ZXA10 C320

Optical Access Convergence Equipment

Configuration Manual (CLI)

Version: V1.2.5

ZTE CORPORATION
No. 55, Hi-tech Road South, ShenZhen, P.R.China
Postcode: 518057
Tel: +86-755-26771900
Fax: +86-755-26770801
URL: http://support.zte.com.cn
E-mail: support@zte.com.cn

LEGAL INFORMATION

Revision History

Revision No.	Revision Date	Revision Reason
R1.0	2013-03-31	First edition

Serial Number: SJ-20130306113233-005

Publishing Date: 2013-03-31 (R1.0)

Contents

About This Manual

Purpose

The ZXA10 C320 Optical Access Convergence Equipment (ZXA10 C320 for short) is a 2U-height OLT device, which satisfies the market requirement for small-capacity OLTs.

This manual provides detailed information about configurations (CLI) on the ZXA10 C320 Optical Access Convergence Equipment.

Intended Audience

This document is intended for:

- Installation and debugging engineer
- System maintenance engineer
- Data configuration engineer

What Is in This Manual

This manual contains the following chapters:

Chapter	Summary
1, Basic Configuration	Describes basic configuration.
2, GPON Service Configuration	Describes GPON service configuration.
3, GPON Service Configuration in Profile Mode	Describes GPON service configuration in profile mode.
4, EPON Service Configuration	Describes EPON service configuration.
5, P2P Service Configuration	Describes P2P service configuration.
6, VLAN Configuration	Describes VLAN configuration.
7, IPTV Configuration	Describes IPTV configuration.
8, QoS Configuration	Describes QoS configuration.
9, ACL Configuration	Describes ACL configuration.
10, ONU Version Upgrade	Describes ONU version remote upgrade.
11, NTP Configuration	Describes NTP configuration.
12, STP Configuration	Describes STP configuration.
13, DHCP Configuration	Describes DHCP configuration.
14, Uplink Protection Configuration	Describes uplink protection configuration.
15, PON Protection Configuration	Describes PON protection configuration.

Chapter	Summary
16, Access Security Configuration	Describes access security configuration.
17, System Security Configuration	Describes system security configuration.
18, Route Protocol Configuration	Describes route protocol configuration.
19, Clock Configuration	Describes clock configuration.

Conventions

This manual uses the following typographical conventions:

Typeface	Meaning
	Note: provides additional information about a certain topic.

Chapter 1
Basic Configuration

Table of Contents

1.1 Management Methods

The ZXA10 C320 supports the following management methods:

- Login Through HyperTerminal

  Before configuring the in-band or out-of-band NM, you can manage the ZXA10 C320 through HyperTerminal.

- Login Through Telnet

  After configuring the in-band or out-of-band NM (see 1.2 NM Configuration), you can manage the ZXA10 C320 through Telent.

- Login Through NMS

  After configuring the in-band or out-of-band NM, you can manage the ZXA10 C320 through NMS.

This manual describes the CLI configuration after login through HyperTerminal or Telnet.

1.1.1 Login Through HyperTerminal

Perform this procedure to log in to the ZXA10 C320 through HyperTerminal.

Context

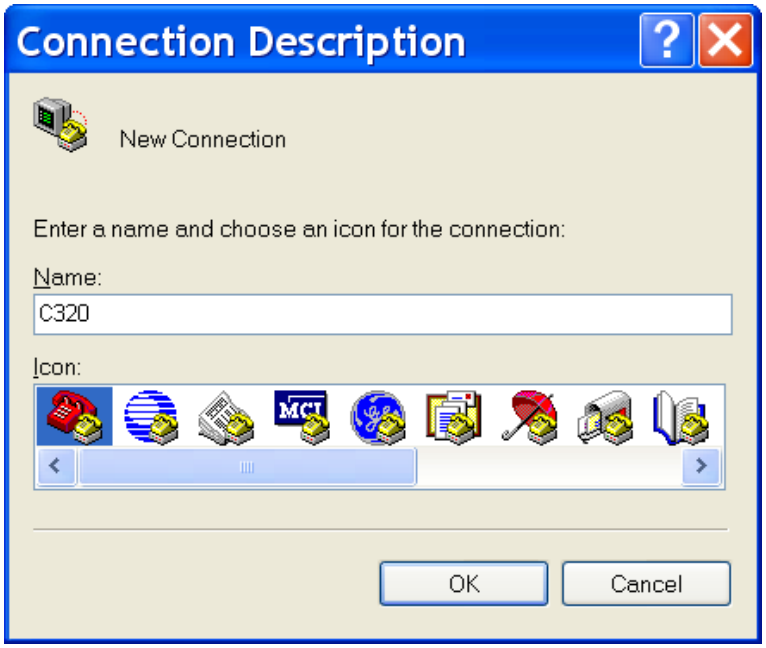
When you log in to the ZXA10 C320 through HyperTerminal, the user name and password are case-sensitive.

This topic takes the Windows XP operating system as the example.

Steps

1. In Windows XP, click **Start > All Programs > Accessories > Communications > HyperTerminal**. The **Connection Description** dialog box is displayed, see Figure 1-1.

Figure 1-1 Connection Description

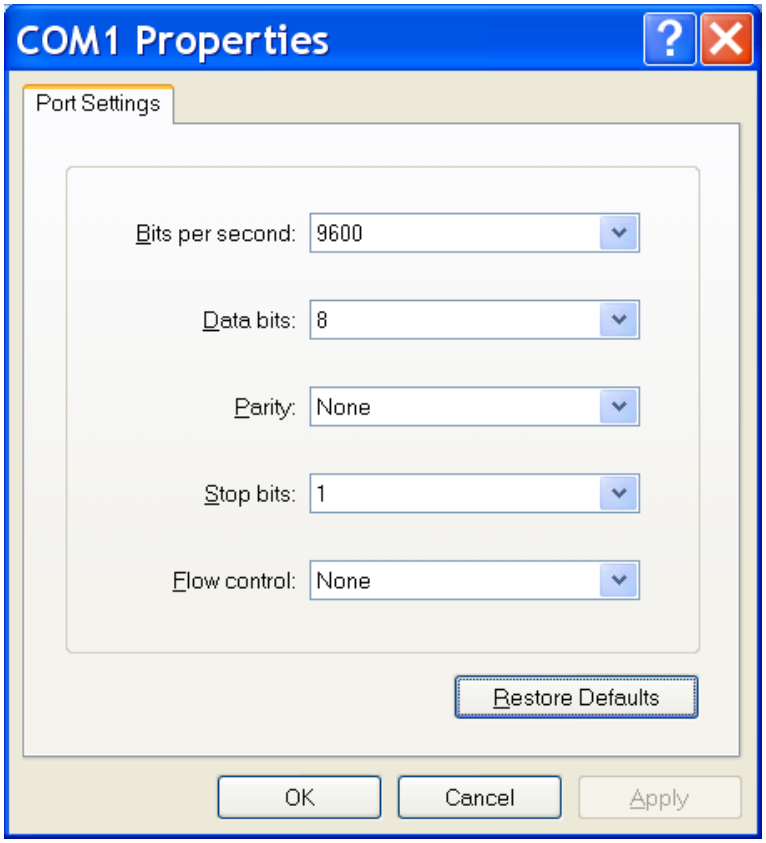


2. Fill in **Name** and click **OK**. The **Connect To** dialog box is displayed, see Figure 1-2.

Figure 1-2 Connect To

3. Select **COM1** or **COM2**, and then click **OK**. The **COM1 Properties** (or **COM2 Properties**) dialog box is displayed.
4. Click **Restore Defaults**, see Figure 1-3, and then click **OK**.

Figure 1-3 COM1 Properties



5. If the system runs properly, the **HyperTerminal** window is displayed. The system enters `ZXAN>` mode. Enter the **enable** command and the password `zxr10` to enter administrator mode (ZXAN#), as shown below.

```
**********************************************
Welcome to ZXAN product C320 of ZTE Corporation
**********************************************
ZXAN>enable
Password:
ZXAN#
```

– End of Steps –

1.1.2 Login Through Telnet

Perform this procedure to log in to the ZXA10 C320 through Telnet.

Prerequisite

Before this operation, make sure that:

- The in-band or out-of-band NM IP address is configured.
- The Telnet computer successfully pings the in-band or out-of-band NM IP address.

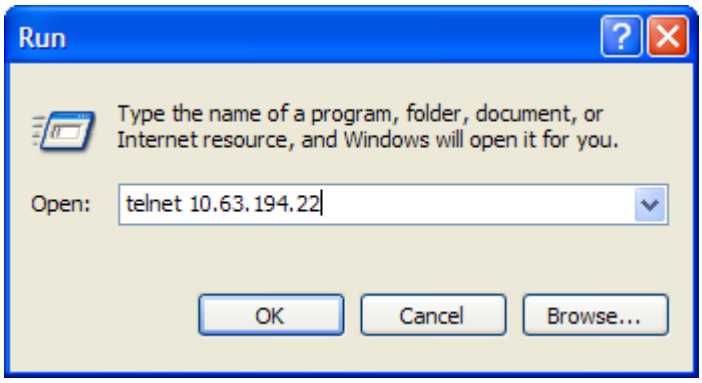
Context

When you log in to the ZXA10 C320 through Telnet, the user name and password are case-sensitive.

Steps

1. In Windows, click **Start > Run** to display the **Run** dialog box, see Figure 1-4.

Figure 1-4 Run Dialog Box



2. In the dialog box, enter `Telnet x.x.x.x`, where, `x.x.x.x` is the NE IP address. Click **OK** to start the Telnet client.
3. If the connection is proper, the login dialog box is displayed. Enter the user name and password (both are `zte` by default) to access administrator mode (ZXAN#), as shown below.

```
**********************************************
Welcome to ZXAN product C320 of ZTE Corporation
**********************************************

Username:zte
Password:
ZXAN#
```

– End of Steps –

1.1.3 Login Through NMS

Before logging in to the device through the NMS, install the SQL Server database and the NetNumen U31 NMS software.

To log in to the NMS, start the SQL Server database, NMS server, and NMS client.

After creating the ZXA10 C320 NE, you can manage the ZXA10 C320 through the NMS.

1.2 NM Configuration

The ZXA10 C320 supports in-band NM and out-of-band NM.

- In in-band NM mode, the ZXA10 C320 accesses the IP network via the service channel (uplink port) to transmit NM information. The in-band NM mode is usually used in practical engineering.
- In out-of-band NM mode, the ZXA10 C320 accesses the NMS via the **10/100M** port on the switching and control card. The non-service channel is used to transmit the management information so that the management channel and service channel are separated. The out-of-band NM mode is usually used in local management and maintenance.

1.2.1 Configuring the In-Band NM

In in-band NM mode, the NM information is transmitted via the service channel of the equipment. The in-band NM mode supports flexible networking and requires no additional equipment.

Prerequisite

Before this operation, make sure that you have logged in to the ZXA10 C320 through HyperTerminal and entered administrator mode.

Configuration Data

Table 1-1 lists the configuration data of the in-band NM.

