 Required Attribute Mask	80000001 (set in the CM Configuration File)
downstream service flow 1 Forbidden Attribute Mask	7FFFFFFE (set in the CM Configuration File)
downstream service flow 2 Required Attribute Mask	80000002 (set in the CM Configuration File)
downstream service flow 2 Forbidden Attribute Mask	7FFFFFFD (set in the CM Configuration File)

Prerequisite

- Network devices and lines are both normal.
- The Provisioning system is normal.

Configuration flowchart

The flow for bonding group configuration is shown in the figure below.

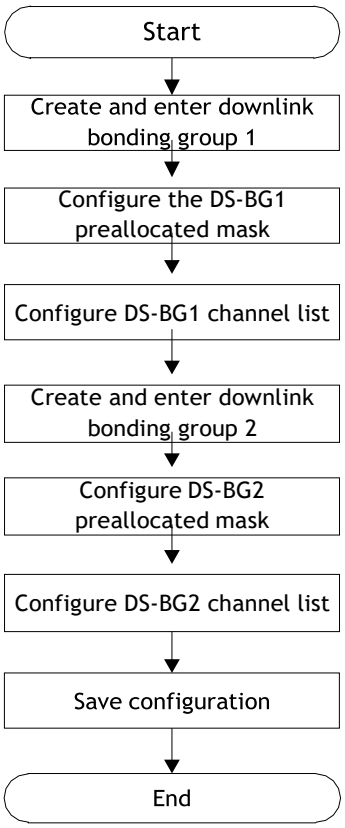

Figure 15-2 Flowchart for bonding group configuration

Procedure

Step 1 Create and enter into the downstream bonding group 1.

```
BT(config)# interface ds bonding-group 1
```

Step 2 Configure the provisioned attribute mask for bonding group 1.

```
BT(config-if-ds-bonding-group1)# bonding-group prov-attr-mask
80000001
```

Step 3 Configure the channel list for bonding group 1.

```
BT(config-if-ds-bonding-group1)# cable downstream 1-4
```

Step 4 Create and enter into the downstream bonding group 2.

```
BT(config)# interface ds bonding-group 2
```

Step 5 Configure the provisioned mask for bonding group 2.

```
BT(config-if-ds-bonding-group2)# bonding-group prov-attr-mask
80000002
```

Step 6 Configure the channel list for bonding group 2.

```
BT(config-if-ds-bonding-group2)# cable downstream 5-8
```

Step 7 Save the configuration.

```
BT(config-if-ds-bonding-group2)# exit
BT(config)# exit
BT# copy running-config startup-config
This will save the configuration to the flash memory.
```

```
Are you sure?(y/n) [n]y
Building configuration.....
Configuration saved successfully.
```

Result

After the configuration is complete, CM obtains the configuration file from Provisioning system and go online; CM downstream flow 1 will be bound to channel 1-4, CM downstream service flow 2 will be bound to channel 5-8, and the downstream channel set for CM will be channel 1-8.

15.2.3 ProvAttrMask for configuring a single channel

Context

Some service flow of CM may require to be bonded to a separate channel, which cooperates CM service flow Required Attribute Mask parameter (bit(0): Bonded bit is 0, which means the highest bit needs to be 0), and CMTS will bind the service flow to a separate channel.

Procedure

Step 1 Enter **"interface cmts 1"** in the configuration view to open cmts view.

Step 2 Use **"cable upstream prov-attr-mask" or "cable downstream prov-attr-mask"** command to configure the ProvAttrMask of upstream or downstream channel.

Step 3 Use **"show running-config"** to view the configuration for single channel attribute mask.

Example

Configure the multicast authentication profile. mask of upstream channel 1 as 7FFFFFF.

```
BT(config)# interface cmts 1
BT(config-if-cmts-1)# cable upstream 1 prov-attr-mask 7fffffff BT(config-
if-cmts-1)# show running-config | include prov-attr-maskcable upstream 1
prov-attr-mask 7fffffff
```

Related Operations

Table 15-2 Related Operations for Configure the multicast authentication file

Operation	Command	Remarks
Restore the ProvAttrMask of the upstream channel to be default 00000000	**no cable upstream** *channel-list* **prov-attr-mask**	
Restore the ProvAttrMask of the downstream channel to be default 00000000	**no cable downstream** *channel-list* **prov-attr-mask**	

15.2.4 Configuration of voice flow default AttrMask

Context

When CM requests to dynamically build the service flow for voice service via DSA, the service flow parameters may not carry the default Attribute Mask parameter, and the voice service flow Attribute Mask parameter set by CMTS will be used to select a channel for this voice service flow.

Procedure

Step 1 In config view, the **"cable docsis30-voice upstream req-attr-mask forb-attr-mask"** or **"cable docsis30-voice downstream req-attr-mask forb-attr-mask"** command can be used to configure the default attribute mask of upstream or downstream voice service flow.

Step 2 Use **"show running-config"** to view the configuration of voice service flow default mask.

Example

Configure the default attribute mask req-attr-mask of upstream voice service flow to be 85555555 and the forb-attr-mask to be 00000000.

```
BT(config)# cable docsis30-voice upstream req-attr-mask 85555555 forb-attr-mask 00000000
BT(config)# show running-config | include voice
cable docsis30-voice upstream req-attr-mask 85555555 forb-attr-mask 00000000
```

Related Operations

Table 15-3 Related Operations for Configure the multicast authentication file

Operation	Command	Remarks
Restore the default attribute mask Required Attribute Mask and Forbidden Attribute Mask of the upstream voice service flow to be default 00000000.	**no cable docsis30-voice upstream attr-mask**	Required Attribute Mask and Forbidden Attribute Mask are both configured to be 00000000.
Restore the default attribute mask Required Attribute Mask and Forbidden Attribute Mask of the downstream voice service flow to be default 00000000.	**no cable docsis30-voice downstream attr-mask**	Required Attribute Mask and Forbidden Attribute Mask are both configured to be 00000000.

Chapter 16 Admission Control Function

16.1 Overview

The admission control function is used to manage the upstream bandwidth of the equipment based on the service flows. According to the current system resource occupancy rates, the function controls and determines if new service flows should be admitted and to allocate bandwidth resources reasonably based on the needs in order to achieve a rational bandwidth resource utilization.

When the system resources cannot satisfy the requirements for a CM registration or dynamic service flow creation, there is a need to rationally manage the access requests from service flows, otherwise a situation where resources are depleted will arise. At the same time, the resource usage of the new service flows will affect the QoS levels for existing service flows, and this will reduce the stability of the system services. With the admission control function, the system can provide a reasonable QoS guarantee, and at the same time, prevent service anomalies as a result of resource depletion. In addition, the function can also be used to reserve bandwidth for a selected service type.

16.2 Admission Control Principles

Admission Control Function for Upstream Bandwidth

Upstream channels support the admission control based on the type of scheduling employed in the service flows, and the following scheduling types are supported: BE, NRTPS, RTPS, UGS-AD and UGS.

CM registration and dynamic service flow creation will trigger the admission control logical check for the upstream channel bandwidth. The BE service flows are divided into two categories: Committed Information Rate (CIR) where the QoS parameters include a minimum guaranteed bandwidth, and Unclassified BE where no minimum guaranteed bandwidth has been configured. The supported BE upstream scheduling type is CIR BE.

For Unclassified BE, the service can utilize the unused exclusive channel bandwidth and the unused channel bandwidth, but such service has the lowest priority, and when there is insufficient bandwidth to meet the demands of other services, those services can then seize these bandwidth resources.

16.2.1 Bandwidth Admission Control Algorithm

This section will describe in detail the admission control algorithm, assuming that the equipment has been correctly configured with the event switch, and the channel bandwidth thresholds have been configured according to the service types. CM registration and dynamic service flow can be triggered any time, and the admission control can also enter the control logic any time.

When an access request from a new service flow on the CMTS equipment has been accepted, the admission control function calculates and updates the bandwidth usage for the service type on every upstream channel,

including the usage status for both exclusive and non-exclusive bandwidth, and the size of the available non-exclusive bandwidth on the channel. So for any new service flow request, the function will compare the current bandwidth usage and threshold in order to decide on the admission control. The specific rules are as follows.

Table 16-1 Specific rules on the admission control

Exclusive bandwidth	Non-exclusive bandwidth	Admission conditions
Y	Y	When the exclusive bandwidth fulfills the condition: Require + Actual-exclusive <= Exclusive, admission is granted. When the exclusive bandwidth cannot fulfill the condition, admission will be granted if the following three conditions are fulfilled: 1. The configured exclusive and non-exclusive bandwidth fulfill the service flow admission condition: Require + Actual-exclusive + Actual-non-exclusive <= Exclusive + Non-exclusive. That is, excluding the available channel bandwidth, the total bandwidth required by the service type cannot exceed the sum of the thresholds for exclusive and non-exclusive bandwidth. The total cannot exceed the sum of thresholds for exclusive and non exclusive bandwidth. 2. Require - (Exclusive - Actual-exclusive) <= (Non-exclusive - Actual-non-exclusive). That is, the required bandwidth, after subtracting the available bandwidth within the exclusive bandwidth threshold range, should be less than or equal to the amount of the bandwidth available within the non-exclusive bandwidth threshold range. 3. Require - (Exclusive - Actual-exclusive) <= RF-Non-exclusive. That is, the required bandwidth, after subtracting the available bandwidth within the exclusive bandwidth threshold range, should be less than or equal to the available non-exclusive bandwidth resources on the channel.
Y	N	If Require - (Exclusive-Actual-exclusive) <= RF-non-exclusive, i.e. the available non-exclusive channel bandwidth resources can satisfy the requirements, admission will be granted.
N	Y	Admission is granted only if the following two conditions are both fulfilled at the same time: The configured non-exclusive bandwidth can fulfill the service flow admission condition: Require + Actual-no-exclusive <= Non-exclusive. Require <= RF-Non-exclusive. There are available non-exclusive bandwidth resources on the channel.
N	N	When the condition is satisfied: Require <= RF-non-exclusive, admission is granted.

16.3 Configuration Admission Control Event Switch

Context

- CMTS supports two types of admission control events: CM registration request and dynamic service flow

creation. When the CM is registered to go online, the CMTS will analyze the upstream service flow parameters in the CM registration request and perform the admission control calculations and process the admission control. When the dynamic service flow is created and activated, the CMTS will analyze the service flow parameters to perform the admission control calculations, and process the admission control.

- By default, the admission control for both the CM registration request and dynamic service flow creation events in the system is not enabled. The admission control function needs to be enabled manually to be effective.
- When the status of the admission control switch is changed, it will clear the record data for the current Admission Control. It is recommended that any changes to the status of the switch should be done when there is no CM online.
- When any switch is enabled, the bandwidth threshold parameters for the Admission Control cannot be modified.

Procedure

Step 1 Use **"cable admission-control event dynamic-service"** command to enable the switch for dynamic service flow admission-control event..

Step 2 Use **"show cable admission-control"** to view the status of the switch for dynamic service flow admission-control event.

Example

$ Configuration enables dynamic service flow access switches..

```
BT(config-if-cmts-1)# cable admission-control event dynamic-service enable
Warning:While the switch is turned on it is not allowed to configure admission
control parameters.
BT(config-if-cmts-1)# show running-config verbose | include dynamic-service
 cable admission-control event dynamic-service enable
```

Related Operations

Table 16-2Related Operations for Configure Admission Control Event Switch

Operation	Command	Remarks
Configure the switch for CM registration request admission-control event	**cable admission-control event cm-registration**	

16.4 Configuration the Bandwidth Threshold Parameters for Admission Control

Context

Configure the thresholds for exclusive and non-exclusive bandwidth for each type of service flow. The sum of the total number of the exclusive bandwidth and the maximum non-exclusive bandwidth for each service flow must all be no more than 100.

Procedure

Step 1 Use **"cable admission-control us-bandwidth sched exclusive"** command to configure the thresholds for exclusive and non-exclusive bandwidth for each type of service flow.

Step 2 Use **"show running-config verbose"** to view the bandwidth threshold for the service flow.

Example

Configure the thresholds for exclusive bandwidth of type BE is 10, thresholds for non-exclusive bandwidth is 50.

```
BT(config-if-cmts-1)# cable admission-control us-bandwidth sched be exclusive
10 non-exclusive 50
BT(config-if-cmts-1)# show running-config verbose | include be exclusive
 cable admission-control us-bandwidth sched be exclusive 10 non-exclusive 50
```

Related Operations

N/A

16.5 Configuration the Alarm Threshold for Admission Control

Context

- The admission control function is based on the configured channel bandwidth thresholds for various types of service flows. When the admission control is in operation, and if the bandwidth allocated to the service type is almost saturated, the equipment will generate an alarm. The equipment supports two level of thresholds: minor and major. When the bandwidth utilization of a certain service type on the channel has reached the threshold value, the alarm will be triggered to inform the user so that the user can proceed with further expansion.
- The handling rules for the two thresholds, minor and major, are as follows: the minor alarm will be triggered if the utilization of the exclusive bandwidth is higher than the minor threshold but lower than the major threshold; the major alarm will be triggered directly if the utilization of the exclusive bandwidth exceeds both the minor and major thresholds; if the utilization of the exclusive bandwidth is lower than both the minor and major thresholds, then a recovery alarm corresponding to the number of alarms that have been triggered for threshold breaches will be activated.
- By default, the minor and major alarm thresholds are 0, that is, no alarm will be triggered.

- The threshold configured for minor must be less than that for major.

Procedure

Step 1 Use **"cable admission-control us-bandwidth sched minor major"** command to configure the minor and major alarm thresholds for various types of service flows.

Step 2 Use **"show cable admission-control"** or **"show running running-config"** to view the modified alarm thresholds for the service flow.

Example

Configure the minor threshold for the BE type service flow as 20, and the major threshold as 70.

```
BT(config-if-cmts-1)# cable admission-control us-bandwidth sched be minor 10major 70
BT(config-if-cmts-1)# show running-config | include minorcable
admission-control us-bandwidth sched be minor 10 major 70
BT(config-if-cmts-1)# show cable admission-control
cm-registration dynamic-service HistorySize last-history-index
disable         disable         64          0
sched-type exclusive non-exclusive minor major
be         00        00            10    70
nrtps      00        00            00    00
rtps       00        00            00    00
ugs-ad     00        00            00    00
ugs        00        00            00    00
```

Related Operations

Table 16-3 Related Operations for Configure Admission Control Threshold

Operation	Command	Remarks
Restore the Admission Control alarm threshold to the default value	**no cable admission-control us-bandwidth sched minor major**	

Chapter 17 ACL Configuration Management

17.1 ACL Overview

ACL (Access Control List) can filter specific packets by configuring a series of matching rules, thus identifying the objects to be filtered. After identifying specific objects, corresponding packets will be allowed or refused to pass by the pre-set policy.

- CMTS supports configuring 192 ACL rules.
- CMTS can apply ACL rules in 2 positions: ingress direction of uplink port and ingress direction of cable port.
- In case the multiple ACL rules are applied on the same position, the process for CMTS treatment is shown as figure below.

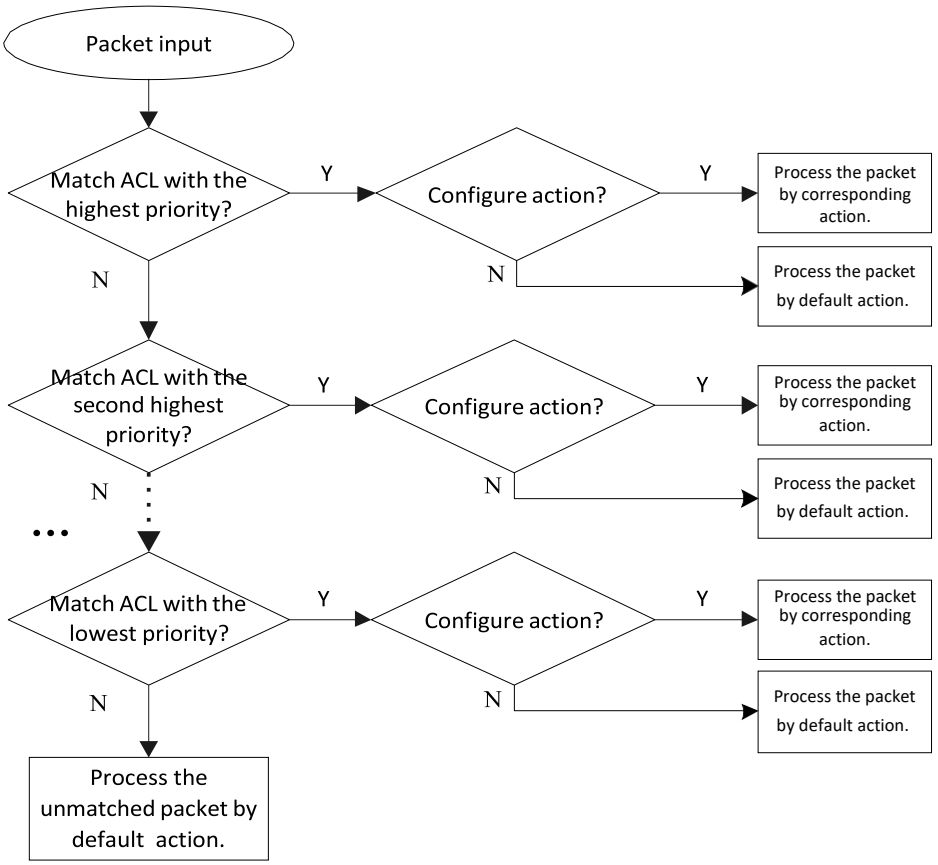

Figure 17-1 Processing in Case of ACL Rule

After the processing of packets starts, the matching will be conducted by ACL rule priority. If some an ACL rule is matched, the packet will be processed according to the ACL rule; if the packet fails to match any ACL rule, the packet will be processed according to the default action.

17.2 Example of Basic ACL

Discard the packets meeting the source IP address condition in the ingress direction of uplink port and cable port through this task.

Data Planning

The data planning for basic ACL configurations is shown as follows.

Table 17-1 Data Planning for Basic ACL Configurations

Item	Data
ACL number	1
Source IP address	1.1.1.1/32
Port	Apply ACL 1 rule on the uplink port and cable port in ingress direction

Prerequisite

The network CMTS and lines are normal.

Configuration flowchart

The process for basic ACL configuration is shown as follows.

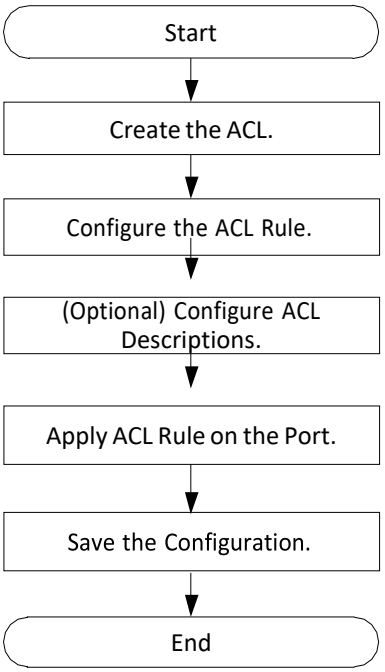

Figure 17-2 Flowchart for Basic ACL Configuration

Procedure

Step 1 Create the ACL.

```
BT(config)# acl 1
```

Step 2 Configure the ACL subrule.

1. Configure the matching conditions.

```
BT(config-acl-1)# match src-ip 1.1.1.1 255.255.255.255
```

2. Configure the action.

```
BT(config-acl-1)# action deny
```

3. (Optional) Configure the priority. By default, the ACL rule priority is 5. The larger value, the higher priority.

```
BT(config-acl-1)# priority 4
```

Step 3 (Optional) Configure the ACL descriptions.

```
BT(config-acl-1)# description acl-deny-1.1.1.1/32
```

Step 4 Configure applying ACL rule at the port.

1. Apply the rule in ingress direction of uplink port.

```
BT(config-acl-1)# acl install uplink ingress
```

2. Apply the rule in ingress direction of cable port.

```
BT(config-acl-1)# acl install cable ingress
```

Step 5 Save the configurations.

```
BT(config-acl-1)# exit
BT(config)# exit
BT# copy running-config startup-config
This will save the configuration to the flash memory.
Are you sure?(y/n) [n]y
Building configuration.....
Configuration saved successfully.
```

Result

According to the ACL rules, the uplink port and the cable port of CMTS will discard the packets from 1.1.1.1/32 in ingress direction.

17.3 Example of the ACL Service VLAN Service

Through this task, add VLAN 20 to the packet with VLAN tag as 10 in case it is upstream, but remove VLAN tag from the packet with VLAN tag as 20 when it is downstream.

Data Planning

The data planning for VLAN services is shown as follows.