Table 1-1 Configuration Data of the In-Band NM

Item	Data
Uplink port	gei_1/3/1
In-band NM VLAN	VLAN ID: 1000
In-band NM IP address	10.1.1.1/24
Next hop IP address	10.1.1.254/24
NM server (SNMP server)	IP address: 10.2.1.1/24 Version: V2C Community name: public Alarm level: NOTIFICATIONS

Steps

1. Enter global configuration mode.

```
ZXAN#configure terminal
Enter configuration commands, one per line.  End with CTRL/Z.
ZXAN(config)#
```

2. Add the uplink port to the in-band NM VLAN.

```
ZXAN(config)#interface gei_1/3/1
ZXAN(config-if)#switchport vlan 1000 tag
ZXAN(config-if)#exit
```

NOTE **Note:**

When you use the **switchport vlan** command to configure the port VLAN, the system automatically creates the VLAN.

3. Configure the in-band NM IP address.

```
ZXAN(config)#interface vlan 1000
ZXAN(config-if)#ip address 10.1.1.1 255.255.255.0
ZXAN(config-if)#exit
```

NOTE **Note:**

The out-of-band and in-band NM IP addresses cannot be in the same network segment.

4. Configure the in-band NM route.

```
ZXAN(config)#ip route 10.2.1.0 255.255.255.0 10.1.1.254
```

5. Configure the SNMP community name.

```
ZXAN(config)#snmp-server community public view allview rw
```

NOTE **Note:**

The SNMP community name should be consistent with that on the NMS.

6. Configure the IP address of the SNMP server (trap server).

```
ZXAN(config)#snmp-server host 10.2.1.1 trap version 2c public enable NOTIFICA
TIONS server-index 1
```

NOTE **Note:**

The ZXA10 C320 supports up to eight SNMP servers and supports third-party NMSs.

7. Save the configuration data.

```
ZXAN(config)#exit
ZXAN#write
```

– End of Steps –

1.2.2 Configuring the Out-of-Band NM

In out-of-band NM mode, the non-service channel is used to transmit the management information so that the management channel and service channel are separated. Compared with the in-band NM mode, the out-of-band NM mode provides more reliable equipment management channel. When the ZXA10 C320 is faulty, the network equipment information can be located in time and monitored in real time.

Prerequisite

You have logged in to the ZXA10 C320 through HyperTerminal and entered administrator mode.

Configuration Data

Table 1-2 lists the configuration data of the out-of-band NM.

Table 1-2 Configuration Data of the Out-of-Band NM

Item	Data
Out-of-band NM IP address	11.1.1.1/24
Next hop IP address	11.1.1.254/24
NM server (SNMP server)	IP address: 10.2.1.1/24 Version: V2C Community name: public Alarm level: NOTIFICATIONS

Steps

1. Enter global configuration mode.

```
ZXAN#configure terminal
Enter configuration commands, one per line.  End with CTRL/Z.
ZXAN(config)#
```

2. Configure the out-of-band NM IP address.

```
ZXAN(config)#interface mng1
ZXAN(config-if)#ip address 11.1.1.1 255.255.255.0
ZXAN(config-if)#exit
```

NOTE **Note:**

The out-of-band and in-band NM IP addresses cannot be in the same network segment.

3. Configure the out-of-band NM route.

```
ZXAN(config)#ip route 10.2.1.0 255.255.255.0 11.1.1.254
```

4. Configure the SNMP community name.

```
ZXAN(config)#snmp-server community public view allview rw
```

NOTE **Note:**

The SNMP community name should be consistent with that on the NMS.

5. Configure the IP address of the SNMP server (trap server).

```
ZXAN(config)#snmp-server host 10.2.1.1 trap version 2c public enable NOTIFICA
TIONS server-index 1
```

NOTE **Note:**

The ZXA10 C320 supports up to eight SNMP servers and supports third-party NMSs.

6. Save the configuration data.

```
ZXAN(config)#exit
ZXAN#write
```

– End of Steps –

1.3 Physical Configuration

The ZXA10 C320 physical configuration includes the following topics:

- Adding a Rack
- Adding a Shelf
- Adding a Daughter-Card
- Adding a Card
- Showing Cards
- Enabling the PnP Function
- Deleting a Daughter-Card
- Deleting a Card
- Resetting a Card
- Swapping the Active/Standby Switching and Control Cards
- Configuring Fans

1.3.1 Adding a Rack

When commissioning the ZXA10 C320, you need to add a rack.

Steps

1. Enter global configuration mode.

```
ZXAN#configure terminal
Enter configuration commands, one per line.  End with CTRL/Z.
ZXAN(config)#
```

2. Add the rack.

```
ZXAN(config)#add-rack rackno 1 racktype C320Rack
```

3. (Optional) Query the rack configuration.

```
ZXAN(config)#show rack
Rack   RackType        SupShelfNum   CfgShelfNum
-----------------------------------------------
1      C320Rack        1             1
```

NOTE **Note:**

'SupShelfNum' is the maximum shelf number supported by the rack.

– End of Steps –

1.3.2 Adding a Shelf

When commissioning the ZXA10 C320, you need to add a shelf in a rack.

Prerequisite

The rack has been added.

Steps

1. Enter global configuration mode.

```
ZXAN#configure terminal
Enter configuration commands, one per line.  End with CTRL/Z.
ZXAN(config)#
```

2. Add the shelf.

```
ZXAN(config)#add-shelf shelfno 1 shelftype C320_SHELF
```

3. (Optional) Query the shelf configuration.

```
ZXAN(config)#show shelf
Rack   Shelf   ShelfType    ConnectId    CleiCode     Serial-Number
-------------------------------------------------------------------
1      1       C320_SHELF   0            UnKnowCleiCode
```

– End of Steps –

Result

After the shelf is added, the system will automatically add two switching and control cards.

```
ZXAN(config)#show card
Rack Shelf Slot CfgType RealType Port  HardVer SoftVer         Status
------------------------------------------------------------------------------
1    1     3    SMXA    SMXA     0     110702  V1.2.5          INSERVICE
1    1     4    SMXA    SMXA     0     110702  V1.2.5          STANDBY
```

1.3.3 Adding a Daughter-Card

The switching and controls cards use uplink daughter-cards to provides two optical uplink interfaces.

Context

The ZXA10 C320 supports four types of uplink daughter cards.

- UCDC/1: provides two GE optical interfaces.
- UCDC/2: provides one GE optical interface (1) and one 10GE optical interface (2).
- UCDC/3: provides one GE optical interface (1) and one 10GE optical interface (2).
- UCDC/4: provides two GE optical interfaces.

Steps

1. Enter global configuration mode.

```
ZXAN#configure terminal
Enter configuration commands, one per line. End with CTRL/Z.
ZXAN(config)#
```

2. Add daughter-cards.

```
ZXAN(config)#add-subcard slotno 3 subcardno 1 UCDC/1
ZXAN(config)#add-subcard slotno 4 subcardno 1 UCDC/1
```

3. (Optional) Query the daughter-card configuration.

```
ZXAN(config)#show subcard
Rack Shelf Slot Sub CfgType RealType Status
------------------------------------------------------------------------------
1    1     3    1   UCDC/1  UCDC/1   INSERVICE
1    1     4    1   UCDC/1  UCDC/1   INSERVICE
```

Table 1-3 describes the daughter-card status.

Table 1-3 Daughter-Card Status Description

Status	Description
INSERVICE	The daughter-card is working normally.
HWONLINE	The daughter-card of incorrect version is inserted into the shelf so that it does not run normally.

Status	Description
OFFLINE	The daughter-card is added but is offline.
TYPEMISMATCH	The daughter-card type is different from the configured type.

– End of Steps –

1.3.4 Adding a Card

When replacing the card type during commissioning or capacity expansion, you need to add a card or cards.

Steps

1. Enter global configuration mode.

```
ZXAN#configure terminal
Enter configuration commands, one per line. End with CTRL/Z.
ZXAN(config)#
```

2. Add cards.

```
ZXAN(config)#add-card slotno 1 ETGO
ZXAN(config)#add-card slotno 2 ETGH
```

3. (Optional) Query the card configuration.

```
ZXAN(config)#show card
Rack Shelf Slot CfgType RealType Port  HardVer SoftVer         Status
--------------------------------------------------------------------------------
1    1     1    ETGO    ETGOB    8     090500  V1.2.5          INSERVICE
1    1     2    ETGH    ETGHG    16    111201  V1.2.5          INSERVICE
1    1     3    SMXA    SMXA     0     110702  V1.2.5          INSERVICE
1    1     4    SMXA    SMXA     0     110702  V1.2.5          STANDBY
```

– End of Steps –

1.3.5 Showing Cards

The card information includes slot number, card type, number of ports, hardware version, software version, and status.

Context

Table 1-4 describes the card status of the ZXA10 C320.

Table 1-4 Card Status Description

Status	Description
INSERVICE	The card is working normally.
CONFIGING	The card is being configured.

Status	Description
CONFIGFAILED	The service configuration for the card fails.
DISABLE	The card is added and is online, but the system fails to receive the card information.
HWONLINE	The card of incorrect version is inserted into the shelf so that it does not run normally.
OFFLINE	The card is added but is offline.
STANDBY	The card is in standby state.
TYPEMISMATCH	The card type is different from the configured type.
NOPOWER	The power card is not powered on.

Steps

1. Query all the cards.

```
ZXAN(config)#show card
Rack Shelf Slot CfgType RealType Port  HardVer SoftVer         Status
------------------------------------------------------------------------------
1    1     1    ETGO    ETGOB    8     090500  V1.2.5          INSERVICE
1    1     2    ETGH    ETGHG    16    111201  V1.2.5          INSERVICE
1    1     3    SMXA    SMXA     0     110702  V1.2.5          INSERVICE
1    1     4    SMXA    SMXA     0     110702  V1.2.5          STANDBY
```

2. Query a certain card.

```
ZXAN(config)#show card slotno 3
Config-Type    : SMXA      Status              : INSERVICE
Real-Type      : SMXA      Serial-Number       : 266650100016
Port-Number    : N/A       BootROM-VER         : V1.2.3P3  2013-02-17 14:41:00
PCB-VER        : 110702    Software-VER        : V1.2.5  2013-03-13 00:28:20
Cpld-VER       : V1.5
Phy-Mem-Size   : 1024MB    Main-CPU            : PowerPC Processor
Cpu-Usage      : 6%        Cpu-Alarm-Threshold : 100%
Mem-Usage      : 28%       Mem-Alarm-Threshold : 100%
Uptime         : 0 Day , 5 Hours , 31 Minutes , 22 Second
Subcard 1  :
Config-Type    : UCDC/1              Real-Type    : UCDC/1
Status         : INSERVICE           Port-Nummber : 0
```

– End of Steps –

1.3.6 Enabling the PnP Function

The ZXA10 C320 supports the plug and play (PnP) function of the card. By default, the PnP function of the ZXA10 C320 is disabled.