Table 17-2 Data Planning for VLAN Service

Item	Data
ACL number	1 and 2
VLAN tag	VLAN 10 and VLAN 20
Port	Apply ACL 1 rule on the uplink port in ingress direction; apply ACL 2 rule on the cable

Item	Data
	port in ingress direction.

Prerequisite

The network CMTS and lines are normal.

Configuration flowchart

The process for configuring VLAN services is shown as follows.

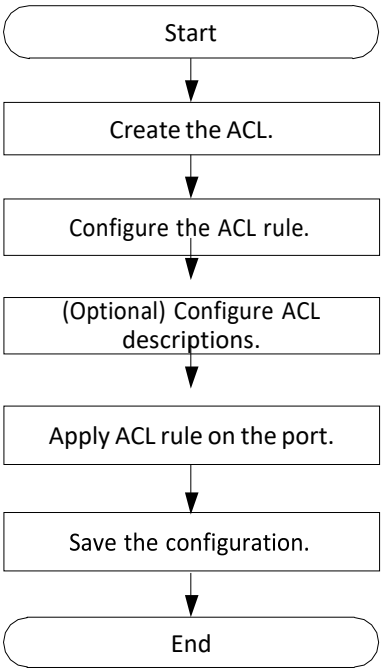

Figure 17-3 Flowchart for Configuring VLAN Service

Procedure

- ACL 1 configuration:

Step 1 Create the ACL 1.

```
BT(config)# acl 1
```

Step 2 Configure the ACL rule.

1. Configure the matching VLAN ID as 10 `BT(config-acl-1)# match vlan 10`Configure the action as
2. add VLAN ID 20.

   ```
   BT(config-acl-1)# action add-vlan 20
   ```
3. Configure the action as permit.

   ```
   BT(config-acl-1)# action permit
   ```
4. Configure the priority as 6.

   ```
   BT(config-acl-1)# priority 6
   ```

Step 3 Configure the ACL descriptions.

```
BT(config-acl-1)# description acl-add-vlan-20
```

Step 4 Configure the applying ACL rule at the cable port ingress.

```
BT(config-acl-1)# acl install cable ingress
```

- ACL 2 configuration:

Step 1 Create the ACL 2.

```
BT(config-acl-1)# exit
BT(config)# acl 2
```

Step 2 Configure the ACL rule.

1. Configure the matching VLAN ID as 20 `BT(config-acl-2)# match vlan 20`Configure the action as
2. remove VLAN.

   ```
   BT(config-acl-2)# action remove-vlan
   ```
3. Configure the action as permit.

   ```
   BT(config-acl-2)# action permit
   ```
4. Configure the priority as 6.

   ```
   BT(config-acl-2)# priority 6
   ```

Step 3 Configure the ACL descriptions.

```
BT(config-acl-2)# description acl-remove-vlan
```

Step 4 Configure the applying ACL rule at the uplink port ingress.

```
BT(config-acl-2)# acl install uplink ingress
```

Step 5 Save the configurations.

```
BT(config-acl-2)# end
BT# copy running-config startup-config
This will save the configuration to the flash memory.
Are you sure?(y/n) [n]y
Building configuration.....
Configuration saved successfully.
```

Result

According to the ACL rules, when CMTS sends upstream the packet with VLAN tag as 10, it will add VLAN20 to the packet, but remove VLAN tag from the packet with VLAN tag as 20 when sending the packet downstream.

17.4 Create the ACL

Users can create the ACL through this task.

Context

CMTS supports creating 60 ACLs.

Procedure

Step 1 Create the ACL rule by using the command "**acl**".

Step 2 Query the created ACL rule by using the command "**show acl**".

Example

$Create an ACL rule.

```
BT(config)# acl 1
BT(config-acl-1)# show acl
+----ACL: 1, prio: 5, desc: acl-1
|   +----Rule :
|   |   + ---Action:
|   |   |   + ---Permit
|   |   +----Match: none
```

Related Operations

Table 17-3 Related Operations for Creating ACL

Operation	Command	Remarks
Delete the ACL rule	**no acl (all |** *acl-id*)	

17.5 Configure the ACL Subrule Matching Conditions

Users can configure the ACL subrule matching conditions through this task.

Context

- When configuring the ACL, it requires specifying the matching condition. Only when the packet meets the matching condition, the action specified by ACL can start.
- ACL can be configured multiple matching conditions, which are of logical "and" relationship. Currently CMTS supports the matching conditions such as: the source and destination MAC address, the source and destination IP(suppot IPv4 and IPv6), the source and destination port, VLAN ID, DSCP, ether type, IP protocol field of the packet, IPV6-Next-Header and IPV6-Flow-Lable.

Procedure

Step 1 Configure the ACL subrule matching conditions by using the command "**match**".

Step 2 Query the configured ACL subrule matching conditions by using the command "**show acl**".

Example

Configure the matching condition of ACL1 as packet with source address 1.1.1.1/24.

```
BT(config-acl-1)# match src-ip 1.1.1.1 255.255.255.0
BT(config-acl-1)# show acl
+----ACL: 1, prio: 5, desc: acl-1
|   +----Rule :
|   |   + ---Action:
|   |   |   + ---Permit
|   |   + ---Match:
|   |       +----Source IPV4 address 1.1.1.1 255.255.255.0
```

Related Operations

Table 17-4 Related Operations for Configuring the Matching Conditions of ACL Subrule

Operation	Command	Remarks
Delete the configurations of ACL subrule matching condition	**no match**	

17.6 Configure the ACL Subrule Action

Users can configure the ACL subrule actions through this task.

Context

ACL action refers to the treatment with the packets meeting the matching conditions.

Currently CMTS supports the following actions: discarding the packet, allowing the packet to pass, adding VLAN tag to the packet, deleting VLAN tag of the packet, and modifying VLAN priority and TPID and DSCP of the packet.

Procedure

Step 1 Configure the ACL subrule action by using the command "**action**".

Step 2 Query the ACL subrule action by using the command "**show acl**".

Example

Configure the action in ACL 1 rule as permit.

```
BT(config-acl-1)# action permit
BT(config-acl-1)# show acl
+----ACL: 1, prio: 5, desc: acl-1
|   +----Rule :
|   |   + ---Action:
|   |   |   + ---Permit
|   |   + ---Match:
|   |       +----Source IPV4 address 172.10.10.10 255.255.255.255
```

Related Operations

Table 17-5 Related Operations for Configuring the Actions of ACL Subrule

Operation	Command	Remarks
Delete the configurations of ACL subrule action	**no action**	

17.7 Configure the ACL Rule Priority

Users can configure the ACL rule priority through this task.

Context

ACL rule priority determines the sequence for matching the ACL rule at the same position. The larger configured value, the higher priority. By default, the ACL rule priority is 5.

Procedure

Step 1 Configure the ACL rule priority by using the command "**priority**".

Step 2 Query the ACL rule priority by using the command "**show acl**".

Example

Configure the priority of ACL 1 rule as 4.

```
BT(config-acl-1)# priority 4
BT(config-acl-1)# show acl
+----ACL: 1, prio: 4, desc: acl-1
|   +----Rule :
|   |   + ---Action:
|   |   |   + ---Permit
|   |   + ---Match:
|   |       +----Source IPV4 address 1.1.1.1 255.255.255.0
```

Related Operations

Table 17-6 Related Operations for Configuring the ACL Rule Priority

Operation	Command	Remarks
Restore the default ACL rule priority	**no priority**	

17.8 Configure the Descriptions of ACL Rule

Users can configure the ACL rule descriptions through this task.

Context

By configuring the ACL rule descriptions, the purpose of the ACL can be indicated, thus avoiding confusion with other ACLs.

Procedure

Step 1 Configure the ACL rule descriptions by using the command "**description**".

Step 2 Query the descriptions of the bound ACL rule by using the command "**show acl**".

Example

Configure the descriptions of ACL 1.

```
BT(config-acl-1)# description acl-permit-1.1.1.1/24
BT(config)# show acl 1
+----ACL: 1, prio: 5, desc: acl-permit-1.1.1.1/24
|   +----Rule :
|   |   + ---Action:
|   |   |   + ---Permit
|   |   +----Match: none
```

Related Operations

Table 17-7 Related Operations for Configuring the Decriptions of ACL Rule

Operation	Command	Remarks
Delete the configured descriptions of ACL rule	**no description**	

17.9 Configure Applying the ACL Rule at the Port

Users can configure applying the ACL rules at the port through this task.

Context

- CMTS can apply the ACL rules in ingress direction of the uplink port and in ingress direction of the cable port.
- Users can apply the ACL rules in different positions to restrict specific packets. The same ACL rule can be applied in different positions simultaneously.

Procedure

Step 1 Configure binding the ACL rule to a port by using the command "**acl install**".

Step 2 Query the information of the port applying the ACL rule by using the command "**show acl**".

Example

Configure binding ACL 1 to the uplink port in ingress direction.

```
BT(config-acl-1)# acl install uplink ingress
BT(config-acl-1)# exit
BT(config)# show acl 1
+----ACL: 1, prio: 4, desc: acl-1, installed
|   +----Installed on port
|   |   + ---Uplink/Ingress
|   +----Rule :
|   |   + ---Action:
|   |   |   + ---Permit
|   |   + ---Match:
|   |       +----Source IPV4 address 1.1.1.1 255.255.255.0
BT(config)# show acl 1 install
AclId      Cmts              Port              Direction
1          1                 Uplink            ingress
```

Related Operations

Table 17-8 Related Operations for Configuring the ACL Rule Application on the Port

Operation	Command	Remarks
Delete the configurations of applying the ACL rule at the port	**no acl install**	
Display all installed of the specified ACL.	**show acl** *acl-id* **install**	
Display all installed of all the ACL.	**show acl install all**	
Display the statistics of the specified ACL	**show acl** *acl-id* **[interface** *cmts-id***] statistics**	

Chapter 18 Network Security Configuration Management

18.1 Configuration Management of Whitelist/Blacklist Accessing CMTS

18.1.1 Overview of Whitelist/Blacklist Accessing CMTS

To guarantee the security of CMTS, the principle of minimum authorization must be followed, that is to specify a part of IP addresses to be added to the whitelist, and only IP addresses in the whitelist is allowed to access CMTS. Meanwhile users are also allowed to specify some IP addresses to be added to the blacklist to refuse IP addresses in the blacklist to access CMTS.

- Operating instructions:
  - When an IP address is added to the blacklist and the whitelist simultaneously, the blacklist may enjoy the higher priority, that is, such IP address is refused to access CMTS.
  - After configuring the whitelist/blacklist for access to CMTS, only if the IP firewall function is enabled, can the whitelist/blacklist take effect.
  - When the whitelist is empty, CMTS will disable the IP firewall function automatically.

18.1.2 Configure the Example of Whitelist/Blacklist Accessing CMTS

Allow and refuse the specified IP address to access CMTS through this task.

Networking Diagram

As shown in follows, users need all network devices in network segment 1.1.1.0/24 except 1.1.1.10/32 to access CMTS.

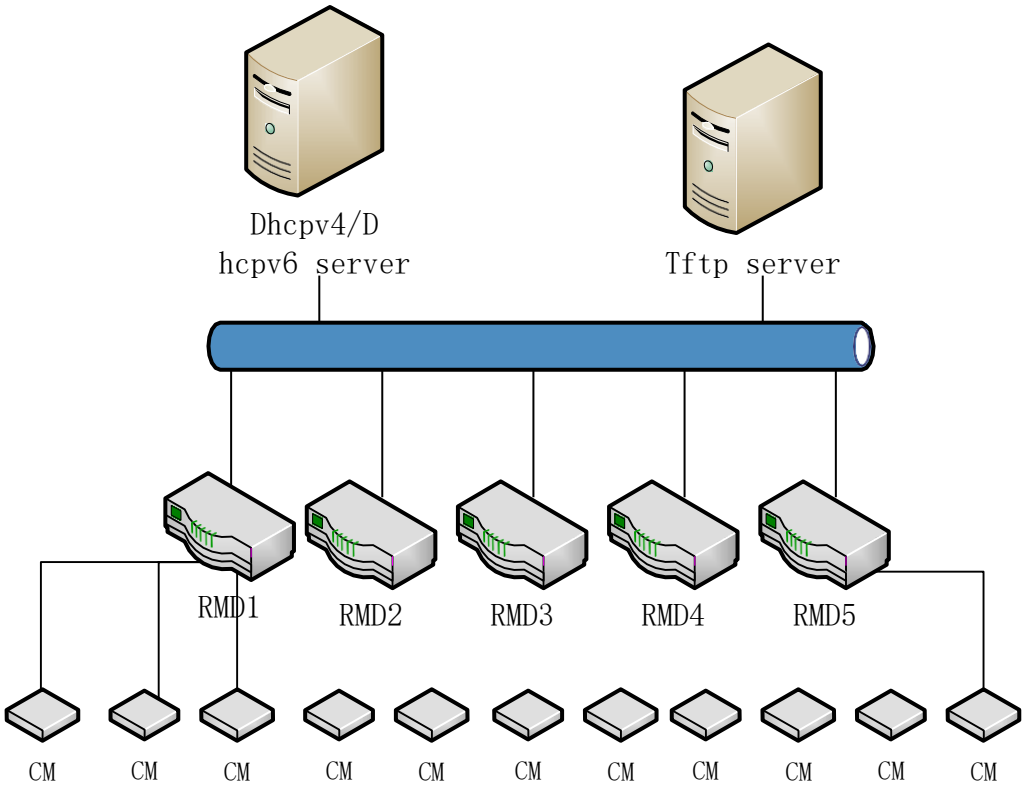

Figure 18-1 Networking Diagram for Configuring the Example of CMTS Whitelist/Blacklist

Data Planning

The data planning for access to the configurations of CMTS whitelis/blacklist.

Table 18-1 Data Planning of Whitelis/Blacklist configuration

Item	Data
Whitelist	1.1.1.0/24
Blacklist	1.1.1.10/32

Prerequisite

The network CMTS and lines are normal.

Configuration flowchart

The process for configuring the access to CMTS whitelist/blacklist is shown as follows.

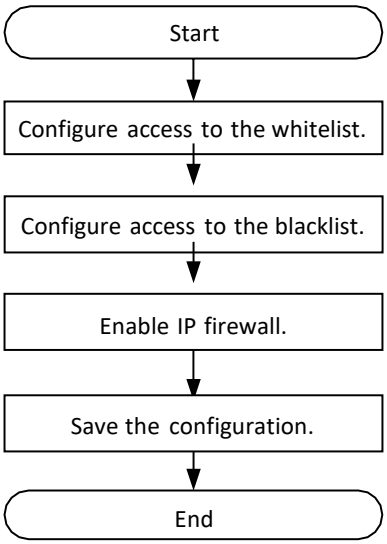

Figure 18-2 Flowchart for Configuring the Access to CMTS Blacklist/Whitelist

Procedure

Step 1 Configure the whitelist.

```
BT(config)# line vty
BT(config-line)# access-permit ssh 1.1.1.0 255.255.255.0
```

Step 2 Configure the blacklist.

```
BT(config-line)# access-deny ssh 1.1.1.10 255.255.255.255
```

Step 3 Enable the IP firewall.

```
BT(config-line)# ip-firewall ssh enable
```

Step 4 Save the configurations.

```
BT(config-line)# exit
BT(config)# exit
BT# copy running-config startup-config
This will save the configuration to the flash memory.
Are you sure?(y/n) [n]y
Building configuration.....
Configuration saved successfully.
```

Result

According to the above configured blacklist/whitelist, all IP addresses in the network segment 1.1.1.0/24 except 1.1.1.10/32 can access CMTS.

18.1.3 Configure the Whitelist Accessing CMTS

Configure the whitelist accessing CMTS through this task.

Context

When an IP address is added to the whitelist and the blacklist simultaneously, the blacklist enjoys the higher priority, that is to refuse the IP address to access CMTS.

After configuring the whitelist accessing CMTS, only if the IP firewall function is enabled, can the whitelist take effect.

Procedure

Step 1 Enter the line view by using the command "**line vty**".

Step 2 Configure the whitelist accessing CMTS by using the command "**access-permit (telnet | ssh | web | snmp)** *ip-address* [*netmask*]".

Step 3 View the information of whitelist by using the command "**show firewall-list**".

Example

IP addresses in the network segment 1.1.1.0/24 are allowed to access CMTS by SSH mode.

```
BT(config)# line vty
BT(config-line)# access-permit ssh 1.1.1.0 255.255.255.0
BT(config-line)# show firewall-list
 ACCESS        MODE      IPADDRESS/MASKBITS
 ---------------------------------------------------------------
 permit        ssh       1.1.1.0/24
 ---------------------------------------------------------------
 ip-firewall   telnet    disable
 ip-firewall   ssh        disable
 ip-firewall   snmp      disable
 ip-firewall   web       disable
```

Related Operations

Table 18-2 Related Operations for Configuring the Access to CMTS Whitelist

Operation	Command	Remarks
Delete the specified IP address in the whitelist	**no access-permit**	

18.1.4 Configure the Blacklist Accessing CMTS

Users can configure the blacklist accessing CMTS through this task.

Context

When an IP address is added to the whitelist and the blacklist simultaneously, the blacklist enjoys the higher priority, that is to refuse the IP address to access CMTS.

After configuring the blacklist accessing CMTS, only if the IP firewall function is enabled, can the blacklist take effect.

Procedure

Step 1 Enter the line view by using the command "**line vty**".

Step 2 Configure the blacklist accessing CMTS by using the command "**access-deny (telnet | ssh | web | snmp)** *ip-address* [*netmask*]".

Step 3 View the information of the blacklist by using the command "**show firewall-list**".

Example

IP addresses in the network segment 2.2.2.0/24 are refused to access CMTS by SSH mode.

```
BT(config)# line vty
BT(config-line)# access-deny ssh 2.2.2.0 255.255.255.0
BT(config-line)# show firewall-list
 ACCESS         MODE     IPADDRESS/MASKBITS
 ---------------------------------------------------------------
 deny           ssh      2.2.2.0/24
 ---------------------------------------------------------------
 ip-firewall   telnet    disable
 ip-firewall   ssh       disable
 ip-firewall   snmp      disable
 ip-firewall   web       disable
```

Related Operations

Table 18-3 Related Operations for Configuring the Access to CMTS Blacklist

Operation	Command	Remarks
Delete the specified IP address in the blacklist	**no access-deny**	

18.1.5 Enable the IP Firewall Function

Users can enable the IP firewall function through this task.

Context

After configuring the whitelist/blacklist accessing CMTS, only if the IP firewall function is enabled, can the whitelist/blacklist take effect.

When the whitelist is empty, CMTS will disable the IP firewall function automatically.

Procedure

Step 1 Enter the line view by using the command "**line vty**".

Step 2 Enable the IP firewall function by using the command "**ip-firewall (telnet | ssh | snmp | web) enable**".

Step 3 View current state of IP firewall function by using the command "**show firewall-list**".

Example

Enable the IP firewall function.

```
BT(config)# line vty
BT(config-line)# access-permit ssh 1.1.1.0 255.255.255.0
BT(config-line)# ip-firewall ssh enable BT(config-line)# show
firewall-list
 ACCESS          MODE     IPADDRESS/MASKBITS
 ----------------------------------------------------------------
 permit          ssh       1.1.1.0/24
 ----------------------------------------------------------------
 ip-firewall    telnet    disable
 ip-firewall    ssh       enable
 ip-firewall    snmp      disable
 ip-firewall    web       disable
```

Related Operations

Table 18-4 Related Operations for Enabling IP Firewall Function

Operation	Command	Remarks
Disable the IP firewall function	**ip-firewall (telnet | ssh | snmp | web) disable**	

18.1.6 Clear the Whitelist/Blacklist

Users can clear the whitelist/blacklist through this task.

Context

After clearing the whitelist, the IP firewall function will be disabled automatically.

Procedure

Step 1 Enter the line view by using the command "**line vty**".

Step 2 Clear the black and white list by using the command "**clear firewall-list**".

Step 3 View the information of blacklist by using the command "**show firewall-list**".

Example

Clear the whitelist/blacklist of CMTS.

```
BT(config)# line vty BT(config-line)# clear
firewall-listThe firewall-list has been
cleared.
BT(config-line)# show firewall-list
 ACCESS        MODE     IPADDRESS/MASKBITS
 ------------------------------------------------------------
 ------------------------------------------------------------
 ip-firewall     telnet     disable
 ip-firewall     ssh        disable
 ip-firewall     snmp       disable
 ip-firewall     web        disable
```

Related Operations

N/A

18.2 SAV Configuration Management

18.2.1 SAV Configuration Overview

SAV (Source Address Verification) function means that CMTS conducts the security check against the source IP address of CPE under CM. Configure SAV function to prevent DOCSIS network from malicious attacks by any unauthorized users.

Main configurations of SAV function are shown as follows:

- Configure security check against CPE under all CMs.
- Configure security check against CPE under online CM for bundle.
- Configure security check against CPE in the specified network segment.
- Cancel security check against CPE with specified IP address under the specified CM.

Besides, CMTS also support SAV Exception List function, which is globally based on CMTS MAC domain rather than CM MAC, if IP address of the CPE is in SAV Exception List, there will be no SAV check for this CPE.

Main configurations of SAV Exception List function are shown as follows:

- Configure network segment to SAV Exception List, no SAV check against CPE with IP address in SAV Exception List.

18.2.2 Example of Security Check against CPE with the Specified IP Address

Achieve the security check against CPE with the specified IP address through this task.

Data Planning

The data planning for configuring the security check against CPE with the specified IP address is shown as follows.

Table 18-5 Data Planning for Configuring the Security Check against CPE with the Specified IP Address

Item	Data
SAV group	1
IP network segment for security check	1.1.1.0/24

Prerequisite

The network CMTS and lines are normal.

Configuration flowchart

The process for configuring the security check against CPE with the specified IP address is shown as follows.

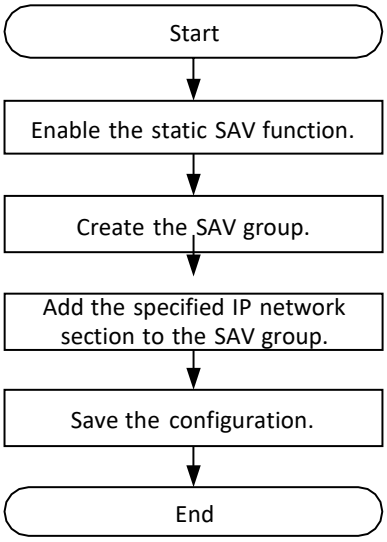

Figure 18-3 Flowchart for Configuring the Security Check against CPE with the Specified IP Address

Procedure

Step 1 Enable the static SAV function.

```
BT(config)# cable source verify enable-sav-static
```

Step 2 Create the SAV group.

```
BT(config)# cable source verify group 1
```

Step 3 Add IP address for the SAV group.

```
BT(config-sav)# prefix 1.1.1.0 24
```

Step 4 Save the configurations.

```
BT(config-sav)# exit
BT(config)# exit
BT# copy running-config startup-config
This will save the configuration to the flash memory.
Are you sure?(y/n) [n]y
```

```
Building configuration.....
Configuration saved successfully.
```

Result

According to the above configurations, The security check conduct of CMTS against CPE is allowing 1.1.1.0/24 subnet IP address to access the network

18.2.3 Configure Security Check against CPE under the CMs

Users can configure security check against CPE under the CMs through this task. After the success of SAV function configuration, only the CPE which get IP address by DHCP dynamic can network connectivity.

Context

To configure security check against CPE under the CMs: global security check (configure in config view) and bundle security check(configure in bundle view).

Global security check: To configure security check against CPE under online CM not for the any bundle, it only needs to enable the global security check in the config view.

Bundle security check: To configure security check against CPE under online CM for the specified bundle, it needs to enable the global SAV function in the config view and the bundle security check in the bundle view.

Procedure

Step 1 Enter the config view by using the command "**`configure terminal`**".

Step 2 Enable the global SAV function by using the command "**`cable source verify enable`**".

By default, CMTS disable the global SAV function.

Step 3 Enter the specified bundle view by using the command "**`interface bundle`**".

Step 4 Enable the SAV function by using the command "**`cable source verify enable`**".

By default, the SAV function is enabled in the bundle view.

(It needs to only configure the step 1-2 if to configure security check against CPE under online CM not for the any bundle)

Example

Configure CMTS to conduct the security check against CPE under online CM for bundle 1.

```
BT# configure terminal BT(config)# cable
source verify enableBT(config)# interface
bundle 1
BT(config-if-bundle1)# cable source verify enable
```

Related Operations

Table 18-6 Related Operations for Configuring the Security Check against CPE under the CMs

Operation	Command	Remarks
Disable the SAV function	**cable source verify disable**	

18.2.4 Cancel the Security Check against CPE with the Specified IP Address under the Specified CM

Users can cancel the security check against CPE with the specified IP address under the specified CM through this task.

Context

For CPE with higher security, users can configure to cancel the security check against its IP address.

Procedure

Step 1 Cancel the security check against CPE with the specified IP address under the specified CM by using the command "**cable modem** *mac-address* **static ip** *ip-address*".

Step 2 View the configuration information of cancelling the security check by using the command "**show cpe static ip**".

Example

Cancel the security check against CPE with IP address 1.1.1.1 under the CM with MAC address 0024.6800.0001.

```
BT(config)# cable modem 0024.6800.0001 static ip 1.1.1.1
BT(config)# show cpe static ip
CMC Index       CM MAC                  CPE IP
 C1             0024.6800.0001          1.1.1.1
```

Related Operations

Table 18-7 Related Operations for Configuring the Security Check against CPE in the Specified Network Segment

Operation	Command	Remarks
Cancel the configuration of security check against the specified IP	**no cable modem static ip**	

18.2.5 Configure network segment to SAV Exception List

Users can configure global network segment in SAV Exception List, no SAV check against CPE with the IP address in SAV Exception List.

Context

For CPE with higher security, users can configure to cancel the SAV check against its IP address which can ensure more flexible use of SAV function..

Procedure

Step 1 Enter the cmts view by using the command "**interface cmts 1**".

Step 2 Configure IPv4 or IPv6 network segment in SAV Exception List by using the command "**cable source verify exception ip-address netmask**".

Step 3 View the configuration information of SAV Exception list by using the command "**show cable source verify exception config**".

Example

Configure the network segment 192.168.10.1/24 in SAV Exception list globally on CMTS.

```
BT(config)# interface cmts 1
BT (config-if-cmts-1)# cable source verify exception ip 192.168.10.1
255.255.255.0
BT (config-if-cmts-1)# show cable source verify exception config
IP_Address                              IP_Mask
192.168.10.1                            255.255.255.0
BT (config-if-cmts-1)# exit
```

Related Operations

Table 18-8 Related Operations for Configuring the Network Segment in SAV Exception list

Operation	Command	Remarks
Configure SAV Exception network segment	**cable source verify exception ip** *ip-address netmask* **cable source verify exception ipv6** *ipv6-address/prefix*	
Delete the network segment from SAV Exception configuration	**no cable source verify exception ip** *ip-address* **no cable source verify exception ipv6** *ipv6-address*	

18.2.6 Cancel the security check against CPE under CM with L2VPN

Users can cancel the security check against CPE under the specified CM with L2VPN through this task.

Context

In some case, it's necessary to disable the SAV function for CPEs under CM with L2VPN configuration, users can configure to cancel the security check against the CPE IP address; when the SAV is needed, it can be

configured to enable again. By default, L2VPN SAV is enabled. Note that it's necessary to configured respectively under IPv4 or IPv6 network.

Procedure

Step 1 Cancle the anti static ip function for CMs with L2VPN by using the command "**cable vpn [ipv6] source verify disable**".

Step 2 View the configuration information of cancelling the security check by using the command "**show running-config**".

Example

Cancel the anti static ip function for CMs with L2VPN.

```
BT(config)# cable vpn source verify disable BT(config)#
cable vpn ipv6 source verify disableBT(config)# show
running-config | include verifycable vpn source verify
disable
cable vpn ipv6 source verify disable
```

Related Operations

Table 18-9 Related Operations for Configuring the Security Check against CPE under CM with L2VPN

Operation	Command	Remarks
Enable the anti static ip function for CMs with L2VPN	**cable vpn [ipv6] source verify enable**	

18.3 IPv6 Routing Filtering

In IPv6 environment, CMTS needs to find a legitimate router to route and forward its message through route discovery. Router Advertisement Guard (RA Guard) function is mainly to filter out some illegal route response messages, to ensure that CMTS can find a legitimate designated router for data forwarding without interference.

18.3.1 Example of Configure IPv6 Routing Filtering

Data Planning

The data plan for configuring IPv6 routing filtering instance is shown in the following table.

Table 18-10 Data Planning for Configure IPv6 Routing Filtering Instance

Item	Data
RA Guard function.	Enable
Cur Hop Limit permissible range in router announcement.	64-128

Router Bulletin'M'Logo Check.	Enable

Item	Data
Router Bulletin'O'Flag Check.	Enable
Ra-guard network prefix list.	Add record 2001:1009:1009::12/96 as permissible
Ra-guard routing address list.	Add record fe80::82f6:2eff:fe11:af23 as permissible

Prerequisite

- Network equipment and lines are normal.

Configuration flowchart

Configure the IPv6 routing filtering process as shown in the following figure.

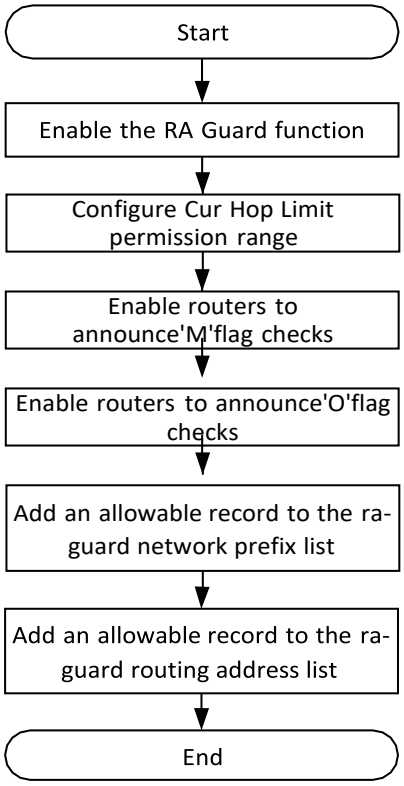

Figure 18-4 Flowchart forConfigure IPv6 Routing Filtering

Procedure

Step 1 Enable the RA Guard function:

```
BT(config)# ipv6 ra-guard enable
```

Step 2 Configuration Cur Hop Limit allows 64-128:

```
BT(config)# ipv6 ra-guard hop-limit 64 128
```

Step 3 Enable the router bulletin'M'flag check:

```
BT(config)# ipv6 ra-guard managed-config-check enable
```

Step 4 Enable the router bulletin'O'flag check:

```
BT(config)# ipv6 ra-guard other-config-check enable
```

Step 5 Add an allowable record to the ra-guard network prefix list:

```
BT(config)# ipv6 ra-guard prefix-list 2001:1009:1009::12/96permit
```

Step 6 Add an allowable record to the ra-guard routing address list:

```
BT(config)# ipv6 ra-guard router-list
fe80::82f6:2eff:fe11:af23 permit
```

Step 7 Save the configuration:

```
BT(config)# end
BT# copy running-config startup-config
This will save the configuration to the flash memory.
Are you sure?(y/n) [n]y
Building configuration.....
Configuration saved successfully.
```

Result

After the configuration is completed, RA Guard analyses the RA messages entering the device and allows the authenticated RA messages to pass and discard illegal RA messages according to the configuration filtering rules.

18.3.2 Enable IPv6 Router Filter Function

Context

- Open the filter function of the device for illegal RA messages. After opening, the device reads the configuration of the filter rules and sets the rules to the corresponding position.
- If this item is not configured, the function is turned off by default.
- The RA Guard switch controls whether IPv6 routing filtering function is turned on or not, but does not restrict the configuration of other filtering conditions. The configuration of filtering conditions under the closed state of the RA Guard will not take effect. The RA Guard switch will read these configurations and set rules to the device to make them effective.

Procedure

Step 1 Uses the "**ipv6 ra-guard enable**" command to turn on the device's filtering function for illegal RA messages.

Step 2 Uses the "**show ipv6 ra-guard config**" command to view the configuration status of the RA Guard switch.

Example

Enable IPv6 router filtering function:

```
BT(config)# ipv6 ra-guard enable
It will take a while to set all rules, use "show ipv6 ra-guard config" command to
check configure status!
BT(config)# show ipv6 ra-guard config
 RA Guard Switch Config Finished. Rules Setting Success.
 ipv6 ra-guard enable
 no ipv6 ra-guard hop-limit
 ipv6 ra-guard managed-config-check disable
 ipv6 ra-guard other-config-check disable
```

Related Operations

Table 18-11 Related Operations of IPv6 routing filter function switch

Operation	Command	Remarks
Disable IPv6 RA Guard function	**ipv6 ra-guard disable**	

18.3.3 Configure Cur Hop Limit Permission Range

Context

- Configuring the range of Cur Hop Limit values in router announcements allowed by devices, RA Guard discards RA messages with illegal Cur Hop Limit values.
- If this item is not configured, it is not checked by default.
- This configuration takes effect when RA Guard is turned on.

Procedure

Step 1 Uses the "**ipv6 ra-guard hop-limit** *limit-min limit-max*" command to configure the range of Cur Hop Limit values allowed by the device.

Step 2 Uses the ""**show ipv6 ra-guard config**" command to view the Cur Hop Limit allowable range configuration values.

Example

Configure the Cur Hop Limit value allowable range:

```
BT(config)# ipv6 ra-guard hop-limit 64 128
BT(config)# show ipv6 ra-guard config
 RA Guard Switch Config Finished. Rules Setting Success.
 ipv6 ra-guard disable
 ipv6 ra-guard hop-limit 64 128
 ipv6 ra-guard managed-config-check disable
 ipv6 ra-guard other-config-check disable
```

Related Operations

Table 18-12 Related Operations of Configure Cur Hop Limit Permission Range

Operation	Command	Remarks
Cancel Cur Hop Limit check.	**no ipv6 ra-guard hop-limit**	After closing, the inspection skips and proceeds directly to the next inspection

18.3.4 Configure to Check the'M'flag in Router Bulletins

Context

- RA Guard supports the inspection of the "Managed address configuration" flag ('M'flag) in RA messages. When this function is turned on, the device discards the RA message marked'M'as 1.
- If this item is not configured, the function is turned off by default.
- This configuration takes effect when RA Guard is turned on.

Procedure

Step 1 Uses the "**ipv6 ra-guard managed-config-check enable**" command to turn on the device to check the'M'identity in the RA message.

Step 2 Uses the "**show ipv6 ra-guard config**" command to view the device's'M'identity to check configuration status.

Example

Enable equipment's'M'identification checking function:

```
BT(config)# ipv6 ra-guard managed-config-check enable
BT(config)# show ipv6 ra-guard config
  RA Guard Switch Config Finished. Rules Setting Success.
    ipv6 ra-guard enable
    no ipv6 ra-guard hop-limit
    ipv6 ra-guard managed-config-check enable
    ipv6 ra-guard other-config-check disable
```

Related Operations

Table 18-13 Related Operations ofConfigure the'M'identification checking function of the equipment

Operation	Command	Remarks
Disable the'M'identification checking function of the device.	**ipv6 ra-guard managed-config-check disable**	

18.3.5 Configure to Check the 'O' Flag in Router Bulletins

Context

- RA Guard supports the detection of "Other configuration" flag ('O'flag) in RA messages. When this function is turned on, the device will discard the RA message marked'O'as 1.
- If this item is not configured, the function is turned off by default.
- This configuration takes effect when RA Guard is turned on.

Procedure

Step 1 Uses the "**ipv6 ra-guard other-config-check enable**" command to configure the device to check the'O'identity in the RA message.

Step 2 Uses the "**show ipv6 ra-guard config**" command to view the device's'O'identity to check configuration status.

Example

Open the device's'O'logo checking function:

```
BT(config)# ipv6 ra-guard other-config-check enable
BT(config)# show ipv6 ra-guard config
 RA Guard Switch Config Finished. Rules Setting Success.
 ipv6 ra-guard enable
 no ipv6 ra-guard hop-limit
 ipv6 ra-guard managed-config-check enable
 ipv6 ra-guard other-config-check enable
```

Related Operations

Table 18-14 Related Operations of Configure the 'O' Identification Checking Function of the Device

Operation	Command	Remarks
Disable the 'O' mark checking function of the device	**ipv6 ra-guard other-config-check disable**	

18.3.6 Add a List of RA Guard Network Prefixes

Context

- Network prefix list configuration includes adding and deleting operations, corresponding to each record, it can be configured as permit or deny two control states. RA Guard matches the RA message with the network prefix and performs two actions to pass or discard it.
- The record priority of deny state in the network prefix list is higher than that of permit state. It will be

used for filtering check first. If the RA message hits the deny record, it will be discarded directly. The record of permit state will be executed after all the deny records are executed, and if the RA message hits, the message will be allowed to pass.

- This configuration takes effect when RA Guard is turned on.

Procedure

Step 1 Uses the "**ipv6 ra-guard prefix-list** *ipv6-address/prefix* **(permit|deny)**" command to configure the device ra-guard network prefix list record.

Step 2 Uses the "**show running-config**" command to view the list of configured ra-guard network prefixes for the device.

Example

Add a record 2001:1009:1009::12/96 to the prefix list of ra-guard network and configure it as permit state:

```
BT(config)# ipv6 ra-guard prefix-list 2001:1009:1009::12/96 permit
BT(config)# show running-config | include prefix-list
 ipv6 ra-guard prefix-list 2001:1009:1009::12/96 permit
```

Related Operations

Table 18-15 Related Operations of Add a List of Network Prefixes.

Operation	Command	Remarks
Delete the list of network prefixes	**no ipv6 ra-guard prefix-list**	

18.3.7 Add a List of RA Guard Routing Addresses

Context

- The routing address list configuration includes adding and deleting operations, corresponding to each record, which can be configured as permit or deny control states. After the RA Guard matches the RAGuard message of the routing address, it performs two actions to make it pass or discard.
- The priority relationship between deny state and permit state records in the routing address list is the same as that in the network prefix list. It should be noted that the execution of deny state record prior to permit state record means that the deny record of network prefix list and routing address list will be unified before the permit record of both is executed.
- The routing address parameter requires the link local address of the router itself.
- This configuration takes effect when RA Guard is turned on.

Procedure

Step 1 Uses the "**ipv6 ra-guard router-list** *ipv6-address* **(permit|deny)**"command to configure the ra-guard routing address list record of the device.

Step 2 Use the "**show running-config**" command to view the list of ra-guard routing addresses that the device has configured.

Example

Add a record fe80::82f6:2eff:fe11:af23 to the ra-guard routing address list and configure it in permitstate:

```
BT(config)# ipv6 ra-guard router-list fe80::82f6:2eff:fe11:af23 permit
BT(config)# show running-config | include router-list
 ipv6 ra-guard router-list fe80::82f6:2eff:fe11:af23 permit
```

Related Operations

Table 18-16 Related Operations of Add a List of Routing Addresses

Operation	Command	Remarks
Delete the routing address list	**no ipv6 ra-guard router-list**	

18.4 Certificate Management

CMTS devices support a three-tier certificate structure:

CM certificate, MFG certificate (ARRIS/Thomson), ROOT certificate (DOCSIS).

Functionally, certificate management includes certificate import, certificate modification, certificate deletion and certificate display.

- Certificate import: CMTS devices support the following two import methods
  - Command Line Import: Execute the commands load root-ca-cer and load mfg-ca-cer (see the command line manual for details).
  - MIB (SNMP) Import: Certificates can be imported by setting the MIB nodes docsBpi2CmtsCACert, docsBpi2CmtsCACertTrust, docsBpi2CmtsCACertStatus.
- Certificate modification: Certificate status can be modified, when only the status of mfg certificate can be modified, and it can only be modified to trust, untrust, chain three states, which can be used in certificate verification process.
- Certificate deletion: Certificates can be deleted, but the system's three root certificates can not be deleted; Certificates are DOCSIS-ROOT, EURO-DOCSIS-ROOT, CABLE-LABS-ROOT, respectively.
- Certificate display: you can use "**show cable privacy**" Command to display the content and status of certificates. Currently, it supports the display of certificate ID, status, usage status, source, subject,

issuer, fingerprint, serial number, expiry date, etc.

18.4.1 Example of Configuration Certificate Check

Data Planning

Table 18-17 Data Planning for CMTS Equipment CRL

Item	Data
The server	FTP/TFTP Server, HTTP Server
CRL ROOT Certificate	DigiCertHighAssuranceEVRootCA.crt
CRL MFG Certificate	DigiCertSHA2ExtendedValidationServerCA.crt
URL of CRL	http://10.10.10.10/sha2-ev-server-g1.crl
FTP/TFTP Server IP	172.16.2.61
HTTP Server IP	10.10.10.10

Prerequisite

- Guarantee that both MFG-CA and ROOT-CA of CRL have been imported.
- Guarantee that the network can work and the CRL server website is correct.
- Since CRL only supports HTTP services, the server only needs to open HTTP services.

Configuration flowchart

The configuration certificate checking process is shown in the following figure.