Steps

1. In global configuration mode, enable the PnP function.

```
ZXAN#configure terminal
Enter configuration commands, one per line.  End with CTRL/Z.
ZXAN(config)#set-pnp enable
```

2. (Optional) Query the PnP status.

```
ZXAN#show pnp
pnp function is enable.
```

NOTE **Note:**

3. (Optional) Query the card configuration.

```
ZXAN(config)#show card
Rack Shelf Slot CfgType RealType Port  HardVer SoftVer         Status
-------------------------------------------------------------------------------
1    1     1    ETGO    ETGOB    8     090500  V1.2.5          INSERVICE
1    1     2    ETGH    ETGHG    16    111201  V1.2.5          INSERVICE
1    1     3    SMXA    SMXA     0     110702  V1.2.5          INSERVICE
1    1     4    SMXA    SMXA     0     110702  V1.2.5          STANDBY
```

– End of Steps –

1.3.7 Deleting a Daughter-Card

When replacing a daughter-card with another daughter-card of different type, you need to delete the existing daughter-card before adding a new daughter-card.

Steps

1. Enter global configuration mode.

```
ZXAN#configure terminal
Enter configuration commands, one per line. End with CTRL/Z.
ZXAN(config)#
```

2. Delete the daughter-card.

```
ZXAN(config)#del-subcard slotno 4 subcardno 1
Confirm to delete subcard? [yes/no]:y
```

3. (Optional) Query the daughter-card configuration.

```
ZXAN(config)#show subcard
Rack Shelf Slot Sub CfgType RealType Status
-------------------------------------------------------------------------------
```

```
1    1     3    1    UCDC/1  UCDC/1   INSERVICE
```

– End of Steps –

1.3.8 Deleting a Card

When replacing a card with another card of different type, you need to delete the existing card before adding a new card.

Steps

1. Enter global configuration mode.

```
ZXAN#configure terminal
Enter configuration commands, one per line. End with CTRL/Z.
ZXAN(config)#
```

2. Delete the card.

```
ZXAN(config)#del-card slotno 2
If the card is deleted, the service data related to the card will also be delete
d. Do you want to delete the card? [yes/no]:y
```

3. (Optional) Query the card configuration.

```
ZXAN(config)#show card
Rack Shelf Slot CfgType RealType Port  HardVer SoftVer         Status
------------------------------------------------------------------------------
1    1     1    ETGO    ETGOB    8     090500  V1.2.5          INSERVICE
1    1     3    SMXA    SMXA     0     110702  V1.2.5          INSERVICE
1    1     4    SMXA    SMXA     0     110702  V1.2.5          STANDBY
```

– End of Steps –

1.3.9 Resetting a Card

You can reset the card to rectify a fault or clear an alarm. For example, when the ZXA10 C320 reports an "abnormal card state" alarm, you can clear the alarm by resetting the card.

Steps

1. In administrator mode, reset the card.

```
ZXAN#reset-card slotno 2
Confirm to reset card? [yes/no]:y
```

– End of Steps –

1.3.10 Swapping the Active/Standby Switching and Control Cards

When the active switching and control card is faulty, you can switch the service to the standby switching and control card to ensure normal service by swapping the active and standby switching and control cards.

Steps

1. In administrator mode, swap the active and standby switching and control cards.

```
ZXAN#swap
Confirm to master swap? [yes/no]:y
```

Note:

You can also swap the active and standby switching and control cards through the following methods:

- Pull out the active switching and control card.
- Press the **RST** button on the active switching and control card.

– End of Steps –

1.3.11 Configuring Fans

This section describes how to configure the fan parameters, such as working mode, speed, and temperature threshold.

Context

The ZXA10 C320 supports configuration of the following fan parameters:

- Working mode
  - → Automatic temperature-control mode
  - → Fixed-speed mode
- Fan speed level

  The options are 0 – 4. This parameter is valid only when the fans are in fixed-speed working mode.
- Fan speed percent

  The fan speed is the maximum fan speed multiplied with the fan speed percent.
- High-temperature threshold

  When the ambient temperature is higher than the high-temperature threshold, the ZXA10 C320 reports a high-temperature alarm and disables the interface card. When the ambient temperature is lower than the high-temperature threshold, the ZXA10 C320 enables the interface card again.

Steps

1. In global configuration mode, configure the fan working mode.

```
ZXAN(config)#fan control temp_level 30 40 50 60
```

Note:

The ZXA10 C320 supports four temperature levels.

You can use the **fan control fixed-speed** command to set fixed-speed working mode, and then use the **fan speed** command to set the fan speed level.

2. Configure the speed percent of each level.

```
ZXAN(config)#fan speed-percent-set 30 45 60 80
```

3. Configure the high-temperature threshold.

```
ZXAN(config)#fan high-threshold 70
```

4. (Optional) Query the fan configuration.

```
ZXAN(config)#show fan
FanControlType               : temperature-control
TemperatureThreshold         : 30  40  50  60 (Celsiur scale)
FanSpeedLevelPercent         : 30%  45%  60%  80%
HighTemperatureThreshold     : 70 (Celsiur scale)
Environment Temperature      : 37 (Celsiur scale)
HighTemperatureProtection    : Threshold  : N/A.(Celsius scale)
                               RestartTime: N/A.(Minute)
Upper Fanboard Status        : online
Filter Status                : normally
Fan SN                       : Invalid.
System Power                 : 123(Watt)
Fan Epm                      : Disable

All fan status:

Upper Fan Tray
-----------------------------------------
fan       Speed
-----------------------------------------
1         0
2         0
-----------------------------------------
```

– End of Steps –

1.4 Configuring the System Time

After the system time is configured, you can query CLI logs and alarms logs in specific time for troubleshooting.

Context

The ZXA10 C320 software maintains the system time. When the NE is powered on, the system acquires the hardware clock and initializes the system time of the NE.

Steps

1. In global configuration mode, configure the time zone.

```
ZXAN(config)#clock timezone utc 8
ZXAN(config)#exit
```

2. In administrator mode, configure the system time.

```
ZXAN#clock set 08:00:00 mar 7 2011
```

3. (Optional) Query the system time.

```
ZXAN#show clock
08:01:55  Mon  Mar 7  2011  utc
```

– End of Steps –

1.5 User Management

Users (operators) refer to the personnel who manage and maintain the ZXA10 C320 after logging in to it through CLI terminals, including console port, telnet, or security shell (SSH).

The user management defines 16 privilege levels (0 – 15). Table 1-5 describes user privileges.

Table 1-5 User Privilege Description

Privilege Level	Description
0–1	When the user logs in and enters operator mode, he can type the **enable** command and the password to enter privilege mode (privilege level is 15), and uses any commands.
2–9	When the user logs in and enters the administrator mode, he can use the commands of level 0 – 9.
10–15	When the user logs in and enters the administrator mode, he can use the commands of level 0 – 15. The user can manages user accounts.

- A user whose privilege level is 0 can only use the commands of level 0.
- A user whose privilege level is 1 can only use the commands of level 0–1.
- A user whose privilege level is 2 can only use the commands of level 0–2, and so on.
- A user whose privilege level is 15 can only use the commands of level 0–15.

1.5.1 Adding a User

When you add a user, you need to configure user properties, including the user name, password and privilege.

Context

Only the user whose privilege is 10 – 15 can add other users. Table 1-6 describes user properties.

Table 1-6 User Properties Description

Property	Description
Username	1 – 16 printable characters (no space), case sensitive The user name must be unique on the ZXA10 C320.
Password	1 – 16 characters, case sensitive
Max-session	Maximum session number, 1 – 16
Privilege	0 – 15

The ZXA10 C320 supports maximum 20 users.

The default user on the ZXA10 C320 is zte, whose password is zte, and the privilege is 15.

Steps

1. Enable the password-encryption function.

```
ZXAN(config)#service password-encryption
```

2. Add a user.

```
ZXAN(config)#username abc password abc privilege 10
```

3. (Optional) Query the user configuration.

```
ZXAN(config)#show username
Username          Password                 Privilege          Max-sessions
zte               dnXspUMqxfJOgln2Hm7Olw== supervisor         16
abc               kAFQmDzST7DWlj99KOF/cg== administrator      16
```

NOTE **Note:**

When the password-encryption function is enabled before you add a user , the displayed password is encrypted one.

– End of Steps –

1.5.2 Modifying a User

It is recommended to modify user password and privilege in time to ensure the security.

Context

Only the user whose privilege is 15 can modify other users.

Steps

1. Modify the user password and privilege.

```
ZXAN(config)#username abc password 123 privilege 15
```

2. (Optional) Query the user configuration.

```
ZXAN(config)#show username
Username          Password                 Privilege          Max-sessions
zte               dnXspUMqxfJOgln2Hm7Olw== supervisor         16
abc               ICy5YqxZB1uWSwcVLSNLcA== supervisor         16
```

– End of Steps –

1.5.3 Deleting a User

It is recommended to delete idle users to ensure the security.

Context

Only the user whose privilege is 15 can delete other users.

Steps

1. Delete the user.

```
ZXAN(config)#no username abc
```

2. (Optional) Query the user configuration.

```
ZXAN(config)#show username
Username          Password                 Privilege          Max-sessions
zte               dnXspUMqxfJOgln2Hm7Olw== supervisor         16
```

– End of Steps –

1.5.4 Disconnecting an Online User

When the number of online users reaches the limit, you can disconnect the specific online user.

Context

Only the user whose privilege is 5 – 15 can disconnect online users.

Steps

1. Query the online users.

```
ZXAN#show users
   Line      User         Idle        Server(s)           Client
   0  con 0               00:41:57    self
   66 vty 0  zte          00:25:25    self                10.60.183.147
 * 67 vty 1  zte          00:00:00    self                10.60.138.40
```

2. Query the TCP connections.

```
ZXAN#show tcp brief
TCB             Local Address             Foreign Address           State
955965472       10.63.196.232.23          10.60.138.40.2202         ESTAB
955962928       10.63.196.232.23          10.60.183.147.2128        ESTAB
```

3. Disconnect the online user.
   - Disconnect the online user by teletypewriter (TTY) line.

     ```
     ZXAN#clear tcp line 66
     ```

   - Disconnect the online user by IP address.

     ```
     ZXAN#clear tcp connect 10.63.196.232 23 10.60.138.40 2202
     ```

– End of Steps –

Chapter 2
GPON Service Configuration

The Gigabit Passive Optical Network (GPON) access is a flexible access technology that provides super bandwidth access in both broadband and narrowband service environments. It supports multiple rate modes and uses a single optical fiber to provide the subscriber with the voice, data, and video services.

Figure 2-1 shows the GPON service networking diagram.

Figure 2-1 GPON Service Networking Diagram

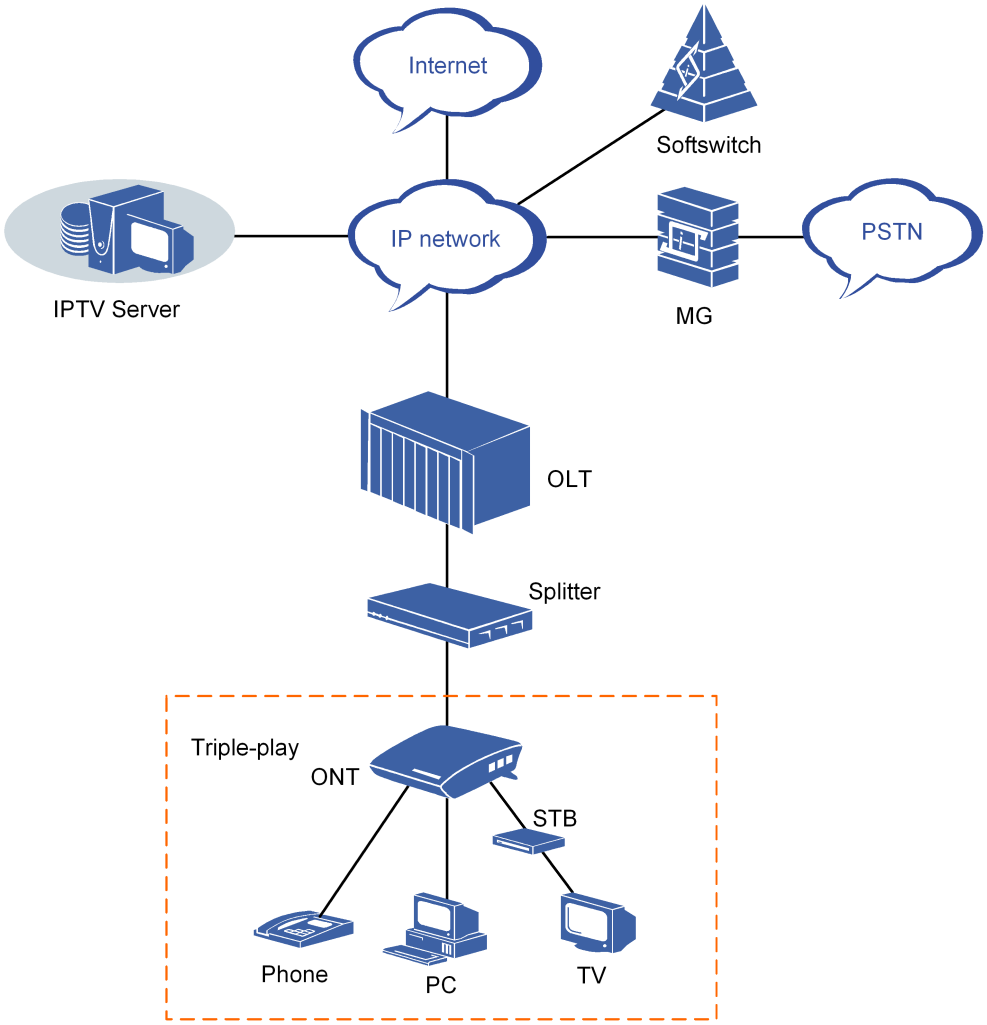


Table of Contents

2.1 Configuring the GPON ONU Type Profile

Before authenticating the GPON optical network unit (ONU), you need to create an ONU type profile if the ONU type does not exist.

Context

The ZXA10 C320 supports the following default GPON ONU types.

- ZTE-F601
- ZTE-F621
- ZTE-F622
- ZTE-F625
- ZTE-F628
- ZTE-F640
- ZTE-F641
- ZTE-F660

On the ZXA10 C320, ZTE-9806, ZTE-F822, and ZTE-F820 are EPON ONU types. If you need to configure the corresponding GPON ONU type, use ZTEG-9806H, ZTEG-F822, and ZTEG-F820 respectively.

You can use the **show onu-type gpon** command to query the default GPON ONU types.

Configuration Data

Table 2-1 lists the configuration data of the GPON ONU type.

Table 2-1 Configuration Data of the GPON ONU Type

Item	Data
ONU type	ZTEG-F620
ONU description	4FE, 2POTS
Maximum T-CONT	7
Maximum number of GEM ports	32

Item	Data
Maximum number of switch units per slot	1
Maximum number of flows per switch unit	32
Number of user ports	ETH: 4 POTS: 2

Steps

1. Enter global configuration mode.

```
ZXAN#configure terminal
Enter configuration commands, one per line. End with CTRL/Z.
ZXAN(config)#
```

2. In PON configuration mode, create an ONU type profile.

```
ZXAN(config)#pon
ZXAN(config-pon)#onu-type ZTEG-F620 gpon description 4FE,2POTS max-tcont 7
max-gemport 32 max-switch-perslot 1 max-flow-perswitch 32
```

NOTE **Note:**

On the ZXA10 C320, the GPON and EPON ONU types must be different.

3. Configure the user port of the ONU type.

```
ZXAN(config-pon)#onu-type-if ZTEG-F620 eth_0/1-4
ZXAN(config-pon)#onu-type-if ZTEG-F620 pots_0/1-2
```

4. (Optional) Query the configured ONU type profile.

```
ZXAN(config-pon)#show onu-type gpon ZTEG-F620

Onu type name :          ZTEG-F620
Pon type :               gpon
Description :            4FE,2POTS
Max tcont :              7
Max gemport :            32
Max switch per slot :    1
Max flow per switch :    32
Max iphost :             2
Service ability N:1 :    support
Service ability 1:M :    support
Service ability 1:P :    support
WiFi mgmt via non OMCI :    disable
Omci send mode :         async
```

```
Default multicast range: none
```

– End of Steps –

2.2 Authenticating the GPON ONU

Before configuring its services, you need to authenticate the GPON ONU that is online for the first time.

Prerequisite

The GPON ONU type profile has been configured by default or manually.

Configuration Data

Table 2-2 lists the configuration data for GPON ONU authentication.

Table 2-2 Configuration Data for GPON ONU Authentication

Item	Data
ONU ID	1
ONU type	ZTEG-F620
SN	ZTEG00000002

Steps

1. Query the unauthenticated ONU.

```
ZXAN(config)#show gpon onu uncfg gpon-olt_1/1/1
OnuIndex                 Sn                  State
------------------------------------------------------------------------
gpon-onu_1/1/1:1         ZTEG00000002        unknown
```

2. In Optical Line Terminal (OLT) interface mode, authenticate the ONU.

```
ZXAN(config)#interface gpon-olt_1/1/1
ZXAN(config-if)#onu 1 type ZTEG-F620 sn ZTEG00000002
[Successful]
ZXAN(config-if)#exit
```

3. (Optional) Query the authenticated ONU.

```
ZXAN(config)#show gpon onu state gpon-olt_1/1/1
OnuIndex               Admin State  Omcc State   O7 State     Phase State
------------------------------------------------------------------------------
gpon-onu_1/1/1:1       enable       enable       operation    working
```

Table 2-3 describes the ONU phase states.

Table 2-3 Descriptions of ONU Phase States

State	Description
offline	The OLT does not find the ONU because the ONU is offline.

State	Description
logging	The OLT has found the ONU and is measuring the distance.
syncMib	The OLT has measured the distance to the ONU and is synchronizing data.
working	The data synchronization completes, and you can configure services.
LOS	The fiber link between the OLT and ONU is faulty so that the ONU is offline.
DyingGasp	The ONU is powered off.

– End of Steps –

2.3 Configuring the T-CONT Bandwidth Profile

The T-CONT bandwidth profile describes the T-CONT flow parameters. By specifying the T-CONT bandwidth profile, you can implement the T-CONT flow control.

Context

The ZXA10 C320 supports 512 transmission container (T-CONT) profiles.

There are the following five types of upstream bandwidths:

- Fixed bandwidth (FBW)
- Assured bandwidth (ABW)
- Non-assured bandwidth
- Best-effort bandwidth
- Maximum bandwidth (MBW)

The priorities of fixed bandwidth, assured bandwidth, non-assured bandwidth, best-effort bandwidth, and maximum bandwidth are in descending order.

A T-CONT bandwidth profile may contains one or multiple types of bandwidths. Five types of T-CONT bandwidth profiles are as follows:

- Fixed bandwidth (type 1)

  Type 1 includes only fixed bandwidth. Type 1 has fixed bandwidth and timeslot. It is applicable to the service that is sensitive to delay and jitter and has fixed or stable flow rate, such as the voice service.

- Assured bandwidth (type 2)

  Type 2 includes only assured bandwidth. Type 2 has fixed bandwidth but not timeslot. It is applicable to the service that is insensitive to delay and jitter and has limited flow rate, such as the video on demand (VOD) service.

- Assured and non-assured bandwidths (type 3)

  Type 3 includes assured and non-assured bandwidths. It has the assured minimum bandwidth and shares the excess bandwidth dynamically. Meanwhile, it is constrained

by the maximum bandwidth. It is applicable to the service that requires service assurance but has a large volume of flow burst, such as the subscription download service.

- Best-effort bandwidth (type 4)

  Type 4 includes only best-effort bandwidth. After the fixed bandwidth, assured bandwidth, and non-assured bandwidth are allocated, type 4 competes for the excess bandwidth. It is applicable to the service that is insensitive to delay and jitter, such as the Web browse service.

- Support all (type 5)

  Type 5 combines the four types and has the characteristics of the four types. It is applicable to most service streams.

The summary of fixed bandwidth and assured bandwidth on a PON port must be no more than 1 Gbps. Table 2-4 lists the parameters of the default T-CONT bandwidth profile.

Table 2-4 Parameters of the Default T-CONT Profile

Parameter	Value
Bandwidth type	1
FBW	10000 kbps
ABW	0
MBW	0

Configuration Data

Table 2-5 lists the configuration data for the T-CONT bandwidth profile.

Table 2-5 Configuration Data for the T-CONT Profile

Item	Data
T-CONT bandwidth profile 1	Profile name: 20M Bandwidth type: type 5 Fixed bandwidth: 2000 kbps Assured bandwidth: 5000 kbps Maximum bandwidth: 20000 kbps
T-CONT bandwidth profile 2	Profile name: 15M Bandwidth type: type 4 Maximum bandwidth: 15000 kbps
T-CONT bandwidth profile 3	Profile name: 10M Bandwidth type: type 3 Assured bandwidth: 5000 kbps Maximum bandwidth: 10000 kbps

Item	Data
T-CONT bandwidth profile 4	Profile name: 5M Bandwidth type: type 2 Assured bandwidth: 5000 kbps
T-CONT bandwidth profile 5	Profile name: 2M Bandwidth type: type 1 Fixed bandwidth: 2000 kbps

Steps

1. In GPON configuration mode, create a T-CONT bandwidth profile.

```
ZXAN(config)#gpon
ZXAN(config-gpon)#profile tcont 20M type 5 fixed 2000 assured 5000 maximum 20000
[Successful]
ZXAN(config-gpon)#profile tcont 15M type 4 maximum 15000
[Successful]
ZXAN(config-gpon)#profile tcont 10M type 3 assured 5000 maximum 10000
[Successful]
ZXAN(config-gpon)#profile tcont 5M type 2 assured 5000
[Successful]
ZXAN(config-gpon)#profile tcont 2M type 1 fixed 2000
[Successful]
```

2. (Optional) Query the T-CONT bandwidth profile configuration.

```
ZXAN(config-gpon)#show gpon profile tcont
Name :default
 Type            FBW(kbps)    ABW(kbps)    MBW(kbps)
 1               10000        0            0
Name :20M
 Type            FBW(kbps)    ABW(kbps)    MBW(kbps)
 5               2000         5000         20000
Name :15M
 Type            FBW(kbps)    ABW(kbps)    MBW(kbps)
 4               0            0            15000
Name :10M
 Type            FBW(kbps)    ABW(kbps)    MBW(kbps)
 3               0            5000         10000
Name :5M
 Type            FBW(kbps)    ABW(kbps)    MBW(kbps)
 2               0            5000         0
Name :2M
 Type            FBW(kbps)    ABW(kbps)    MBW(kbps)
 1               2000         0            0
```

– End of Steps –

2.4 Configuring the GPON ONU IP Profile

Using the GPON ONU IP profile, you can configure IP addresses for GPON ONUs in batches.