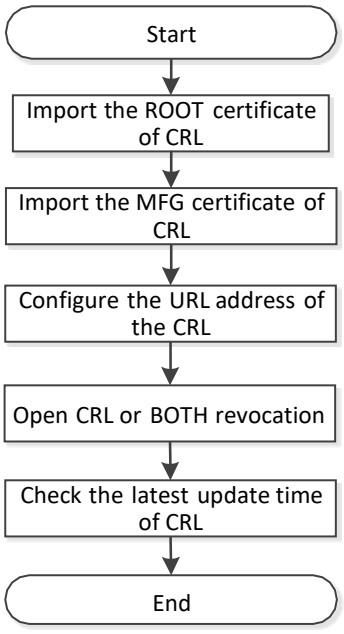

Figure 18-5 Flowchart for Configuration Certificate

Procedure

Step 1 Import the corresponding root certificate

```
BT# load root-ca-cer tftp 172.16.2.61 root1.der
```

Step 2 Import the corresponding MFG certificate

```
BT# load mfg-ca-cer tftp 172.16.2.61 mfg.der
```

Step 3 Choose the method of revocation

```
BT# configure terminal
BT(config)# cable privacy revocation methods crl
```

Step 4 Configure CRL website

```
BT(config)# cable privacy crl url
http://10.10.10.10/mycrl.crl
```

Step 5 Shows the last update time of CRL:

```
BT# show crl latest-update-time
```

Result

After the configuration is completed, CRL is successful, CM will validate CRL, otherwise the default CRL is good and go online.

18.5 CM Loopback Detection

18.5.1 Overview

In order to prevent loopback of Cable Modem from causing network abnormality, CMTS supports the configuration of turning on or off loopback detection function of Cable Modem. After the loopback detection of Cable Modem is turned on, CMTS will send a specific broadcast message to all online Cable Modem at regular intervals. If CMTS receives the same message, it is considered that there is a loop in Cable Modem. The Cable Modem of the detected loop is added to the blacklist, and its upstream service flow is disabled to avoid a large number of broadcast messages entering the CMTS causing network exceptions.

18.5.2 Configure Loopback Detection

Context

Enable CM loopback detection function

Procedure

Step 1 Enable cm loopback detection switch.

Step 2 Configures the sending interval of loopback detection message as 10 seconds.

Example

Configure the sending interval of loopback detection message to be 10 seconds:

```
BT(config)# cable loopback-detect enable BT(config)# cable
loopback-detect packet-interval 10BT(config)#
```

Related Operations

N/A

18.5.3 Configure to View Loopback CM and Remove Loopback Blacklist

Context

- Check the CM information of the detected loop.
- Recover the normal communication of CM with loop after manually removing the loop fault.

Procedure

Step 1 Check the loopback CM.

Step 2 Remove the manually excluded CM from the blacklist.

Example

Remove the CM of the viewed loop from the blacklist and resume its normal communication.

```
BT(config)# show cable loopback-detect black-list
MAC Address         Loop-back Time
0024.0000.1112      1970-01-01 00:09:32
4432.c83c.88e4      2019-08-29 10:15:53
BT(config)#
BT(config)# no cable loopback-detect black-list 0024.0000.1112
BT(config)#
```

Related Operations

N/A

Chapter 19 Multicast Management

19.1 CM Multicast Authorization Management

19.1.1 Overview

The CMTS device provides the multicast authorization configuration and query commands, as well as the entries for multicast authorization and multicast relationship maintenance. The following figure shows multicast authorization:

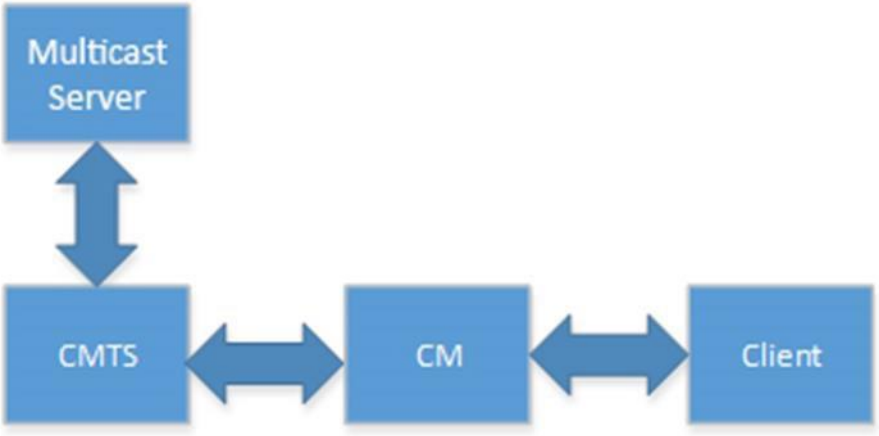

Figure 19-1 Networking Diagram for Multicast Authorization

In the multicast environment, the relationship between all roles in the above figure are as follows:

- CMTS: It performs multicast authorization based on the multicast authorization configuration, and maintains the multicast forwarding relationship entries.
- Multicast server: It processes the multicast messages and pushes streams of multicast programs.
- CM: It forwards multicast packets.
- Client: It receives multicast programs.

The multicast program authorization process is as follows:

1. The client initiates a join request to join a specified multicast group, for example, 225.1.1.1.
2. The CMTS parses the join packet to obtain the IP address of the multicast group, 225.1.1.1.
3. The CMTS searches for the multicast authorization rule by matching 225.1.1.1 with the group IP of the rule. The following two matching results are available:
    - A matched rule is found:
        - If the rule is deny, the client is prohibited to join the multicast group.

- If the rule is permit, the client is allowed to join the multicast group.
- No matched rule is found: The default action is used. (If the default action is not configured, the rule is deny.)

The CMTS multicast authorization management aims to configure and manage the multicast authorization function so that the CMTS can control permissions of users for watching multicast programs.

The following methods can be used to determine the multicast authorization profile used by a customer:

- The multicast authorization profile is specified in the CM configuration file. This method has a higher priority.
- The multicast authorization profile is configured through the ANC1000 system.

You can use the command line to perform the following configuration:

- Configure a multicast authorization profile: A multicast authorization profile is a set of rules for adding IP multicast to an authorization session.
  - Create a multicast authorization profile: The system allows you to create 16 multicast authorization profiles. After a multicast authorization profile is successfully created, the system directly enters the multicast view.
  - Specify the default multicast authorization profile: Only a multicast authorization profile that is configured as a default file can take effect.
  - Configure a multicast authorization rule: A multicast authorization rule is the rule for adding IP multicast to an authorization session.
  - Multicast authorization profile description: It describes a multicast authorization profile so that users can distinguish between different multicast authorization profiles.
- Configure the default multicast authorization action: If the CM cannot find a matched multicast authorization profile, the default action is conducted to forward packets.
- Configure the number of multicast sessions to which a CM is allowed to add.
- Enable the multicast authorization function: The multicast authorization function is disabled by default. To use this function, you must manually enable the function.

19.1.2 Example of Configure Multicast

Through IP multicast to achieve multicast program viewing services.

Networking Diagram

CMTS is connected by router and Multicast Server, Multicast Server is responsible for pushing multicast streams and Player is responsible for receiving multicast programs. The specific networking diagram is as follows:

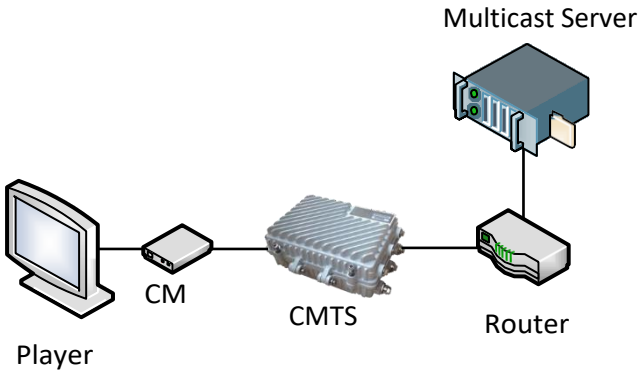

Figure 19-1 Multicast Multicast Network Graph

Data Planning

The basic multicast configuration data planning is shown in the following table.

Table 19-1 Data Planning for Multicast Configuration

Item	Data
Multicast authorization status	Enable
Maximum number of multicast sessions per CM allowed to join	20
Multicast default behavior	deny
Multicast profile	IPTV
Profile authentication	Default
Description information of multicast profile	IP multicast
Multicast authorization rules.	Rule ID: 1 Rule: permit Priority: 1 Source address: 0.0.0.0/0 Destination address: 225.0.0.0/24

Prerequisite

Network CMTS equipment and lines are normal.

Configuration flowchart

The basic multicast configuration process is shown in the following figure.

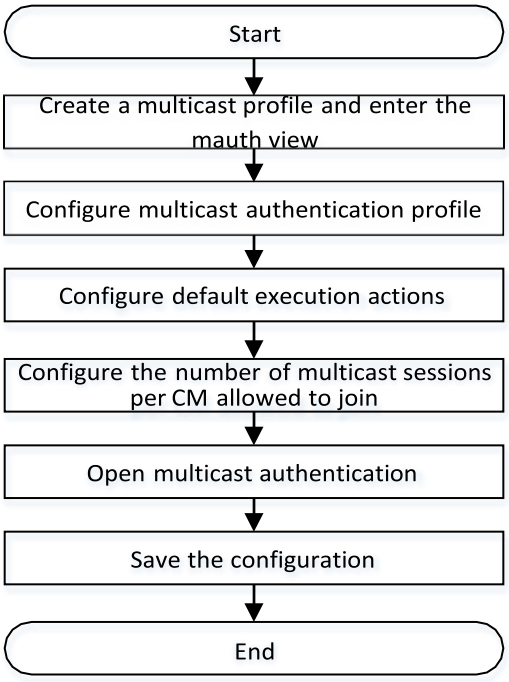

Figure 19-2 Flowchart for Basic Multicast Configuration

Procedure

Step 1 Configure the profile name of multicast to IPTV and enter the mauth view.

```
BT(config)# cable multicast authorization profile IPTV
```

Step 2 Configure multicast authorization profile

1. Set profile to take effect.

   ```
   BT(config-mauth)# cable multicast authorization profiledefault
   ```

2. The description information for configuring multicast profile is IP multicast.

   ```
   BT(config-mauth)# cable multicast authorization profile
   description "IP multicast"
   ```

3. Configure multicast authorization rules.

   ```
   BT(config-mauth)# cable session-rule 1 permit 0.0.0.0/0
   225.0.0.0/24 priority 1
   ```

Step 3 If the configuration cannot match any profile, the default multicast execution action takes effect.

1. Exit the mauth view

   ```
   BT(config-mauth)# end
   ```

2. Multicast default execution action is deny

   ```
   BT(config)# cable multicast authorization default-actiondeny
   ```

Step 4 Configures the maximum number of multicast multicast sessions allowed to join for each CM to be 20.

```
BT(config)# cable multicast authorization max-session-num 20
```

Step 5 Enable multicast authorization

```
BT(config)# cable multicast authorization enable
```

Step 6 Save the configuration

```
BT(config)# exit
BT# copy running-config startup-config
This will save the configuration to the flash memory.
Are you sure?(y/n) [n]y
Building configuration.....
Configuration saved successfully.
```

Result

According to the multicast authorization rules, users can only watch 225.0.0 multicast programs.

19.1.3 Configure the Multicast Authorization File

Context

You can perform this task to configure a multicast authorization profile. A multicast authorization profile is a set of rules for adding IP multicast to an authorization session. The task includes the following operations:

- Create a multicast authorization profile: The system allows you to create 16 multicast authorization profiles. After a multicast authorization profile is successfully created, the system directly enters the multicast view.
- Specify the default multicast authorization profile: The CMTS uses only the default multicast authorization profile for matching.
- Configure a multicast authorization rule: A multicast authorization rule is the rule for adding IP multicast to an authorization session. Parameters to be configured include the multicast session rule ID, multicast authorization action, multicast source IP address, multicast destination address, and multicast session priority.
  - Multicast session rule ID: All the multicast authorization profiles share 2048 multicast authorization rules. In the same multicast authorization profile, the multicast authorization rule ID ranges from 1 to 65535.
  - Multicast authorization action: The multicast authorization actions supported by the CMTS include permit and deny.
  - Source IP address: It specifies a valid unicast address.
  - Destination IP address: It specifies a valid multicast address.
  - Priority: The priority value supported by the system ranges from 0 to 255. A larger value indicates a higher priority. When a conflict occurs during rule matching, a rule with a higher priority is selected for matching.

- Multicast authorization profile description: It describes a multicast authorization profile so that users can distinguish between different multicast authorization profiles. The description is a string of up to 255 characters.

Procedure

Step 1 Create the multicast authorization profile by using the command "**cable multicast authorization profile**".

Step 2 Configure the multicast authorization default profile by using the command "**cable multicast authorization profile default**".

Step 3 Configure the sessionrule of the porfile by using the command "**cable session-rule**".

Step 4 (Option)Configure the multicast authorization profile description by using the command "**cable multicast authorization profile description**".

Step 5 Query the multicast authorization running configuration by using the command "**show cmts multicast running-config**".

Example

Configure the multicast authorization profile.

```
BT(config)# cable multicast authorization profile permit
BT(config-mauth)# cable multicast authorization profile description multicast-test
BT(config-mauth)# cable session-rule 1 permit 0.0.0.0/0 224.1.1.2/32 priority1
BT(config-mauth)# cable multicast authorization profile default
BT(config-mauth)# exit
BT(config)# cable multicast authorization max-session-num 8
BT(config)# show cmts multicast running-config
!cmts multicast configuration:
cable multicast authorization enable
cable multicast authorization max-session-num 8
cable multicast authorization default-action deny
cable multicast session age-time 300
cable multicast authorization profile permit
 cable multicast authorization profile default
 cable multicast authorization profile description multicast-test
 cable session-rule 1 permit 0.0.0.0/0 224.1.1.2/32 priority 1
exit
```

Related Operations

Table 19-1 Related Operations for Configure the multicast authorization file

Operation	Command	Remarks
Delete the multicast authorization file	**no cable multicast authorization profile**	
Delete the multicast authorization default file	**no cable multicast authorization profile default**	

19.1.4 Configure the Default Action of Multicast Authorization

Context

Users can configure default action of multicast authorization through this operation. If the multicast authorization profile of CM not authorize a multicast session, CM has a default action. By default, the default action is deny.

Procedure

Step 1 Configure the default action of multicast authorization by using the command "**cable multicast authorization default-action permit**".

Step 2 Query the multicast authorization information by using the command "**show cmts multicast running-config**".

Example

Configure the default action of multicast authorization.

```
BT(config)# cable multicast authorization default-action permit
BT(config)# show cmts multicast running-config
!cmts multicast configuration:
cable multicast authorization enable
cable multicast authorization max-session-num 0
cable multicast authorization default-action permit
cable multicast session age-time 300
cable multicast authorization profile permit
 cable multicast authorization profile default
 cable multicast authorization profile description multicast-test
 cable session-rule 1 permit 0.0.0.0/0 224.1.1.2/32 priority 1
exit
```

Related Operations

Table 19-2 Related Operations for Configure the default action

Operation	Command	Remarks
Configure the default action of multicast	**cable multicast authorization default-action (permit |**	

Operation	Command	Remarks
authorization	**deny)**	

19.1.5 Configure the Default Maximum Number of Sessions CM Joined

Context

Use this command to configure the number of multicast sessions that CM joined. Each CM has a maximum number of allowed to join the multicast session, if the CM configuration file is specified, the use of the value of the configuration file, if not specified, then use the default value.

Procedure

Step 1 Configure each CM to join the number of sessions by using the command "**cable multicast authorization max-session-num**".

Step 2 Query the configure information by using the command"**show cmts multicast running-config**".

Example

Configuring each CM to join the multicast session number is 5.

```
BT(config)# cable multicast authorization max-session-num 5
BT(config)# show cmts multicast running-config
!cmts multicast configuration:
cable multicast authorization enable
cable multicast authorization max-session-num 5
cable multicast authorization default-action permit
cable multicast authorization profile permit
 cable multicast authorization profile default
 cable multicast authorization profile description multicast-test
 cable session-rule 1 permit 0.0.0.0/0 224.1.1.2/32 priority 1
exit
```

Related Operations

N/A

19.1.6 Enable the Multicast Authorization

Context

Users can enable the multicast authorization through this task.

Procedure

Step 1 Enable the multicast authorization by using the command "**cable multicast authorization enable**".

Step 2 Query the multicast authorization information by using the command "**show cmts multicast running-config**".

Example

Enable the multicast authorization.

```
BT(config)# cable multicast authorization enable
BT(config)# show cmts multicast running-config
!cmts multicast configuration:
cable multicast authorization enable
cable multicast authorization max-session-num 0
cable multicast authorization default-action deny
cable multicast session age-time 300
```

Related Operations

Table 19-3 Related Operations for Configuring the Security Check against CPE under the CMs

Operation	Command	Remarks
Disable the multicast authorization	**cable multicast authorization disable**	

19.2 Multicast QoS Management

19.2.1 Overview

The multicast QoS function provides different QoS for different multicast sessions. The multicast channel binding technology can be used to plan the multicast service in a specified channel set, preventing interference with other services.

The multicast QoS mechanism is similar to the QoS mechanism of unicast service flows of a single CM. The downstream multicast data flow is matched against a multicast classifier so that the data flow is classified into different downstream multicast service flows. Based on the QoS parameter of the multicast service flow, the CMTS ensures the QoS of the multicast service flow.

One duplication of a multicast session indicates that the session is forwarded on one DCS. The CMTS selects a DCS and allocates a DSID for forwarding of a specified multicast session (S, G). The DSIC identifies a specified multicast session that is forwarded on a specified DCS.

The multicast QoS configuration mainly includes the multicast group configuration (GC), and multicast group QoS configuration (GQC).

- GC: It defines the multicast service flow classifier rules to be used by a specific multicast session, for example, the group IP address and source IP address of the multicast session. It is associated with a GQC ID.
- GQC: It is used to associate with the GC and the Service Class Name used by the GC.
- Service Class Name: It is the service flow QoS parameter set, which includes the configuration of Required Attribute Mask and Forbidden Attribute Mask. It is used to match the ProvAttrMask of the binding group, and determine the channel set of the service flow based on the channel set in the binding group.

19.2.2 Example of Security Check against CPE with the Specified IP Address

Different multicast programs have different requirements for the image definition. Different QoS resources can be allocated to the high definition (HD) and standard definition programs. In this way, a higher bandwidth can be assured for HD programs, and operators' deployment requirements can be satisfied.

This example allows users to watch specified multicast programs and ensure the quality of programs.

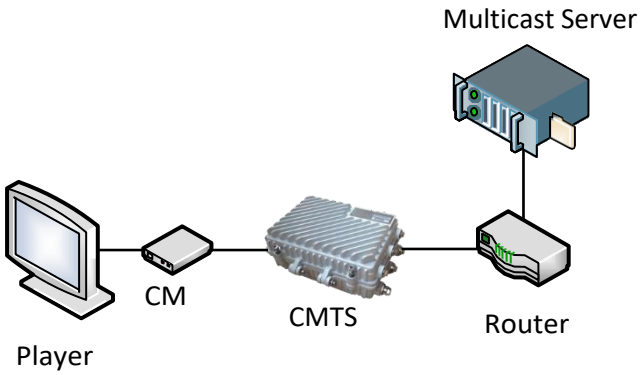

Figure 19-2 Networking Diagram of Multicast QoS

Data Planning

By the following configuration, through the following configuration, two sets of multicast programs 230.0.1.1/32 and 230.0.1.2/32 are deployed for users under CMTS, and their respective quality of service is guaranteed.

Table 19-4 Data Planning for Configuring the Security Check against CPE with the Specified IP Address

Item	Data
GQC configuration	GQC1 corresponds to the program: Mpeg2SD GQC2 corresponds to the program: Mpeg2HD
GC configuration	GC1 corresponds to GQC1, multicast group IP address 232.0.1.1/32, source IP address 0.0.0/0. GC2 corresponds to GQC2, multicast group IP address 232.0.1.2/32, source IP address 0.0.0/0.

Item	Data
Service Class	Service Class1 name : Mpeg2SD, the minimum rate : 4M bps, maxmum rate : 5M bps, maxmum burst : 1M bytes, Required Attribute Mask : 0x80000001, Forbidden Attribute Mask: 0x00000000. Service Class1 name : Mpeg2HD, the minimum rate : 4M bps, maxmum rate : 16M bps, maxmum burst : 1M bytes, Required Attribute Mask : 0x80000002, Forbidden Attribute Mask: 0x00000000.
Bonding group	Bonding group 1: Provision Attribute Mask : 0x80000001, downstream channels: 5-8 Bonding group 2: Provision Attribute Mask : 0x80000002, downstream channels: 9-12

Prerequisite

The network CMTS and lines are normal.

Configuration flowchart

The process for configuring the security check against CPE with the specified IP address is shown as follows.