Context

The ZXA10 C320 supports the following three IP address allocation modes:

- Static allocation mode
- Dynamic Host Configuration Protocol (DHCP) mode
- Point to Point Protocol over Ethernet (PPPoE) mode

One ONU can use only one IP address allocation mode.

The ONU IP profile is applicable to only the static allocation mode.

Configuration Data

Table 2-6 lists the configuration data of the GPON ONU IP profile.

Table 2-6 Configuration Data of the GPON ONU IP Profile

Item	Data
Profile name	ip-test
IP address allocation mode	static
Gateway IP address	1.2.3.1

Steps

1. In GPON configuration mode, configure the ONU IP profile.

```
ZXAN(config)#gpon
ZXAN(config-gpon)#onu profile ip ip-test static gateway 1.2.3.1
```

2. (Optional) Query the ONU IP profile.

```
ZXAN(config-gpon)#show gpon onu profile ip

Profilename:   ip-test
Gateway:       1.2.3.1
Primary DNS:   0.0.0.0 Secondary DNS: 0.0.0.0
```

– End of Steps –

2.5 Configuring the GPON ONU VLAN Profile

Using the GPON ONU VLAN profile, you can configure VLANs for GPON ONUs in batches.

Configuration Data

Table 2-7 lists the configuration data of the GPON VLAN profile.

Table 2-7 Configuration Data of the GPON VLAN Profile

Item	Data
Profile name	vlan-test
Tag mode	Tag
VLAN ID	300
Priority	7

Steps

1. In GPON configuration mode, configure the ONU VLAN profile.

```
ZXAN(config)#gpon
ZXAN(config-gpon)#onu profile vlan vlan-test tag-mode tag cvlan 300 priority 7
```

2. (Optional) Query the ONU VLAN profile.

```
ZXAN(config-gpon)#show gpon onu profile vlan

Profile name:  vlan-test
Tag mode:      tag
CVLAN:         300
CVLAN priority:7
```

– End of Steps –

2.6 Configuring the VoIP Access Code Profile

The VoIP access code profile can be used to configure access codes for VoIP advanced services, which are based on SIP, for GPON ONUs in batches.

Context

You can set up relation between access codes and corresponding services on ONUs by configuring a VoIP access code profile. When a subscriber dials an access code, the corresponding service is activated on the ONU (SIP agent), and then processed according to the service procedure.

Configuration Data

Table 2-8 lists the configuration data of the VoIP service application profile.。

Table 2-8 Configuration Data of the VoIP Access Code Profile

Item	Data
Profile name	abc
Access code for call hold	***

Steps

1. In GPON configuration mode, configure the VoIP access code profile.

```
ZXAN(config)#gpon
ZXAN(config-gpon)#onu profile voip-accesscode abc call-hold ***
```

2. (Optional) Query the VoIP access code profile.

```
ZXAN(config-gpon)#show gpon onu profile voip-accesscode

Profile-name:                       abc
  cancel-call-waiting:
  call-hold:                        ***
  call-park:
  cid-activate:
  cid-deactivate:
  no-disturb-activation:
  no-disturb-deactivation:
  no-disturb-pin-change:
  emergency-srv-num:
  intercom-service:
  unattend-blind-call-transfer:
  attend-call-transfer:
```

– End of Steps –

2.7 Configuring the VoIP Service Application Profile

The VoIP service application profile can be used to configure VoIP advanced services, which are based on SIP, for GPON ONUs in batches.

Configuration Data

Table 2-9 lists the configuration data of the VoIP service application profile.

Table 2-9 Configuration Data of the VoIP Service Application Profile

Item	Data
Profile name	voip-service
Call waiting	Enable
Call transfer	Enable
Call hold	Enable
3-way call	Enable

Steps

1. In GPON configuration mode, configure the VoIP service application profile.

```
ZXAN(config)#gpon
```

```
ZXAN(config-gpon)#onu profile voip-appsrv voip-service call-waiting enable
call-transfer enable call-hold enable 3way enable
```

2. (Optional) Query the VoIP service application profile.

```
ZXAN(config-gpon)#show gpon onu profile voip-appsrv

Profile-name:                       voip-service
  calling-num:                      disable
  calling-name:                     disable
  cid-blocking:                     disable
  cid-num-permanent-status:         disable
  cid-name-permanent-status:        disable
  anonymous-cid-blocking:           disable
  call-wating:                      enable
  cid-announcement:                 disable
  3way:                             enable
  call-transfer:                    enable
  call-hold:                        enable
  call-park:                        disable
  no-disturb:                       disable
  emergency-call-flash:             disable
  emergency-originate-hold:         disable
  6way:                             disable
  message-waiting-splash-ring:      disable
  message-wating-special-dialtone:  disable
  message-waiting-visual-ind:       disable
  call-forwarding-ind:              disable
  direct-connect-feature:           disable
  dialtone-delay:                   disable
  direct-connect-uri:
    Validation scheme:              disable
    Username:
    Password:
    Realm:
  bridge-line-agent-uri:
    Validation scheme:              disable
    Username:
    Password:
    Realm:
  conference-factory-uri:
    Validation scheme:              disable
    Username:
    Password:
    Realm:
```

– End of Steps –

2.8 Configuring the Dial Plan Table

A dial plan establishes the expected number and pattern of digits for a telephone number, which includes country codes, access codes, area codes and all combinations of digits dialed.

Steps

1. In GPON configuration mode, create the dial plan table.

```
ZXAN(config)#gpon
ZXAN(config-gpon)#onu profile dial-plan-table test
```

2. Configure the dial plan token.

```
ZXAN(config-gpon)#onu profile dial-plan test 1 token X*.X.#|#X.*.X.##
ZXAN(config-gpon)#onu profile dial-plan test 2 token #X.*.X.T|#X.*.X.#T
ZXAN(config-gpon)#onu profile dial-plan test 3 token X*.X.T|**.X.*.X.*.X.##
ZXAN(config-gpon)#onu profile dial-plan test 4 token **.X.*.X.*.X.#T
ZXAN(config-gpon)#onu profile dial-plan test 5 token #X.*.X.*.X.##
```

3. (Optional) Query the dial plan table configuration.

```
ZXAN(config-gpon)#show gpon onu profile dial-plan-table test
TableName MaxSize   Critical  Partial   Format
-------------------------------------------------------------------
test      16        4000      16000     h248
ZXAN(config-gpon)#show gpon onu profile dial-plan test
Dial plan id     Dial plan token
-------------------------------------
1                X*.X.#|#X.*.X.##
2                #X.*.X.T|#X.*.X.
                 #T
3                X*.X.T|**.X.*.X.
                 *.X.##
4                **.X.*.X.*.X.#T
5                #X.*.X.*.X.##
```

– End of Steps –

2.9 Configuring the GPON SIP Profile

Using the GPON SIP profile, you can configure the GPON ONU SIP parameters for GPON ONUs in batches.

Prerequisite

Before this operation, make sure that:

- The access code profile has been configured.
- The service application profile has been configured.

- The dial plan table has been configured.

Configuration Data

Table 2-10 lists the configuration data of the Session Initiation Protocol (SIP) profile.

Table 2-10 Configuration Data of the GPON SIP Profile

Item	Data
Profile name	sip-test
Access code profile	abc
Service application profile	voip-service
Dial plan table	test
IP address of the proxy server	1.2.3.1

Steps

1. In GPON configuration mode, configure the SIP profile.

```
ZXAN(config)#gpon
ZXAN(config-gpon)#onu profile sip sip-test proxy 1.2.3.1
ZXAN(config-gpon)#onu profile sip sip-test accesscode abc
ZXAN(config-gpon)#onu profile sip sip-test appsrv voip-service
ZXAN(config-gpon)#onu profile sip sip-test dial-plan test
```

2. (Optional) Query the SIP profile.

```
ZXAN(config-gpon)#show gpon onu profile sip name sip-test

Profile name :                  sip-test
  Proxy server:                 1.2.3.1
  Outbound proxy:               1.2.3.1
  Registrar:                    1.2.3.1
    Validation scheme:          disable
  UDP port:                     5060
  DSCP/TOS:                     0
  Media UDP port:               5060
  Media DSCP/TOS:               0
  DNS1:                         0.0.0.0
  DNS2:                         0.0.0.0
  Registration expiration time: 3600(s)
  Re-registration time:         360(s)
  Softswitch vendor:
  Dial plan table name:         test
  Release timer:                10(s)
  ROH timer:                    15(s)
  Link test:                    disable
  Link test interval:           N/A
```

```
appsrv:                         voip-service
accesscode:                     abc
```

– End of Steps –

2.10 Configuring the GPON MGC Profile

Using the GPON MGC profile, you can configure MGC parameters for GPON ONUs in batches.

Context

The ZXA10 C320 supports the following two Media Gateway Controller (MGC) protocols.

- MGCP
- H.248

Configuration Data

Table 2-11 lists the configuration data of the GPON MGC profile.

Table 2-11 Configuration Data of the GPON MGC Profile

Item	Data
Profile name	mgc-test
Active server IP address	1.2.3.1
Standby server IP address	1.2.3.2
User TID	Prefix: user Postfix length: 5 Postfix start number: 1
RTP TID	Prefix: rtp Postfix length: 5 Postfix start number: 1

Steps

1. In GPON configuration mode, configure the active and standby MGC servers.

```
ZXAN(config)#gpon
ZXAN(config-gpon)#onu profile mgc mgc-test server1 1.2.3.1
ZXAN(config-gpon)#onu profile mgc mgc-test server2 1.2.3.2
```

2. In GPON configuration mode, configure the user Terminal Identification (TID) and Real-time Transport Protocol (RTP) TID.

```
ZXAN(config-gpon)#onu profile mgc mgc-test user-tid prefix user postfix-len 5
postfix-start 1
ZXAN(config-gpon)#onu profile mgc mgc-test rtp-tid prefix rtp postfix-len 5
postfix-start 1
```

3. (Optional) Query the MGC profile.

```
ZXAN(config-gpon)#show gpon onu profile mgc

Profile name:             mgc-test
  Server1:                1.2.3.1
    Validation scheme:    disable
    Username:             N/A
    Password:             N/A
    Realm:                N/A
  Server2:                1.2.3.2
    Validation scheme:    disable
    Username:             N/A
    Password:             N/A
    Realm:                N/A
  UDP port:               2944
  DSCP/TOS:               0
  Media UDP port:         2944
  Media DSCP/TOS:         0
  Message format:         text long
  Version:                1
  Maximum retry time:     0(s)
  Maximum retry attempts: 0(s)
  Service change delay:   0(s)
  Softswitch vendor:
  User TID:
    Prefix:               user
    Postfix length:       5
    Postfix start number: 1
  RTP TID:
    Prefix:               rtp
    Postfix length:       5
    Postfix start number: 1
  Heart beat:             service change
  RTP link detect:        disable
  Number shortest match:  disable
  Digit map long timer:   20000(ms)
  Digit map short timer:  5000(ms)
  Digit map start timer:  10000(ms)
  Heart beat interval:    60000(ms)
  Rereg timer min:        60000(ms)
  Rereg timer max:        120000(ms)
  Regmsg retran timer:    2000(ms)
  Total retran timer:     10000(ms)
```

– End of Steps –

2.11 Configuring the GPON Broadband Service

After you configure the GPON broadband service, the subscriber can access the Internet.