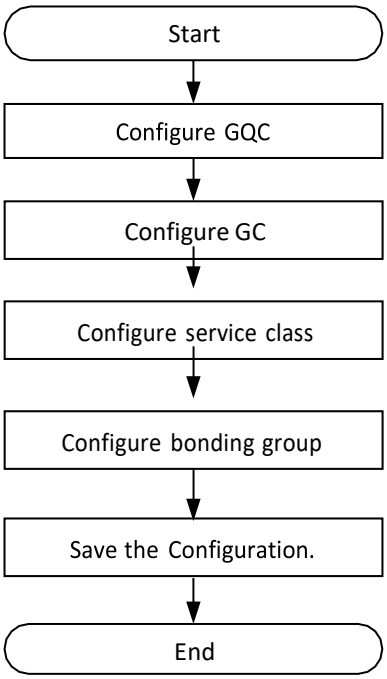

Figure 19-3 Flowchart for Configuring the Muticast Session QOS

Procedure

Step 1 Configure the GQC.

1. Configure the service class name of GQC1 as Mpeg2SD.

   `BT(config)# cable multicast group-qos config 1 service-class-name Mpeg2SD`

2. Configure the service class name of GQC2 as Mpeg2HD..

```
BT(config)# cable multicast group-qos config 2 service-class-name Mpeg2HD
```

Step 2 Configure the GC.

1. Create the GC1 and enter the mqos view.

   ```
   BT(config)# cable multicast group config 1
   ```

2. Configure the GQC for the GC.

   ```
   BT(config-mqos-1)# group-qos config 1
   ```

3. Configure the IP address of multicast group to 232.0.1.1/32, and the source IP address to 0.0.0/0 (i.e., no source is specified).

   ```
   BT(config-mqos-1)# session-range grp-ip 232.0.1.1/32 src-ip 0.0.0.0/0
   ```

4. Exit the mqos view.

   ```
   BT(config-mqos-1)# exit
   ```

5. Create the GC2 and enter the mqos view.

   ```
   BT(config)# cable multicast group config 2
   ```

6. Configure the GQC for the GC.

   ```
   BT(config-mqos-2)# group-qos config 2
   ```

7. Configure the IP address of multicast group to 232.0.1.2/32 and the source IP address to 0.0.0/0 (i.e., no source is specified).

   ```
   BT(config-mqos-2)# session-range grp-ip 232.0.1.2/32 src-ip 0.0.0.0/0
   ```

8. Exit the mqos view.

   ```
   BT(config-mqos-2)# exit
   ```

Step 3 Configure the Service Class.

1. Create the ServiceClass Mpeg2SD.

   ```
   BT(config)# cable service-class name Mpeg2SD
   ```

2. Configure the minimum rate as 4M bps of the ServiceClass Mpeg2SD. `BT(config)# cable service-class name Mpeg2SD min-rate4000000`

3. Configure the maxmum rate as 5M bps of the ServiceClass Mpeg2SD.

   ```
   BT(config)# cable service-class name Mpeg2SD max-rate5000000
   ```

4. Configure the maxmum burst as 1M byte of the ServiceClass Mpeg2SD.

   ```
   BT(config)# cable service-class name Mpeg2SD max-burst1000000
   ```

   Create the Required Attribute Mask as 0x80000001 of the ServiceClass Mpeg2SD.

   ```
   BT(config)# cable service-class name Mpeg2SD req-attr-mask 0x80000001
   ```

   Configure the Forbidden Attribute Mask as 0x00000000 of the ServiceClass Mpeg2SD.

```
BT(config)# cable service-class name Mpeg2SD forb-attr-mask
0x00000000
```

7. Create the ServiceClass Mpeg2HD.

```
BT(config)# cable service-class name Mpeg2HD
```

8. Configure the minimum rate as 4M bps of the ServiceClass Mpeg2SD. `BT(config)# cable service-class name Mpeg2HD min-rate4000000`
9. Configure the maxmum rate as 5M bps of the ServiceClass Mpeg2HD.

```
BT(config)# cable service-class name Mpeg2HD max-rate5000000
```

10. Configure the maxmum burst as 1M byte of the ServiceClass Mpeg2HD.

```
BT(config)# cable service-class name Mpeg2HD max-burst1000000
```

11. Create the Required Attribute Mask as 0x80000002 of the ServiceClass Mpeg2HD.

```
BT(config)# cable service-class name Mpeg2HD req-attr-mask
0x80000002
```

12. Configure the Forbidden Attribute Mask as 0x00000000 of the ServiceClass Mpeg2HD.

```
BT(config)# cable service-class name Mpeg2HD forb-attr-mask
0x00000000
```

Step 4 Configure the bonding group.

1. Create the downstream bonding group 1 and enter the ds bonding group view.

```
BT(config)# interface ds bonding-group 1
```

Configure the

2. Provision Attribute Mask as 0x80000001.

```
BT(config-if-ds-bonding-group1)# bonding-group prov-attr-mask
0x80000001
```

3. Add the downstream channels 5-8 to the bonding group.

```
BT(config-if-ds-bonding-group1)# cable downstream 5-8
```

4. Exit the bonding group view.

```
BT(config-if-ds-bonding-group1)# exit
```

5. Create the downstream bonding group 2 and enter the ds bonding group view.

```
BT(config)# interface ds bonding-group 2
```

Configure the

6. Provision Attribute Mask as 0x80000002.

```
BT(config-if-ds-bonding-group2)# bonding-group prov-attr-mask
0x80000002
```

7. Add the downstream channels 5-8 to the bonding group.

```
BT(config-if-ds-bonding-group2)# cable downstream 5-8
```

8. Exit the bonding group view.

```
BT(config-if-ds-bonding-group2)# exit
```

Step 5 Save the configurations.

```
BT(config)# end
```

```
BT# copy running-config startup-config
This will save the configuration to the flash memory.
Are you sure?(y/n) [n]y
Building configuration.....
Configuration saved successfully.
```

Result

According to the above configurations, The users with IP address 10.10.10.250.32 can receive the programs of the multicast sources address 232.0.1.1/32 and 232.0.1.2/32, and guarantee the service quality of the programs.

19.3 DSG Configuration

19.3.1 Functional Principle

DSG (DOCSIS Set-top gateway) standard defines the specification of uploading OOB message in DOCSIS channel. DSG architecture can be divided into DSG Server, DSG Agent and Set-top Device, as shown in the following figure:

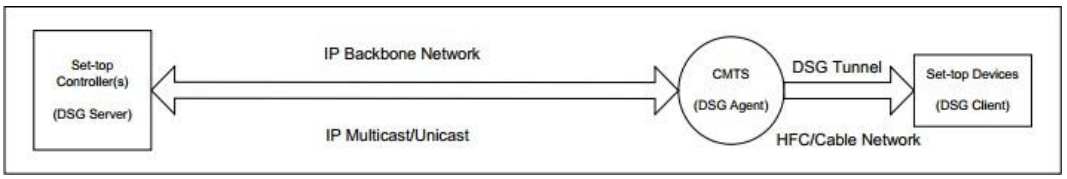

Figure 19-4 Schematic diagram of DSG function

The role of CA / SI / EPG and other servers is CMTS server. CMTS plays the role of DSG agent. Set-top Device refers to the STB(set-top box) with built-in CM that supports DSG functions. A set top device can have multiple DSG clients, but only one DSG client controller is included. DSG client controller filters and accepts tunnel data by identifying the list of customers configured in tunnel. When there are DSG clients in the set-top box device in the customer list, the data of this tunnel will be accepted, otherwise it will be discarded. DSG client is the final receiver of DSG server data.

DSG eCM is a Cable Modem with DSG function built into set top device.

DOCSIS standard defines DCD (Downstream Channel Descriptor) message, which is a DOCSIS MAC management message with DSG address table entries, used to manage DSG tunnel. In advanced mode, it is sent by DSG agent periodically and transmitted to client controller after receiving by eCM.

DCD messages are based on DOCSIS channel management, and each channel must be unique. The total length of DCD message is not allowed to exceed 1522 bytes. If the length exceeds 1522 bytes, at least one partition information shall be sent per second. The format of DCD message is as follows:

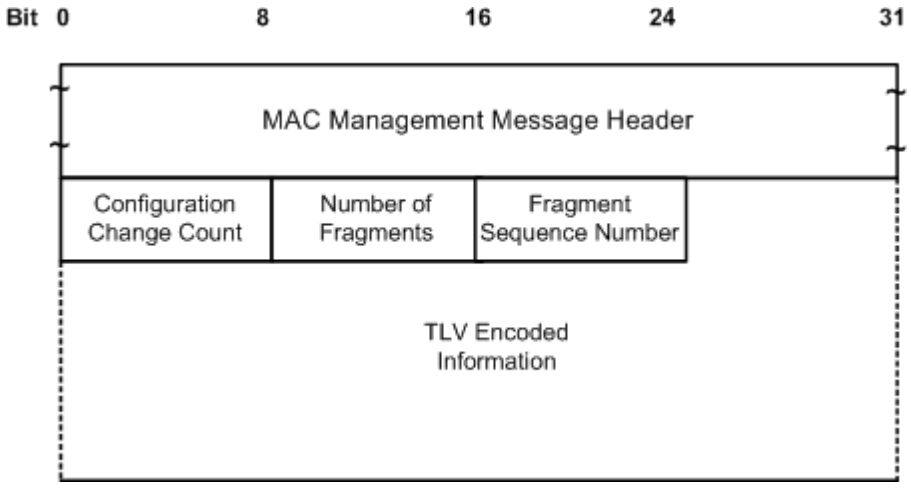

Figure 19-5 DCD message format

- Configuration Change Count: indicates the number of changes of DCD related parameters of the downstream channel, which is increased by 1 for each change. For the same DCD message, this value is the same in each fragment.
- Number of Fragments: refers to the number of DCD messages.
- Fragment Sequence Number: indicates the fragment number of DCD message, which is used for DCD message reorganization.
- TLV Encoded Information: other relevant parameters are packed in TLV information. If the configuration of these parameters changes in the business transmission phase, DSG agent will dynamically modify the corresponding parameters in DCD message, and increase the value of configuration change count. The parameters in TLV information can be divided into three categories:

Type	Length	Name	DSG Agent	DSG Client Controller	Mandatory/Optional in DCD	Repeatable in DCD
23	-	Downstream Packet Classification Encoding	√	√	O	√
23.2	2	Classifier Identifier	√	√	M	
23.5	1	Classifier Priority	√	√	M	
23.9	-	IP Packet Classification Encodings	√	√	M	
23.9.3	4	Source IP Address	√	√	O	
23.9.4	4	Source IP Mask	√	√	O	
23.9.5	4	Destination IP Address	√	√	M	
23.9.9	2	Destination TCP/UDP Port Start		√	O	
23.9.10	2	Destination TCP/UDP Port End		√	O	
50	-	DSG Rule		√	O	√
50.1	1	DSG Rule Identifier		√	M	
50.2	1	DSG Rule Priority		√	M	
50.3	n	DSG UCID List (Deprecated)		√	O	
50.4	-	DSG Client ID		√	M	
50.4.1	2	DSG Broadcast		√	O	
50.4.2	6	DSG Well-Known MAC Address		√	O	√
50.4.3	2	CA System ID		√	O	
50.4.4	2	Application ID		√	O	√
50.5	6	DSG Tunnel Address	√	√	M	
50.6	2	DSG Classifier Identifier	√	√	O	√
50.43	-	DSG Rule Vendor-Specific Parameters		√	O	√
51	-	DSG Configuration		√	O	
51.1	4	DSG Channel List Entry		√	O	√
51.2	2	DSG Initialization Timeout (Tdsg1)		√	O	
51.3	2	DSG Operational Timeout (Tdsg2)		√	O	
51.4	2	DSG Two-way Retry Timer (Tdsg3)		√	O	
51.5	2	DSG One-way Retry Timer (Tdsg4)		√	O	
51.43	-	DSG Config Vendor-Specific Parameters		√	O	√

Figure 19-6 Parameters in TLV information

DSG agent device needs to convert OOB message sent by DSG server into tunnel data and broadcast it to set-top box. At the same time, DSG agent periodically sends DCD message to STB. DSG client controller in STB receives or filters tunnel data flow according to the client list information carried in DCD message. STB only receives its own tunnel data.

19.3.2 Configure DSG Parameters

Context

Through this task, users can configure DSG parameters and tell DSG clients which downstream frequency points, timers and other information to use through DCD messages.

Procedure

Step 1 Use the **`cable dsg channel-list`** command to configure the downstream frequency.

Step 2 Use the **`cable dsg timer`** command to configure the timer.

Step 3 Use **`cable dsg vendor-param`** to configure vendor parameters.

Step 4 Apply the above configuration to downstream channel 1.

Step 5 Downstream channel 1 enables DCD.

Example

Create channel-list 100 to configure the frequency 510MHz and 518 MHz of DSG tunnel transmission.

```
BT(config)# cable dsg channel-list 100 channel-index 1 frequency 510000000
BT(config)# cable dsg channel-list 100 channel-index 2 frequency 518000000
BT(config)# cable dsg timer 100 tdsg1 10 tdsg2 20 tdsg3 30 tdsg4 40
BT(config)# cable dsg vendor-param 100 vendor 1 oui 002468
BT(config)# interface cmts 1
BT(config-if-cmts-1)# cable downstream 1 dsg channel-list 100
BT(config-if-cmts-1)# cable downstream 1 dsg timer 100 BT(config-if-
cmts-1)# cable downstream 1 dsg vendor-param 100BT(config-if-cmts-1)#
cable downstream 1 dsg dcd-enable BT(config-if-cmts-1)# exit
BT(config)# show cable dsg running-config
! DSG configuration:
cable dsg vendor-param 100 vendor 1 oui 002468
cable dsg channel-list 100 channel-index 1 frequency 510000000
cable dsg channel-list 100 channel-index 2 frequency 518000000
cable dsg timer 100 tdsg1 10 tdsg2 20 tdsg3 30 tdsg4 40
!End
BT(config)# interface cmts 1
BT(config-if-cmts-1)# show cable dsg running-config
 cable downstream 1 dsg timer 100
 cable downstream 1 dsg vendor-param 100
 cable downstream 1 dsg channel-list 100
```

Related Operations

Table 19-5 Related operations for configure DSG parameters

Operation	Command	Remarks
Downstream channel is associated with DSG frequency	**cable downstream dsg channel-list**	
Downstream channel is associated with DSG timer	**cable downstream dsg timer**	
Downstream channel is associated with DSG manufacturer parameters	**cable downstream dsg vendor-param**	
Downstream channels use DCD messages	**cable downstream dsg dcd-enable**	

19.3.3 Configure DSG Rules

Context

- Users can configure DSG rules through this task.

- Create a classifier to replace the destination MAC with 0100.5e00.0003 for the downstream multicast message with the destination address of 225.0.0.2 and the source address of 192.168.1.0/24, and then send it to the DSG client.
- The classifier is associated with the downstream channel, so that the multicast message matching the classifier is sent to the DSG client through the specified downstream channel.

Procedure

Step 1 Use the **cable dsg client-list** command to configure the DSG client list.

Step 2 Use the **cable dsg tunnel-group** command to create a tunnel group.

Step 3 Use the **cable dsg tunnel** command to create a tunnel.

Step 4 Use the **cable dsg classifier** command to create a classifier.

Step 5 Use the **cable downstream dsg tunnel-group** command to associate the classifier with the downstream channel.

Example

Configures DSG classifier rules and associates them with downstream channels.

```
BT(config)# cable dsg client-list 1 client 1 mac-address 0024.6833.3334
BT(config)# cable dsg tunnel-group 1 channel 1 rule-priority 255 BT(config)#
cable dsg tunnel 1 mac-address 0100.5e00.0002 tunnel-group 1client-list 1
BT(config)# cable dsg classifier 1 tunnel 1 dest-ip 225.0.0.2 priority 255
src-ip 192.168.1.0 src-ip-prefix-len 24  in-dcd
BT(config)#interface cmts 1
BT(config-if-cmts-1)# cable downstream 1 dsg tunnel-group 1 channel 1
BT(config-if-cmts-1)# exit
```

View the configured rules.

```
BT(config)# show cable dsg running-config
! DSG configuration:
cable dsg client-list 1 client 1 mac-address 0024.6833.3334
cable dsg tunnel-group 1 channel 1 rule-priority 255
cable dsg tunnel 1 mac-address 0100.5e00.0002 tunnel-group 1 client-list 1
cable dsg classifier 1 tunnel 1 dest-ip 225.0.0.2 priority 255 src-ip 192.168.1.0
src-ip-prefix-len 24 in-dcd
!End
BT(config)# interface cmts 1
BT(config-if-cmts-1)# show cable dsg running-config
 cable downstream 1 dsg tunnel-group 1 channel 1
```

Related Operations

N/A

Annex 1 Abbreviations

AAA	Authentication Authorization Accounting
ACL	Access Control List
ASCII	American Standard Code for Information Interchange
ATDMA	Advanced Time Division Multiple Access
CLI	Command Line Interface
CMTS	Cable Modem Terminal Systems
CM	Cable Modem
COS	Class of Service
CPE	Customer Premises Equipment
CPU	Central Processing Unit
DBC	Dynamic Bonding Change
DCC	Dynamic Channel Change
DHCP	Dynamic Host Configuration Protocol
DOCSIS	Data-over-Cable Service Interface Specification
DSCP	Differentiated Services Code Point
DSID	Downstream Identification
eMTA	Embedded Media Transport Agent
EQAM	Edge Quadrature Amplitude Modulation
FEC	Forward Error Correction
FTP	File Transfer Protocol
HFC	Hybrid Fiber Coax
ID	Identification
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IUC	Interval Usage Code
MAC	Media Access Control
MDD	MAC Domain Descriptor
MDF	Multicast DSID Forwarding
MGMT	Management
MIC	Message Integrity Check
MTA	Media Transport Agent
NCP	Next Codeword Pointer
OLT	Optical Line Terminal
PC	Personal Computer
PLR	Packet Loss Rate
PON	Passive Optical Network
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service

QPSK	Quad-Phase Shift Key
RA	Router Advertisement
RADIUS	Remote Authentication Dial in User Service
RAM	Random Access Memory
REG-REQ	Registration Request
REG-REQ-MP	Multipart Registration Request
RF	Radio Freqency
RNG-RSP	Ranging Response
SAC	Selectable Active Codes
SAV	Source Address Verification
SCDMA	Synchronous Code Division Multiple Access
SEND	Secure Neighbor Discovery
SNR	Signal to Noise Ratio
SNMP	Simple Network Management Protocol
SSH	Secure Shell
STB	Set Top Box
UCD	Upstream Channel Descriptor
UDC	Upstream Drop Classifier
UTC	Universal Time Coordinated
VLAN	Virtual Local Area Network

Annex 2 Trap Alarms

1. 4263314956: Upstream Signal Quality Bad

Items	Description
Alarm ID	4263314956
Alarm Description	The Signal Quality Features of Upstream Channel are Bad
Alarm type	Fault Alarm
Alarm features	1 System online time 2 Sequence number 3 Alarm OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 4 Alarm Level: warning 5 Enevt ID: 4263314956 6 Alarm Description: CMTS-MAC=%02x%02x.%02x%02x.%02x%02x; UpChannel %d:[SNR=%fdb;] [Uncorrectables=%u;][Correctables=%u;] 7 Time of the Alarm Happened: While the quality feature of Upstream channel is abnormal. Form: YYYY-MM-DD-HH-MM-SS Such as 20140830171500 8 System Name: BT
Causes	The signal quality feature of upstream channel is lower than the alarm threshold
Conditions to clear	The signal quality feature of upstream channel is higher than the alarm threshold
Business affection	May cause loss of data, or error. If too serious, online state of CM may affect.
Advised actions	Investigation of line quality, adjust the configuration of upstream channel modulation and frequency.
Marks	We can configure the alarm threshold of upstream quality parameter by using the command **`cable upstream (snr | correcteds | uncorrectables) threshold-warning`** *`warnning`* **`threshold-recovery`** *`recovery`*

2. 4263314957: Upstream Signal Quality Recovery

Items	Description
Alarm ID	4263314957
Alarm Description	The Signal Quality Features of Upstream Channel are back to normal
Alarm type	Recovery Alarm
Alarm features	1 System online time 2 Sequence number 3 Alarm OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 4 Alarm Level: warning 5 Enevt ID: 4263314957 6 Alarm Description: CMTS-MAC=%02x%02x.%02x%02x.%02x%02x; UpChannel %d:[SNR=%fdb] [Uncorrectables=%u][Correctables=%u] threshold-recovery; 7 Time of the Alarm Happened: While the quality feature of Upstream channel is back to

Items	Description
	normal. Form: YYYY-MM-DD-HH-MM-SS Such as 20140830171500 8 System Name: BT
Causes	The signal quality feature of upstream channel is higher than the alarm threshold
Conditions to clear	The signal quality feature of upstream channel is lower than the alarm threshold
Business affection	Clearing alarm 4263314956
Advised actions	N/A
Marks	We can configure the recovery threshold of upstream quality parameter by using the command **`cable upstream (snr | correcteds | uncorrectables) threshold-warning`** *`warnning`* **`threshold-recovery`** *`recovery`*

3. 4263314959: Upstream Channel Quality Recovery

Items	Description
Alarm ID	4263314959
Alarm Description	The upstream channel quality back to normal
Alarm type	Recovery Alarm
Alarm features	1 System online time 2 Sequence number 3 Alarm OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 4 Alarm Level: notice 5 Event ID: 4263314959 6 Alarm Description: CMTS-MAC=%02x%02x.%02x%02x.%02x%02x,channel:%d;spectrum-group quality to good,current snr %.1f,corrCode rate %d,unCorrCode rate %d. 7 Time when the alarm occurred. Example: Jan 01 1970 01:09:03 8 System Name: BT
Causes	Upstream channel quality recover by hopping to another proper spectrum group.
Conditions to clear	N/A
Effect on business	Clearing alarm 4263314960
Advised actions	N/A
Marks	N/A

4. 4263314960: Upstream Channel Quality Abnormal

Items	Description
Alarm ID	4263314960
Alarm Description	The upstream channel quality abnormal
Alarm type	Fault Alarm
Alarm features	1 System online time 2 Sequence number 3 Alarm OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 4 Alarm Level: notice

Items	Description
	5 Event ID: 4263314960 6 Alarm Description: CMTS-MAC=%02x%02x.%02x%02x.%02x%02x,channel:%d,spectrum-group quality to bad,current snr %.1f,corrCode rate %d,unCorrCode rate %d. 7 Time when the alarm occurred. Example: Jan 01 1970 01:09:03 8 System Name: BT
Causes	Upstream channel quality abnormal, meet the condition of hop.
Conditions to clear	Upstream channel quality recover by hopping to another proper spectrum group.
Effect on business	N/A
Advised actions	N/A
Marks	N/A

5. 4263314963: Channel Utilization High

Items	Description
Alarm ID	4263314963
Alarm Description	Channel utilization is too high
Alarm type	Failure Alarm
Alarm features	1 System online time 2 Sequence number 3 Alarm OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 4 Alarm Level: Warning 5 Enevt ID: 4263314963 6 Alarm Description: CMTS-MAC=%02x%02x.%02x%02x.%02x%02x; UpChannel / DownChannel %d: The channel utilization is too high at Level Major (u%%). 7 Time of the Alarm Happened: Channel utilization is is more than major Alarm thresholdvalue. Form: YYYY-MM-DD-HH-MM-SS Such as 20140830171500 8 System Name: BT
Causes	Channel utilization is more than alarm threshold value.
Conditions to clear	Channel utilization is less than recovery threshold value.
Business affection	It may cause partial processing of data loss.
Advised actions	N/A
Marks	We can configure the threshold of channel utilization by using the command **`cable (upstream|downstream) util threshold-warning`** *`warning-minor warning-major warning-ciritcal`* **`threshold-recovery`** *`recovery-minor recovery-major recovery-ciritcal`*

6. 4263314964: Channel Utilization Clear

Items	Description
Alarm ID	4263314964
Alarm Description	Channel utilization is lower than the threshold of recovery.