Note:

After configuring the service of a certain ONU in non-profile mode, you cannot configure its service in profile mode any more.

Prerequisite

- The GPON ONU has been authenticated.
- The T-CONT bandwidth profile has been configured.

Configuration Data

Table 2-12 lists the configuration data of the GPON broadband service.

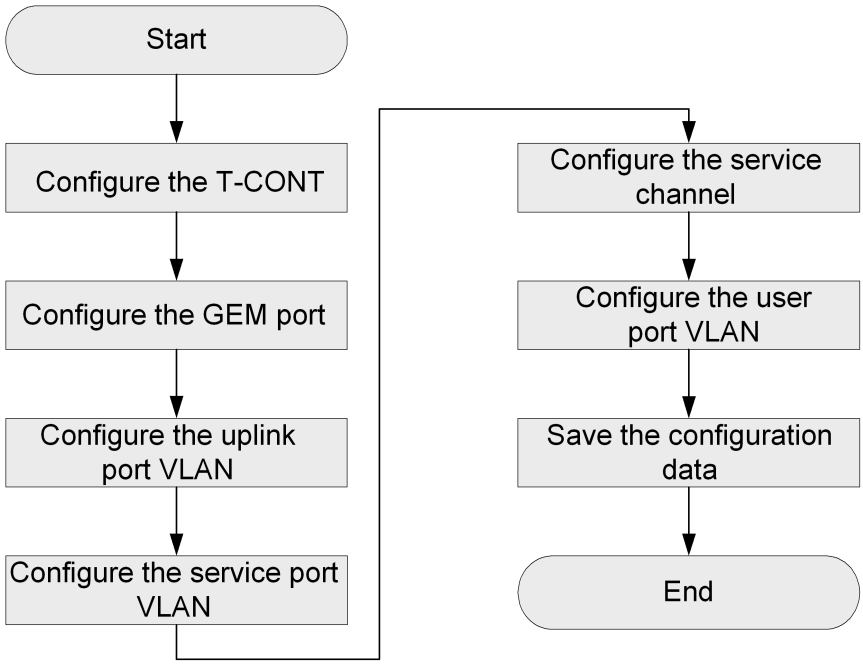
Table 2-12 Configuration Data of the GPON Broadband Service

Item	Data
Service VLAN ID	100
Service priority	0
Uplink port	gei_1/3/1
Service port	ONU interface: gpon-onu_1/1/1:1 Service-port ID: 1 Virtual port ID: 1
T-CONT	Index: 1 Name: T1 T-CONT bandwidth profile: 10M
GEM Port	Index: 1 Name: gemport1 T-CONT index: 1
Service channel	Name: HSI Service type: internet GEM port index: 1 Priority: 0 VLAN ID: 100
User port VLAN	Port: eth_0/1 VLAN mode: tag (The untagged upstream packet is tagged with PVID.) VLAN ID: 100 Priority: 0

Configuration Flowchart

Figure 2-2 shows the configuration flowchart of the GPON broadband service.

Figure 2-2 Configuration Flowchart of the GPON Broadband Service



Steps

1. In ONU interface mode, configure the T-CONT.

```
ZXAN(config)#interface gpon-onu_1/1/1:1
ZXAN(config-if)#tcont 1 name T1 profile 10M
```

2. Configure the GEM port.

```
ZXAN(config-if)#gemport 1 name gemport1 unicast tcont 1
ZXAN(config-if)#exit
```

3. In uplink interface configuration mode, configure the uplink port VLAN.

```
ZXAN(config)#interface gei_1/3/1
ZXAN(config-if)#switchport vlan 100 tag
ZXAN(config-if)#exit
```

4. In ONU interface mode, configure the service port VLAN.

```
ZXAN(config)#interface gpon-onu_1/1/1:1
ZXAN(config-if)#service-port 1 vport 1 user-vlan 100 vlan 100
ZXAN(config-if)#exit
```

Note:

By default, the mapping mode between the virtual port and the GEM port is 1:1.

5. In ONU remote management mode, configure the service channel.

```
ZXAN(config)#pon-onu-mng gpon-onu_1/1/1:1
ZXAN(gpon-onu-mng)#service HSI type internet gemport 1 cos 0 vlan 100
```

6. Configure the user port VLAN.

```
ZXAN(gpon-onu-mng)#vlan port eth_0/1 mode tag vlan 100 priority 0
ZXAN(gpon-onu-mng)#end
```

7. Save the configuration data.

– End of Steps –

2.12 Configuring the GPON Multicast Service

After you configure the GPON multicast service, subscribers can receive multicast service streams.

Prerequisite

- The GPON ONU has been authenticated.
- The T-CONT bandwidth profile has been configured.

Configuration Data

Table 2-13 lists the configuration data of the GPON multicast service.

Table 2-13 Configuration Data of the GPON Multicast Service

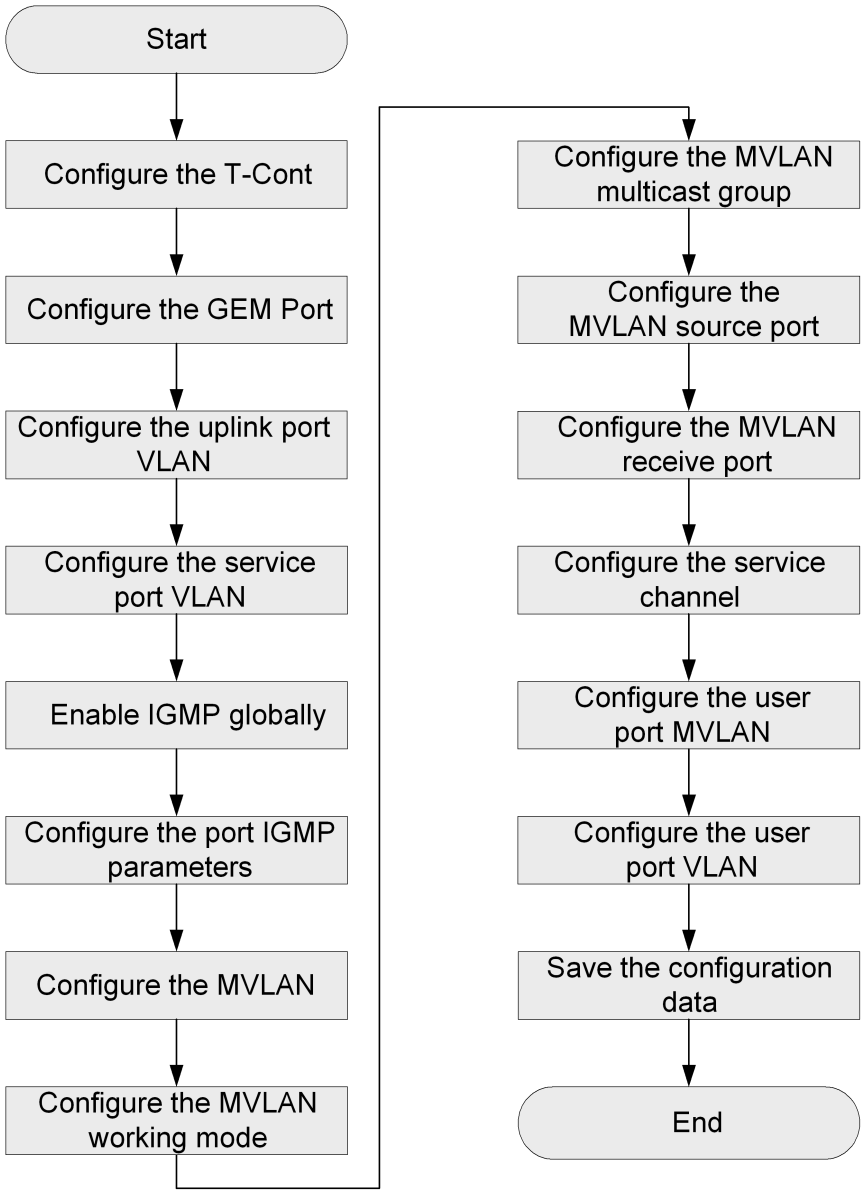
Item	Data
Multicast VLAN (MVLAN) ID	200
Service priority	5
MVLAN working mode	Proxy
MVLAN multicast group	224.1.1.1 – 224.1.1.3
Uplink port	gei_1/3/1
Service port	ONU interface: gpon-onu_1/1/1:1 Service-port ID: 2 Virtual port ID: 2
T-CONT	Index: 2 Name: T2 T-CONT bandwidth profile: 5M

Item	Data
GEM Port	Index: 2 Name: gemport2 T-CONT index: 2
Service channel	Name: mulitcast Service type: iptv GEM port index: 2 Priority: 5 VLAN ID: 200
User port VLAN	MVLAN ID: 200 MVLAN tag stripping: enable
User port VLAN	Port: eth_0/2 VLAN mode: tag (The untagged upstream packet is tagged with PVID.) VLAN ID: 200 Priority: 5

Configuration Flowchart

Figure 2-3 shows the configuration flowchart of the GPON multicast service.

Figure 2-3 Configuration Flowchart of the GPON Multicast Service



Steps

1. In ONU interface mode, configure the T-CONT.

```
ZXAN(config)#interface gpon-onu_1/1/1:1
ZXAN(config-if)#tcont 2 name T2 profile 5M
```

2. Configure the GEM port.

```
ZXAN(config-if)#gemport 2 name gemport2 unicast tcont 2
ZXAN(config-if)#exit
```

3. In uplink interface configuration mode, configure the uplink port VLAN.

```
ZXAN(config)#interface gei_1/3/1
ZXAN(config-if)#switchport vlan 200 tag
ZXAN(config-if)#exit
```

4. In ONU interface mode, configure the service port VLAN.

```
ZXAN(config)#interface gpon-onu_1/1/1:1
ZXAN(config-if)#service-port 2 vport 2 user-vlan 200 vlan 200
ZXAN(config-if)#exit
```

NOTE **Note:**

By default, the mapping mode between the virtual port and the GEM port is 1:1.