Items	Description
Alarm type	Recovery Alarm
Alarm features	1 System online time 2 Sequence number 3 Alarm OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 4 Alarm Level: Notice 5 Enevt ID: 4263314964 6 Alarm Description: CMTS-MAC=%02x%02x.%02x%02x.%02x%02x; UpChannel / DownChannel %d: The channel utilization recovery from Level Major (u%%). 7 Time of the Alarm Happened: While the CPU utilization is lower than the recoverythreshold. Form: YYYY-MM-DD-HH-MM-SS Such as 20140830171500 8 System Name: BT
Causes	Channel utilization is lower than the recovery threshold.
Conditions to clear	CPU utilization alarm threshold is set reasonable .
Business affection	Clearing alarm 4263314963
Advised actions	N/A
Marks	We can configure the recovery threshold of channel utilization by using the command **`cable (upstream | downstream) util threshold-warning`** *`warning-minor warning-major warning-ciritcal`* **`threshold-recovery`** *`recovery-minor recovery-major recovery-ciritcal`*

7. 4263316225: System Memory Utilization High

Items	Description
Alarm ID	4263316225
Alarm Description	System memory utilization is higher than the threshold of alarm.
Alarm type	Event Alarm
Alarm features	1 System online time 2 Sequence number 3 Alarm OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 4 Alarm Level: warning 5 Event ID: 4263316225 6 Alarm Description: CMTS-MAC=%02x%02x.%02x%02x.%02x%02x; memory usage too high, current usage %d%; 7 Time when the Alarm occurred: System memory utilization is bigger than the alarmthreshold value. Form: YYYY-MM-DD-HH-MM-SS Such as 20140830171500 8 System Name: BT
Causes	The heavy equipment load.
Conditions to clear	System memory utilization is less than the recovery threshold value
Effect on business	High memory utilization may result in system reboot.
Advised actions	N/A
Marks	N/A

8. 4263316226: System Memory Utilization Clear

Items	Description
Alarm ID	4263316226
Alarm Description	System memory utilization is less than the threshold of alarm.
Alarm type	Event Alarm
Alarm features	1 System online time 2 Sequence number 3 Alarm OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 4 Alarm Level: notice 5 Event ID: 4263316226 6 Alarm Description: CMTS-MAC=%02x%02x.%02x%02x.%02x%02x; memory usage recovery, current usage %d %; 7 Time when the alarm occurred: System memory utilization is less than the alarm threshold value. Form: YYYY-MM-DD-HH-MM-SS Such as 20140830171500 8 System Name: BT
Causes	The heavy equipment load became normal.
Conditions to clear	System memory usage threshold is set reasonably.
Effect on business	Clearing alarm 4263316225
Advised actions	N/A
Marks	N/A

9. 4263316227: System Temperature High

Items	Description
Alarm ID	4263316227
Alarm Description	The system temperature is too high
Alarm type	Event Alarm
Alarm features	1 System online time 2 Sequence number 3 Alarm OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 4 Alarm Level: warning 5 Enevt ID: 4263316227 6 Alarm Description: [US] [DS] Temperature Alarm:[red] [yellow], CMTS-MAC = %02x%02x.%02x%02x.%02x%02x; 7 Time of the Alarm Happened: While the system temperature is too high. Form: YYYY-MM-DD-HH-MM-SS Such as 20140830171500 8 System Name: BT
Causes	1. The high temperature of the outside world lead to slow heat dissipation. 2. The system alarm threshold is lower than the normal .
Conditions to clear	1. System temperature return to normal. 2. The system alarm threshold is set reasonable .
Business affection	Over temperature may lead to crash or chipset burn up.

Advised actions	1. The device should avoid violent sunshine.

Items	Description
	2. Ventilation is needed.
Marks	We can configure the alarm threshold of temperature by using the command **cable temperature alarm threshold red** *red-threshold* **yellow** *yellow-threshold*

10.4263316228: System Temperature Recovery

Items	Description
Alarm ID	4263316228
Alarm Description	The system temperature is back to normal
Alarm type	Recovery Alarm
Alarm features	1 System online time 2 Sequence number 3 Alarm OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 4 Alarm Level: warning 5 Enevt ID: 4263316228 6 Alarm Description: [US] [DS] Temperature Recover, CMTS-MAC =%02x%02x.%02x%02x.%02x%02x; 7 Time of the Alarm Happened: While the system temperature is back to normal. Form: YYYY-MM-DD-HH-MM-SS Such as 20140830171500 8 System Name: BT
Causes	N/A
Conditions to clear	System temperature threshold is set reasonable .
Business affection	Clearing alarm 4263316227
Advised actions	N/A
Marks	We can configure the alarm threshold of temperature by using the command **cable temperature alarm threshold red** *red-threshold* **yellow** *yellow-threshold*

11.4263316229: CPU Utilization High

Items	Description
Alarm ID	4263316229
Alarm Description	CPU utilization is too high to handles all messages
Alarm type	Event Alarm
Alarm features	1 System online time 2 Sequence number 3 Alarm OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 4 Alarm Level: warning 5 Enevt ID: 4263316229 6 Alarm Description: CPU utilization is too high! d%% 7 Time of the Alarm Happened: CPU utilization is too high. Form: YYYY-MM-DD-HH-MM-SS

Items	Description
	Such as 20140830171500 8 System Name: BT
Causes	CPU utilization will high when the system deal with a lot of data abruptly.
Conditions to clear	1. CPU utilization return to normal. 2. CPU utilization alarm threshold is set reasonable .
Business affection	It may cause partial processing of data loss.
Advised actions	N/A
Marks	We can configure the threshold of CPU utilization by using the command **sysmoni main-cpu-utili threshold-warning** *warning* **threshold-recovery** *recovery*

12.4263316230: CPU Utilization Recovery

Items	Description
Alarm ID	4263316230
Alarm Description	CPU utilization is lower than the threshold of recovery.
Alarm type	Recovery Alarm
Alarm features	1 System online time 2 Sequence number 3 Alarm OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 4 Alarm Level: warning 5 Enevt ID: 4263316230 6 Alarm Description: CPU utilization change to nomal! d%% 7 Time of the Alarm Happened: While the CPU utilization is lower than the recoverythreshold. Form: YYYY-MM-DD-HH-MM-SS Such as 20140830171500 8 System Name: BT
Causes	Reduce the amount of data to a certain value
Conditions to clear	CPU utilization alarm threshold is set reasonable .
Business affection	Clearing alarm 4263316229
Advised actions	N/A
Marks	We can configure the recovery threshold of CPU utilization by using the command **sysmoni main-cpu-utili threshold-warning** *warning* **threshold-recovery** *recovery*

13.4263316231: Docsis Chip Temperature High

Items	Description
Alarm ID	4263316231
Alarm Description	The docsis chip temperature is too high
Alarm type	Event Alarm
Alarm features	1 System online time 2 Sequence number 3 Alarm OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0

Items	Description
	4 Alarm Level: warning 5 Enevt ID: 4263316231 6 Alarm Description: DOCSIS MAC Temperature Alarm:[red] [yellow],CMTS-MAC=%02x%02x.%02x%02x.%02x%02x; 7 Time of the Alarm Happened: While the docsis chip temperature is too high. Form: YYYY-MM-DD-HH-MM-SS Such as 20140830171500 8 System Name: BT
Causes	1. The high temperature of the outside world lead to slow heat dissipation. 2. The system alarm threshold is lower than the normal .
Conditions to clear	1. Docsis chip temperature return to normal. 2. Docsis chip alarm threshold is set reasonable.
Business affection	Over temperature may lead to crash or chipset burn up.
Advised actions	1. The device should avoid violent sunshine. 2. Ventilation is needed.
Marks	We can configure the alarm threshold of temperature by using the command **`cable temperature alarm threshold red`** *`red-threshold`* **`yellow`** *`yellow-threshold`*

14.4263316232: Docsis Chip Temperature Recovery

Items	Description
Alarm ID	4263316232
Alarm Description	The docsis chip temperature is back to normal
Alarm type	Recovery Alarm
Alarm features	1 System online time 2 Sequence number 3 Alarm OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 4 Alarm Level: notice 5 Enevt ID: 4263316232 6 Alarm Description: DOCSIS MAC Temperature Recover,CMTS-MAC=%02x%02x.%02x%02x.%02x%02x; 7 Time of the Alarm Happened: While the docsis chip temperature is back to normal. Form: YYYY-MM-DD-HH-MM-SS Such as 20140830171500 8 System Name: BT
Causes	1. Docsis chip temperature return to normal. 2. Docsis chip alarm threshold is set reasonable.
Conditions to clear	1. The high temperature of the outside world lead to slow heat dissipation. 2. The system alarm threshold is lower than the normal.
Business affection	Clearing alarm 4263316231
Advised actions	N/A

Marks	We can configure the alarm threshold of temperature by using the command **cable temperature alarm threshold red** *red-threshold* **yellow** *yellow-threshold*

15.4263317513: CM Partial Service Alarm

Items	Description
Alarm ID	4263317513
Alarm Description	CM is in partial service state for one or more channels in the TCS and/or the RCS are unusable.
Alarm type	Event Alarm
Alarm features	1 System online time 2 Sequence number 3 Alarm OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 4 Alarm Level: warning 5 Event ID: 4263317513 6 Alarm Description: <CM-MAC=%02x%02x.%02x%02x.%02x%02x> - Partial Service with <US:US_SET> <DS:DS_SET> 7 Time when the alarm occurred: one or more channels of the CM are unusable. Example:Jan 01 1970 01:09:03 8 System Name: BT
Causes	one or more channels of the CM are unusable
Conditions to clear	all of the channels in the TCS and the RCS are usable
Effect on business	N/A
Advised actions	N/A
Marks	N/A

16.4263317514: CM Partial Service Recovery

Items	Description
Alarm ID	4263317514
Alarm Description	CM recover from partial service state for all of the channels in the TCS and the RCS are usable.
Alarm type	Event Alarm
Alarm features	1 System online time 2 Sequence number 3 Alarm OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 4 Alarm Level: warning 5 Event ID: 4263317514 6 Alarm Description: <CM-MAC=%02x%02x.%02x%02x.%02x%02x> - Partial Service Recovery 7 Time when the alarm occurred: all of the channels in the TCS and the RCS are usable. Example: Jan 01 1970 01:09:03 8 System Name: BT
Causes	all of the channels in the TCS and the RCS are usable
Conditions to clear	N/A
Effect on business	Clearing alarm 4263317513
Advised actions	N/A
Marks	N/A

17.4263319042: UpLink Rate of Flow High

Items	Description
Alarm ID	4263319042
Alarm Description	UpLink rate of flow is too high
Alarm type	Failure Alarm
Alarm features	1 System online time 2 Sequence number 3 Alarm OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 4 Alarm Level: warning 5 Enevt ID: 4263319042 6 Alarm Description: CMTS-MAC=%02x%02x.%02x%02x.%02x%02x; Uplink Port %d send/receive utilization is high at Level Major (now %d%). 7 Time of the Alarm Happened: Uplink interface traffic is more than the relevant alarm threshold value. Form: YYYY-MM-DD-HH-MM-SS Such as 20140830171500 8 System Name: BT
Causes	1. User data traffic is too large & uplink interface traffic is more than the stated threshold in a certain time. 2. Uplink interface speed setting is not right.For example,setting 1000Mbps to 100Mbps,which will make the uplink interface bandwidth critical even if the user data traffic is not so large.
Conditions to clear	1. Reduce the user data traffic.Normally we have to reduce the quantity of users who are using in the same device. 2. Check if the uplink interface settingis expected. 3. Set the threshold in a higher value
Business affection	Appearance of alarm mean that the users' network speed can't meet their demand. Network in users' part is slow.Buffer is often needed when they watch online video.All of those will decrease the users' experience
Advised actions	If the alarm exist in a long time.we have to check if the threshold value is too low.If the threshold value is reasonable & the speed of uplink interface setting is right,then the alarm shows that the bandwidth provided from the device can't meet the users' demand.We have to increase the devices or decrease the quantity of users who are using in the same device.
Marks	We can configure the upLink rate of flow threshold by using the command **`uplink (egress | ingress) util threshold-warning`** *`warning-minor warning-major warning-ciritcal`* **`threshold-recovery`** *`recovery-minor recovery-major recovery-ciritcal`*

18.4263319043: UpLink Rate of Flow Clear

Items	Description
Alarm ID	4263319043
Alarm Description	UpLink rate of flow is lower than the threshold of recovery.
Alarm type	Recovery Alarm

Alarm features	1 System online time

Items	Description
	2 Sequence number 3 Alarm OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 4 Alarm Level: warning 5 Enevt ID: 4263319043 6 Alarm Description: CMTS-MAC=%02x%02x.%02x%02x.%02x%02x; Uplink Port %d send/receive utilization is recovery from Level Major (now %d%). 7 Time of the Alarm Happened: :Uplink interface traffic is less than the relevant recovery threshold value. Form: YYYY-MM-DD-HH-MM-SS Such as 20140830171500 8 System Name: BT
Causes	User data traffic comes down & uplink interface traffic is less than the stated recovery threshold in a certain time.
Conditions to clear	N/A
Business affection	Clearing alarm 4263319042
Advised actions	N/A
Marks	We can configure the upLink rate of flow threshold by using the command **uplink (egress | ingress) util threshold-warning** *warning-minor warning-major warning-ciritcal* **threshold-recovery** *recovery-minor recovery-major recovery-ciritcal*

19.4263328001: Abnormal Alarm of Low Input Optical Power of Optical Receiver

Items	Description
Alarm ID	4263328001
Alarm Description	Abnormal alarm is triggered when the input power of optical receiver is too low
Alarm type	Fault Alarm
Alarm features	1 System online time 2 Sequence number 3 Alarm OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 4 Alarm Level: error 5 Event ID: 4263328001 6 Alarm Description: <CMTS-MAC=%02x%02x.%02x%02x.%02x%02x>; CATV input opticalpower (%d.%d dBm < %d.%d dBm) is too low; 7 Time when the alarm occurred: The alarm is triggered when the input light power of the optical receiver is too low. Example: Jan 01 1970 01:09:03 8 System Name: BT
Causes	When the input power of optical receiver is too low, it is less than the corresponding alarm threshold.
Conditions to clear	The input optical power of the optical receiver returns to normal, which is greater than or equal to the too low recovery threshold.
Effect on business	N/A
Advised actions	N/A

Items	Description
Marks	N/A

20.4263328002: Abnormal Recovery of Input Optical Power of Optical Receiver

Items	Description
Alarm ID	4263328002
Alarm Description	Abnormal recovery of low input power of optical receiver
Alarm type	Recovery Alarm
Alarm features	1 System online time 2 Sequence number 3 Alarm OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 4 Alarm Level: notification 5 Event ID: 4263328002 6 Alarm Description: <CMTS-MAC=%02x%02x.%02x%02x.%02x%02x>;CATV input opticalpower (%d.%d dBm >= %d.%d dBm) too low status was recoverd; 7 Time when the alarm occurred: The optical receiver recovers from the abnormal state oftoo low input light power. Example: Jan 01 1970 01:09:03 8 System Name: BT
Causes	The optical receiver recovers from the abnormal state of too low input optical power.
Conditions to clear	The optical receiver recovers from the abnormal state of too low input optical power, which is greater than or equal to the corresponding too low recovery threshold.
Effect on business	N/A
Advised actions	N/A
Marks	N/A

21.4263328003: Abnormal Alarm of High Input Optical Power of Optical receiver

Items	Description
Alarm ID	4263328003
Alarm Description	Abnormal alarm is triggered when the input power of optical receiver is too high.
Alarm type	Fault Alarm
Alarm features	1 System online time 2 Sequence number 3 Alarm OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 4 Alarm Level: error 5 Event ID: 4263328003 6 Alarm Description: <CMTS-MAC=%02x%02x.%02x%02x.%02x%02x>;CATV input opticalpower (%d.%d dBm > %d.%d dBm) is too high;

Items	Description
	7 Time when the alarm occurred: The alarm is triggered when the input light power of the optical receiver is too high.Example: Jan 01 1970 01:09:03 8 System Name: BT
Causes	The input light power of the optical receiver is too high, which is larger than the corresponding alarm threshold.
Conditions to clear	The input power recovery of the optical receiver is less than or equal to the corresponding high recovery threshold.
Effect on business	N/A
Advised actions	N/A
Marks	N/A

22.4263328004: Abnormal Recovery of Over-high Input Optical Power of Optical Receiver

Items	Description
Alarm ID	4263328004
Alarm Description	Abnormal recovery of input light power of optical receiver is too low or too high
Alarm type	Recovery Alarm
Alarm features	1 System online time 2 Sequence number 3 Alarm OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 4 Alarm Level: notification 5 Event ID: 4263328004 6 Alarm Description: <CMTS-MAC=%02x%02x.%02x%02x.%02x%02x>;CATV input opticalpower (%d.%d dBm <= %d.%d dBm) too high status was recoverd 7 Time when the alarm occurred: The optical receiver recovers from the abnormal state of excessive input light power. Example: Jan 01 1970 01:09:03 8 System Name: BT
Causes	The input power recovery of optical receiver is less than or equal to the corresponding high recovery threshold.
Conditions to clear	The input power recovery of optical receiver is less than or equal to the corresponding high recovery threshold.
Effect on business	N/A
Advised actions	N/A
Marks	N/A

23.4263330049: Service Flow Application High

Items	Description
Alarm ID	4263330049
Alarm Description	Service flow application is higher than the threshold of alarm.

Items	Description
Alarm type	Event Alarm
Alarm features	1 System online time 2 Sequence number 3 Alarm OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 4 Alarm Level: notice 5 Event ID: 4263330049 6 Alarm Description: CMTS-MAC=%02x%02x.%02x%02x.%02x%02x;upstream channel %d;schedule type be/nrtps/rtps/ugs-ad/ugs ;minor /major alarm;bandwidth percent %.2f; 7 Time when the Alarm occurred: Upstream service flow application is more than the alarm threshold value. Example: <NOTICE>Dec 29 2010 16:52:26 BT CMTS[BT]:<admissionCtrl><6017> CMTS-MAC=0024.6851.E537;upstream channel 2;schedule typ 8 System Name: BT
Causes	Upstream service flow application is more than the alarm threshold value.
Conditions to clear	Upstream service flow application is less than the recovery threshold value
Effect on business	N/A
Advised actions	N/A
Marks	Configuring the threshold value of the Upstream service flow application : $cable admission-control us-bandwidth sched be/nrtps/rtps/ugs-ad/ugs minor %d (major %d)

24.4263330050: Service Flow Application Clear

Items	Description
Alarm ID	4263330050
Alarm Description	Service flow application is less than the threshold of alarm.
Alarm type	Recovery Alarm
Alarm features	1 System online time 2 Sequence number 3 Alarm OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 4 Alarm Level: notice 5 Event ID: 4263330050 6 Alarm Description: CMTS-MAC=%02x%02x.%02x%02x.%02x%02x;upstream channel %d;schedule type be/nrtps/rtps/ugs-ad/ugs ;minor/major recovery;bandwidth percent %.2f; 7 Time when the alarm occurred: Upstream service flow application is less than the alarm threshold value. Example: <NOTICE>Dec 29 2010 16:51:47 BT CMTS[BT]:<admissionCtrl><4263330050> CMTS-MAC=0024.6851.E537;upstream channel 1;schedule typ 8 System Name: BT
Causes	Upstream service flow application is less than the alarm threshold value.
Conditions to clear	N/A
Effect on business	N/A

Items	Description
Advised actions	N/A
Marks	Configuring the threshold value of the Upstream service flow application : $cable admission-control us-bandwidth sched be/nrtps/rtps/ugs-ad/ugs minor %d (major %d)

Annex 3 Trap Event

1. 4263314945: Link Discover

Items	Description
Event ID	4263314945
Event Description	Discover the link of the docsis core chip
Event type	Normal event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: notice 4 Event ID: 4263314945 5 Event Description: CMTS:CMC Link Discovery; CMTS-MAC=%02x%02x.%02x%02x.%02x%02x; 6 Time when the event occurred. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	The docsis core chip bootup
Conditions to clear	N/A
Effect on business	N/A
Advised actions	N/A
Marks	N/A

2. 4263314946: Link Lose

Items	Description
Event ID	4263314946
Event Description	Lose the link of the docsis core chip
Event type	Normal event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: notice 4 Event ID: 4263314946 5 Event Description: CMTS: CMC Link lose; CMTS-MAC=%02x%02x.%02x%02x.%02x%02x; 6 Time when the event occurred. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	N/A
Conditions to clear	N/A
Effect on business	Reboot the device
Advised actions	N/A
Marks	N/A

3. 4263314948: Downstream Parameter Change

Items	Description
Event ID	4263314948
Event Description	The downstream parameter change
Event type	Event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: Notice 4 Event ID: 4263314948 5 Event Description: CMTS-MAC=%02x%02x.%02x%02x.%02x%02x;DS %d changed; module:%s->%s; annex:%s->%s; freq:%lu->%lu; intleave:%s->%s; powLevel:%.1f->%.1f; 6 Time when the event occurred. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	Configure the downstream parameter
Conditions to clear	N/A
Effect on business	N/A
Advised actions	N/A
Marks	Not all the parameter in the event description will be displayed, only those which have been changed will be taken in the event description.

4. 4263314949: Downstream Shutdown

Items	Description
Event ID	4263314949
Event Description	Shutdown the downstream
Event type	Normal event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: notice 4 Event ID: 4263314949 5 Event Description: CMTS-MAC=%02x%02x.%02x%02x.%02x%02x;DS %d changed;adminStatus:up->down; 6 Time when the event occurred. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	Shutdown the downstream
Conditions to clear	N/A
Effect on business	N/A
Advised actions	N/A
Marks	N/A

5. 4263314950: Downstream Enable

Items	Description
Event ID	4263314950
Event Description	Enable the downstream
Event type	Event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: Notice 4 Event ID: 4263314950 5 Event Description: CMTS-MAC=%02x%02x.%02x%02x.%02x%02x;DS %d changed;adminStatus:down->up; 6 Time when the event occurred. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	Enable the downstream
Conditions to clear	N/A
Effect on business	N/A
Advised actions	N/A
Marks	N/A

6. 4263314951: Upstream Shutdown

Items	Description
Event ID	4263314951
Event Description	Shutdown the downstream
Event type	Event
Event level	Minor
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: Notice 4 Event ID: 4263314951 5 Event Description: CMTS-MAC=%02x%02x.%02x%02x.%02x%02x;US %d changed;adminStatus:up->down; 6 Time when the event occurred. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	Shutdown the upstream
Conditions to clear	N/A
Effect on business	N/A
Advised actions	N/A
Marks	N/A

7. 4263314952: Upstream Enable

Items	Description
Event ID	4263314952

Items	Description
Event Description	Enable the upstream
Event type	Event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: Notice 4 Event ID: 4263314952 5 Event Description: CMTS-MAC=%02x%02x.%02x%02x.%02x%02x;US %d changed;adminStatus:down->up; 6 Time when the event occurred. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	Enable the upstream
Conditions to clear	N/A
Effect on business	N/A
Advised actions	N/A
Marks	N/A

8. 4263314953: Upstream Parameter Change

Items	Description
Event ID	4263314953
Event Description	Upstream parameter change
Event type	Event
Event level	Minor
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: Notice 4 Event ID: 4263314953 5 Event Description: CMTS-MAC=%02x%02x.%02x%02x.%02x%02x;US %d changed; chanWidth:%s->%s; profType:%s->%s; freq:%lu->%lu; chanMode:v%d->v%d; comMode:%s->%s; powerlevel:%.1f->%.1f; 6 Time when the event occurred. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	Configure the upstream parameter
Conditions to clear	N/A
Effect on business	N/A
Advised actions	N/A
Marks	Not all the parameter in the event description will be displayed, only those which have been changed will be taken in the event description.

9. 4263314954: CMC Configure Failed

Items	Description
Event ID	4263314954
Event Description	CMC configure failed
Event type	Event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: Error 4 Event ID: 4263314953 5 Event Description: CmcConfigFail;CmcMac=%02x%02x.%02x%02x.%02x%02x;%s 6 Time when the event occurred. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	CMC configure failed
Conditions to clear	N/A
Effect on business	This may lead CMC online failed.
Advised actions	N/A
Marks	The last %s in the event description describes the failed reason, it will differ by different failed reason.

10.4263314955: CMC Reset

Items	Description
Event ID	4263314955
Event Description	CMC reset
Event type	Event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: Notice 4 Event ID: 4263314955 5 Event Description: Manual reset CMTS-MAC=%02x%02x.%02x%02x.%02x%02x is %s. 6 Time when the event occurred. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	Reset the CMC manually
Conditions to clear	N/A
Effect on business	This will lead the reboot of the docsis core chip
Advised actions	N/A
Marks	The last %s in the event description describes the result of the reset. If success it will be “successful”, if failed it will be “failed”.

11.4263314958: Spectrum Group Hop

Items	Description
Event ID	4263314958
Event Description	Spectrum group hop

Items	Description
Event type	Normal event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: notice 4 Event ID: 4263314958 5 Event Description: CMTS-MAC=%02x%02x.%02x%02x.%02x%02x,channel:%d,spectrum-group hop to:frequency %d,width %d,power %.1f,modulation %s,current snr %.1f,corrCode rate %d,uncorrCode rate %d. 6 Time when the event occurred. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	The upstream channel abnormal
Conditions to clear	N/A
Effect on business	N/A
Advised actions	N/A
Marks	N/A

12.4263314967: State Synchronization Buffer Overflow

Items	Description
Event ID	4263314967
Event Description	State synchronization buffer overflow
Event type	Event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: Warning 4 Event ID: 4263314967 5 Event Description: State SYNC cache full. 6 Time when the event occurred. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	When state synchronization occurs, part of the OAM messages enter the buffer, and a large number of OAMs cause the buffer to be full.
Conditions to clear	N/A
Effect on business	Loss of some new information
Advised actions	When the buffer is full, new OAM information is discarded
Marks	N/A

13.4263314968: Failure of State Synchronization

Items	Description
Event ID	4263314968
Event Description	Failure of state synchronization
Event type	Event

Items	Description
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: Warning 4 Event ID: 4263314968 5 Event Description: State SYNC failed. 6 Time when the event occurred. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	Synchronization timeout of a module state and failure after three retransmissions of the module synchronization request
Conditions to clear	N/A
Effect on business	CMTS state synchronization failure
Advised actions	CMTS reconnection
Marks	N/A

14.4263316481: CM Can not Get IPv4 Configuration File

Items	Description
Event ID	4263316481
Event Description	CM can not get IPv4 configuration file
Event type	Event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: Warning 4 Event ID: 4263316481 5 Event Description: IPv4 Local Provisioning CM configuration file does not exist.CM-MAC = %02x:%02x:%02x:%02x:%02x:%02x; File = %s. 6 Time when the event occurred: System power on. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	The configuration file assigned to CM by Local Provisioning does not exist, or CM requests a configuration file that does not exist.
Conditions to clear	Check whether the Ipv4 configuration file allocated by Local Provisioning for CM exists.
Effect on business	The CM in question will not be able to download the configuration file successfully and go online.
Advised actions	N/A
Marks	N/A

4263317505: CM Offline

Items	Description
Event ID	4263317505
Event Description	CM offline
Event type	Event

Items	Description
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: Notice 4 Event ID: 4263317505 5 Event Description: Cable Modem Monitor: CM-MAC=%02x%02x.%02x%02x.%02x%02x; under CMTS-MAC=%02x%02x.%02x%02x.%02x%02x is offline. ipv4 address --,ipv6 address --. 6 Time when the event occurred. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	Enable the switch of CM monitor and take off an online CM.
Conditions to clear	N/A
Effect on business	N/A
Advised actions	N/A
Marks	N/A

16.4263317507: CM Online

Items	Description
Event ID	4263317507
Event Description	CM Online
Event type	Event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: Notice 4 Event ID: 4263317507 5 Event Description: Cable Modem Monitor: CM-MAC=%02x%02x.%02x%02x.%02x%02x; under CMTS-MAC=%02x%02x.%02x%02x.%02x%02x is online. ipv4 address --,ipv6 address --. 6 Time when the event occurred. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	Enable the switch of CM monitor and make a CM online.
Conditions to clear	N/A
Effect on business	N/A
Advised actions	N/A
Marks	N/A

17.4263317508: CM Frequency Switch Time Out

Items	Description
Event ID	4263317508
Event Description	The CM frequency switch time out
Event type	Event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0

Items	Description
	3 Event Level: Warning 4 Event ID: 4263317508 5 Event Description: Failed to change ds-frequency;CM MAC= %02x%02x.%02x%02x.%02x%02x. 6 Time when the event occurred. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	Time when the command of CM frequency switch has input, but the CM do not scam on the old CMTS.
Conditions to clear	N/A
Effect on business	Frequency point migration failure
Advised actions	N/A
Marks	N/A

18.4263317509: CM IPv4 Conflict

Items	Description
Event ID	4263317509
Event Description	CM IPv4 conflict
Event type	Event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: Error 4 Event ID: 4263317509 5 Event Description: cm ipv4 %d.%d.%d.%d conflict, reset previous cm %02x%02x.%02x%02x.%02x%02x. 6 Time when the alarm occurred: If detect the IP address is conflict with the previousonlined IP address then trigger the event. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	Abnormal or configuration errors caused by the DHCP server assigned the same IP address to different CM.
Conditions to clear	Check the DHCP server and restore normal configuration.
Effect on business	The CM will be restarted, maybe lose the transmission data.
Advised actions	N/A
Marks	N/A

19.4263317510: CM IPv6 Conflict

Items	Description
Event ID	4263317510
Event Description	CM IPv6 conflict
Event type	Event
Event features	1 System online time

Items	Description
	2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: Error 4 Event ID: 4263317510 5 Event Description: cm ipv6 %02x:%02x:%02x:%02x:%02x:%02x:%02x:%02x conflict, reset previous cm %02x%02x.%02x%02x.%02x%02x. 6 Time when the alarm occurred: If detect the IPv6 address is conflict with the previous onlined IPv6 address, then trigger the event. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	Abnormal or configuration errors caused by the DHCPv6 server assigned the same IPv6 address to different CM.
Conditions to clear	Check the DHCPv6 server and restore normal configuration.
Effect on business	The CM will be restarted, maybe lose the transmission data.
Advised actions	N/A
Marks	N/A

20.4263317511: CM REG Failed

Items	Description
Event ID	4263317511
Event Description	CM REG Failed
Event type	Event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: Critical 4 Event ID: 4263317511 5 Event Description: CMTS-MAC: %02x%02x.%02x%02x.%02x%02x;CM-MAC: %02x%02x.%02x%02x.%02x%02x; REG-REQ rejected; confirmation code:%d REG REQ rejected-Major classifier error;CMTS-MAC: %02x%02x.%02x%02x.%02x%02x;CM-MAC: %02x%02x.%02x%02x.%02x%02x;CM-QOS=1.1;CM-VER=3.0; 6 Time when the event occurred. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	Make a wrong CM config file, then CM will get REG-REQ rejected.
Conditions to clear	N/A
Effect on business	N/A
Advised actions	N/A
Marks	N/A

21.4263317512: CM Frequency Switch Rescan

Items	Description
Event ID	4263317512

Items	Description
Event Description	The CM frequency switch rescan event
Event type	Event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: Notice 4 Event ID: 4263317512 5 Event Description: change ds-frequency;CM MAC= %02x%02x.%02x%02x.%02x%02x has rescan. 6 Time when the event occurred. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	Time when the command of CM frequency switch has input, but the CM rescan on the old CMTS.
Conditions to clear	N/A
Effect on business	N/A
Advised actions	N/A
Marks	N/A

22.4263317518: CM Maximum Active Quantity Alarm

Items	Description
Event ID	4263317518
Event Description	CM maximum active quantity alarm
Event type	Event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1 3 Event Level: Warning 4 Event ID: 4263317518 5 Event Description: CM active number warning threshold --, percent -- 6 Time when the event occurred. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	Alarm threshold reached
Conditions to clear	Modify the threshold percentage, or configure the value of max-number
Effect on business	N/A
Advised actions	N/A
Marks	N/A

23.4263317519: CM Maximum Active Number Recovery

Items	Description
Event ID	4263317519
Event Description	CM maximum active number recovery
Event type	Event

Items	Description
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1 3 Event Level: notice 4 Event ID: 4263317519 5 Event Description: CM active number recovery threshold --, percent -- 6 Time when the event occurred. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	The number of CM active falls below the recovery threshold.
Conditions to clear	N/A
Effect on business	N/A
Advised actions	N/A
Marks	N/A

24.4263317761: IP Packet From Invalid Source

Items	Description
Event ID	4263317761
Event Description	IP packet from invalid source
Event type	Event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: Warning 4 Event ID: 4263317761 5 Event Description: CMTS MAC=%02x%02x.%02x%02x.%02x%02x; IP packet from invalid source. IP=%d.%d.%d.%d, MAC=%02x%02x.%02x%02x.%02x%02x, CM-MAC=%02x%02x.%02x%02x.%02x%02x , DETECTED=%d. 6 Time when the alarm occurred: IP packet from invalid source. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	N/A
Conditions to clear	N/A
Effect on business	N/A
Advised actions	N/A
Marks	N/A

25.4263318529: CPE IPv4 Conflict

Items	Description
Event ID	4263318529
Event Description	CPE IPv4 conflict
Event type	Event
Event features	1 System online time

Items	Description
	2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: Error 4 Event ID: 4263318529 5 Event Description: CPE IP conflict, action: delete early CPE and reset its CM;conflict CPE-IP=%d.%d.%d.%d, vlan=%d;early CPE connected CM-MAC=%02x%02x.%02x%02x.%02x%02x;later CPE connected CM-MAC=%02x%02x.%02x%02x.%02x%02x. 6 Time when the alarm occurred: If detect the IP address is conflict with the previous onlined IP address when received the CPE ACK message, then trigger the event. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	Abnormal or configuration errors caused by the DHCP server assigned the same IP address to different CPE.
Conditions to clear	Check the DHCP server and restore normal configuration.
Effect on business	The CM and CPE will be restarted, maybe lose the transmission data.
Advised actions	N/A
Marks	N/A

26.4263318530: CPE IPv6 Conflict

Items	Description
Event ID	4263318530
Event Description	CPE IPv6 conflict
Event type	Event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: Error 4 Event ID: 4263318530 5 Event Description: CPE IPV6 conflict, action: delete early CPE and reset its CM;conflict CPE-IP=X:X::X:X;early CPE connected CM-MAC=%02x%02x.%02x%02x.%02x%02x;later CPE connected CM-MAC=%02x%02x.%02x%02x.%02x%02x. 6 Time when the alarm occurred: If detect the IPv6 address is conflict with the previous onlined IPv6 address when received the CPE ACK message, then trigger the event. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	Abnormal or configuration errors caused by the DHCPv6 server assigned the same IPv6 address to different CPE.
Conditions to clear	Check the DHCPv6 server and restore normal configuration.
Effect on business	The CM and CPE will be restarted, maybe lose the transmission data.
Advised actions	N/A
Marks	N/A

27.4263319041: Uplink Port Up/Down

Items	Description
Event ID	4263319041
Event Description	Uplink port up or down
Event type	Normal event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: notice 4 Event ID: 4263319041 5 Event Description: Uplink[%d] link up/down. 6 Time when the event occurred. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	Pull out the cable from the uplink port or insert the cable into the uplink port.
Conditions to clear	N/A
Effect on business	This will effect the work of the network.
Advised actions	N/A
Marks	N/A

28.4263320577: Login Failed

Items	Description
Event ID	4263320577
Event Description	User login failed
Event type	Event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: Info 4 Event ID: 4263320577 5 Event Description: user@address(mode) login failed:reason. Mode is telnet/ssh/console/web; 6 Time when the event occurred. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	User login failed
Conditions to clear	N/A
Effect on business	N/A
Advised actions	N/A
Marks	N/A

29.4263320578: Login Success

Items	Description
Event ID	4263320578

Items	Description
Event Description	User login success
Event type	Event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: Info 4 Event ID: 426332058 5 Event Description: user@address(mode) login successfully. Mode is telnet/ssh/console/web; 6 Time when the event occurred. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	User login successfully
Conditions to clear	N/A
Effect on business	N/A
Advised actions	N/A
Marks	N/A

30.4263320833: DHCPv4 IPv4 Address Conflict

Items	Description
Event ID	4263320833
Event Description	Address conflict between DHCPv4 acquired address and locally configured IPv4 address
Event type	Event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: Notice 4 Event ID: 4263320833 5 Event Description: CMTS-MAC= cmts ipv4 %d.%d.%d.%d is conflicted. 6 Time when the event occurred. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	Send this event when DHCP acquires an IP address conflict with the local configuration
Conditions to clear	Modify static IP or DHCP server, etc.
Effect on business	Failure to configure IP addresses after conflict affects the functions of CMTS, on-line device connection and automatic deployment.
Advised actions	N/A
Marks	N/A

31.4263320834: DHCPv6 IPv6 Address Conflict

Items	Description
Event ID	4263320834
Event Description	Address conflict between DHCPv6 acquired address and locally configured Ipv6 address
Event type	Event

Items	Description
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: Notice 4 Event ID: 4263320834 5 Event Description: CMTS-MAC= cmts ipv6 %d.%d.%d.%d is conflicted. 6 Time when the event occurred. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	DHCP sends this event when it gets IPv6 address conflict with local configuration
Conditions to clear	Modify static IPv6 or DHCPv6 server, etc.
Effect on business	Failure to configure IPv6 addresses after conflict affects the functions of CMTS, on-line device connection and automatic deployment.
Advised actions	N/A
Marks	N/A

32.4263321857: Failure to Upgrade Equipment

Items	Description
Event ID	4263321857
Event Description	Failure to upgrade equipment
Event type	Event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: Error 4 Event ID: 4263321857 5 Event Description: %s. 6 Time when the event occurred. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	Failure to upgrade equipment
Conditions to clear	N/A
Effect on business	N/A
Advised actions	N/A
Marks	N/A

33.4263321858: Successful Upgrade of Equipment

Items	Description
Event ID	4263321858
Event Description	Successful upgrade of equipment
Event type	Event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: Notice

Items	Description
	4 Event ID: 4263321858 5 Event Description: Upgrade the system OK. 6 Time when the event occurred. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	Successful upgrade of equipment
Conditions to clear	N/A
Effect on business	N/A
Advised actions	N/A
Marks	N/A