5. Enable IGMP globally.

```
ZXAN(config)#igmp enable
```

6. Configure the port IGMP parameters.

```
ZXAN(config)#interface gpon-onu_1/1/1:1
ZXAN(config-if)#igmp fast-leave enable vport 2
ZXAN(config-if)#exit
```

7. Configure the MVLAN.

```
ZXAN(config)#igmp mvlan 200
```

8. (Optional) Configure the MVLAN working mode.

```
ZXAN(config)#igmp mvlan 200 work-mode proxy
```

9. Configure the MVLAN multicast group.

```
ZXAN(config)#igmp mvlan 200 group 224.1.1.1 to 224.1.1.3
```

10. Configure MVLAN source port.

```
ZXAN(config)#igmp mvlan 200 source-port gei_1/3/1
```

11. Configure the MVLAN receive port.

```
ZXAN(config)#igmp mvlan 200 receive-port gpon-onu_1/1/1:1 vport 2
```

12. In ONU remote management mode, configure the service channel.

```
ZXAN(config)#pon-onu-mng gpon-onu_1/1/1:1
ZXAN(gpon-onu-mng)#service multicast type iptv gemport 2 cos 5 vlan 200
```

13. Configure the user port MVLAN.

```
ZXAN(gpon-onu-mng)#multicast vlan add vlanlist 200
ZXAN(gpon-onu-mng)#multicast vlan tag-strip port eth_0/2 enable
```

14. Configure the user port VLAN.

```
ZXAN(gpon-onu-mng)#vlan port eth_0/2 mode tag vlan 200 priority 5
ZXAN(gpon-onu-mng)#end
```

15. Save the configuration data.

– End of Steps –

2.13 Configuring the GPON Voice Service (SIP)

After you configure the GPON voice service, subscribers can make and answer phone calls. This section takes the SIP protocol as an example.

Prerequisite

- The GPON ONU has been authenticated.
- The T-CONT bandwidth profile has been configured.
- The GPON VoIP IP profile has been configured.
- The GPON VoIP VLAN profile has been configured.
- The GPON SIP profile has been configured.

Configuration Data

Table 2-14 lists the configuration data of the GPON voice service.

Table 2-14 Configuration Data of the GPON Voice Service

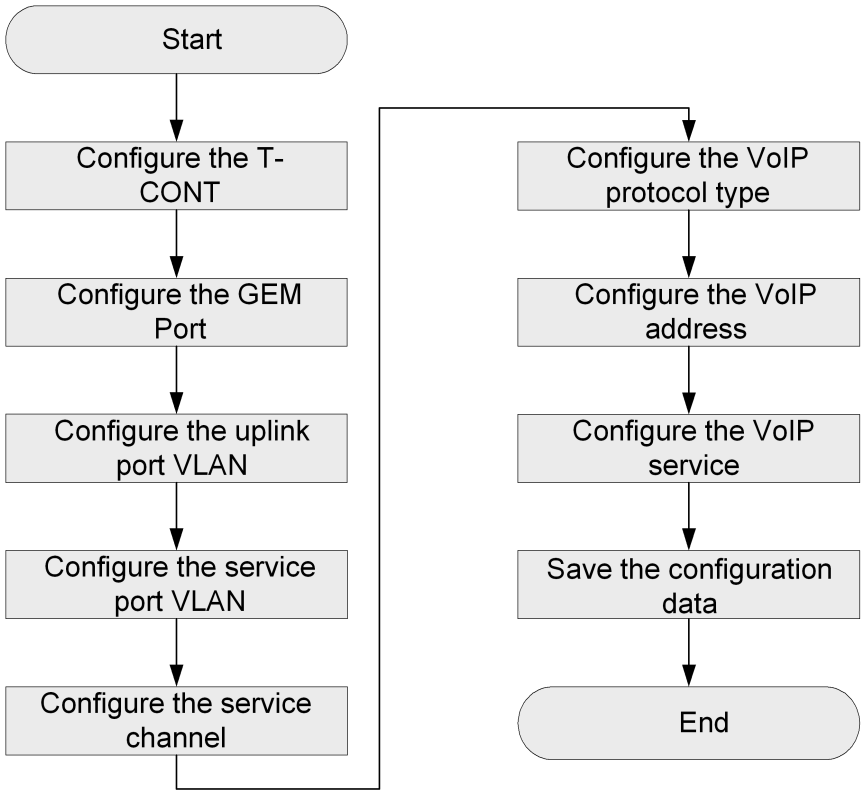
Item	Data
Service VLAN ID	300
Service priority	7
Uplink port	gei_1/3/1
Service port	ONU interface: gpon-onu_1/1/1:1 Service-port ID: 3 Virtual port ID: 3
T-CONT	Index: 3 Name: voip T-CONT bandwidth profile: 2M
GEM Port	Index: 3 Name: gemport3 T-CONT index: 3
Service channel	Name: voip-sip Service type: voip GEM port index: 3 Priority: 7 VLAN ID: 300
VoIP protocol	SIP
VoIP address	IP address allocation mode: static VoIP IP profile: ip-test IP address: 1.2.3.4/24 VoIP VLAN profile: vlan-test

Item	Data
VoIP service	Port: pots_0/1 SIP profile: sip-test User ID: 12345 User name: 12345 Password: 12345

Configuration Flowchart

Figure 2-4 shows the configuration flowchart of the GPON voice service.

Figure 2-4 Configuration Flowchart of the GPON Voice Service



Steps

1. In ONU interface configuration mode, configure the T-CONT.

```
ZXAN(config)#interface gpon-onu_1/1/1:1
ZXAN(config-if)#tcont 3 name voip profile 2M
```

2. Configure the GEM port.

```
ZXAN(config-if)#gemport 3 name gemport3 unicast tcont 3
ZXAN(config-if)#exit
```

3. In uplink interface configuration mode, configure the uplink port VLAN.

```
ZXAN(config)#interface gei_1/3/1
ZXAN(config-if)#switchport vlan 300 tag
```

```
ZXAN(config-if)#exit
```

4. In ONU interface configuration mode, configure the service port VLAN.

```
ZXAN(config)#interface gpon-onu_1/1/1:1
ZXAN(config-if)#service-port 3 vport 3 user-vlan 300 vlan 300
ZXAN(config-if)#exit
```

NOTE **Note:**

By default, the mapping mode between the virtual port and the GEM port is 1:1.

5. In ONU remote management mode, configure the service channel.

```
ZXAN(config)#pon-onu-mng gpon-onu_1/1/1:1
ZXAN(gpon-onu-mng)#service voip-sip type voip gemport 3 cos 7 vlan 300
```

6. (Optional) Configure the VoIP protocol type.

```
ZXAN(gpon-onu-mng)#voip protocol sip
```

7. Configure the VoIP address.

```
ZXAN(gpon-onu-mng)#voip-ip mode static ip-profile ip-test ip-address 1.2.3.4
mask 255.255.255.0 vlan-profile vlan-test
```

8. Configure the VoIP service.

```
ZXAN(gpon-onu-mng)#sip-service pots_0/1 profile sip-test userid 12345 username
12345 password 12345
ZXAN(gpon-onu-mng)#end
```

9. Save the configuration data.

– End of Steps –

2.14 Configuring the GPON Voice Service (H.248)

After you configure the GPON voice service, subscribers can make and answer phone calls. This section takes the H.248 protocol as an example.

Prerequisite

- The GPON ONU has been authenticated.
- The T-CONT bandwidth profile has been configured.
- The GPON VoIP IP profile has been configured.
- The GPON VoIP VLAN profile has been configured.
- The GPON MGC profile has been configured.

Configuration Data

Table 2-15 lists the configuration data of the GPON voice service.

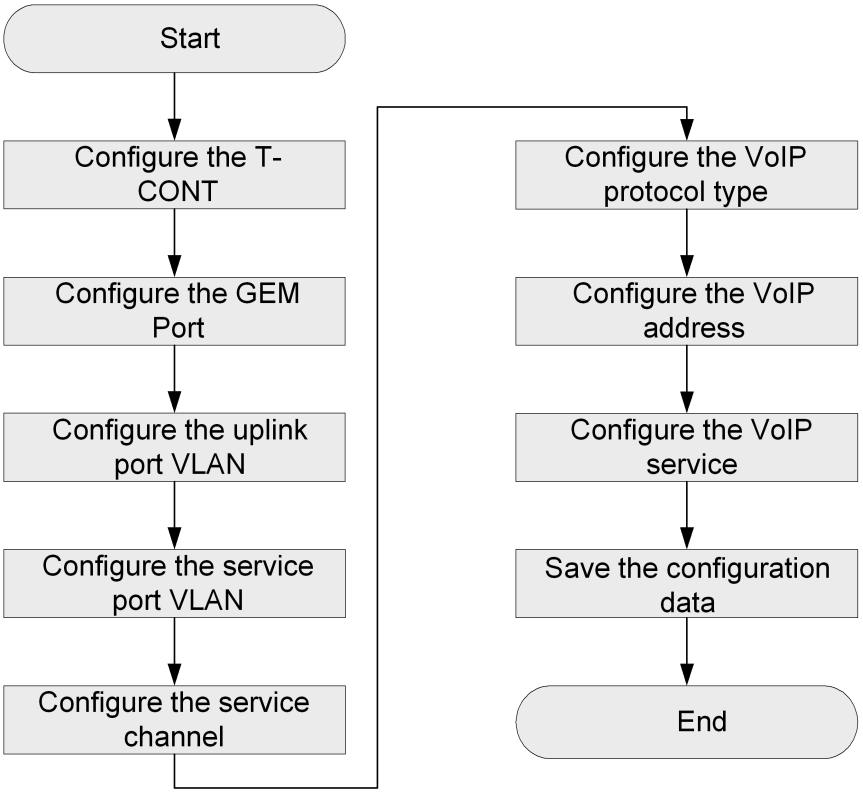
Table 2-15 Configuration Data of the GPON Voice Service

Item	Data
Service VLAN ID	300
Service priority	7
Uplink port	gei_1/3/1
Service port	ONU interface: gpon-onu_1/1/1:1 Service-port ID: 3 Virtual port ID: 3
T-CONT	Index: 3 Name: voip T-CONT bandwidth profile: 2M
GEM Port	Index: 3 Name: gemport3 T-CONT index: 3
Service channel	Name: voip-h248 Service type: voip GEM port index: 3 Priority: 7 VLAN ID: 300
VoIP protocol	H.248
Domain name	iad.zte.com.cn
VoIP address	IP address allocation mode: static VoIP IP profile: ip-test IP address: 1.2.3.4/24 VoIP VLAN profile: vlan-test
VoIP service	Port: pots_0/1 MGC profile: mgc-test

Configuration Flowchart

Figure 2-5 shows the configuration flowchart of the GPON voice service.

Figure 2-5 Configuration Flowchart of the GPON Voice Service



Steps

1. In ONU interface configuration mode, configure the T-CONT.

```
ZXAN(config)#interface gpon-onu_1/1/1:1
ZXAN(config-if)#tcont 3 name voip profile 2M
```

2. Configure the GEM port.

```
ZXAN(config-if)#gemport 3 name gemport3 unicast tcont 3
ZXAN(config-if)#exit
```

3. In uplink interface configuration mode, configure the uplink port VLAN.

```
ZXUAS(config)#interface fei_1/20
```

4. In ONU interface configuration mode, configure the service port VLAN.

```
ZXAN(config)#interface gpon-onu_1/1/1:1
ZXAN(config-if)#service-port 3 vport 3 user-vlan 300 vlan 300
ZXAN(config-if)#exit
```

NOTE **Note:**

By default, the mapping mode between the virtual port and the GEM port is 1:1.