34.4263322369: Execute Command Successfully

Items	Description
Event ID	4263322369
Event Description	User execute command successfully
Event type	Event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: Info 4 Event ID: 4263322369 5 Event Description: user@address(mode) execute command "{command}" successfully. Mode is telnet/ssh/console; 6 Time when the event occurred. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	User execute command successfully
Conditions to clear	N/A
Effect on business	N/A
Advised actions	N/A
Marks	N/A

35.4263322370: Execute Command Failed

Items	Description
Event ID	4263322370
Event Description	User execute command failed
Event type	Event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: Info 4 Event ID: 4263322370 5 Event Description: user@address(mode) execute command "{command}" failed. Mode is telnet/ssh/console;

Items	Description
	6 Time when the event occurred. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	User execute command failed
Conditions to clear	N/A
Effect on business	N/A
Advised actions	N/A
Marks	N/A

36.4263322371: Reboot the System

Items	Description
Event ID	4263322371
Event Description	Reboot the system
Event type	Event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: Notice 4 Event ID: 4263322371 5 Event Description(one of the following according to different reboot reason): Reboot the system. Sysmoni detect cold boot! Sysmoni detect crash reboot event - The dolmgmt.app has crashed. Sysmoni detect crash reboot event - The dolagent.app has crashed. Sysmoni reboot system for boot event %d desc is %s. 6 Time when the event occurred: System reboot. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	1. Execute **phy** (*epon*|*fiber*|*copper*) 2. Execute **reboot** 3. The system hangup abnormally
Conditions to clear	N/A
Effect on business	The event will lead to the reboot of the system.
Advised actions	N/A
Marks	N/A

37.4263322372: System Power On

Items	Description
Event ID	4263322372
Event Description	System power on
Event type	Normal event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0

Items	Description
	3 Event Level: notice 4 Event ID: 4263322372 5 Event Description: system power on. 6 Time when the event occurred: System power on. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	Reboot the device
Conditions to clear	N/A
Effect on business	Reboot the device
Advised actions	N/A
Marks	N/A

38.4263324673: Zero Touch Failed

Items	Description
Event ID	4263324673
Event Description	Zero Touch failed
Event type	Event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: Notice 4 Event ID: 4263324673 5 Event Description: %s. 6 Time when the event occurred. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	Zero Touch deployment failed to send this event
Conditions to clear	N/A
Effect on business	N/A
Advised actions	N/A
Marks	N/A

39.4263324674: Zero Touch Complete

Items	Description
Event ID	4263324674
Event Description	Zero touch completed
Event type	Event
Event level	Notice
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: Notice 4 Event ID: 4263324674 5 Event Description: Zero-touch

Items	Description
	successfully;CmtsMac=%02x%02x.%02x%02x.%02x%02x;IP=%s;Sn=%s. 6 Time when the event occurred. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	While the zero touch completed with config changing.
Conditions to clear	N/A
Effect on business	N/A
Advised actions	N/A
Marks	N/A

40.4263325185: Failed to Request NTP Server

Items	Description
Event ID	4263325185
Event Description	Failed to request NTP server
Event type	Event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: Notice 4 Event ID: 4263325185 5 Event Description: connect host %s timeout ,ntp server connect fails!. 6 Time when the event occurred. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	The device failed to successfully request NTP synchronization from NTP server
Conditions to clear	Check whether the communication between NTP server and device is normal, whether the configuration of NTP server is normal, etc.
Effect on business	The device cannot synchronize time from the configured NTP server
Advised actions	N/A
Marks	N/A

41.4263329025: MAC Conflict

Items	Description
Event ID	4263329025
Event Description	MAC Conflict
Event type	Event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: Warning 4 Event ID: 4263329025 5 Event Description: MAC conflict, MAC index= %u; early device: <P1>; later device: <P2>. Among them: <P1>, <P2> is <CM-MAC>, <CPE-MAC> or <MAC> (in some cases, the type of equipment can not be determined)

Items	Description
	<CM-MAC>: CM MAC Address; Format*: "CM-MAC = xx: xx: xx: xx: xx: xx: xx" <CPE-MAC>: CPE MAC Address; Format*: "CPE-MAC = xx: xx: xx: xx: xx: xx: xx" <MAC>: MAC Address; Format*: "MAC = xx: xx: xx: xx: xx: xx: xx" 6 Time when the FPGA HASH conflict occurred. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	MAC Conflict in FPGA
Conditions to clear	N/A
Effect on business	New MAC addresses may use old MAC rules, and new MAC rules may not.
Advised actions	N/A
Marks	N/A

42.4263329282: CM Can not Get IPv6 Configuration File

Items	Description
Event ID	4263329282
Event Description	CM can not get Ipv6 configuration file
Event type	Event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: Warning 4 Event ID: 4263329282 6 Event Description: IPv6 Local Provisioning CM configuration file does not exist.CM-MAC = %02x:%02x:%02x:%02x:%02x:%02x; File = %s. 6 Time when the event occurred: System power on. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	The configuration file assigned to CM by Local Provisioning does not exist, or CM requests a configuration file that does not exist.
Conditions to clear	Check whether the IPv6 configuration file allocated by Local Provisioning for CM exists.
Effect on business	The CM in question will not be able to download the configuration file successfully and go online.
Advised actions	N/A
Marks	N/A

43.4263330051: CM Dynamic Service Flow Reject

Items	Description
Event ID	4263330051
Event Description	CM Dynamic service flow reject.
Event type	Event

Items	Description
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: Info 4 Event ID: 4263330051 5 Event Description: Dynamic-service flow failed;us-channel %d;schedule type %s;Ex %.2f;NonEx %.2f;Active-Ex %.2f;Active-NonEx %.2f;gRFNonEx %.2f; 6 Time when the event occurred. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	While the percent of dynamic service flow beyond the threshold of admission control.
Conditions to clear	N/A
Effect on business	N/A
Advised actions	N/A
Marks	N/A

44.4263330052: CM Static Service Flow Warning

Items	Description
Event ID	4263330052
Event Description	CM static service flow warning.
Event type	Event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: Info 4 Event ID: 4263330052 5 Event Description: Cm registration flow too large;us-channel %d;schedule type %s;Ex %.2f;NonEx %.2f;Active-Ex %.2f;Active-NonEx %.2f;gRFNonEx %.2f; 6 Time when the event occurred. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	While the percent of static service flow beyond the threshold of admission control.
Conditions to clear	N/A
Effect on business	N/A
Advised actions	N/A
Marks	N/A

45.4263330561: CM Rejected by the Access List

Items	Description
Event ID	4263330561
Event Description	Zero touch completed
Event type	Event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0

Items	Description
	3 Event Level: Info 4 Event ID: 4263330561 5 Event Description: CMTS-MAC=%02x%02x.%02x%02x.%02x%02x; CM-MAC=%02x%02x.%02x%02x.%02x%02x; Access white-list reject; 6 Time when the event occurred. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	The CM does not access the rule of access list.
Conditions to clear	30 minutes passed while the CM send reject syslog first.
Effect on business	N/A
Advised actions	N/A
Marks	N/A

46.4263331842: Binding Group Flow Out of Overflow Threshold

Items	Description
Event ID	4263331842
Event Description	Binding group flow out of overflow threshold event
Event type	Event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1 3 Event Level: Notice 4 Event ID: 4263331842 5 Event Description: CMTS-MAC: <CmtsMac>; bonding group <bg-id> overflow; current load: 195000Kbps 6 Time when the event occurred: Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	Because users plan too many programs on a dedicated multicast binding group, or the traffic of multicast programs on a shared binding group overlaps with the unicast traffic on the Internet, load balancing has not yet worked.
Conditions to clear	N/A
Effect on business	The experience of watching multicast programs and surfing the Internet is not good.
Advised actions	Optimize multicast programming, or enable load balancing and wait for a while
Marks	N/A

47.4263333121: MAC Conflict Event

Items	Description
Event ID	4263333121
Event Description	MAC conflict event
Event type	Event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0

Items	Description
	3 Event Level: Warning 4 Event ID: 4263333121 5 Event Description:“MAC conflict, MAC index= %u; early device: <P1>; later device: <P2>” <P1>, <P2> is <CM-MAC>, <CPE-MAC> or <MAC> (in some cases, the type of device can not be determined) <CM-MAC>: CM MAC Address; Format*: "CM-MAC = xx: xx: xx: xx: xx: xx: xx" <CPE-MAC>: CPE MAC Address; Format*: "CPE-MAC = xx: xx: xx: xx: xx: xx: xx" <MAC>: MAC Address; Format*: "MAC = xx: xx: xx: xx: xx: xx: xx" 6 Time of alarm: A HASH collision occurs on the FPGA, and the MAC address that is collidedis the current online CM or CPE (including when CPE does not delete the list item after CM is offline) Time when the event occurred: System power on. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	MAC conflicts in FPGA.
Conditions to clear	N/A
Effect on business	New MAC addresses may use old MAC rules, and new MAC rules may not.
Advised actions	N/A
Marks	N/A

48.4263336450: CM Request Profile Authentication Failed

Items	Description
Event ID	4263336450
Event Description	Registration authentication failure
Event type	Event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: Warning 4 Event ID: 4263336450 5 Event Description: CM TFTP Requests discard: Configuration file name authorization failure. <P1> P1 = <CM-MAC>;<CMTS-MAC>;<Learned file>;<Request file> 6 Time when the event occurred: Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	The profile name requested by CM TFTP does not match the profile name specified by DHCP
Conditions to clear	Close TFTP proxy or replace CM
Effect on business	CM failed to get the profile through TFTP, unable to go online
Advised actions	Close TFTP proxy or replace CM
Marks	N/A

49.4263336705: CM Loopback Occured

Items	Description
Event ID	4263336705
Event Description	CM Loopback occured
Event type	Event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: Warning 4 Event ID: 4263336705 5 Event Description: Cable Modem loopback occured.<P1><P2> P1 = <CM-MAC>;<CMTS-MAC>;<Occur time> P2 = Black-list of loopback is full, can not limite this CM. 6 Time when the event occurred: Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	A loopback is generated by CM or the CPE under it.
Conditions to clear	Check the network environment of CM.
Effect on business	CM will form a broadcast storm, affecting its business. It will even affect the business of CMTS and uplink.
Advised actions	After troubleshooting the loopback fault of CM, manually remove the loopback cm blacklist.
Marks	N/A

50.66030400: Failed to retrieve CRL

Items	Description
Event ID	66030400
Event Description	CMTS: Failed to retrieve CRL
Event type	Event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1 3 Event Level: Warning 4 Event ID: 66030400 6 Event Description: Failed to retrieve CRL from<P1> P1 = CRL Server IP 6 Time when the event occurred: System power on. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	Failed to obtain CRL.
Conditions to clear	N/A
Effect on business	It has influence on certificate CRL revocation verification and certificate CRL revocation verification.
Advised actions	N/A
Marks	N/A

51.66030401: Failed to retrieve OCSP status

Items	Description
Event ID	66030401
Event Description	CMTS: Failed to retrieve OCSP status
Event type	Event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1 3 Event Level: Warning 4 Event ID: 66030401 6 Event Description: Failed to retrieve OCSP status 6 Time when the event occurred: System power on. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	OCSP acquisition failed.
Conditions to clear	N/A
Effect on business	OCSP validation affecting certificates.
Advised actions	N/A
Marks	N/A

52.66030402: CRL Data Not Available

Items	Description
Event ID	66030402
Event Description	CMTS: CRL data not available
Event type	Event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1 3 Event Level: Warning 4 Event ID: 66030402 5 Event Description: CRL data not available when validating CM certificate chain<TAGS> 6 Time when the event occurred: System power on. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	CRL is not available for certificate CRL validation.
Conditions to clear	N/A
Effect on business	CRL validation affecting certificates.
Advised actions	N/A
Marks	N/A

53.67030100: DCC-RSP not Receive on Old Channel

Items	Description
Event ID	67030100
Event Description	DCC-RSP not receive on old channel
Event type	Event
Event features	1 System online time

Items	Description
	2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1 3 Event Level: Warning 4 Event ID: 67030100 5 Event Description: DCC-RSP not receive on old channel; CM-MAC: %02x%02x.%02x%02x.%02x%02x;CM-QOS=1.1;CM-VER=2.0; CMTS-VER=3.0; 6 Time when the event occurred: System power on. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	CMTS did not receive DCC-RSP messages from CM over the old channel.
Conditions to clear	N/A
Effect on business	N/A
Advised actions	N/A
Marks	N/A

54.67030200: DCC-RSP not Receive on New Channel

Items	Description
Event ID	67030200
Event Description	DCC-RSP not receive on new channel
Event type	Event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1 3 Event Level: Warning 4 Event ID: 67030200 5 Event Description: DCC-RSP not receive on new channel; CM-MAC: %02x%02x.%02x%02x.%02x%02x;CM-QOS=1.1;CM-VER=2.0; CMTS-VER=3.0; 6 Time when the event occurred: System power on. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	CMTS did not receive DCC-RSP messages from CM on the new channel.
Conditions to clear	N/A
Effect on business	N/A
Advised actions	N/A
Marks	N/A

55.67030300: DCC-RSP Rejected Unspecified Reason

Items	Description
Event ID	67030300
Event Description	DCC-RSP rejected unspecified reason
Event type	Event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1 3 Event Level: Warning

Items	Description
	4 Event ID: 67030300 5 Event Description: DCC-RSP rejected unspecified reason; CM-MAC: %02x%02x.%02x%02x.%02x%02x;CM-QOS=1.1;CM-VER=2.0; CMTS-VER=3.0; 6 Time when the event occurred: System power on. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	CMTS received an unspecified DCC-RSP response from CM.
Conditions to clear	N/A
Effect on business	N/A
Advised actions	N/A
Marks	N/A

56.67030400: DCC-RSP Rejected Unknown Transaction ID

Items	Description
Event ID	67030400
Event Description	DCC-RSP rejected unknown transaction ID
Event type	Event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1 3 Event Level: Warning 4 Event ID: 67030400 5 Event Description: DCC-RSP rejected unknown transaction ID; CM-MAC: %02x%02x.%02x%02x.%02x%02x;CM-QOS=1.1;CM-VER=2.0; CMTS-VER=3.0; 6 Time when the event occurred: System power on. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	CMTS receives DCC-RSP of CM's unknown Transaction ID.
Conditions to clear	N/A
Effect on business	N/A
Advised actions	N/A
Marks	N/A

57.67030500: DCC-RSP Rejected DCC-RSP Rejected Authentication Failure

Items	Description
Event ID	67030500
Event Description	DCC-RSP rejected DCC-RSP rejected authentication failure event
Event type	Event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: Warning 4 Event ID: 67030500 5 Event Description: DCC-RSP rejected DCC-RSP rejected authentication failure

Items	Description
	6 Time when the event occurred: System power on. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	The reported DCC-RSP message was rejected due to authorization failure.
Conditions to clear	N/A
Effect on business	N/A
Advised actions	N/A
Marks	N/A

58.67030600: DCC-RSP Rejected Message Syntax Error

Items	Description
Event ID	67030600
Event Description	DCC-RSP rejected message syntax error event
Event type	Event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: Warning 4 Event ID: 67030600 5 Event Description: DCC-RSP rejected message syntax error 6 Time when the event occurred: System power on. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	The reported DCC-RSP was rejected due to a message grammar error.
Conditions to clear	N/A
Effect on business	N/A
Advised actions	N/A
Marks	N/A

59.67060100: Unknown DBC transaction

Items	Description
Event ID	67060100
Event Description	Unknown DBC transaction
Event type	Event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: Notice 4 Event ID: 67060100 5 Event Description: Unknown DBC transaction 6 Time when the event occurred: System power on. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	The reported DBC-RSP cannot be traced through transaction ID.
Conditions to clear	N/A

Items	Description
Effect on business	N/A
Advised actions	N/A
Marks	N/A

60.67060200: DBC-REQ Eejected Event

Items	Description
Event ID	67060200
Event Description	DBC-REQ rejected event
Event type	Event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: Warning 4 Event ID: 67060200 5 Event Description: DBC-REQ rejected Confirmation code <ConfirmationCode> <Confirmation> 6 Time when the event occurred: System power on. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	The reported DBC-RSP indicates that DBC-REQ was rejected.
Conditions to clear	N/A
Effect on business	N/A
Advised actions	N/A
Marks	N/A

61.67060300: DBC-RSP Not Receive Event

Items	Description
Event ID	67060300
Event Description	DBC-RSP not receive event
Event type	Event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: Warning 4 Event ID: 67060300 5 Event Description: DBC-RSP not receive 6 Time when the event occurred: System power on. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	DBC-RSP could not be received.
Conditions to clear	N/A
Effect on business	N/A
Advised actions	N/A
Marks	N/A

62.67060400: Bad CM DBC-RSP Event

Items	Description
Event ID	67060400
Event Description	Bad CM DBC-RSP event
Event type	Event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: Warning 4 Event ID: 67060400 5 Event Description: Bad CM DBC-RSP <P1="unspecified reason" |"authentication failure" |"msg syntax error"> 6 Time when the event occurred: System power on. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	The reported DBC-RSP has an exception, possibly due to message grammar errors, authorization failures, and other unknown reasons.
Conditions to clear	N/A
Effect on business	N/A
Advised actions	N/A
Marks	N/A

63.67060500: DBC-RSP Partial Service

Items	Description
Event ID	67060500
Event Description	DBC-RSP Partial Service
Event type	Event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: Warning 4 Event ID: 67060500 5 Event Description: DBC-RSP Partial Service 6 Time when the event occurred. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	CM is reported of Partial Service State through DBC-RSP message
Conditions to clear	N/A
Effect on business	N/A
Advised actions	N/A
Marks	N/A

64.73000501: Configuration File TLV Authentication Failed in CM Registration Request

Items	Description
Event ID	73000501
Event Description	Registration authentication failure
Event type	Event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: Warning 4 Event ID: 73000501 5 Event Description: Registration authentication failure: REG REQ rejected -TLV parametersdo not match learned config file TLV parameters .<P1> P1 = <CM-MAC>;<CMTS-MAC> 6 Time when the event occurred. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	The configuration file TLV in the CM registration request is inconsistent with the configuration file learned by CMTS.
Conditions to clear	Close TFTP proxy or replace CM
Effect on business	CM failed to register on CMTS, unable to go online
Advised actions	Close TFTP proxy or replace CM
Marks	N/A

65.73010800: CM Link Address not Conform to EUI-64 Format

Items	Description
Event ID	73010800
Event Description	CM link address does not conform to EUI-64 format
Event type	Event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: Warning 4 Event ID: 73010800 6 Event Description: Network Access has Invalid Parameter.<P1> P1 = <CM-MAC>;<CM-QOS>;<CM-VER>;<CMTS-VER> 6 Time when the event occurred: System power on. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	CM link address does not conform to EUI-64 format
Conditions to clear	CM should update software or generate link addresses in EUI-64 format
Effect on business	CM can't get IPv6 address properly
Advised actions	N/A
Marks	N/A

66.73055400: REG-ACK TCS Partial Service

Items	Description
Event ID	73055400
Event Description	REG-ACK partial service of TCS
Event type	Event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: Notice 4 Event ID: 73055400 5 Event Description: Received REG-ACK with TCS - Partial Service 6 Time when the event occurred. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	CM is reported of TCS Partial Service State through REG-ACK message
Conditions to clear	N/A
Effect on business	N/A
Advised actions	N/A
Marks	N/A

67.73055500: REG-ACK RCS Partial Service

Items	Description
Event ID	73055500
Event Description	REG-ACK partial service of RCS
Event type	Event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: Notice 4 Event ID: 73055500 5 Event Description: Received REG-ACK with RCS - Partial Service 6 Time when the event occurred. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	CM is reported of RCS Partial Service State through REG-ACK message
Conditions to clear	N/A
Effect on business	N/A
Advised actions	N/A
Marks	N/A

68.75010100: Service Flow Assign Fail Event

Items	Description
Event ID	75010100
Event Description	Service Flow Assign Fail Event
Event type	Event
Event features	1 System online time

Items	Description
	2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: Notice 4 Event ID: 75010100 5 Event Description: Attribute Masks for SF(SFID < SFID >) do not satisfythose in the SCN < SCN > 6 Time when the event occurred. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	Service Flow match the bonding group or the channel.
Conditions to clear	N/A
Effect on business	N/A
Advised actions	N/A
Marks	N/A

69.82010300: CM Rang Fail Event

Items	Description
Event ID	82010300
Event Description	CM rang fail event
Event type	Event
Event features	1 System online time 2 Event OID: 1.3.6.1.4.1.4491.2.1.20.0.1.0 3 Event Level: Warning 4 Event ID: 82010300 5 Event Description: Unable to Successfully Rang CM Retries Exhausted< CM-MAC >! 6 Time when the event occurred. Example: Jan 01 1970 01:09:03 7 System Name: BT
Causes	CM rang fail, abort.
Conditions to clear	N/A
Effect on business	N/A
Advised actions	N/A
Marks	N/A