5. In ONU remote management mode, configure the service channel.

```
ZXAN(config)#pon-onu-mng gpon-onu_1/1/1:1
ZXAN(gpon-onu-mng)#service voip-h248 type voip gemport 3 cos 7 vlan 300
```

6. Configure the VoIP protocol type.

```
ZXAN(gpon-onu-mng)#voip protocol h248 domain iad.zte.com.cn
```

7. Configure the VoIP address.

```
ZXAN(gpon-onu-mng)#voip-ip mode static ip-profile ip-test ip-address 1.2.3.4
mask 255.255.255.0 vlan-profile vlan-test
```

8. Configure the VoIP service.

```
ZXAN(gpon-onu-mng)#mgc-service pots_0/1 profile mgc-test
ZXAN(gpon-onu-mng)#end
```

9. Save the configuration data.

– End of Steps –

This page intentionally left blank.

Chapter 3
GPON Service Configuration in Profile Mode

Table of Contents

3.1 Configuring the GPON ONU Line Profile

Using the GPON ONU line profile, you can configure T-CONTs and GEM ports for GPON ONUs in batches.

Prerequisite

The T-CONT bandwidth profile has been configured. (See 2.3 Configuring the T-CONT Bandwidth Profile for details.)

Configuration Data

Table 3-1 lists the configuration data of the ONU line profile.

Table 3-1 Configuration Data of the GPON ONU Line Profile

Item	Data
Profile name	line-ftth
T-CONT 1	Index: 1 Name: T1-10M T-CONT bandwidth profile: 10M
T-CONT 2	Index: 2 Name: T2-5M T-CONT bandwidth profile: 5M
T-CONT 3	Index: 3 Name: T3-2M T-CONT bandwidth profile: 2M
GEM Port 1	Index: 1 Name: gemport1 T-CONT index: 1

Item	Data
GEM Port 2	Index: 2 Name: gemport2 T-CONT index: 2
GEM Port 3	Index: 1 Name: gemport3 T-CONT index: 3

Steps

1. In PON configuration mode, create an ONU line profile.

```
ZXAN(config)#pon
ZXAN(config-pon)#onu-profile gpon line line-ftth
ZXAN(config-gpon-line)#
```

2. Configure the T-CONT.

```
ZXAN(config-gpon-line)#tcont 1 name T1-10M profile 10M
ZXAN(config-gpon-line)#tcont 2 name T2-5M profile 5M
ZXAN(config-gpon-line)#tcont 3 name T3-2M profile 2M
```

3. Configure the GEM port.

```
ZXAN(config-gpon-line)#gemport 1 name gemport1 unicast tcont 1
ZXAN(config-gpon-line)#gemport 2 name gemport2 unicast tcont 2
ZXAN(config-gpon-line)#gemport 3 name gemport3 unicast tcont 3
ZXAN(config-gpon-line)#exit
```

4. (Optional) Query the ONU line profile.

```
ZXAN(config-gpon-line)#show pon onu-profile gpon line line-ftth
Profile Name  : line-ftth
Profile Status : normal
Bound onu list:

ZXAN(config-gpon-line)#show pon onu-profile gpon line line-ftth cfg
  tcont 1 name T1-10M profile 10M
  tcont 2 name T2-5M profile 5M
  tcont 3 name T3-2M profile 2M
  gemport 1 unicast tcont 1 dir both
  gemport 2 unicast tcont 2 dir both
  gemport 3 unicast tcont 3 dir both
```

– End of Steps –

3.2 Configuring the GPON ONU Remote Management Profile

When the configuration of GPON ONUs are the same, you can remotely configure ONUs in batches using the GPON ONU remote management profile, including configuring service channels and user port VLANs.

Prerequisite

- The GPON ONU VLAN profile has been configured. (See 2.5 Configuring the GPON ONU VLAN Profile for details.)
- The GPON MGC profile has been configured. (See 2.10 Configuring the GPON MGC Profile for details.)

Configuration Data

Table 3-2 lists the configuration data of the ONU remote management profile.

Table 3-2 Configuration Data of the GPON ONU Remote Management Profile

Item	Data
Profile name	remote-ftth
Broadband service channel	Name: data Service type: internet GEM port index: 1 Priority: 0 VLAN ID: 100
Multicast service channel	Name: igmp Service type: iptv GEM port index: 2 Priority: 5 VLAN ID: 200
Voice service channel	Name: voice Service type: voip GEM port index: 3 Priority: 7 VLAN ID: 300
Broadband service UNI	Port: eth_0/1 VLAN mode: tag (The untagged upstream packet is tagged with PVID.) VLAN ID: 100 Priority: 0

Item	Data
Multicast service UNI	Port: eth_0/2 VLAN mode: tag VLAN ID: 200 Priority: 5 MVLAN ID: 200 MVLAN tag stripping: enable
VoIP protocol	Protocol: H.248 Domain name: iad.zte.com.cn
VoIP address	IP address allocation mode: DHCP GPON ONU VLAN profile: vlan-test
Voice service UNI	Port: pots_0/1 GPON MGC profile: mgc-test

Steps

1. In PON configuration mode, create an ONU remote management profile.

```
ZXAN(config)#pon
ZXAN(config-pon)#onu-profile gpon remote remote-ftth
ZXAN(config-gpon-remote)#
```

2. Configure service channels.

```
ZXAN(config-gpon-remote)#service data type internet gemport 1 cos 0 vlan 100
ZXAN(config-gpon-remote)#service igmp type iptv gemport 2 cos 5 vlan 200
ZXAN(config-gpon-remote)#service voice type voip gemport 3 cos 7 vlan 300
```

3. Configure user port VLANs.

```
ZXAN(config-gpon-remote)#vlan port eth_0/1 mode tag vlan 100 priority 0
ZXAN(config-gpon-remote)#vlan port eth_0/2 mode tag vlan 200 priority 5
```

4. Configure the user port MVLAN.

```
ZXAN(config-gpon-remote)#multicast vlan add vlanlist 200
ZXAN(config-gpon-remote)#multicast vlan tag-strip port eth_0/2 enable
```

5. Configure the VoIP protocol type.

```
ZXAN(config-gpon-remote)#voip protocol h248 domain iad.zte.com.cn
```

6. Configure the VoIP address and VLAN.

```
ZXAN(config-gpon-remote)#voip-ip mode dhcp vlan-profile vlan-test
```

7. Configure the user port VoIP service.

```
ZXAN(config-gpon-remote)#mgc-service pots_0/1 profile mgc-test
ZXAN(config-gpon-remote)#exit
```

8. (Optional) Query the ONU remote management profile.

```
ZXAN(config-gpon-remote)#show pon onu-profile gpon remote remote-ftth
Profile Name  : remote-ftth
```

```
Profile Status : normal
Bound onu list:

ZXAN(config-gpon-remote)#show pon onu-profile gpon remote remote-ftth cfg
  service data type internet gemport 1 cos 0 vlan 100
  service igmp type iptv gemport 2 cos 5 vlan 200
  service voice type voip gemport 3 cos 7 vlan 300
  voip protocol h248 domain iad.zte.com.cn
  voip-ip mode dhcp vlan-profile vlan-test host 1
  mgc-service pots_0/1 profile mgc-test
  vlan port eth_0/1 mode tag vlan 100
  vlan port eth_0/2 mode tag vlan 200 priority 5
  multicast vlan add vlanlist 200
  multicast vlan tag-strip port eth_0/2 enable
```

– End of Steps –

3.3 Configuring the GPON Service

The ZXA10 C320 connects the ONU via the GPON port to provide the Internet, video, and voice services. This section describes how to configure the GPON service in profile mode.

NOTE **Note:**

After configuring the service of an ONU in profile mode, you cannot configure its service in non-profile mode any more.

Prerequisite

- The GPON ONU has been authenticated.
- The GPON ONU line profile has been configured.
- The GPON ONU remote management profile has been configured.
- The ONU supports profile configuration mode, and the ONU UNIs are consistent with the UNIs in the ONU profiles.

Configuration Data

Table 3-3 lists the configuration data of the GPON service.

Table 3-3 Configuration Data of the GPON Service

Item	Data
Broadband service VLAN ID	100
Multicast service VLAN ID	200

Item	Data
Voice service VLAN ID	300
Uplink port	gei_1/3/1
Broadband service port	ONU interface: gpon-onu_1/1/1:1 Service-port ID: 1 Virtual port ID: 1
Multicast service port	ONU interface: gpon-onu_1/1/1:1 Service-port ID: 2 Virtual port ID: 2
Voice service port	ONU interface: gpon-onu_1/1/1:1 Service-port ID: 3 Virtual port ID: 3
GPON ONU line profile	line-ftth
GPON ONU remote management profile	remote-ftth
MVLAN working mode	Proxy
MVLAN multicast group	224.1.1.1 – 224.1.1.3

Steps

1. In uplink interface configuration mode, configure the uplink port VLANs.

```
ZXAN(config)#interface gei_1/3/1
ZXAN(config-if)#switchport vlan 100,200,300 tag
ZXAN(config-if)#exit
```

2. In OLT interface configuration mode, specify the ONU line profile and ONU remote management profile.

```
ZXAN(config)#interface gpon-olt_1/1/1
ZXAN(config-if)#onu 1 profile line line-ftth
.[Successful]
ZXAN(config-if)#onu 1 profile remote remote-ftth
.[Successful]
ZXAN(config-if)#exit
```

3. In ONU interface configuration mode, configure the service port VLANs.

```
ZXAN(config)#interface gpon-onu_1/1/1:1
ZXAN(config-if)#service-port 1 vport 1 user-vlan 100 vlan 100
ZXAN(config-if)#service-port 2 vport 2 user-vlan 200 vlan 200
ZXAN(config-if)#service-port 3 vport 3 user-vlan 300 vlan 300
ZXAN(config-if)#exit
```

NOTE **Note:**

By default, the mapping mode between the virtual port and the GEM port is 1:1.

4. (Optional) Enable IGMP globally.

```
ZXAN(config)#igmp enable
```

NOTE **Note:**

The global IGMP protocol of the ZXA10 C320 is enabled by default.

5. Configure the port IGMP parameters.

```
ZXAN(config)#interface gpon-onu_1/1/1:1
ZXAN(config-if)#igmp fast-leave enable vport 2
ZXAN(config-if)#exit
```

6. Configure the MVLAN.

```
ZXAN(config)#igmp mvlan 200
```

7. (Optional) Configure the MVLAN working mode.

```
ZXAN(config)#igmp mvlan 200 work-mode proxy
```

8. Configure the MVLAN multicast group.

```
ZXAN(config)#igmp mvlan 200 group 224.1.1.1 to 224.1.1.3
```

9. Configure the MVLAN source port.

```
ZXAN(config)#igmp mvlan 200 source-port gei_1/3/1
```

10. Configure the MVLAN receive port.

```
ZXAN(config)#igmp mvlan 200 receive-port gpon-onu_1/1/1:1 vport 2
```

11. Save the configuration data.

– End of Steps –

This page intentionally left blank.

Chapter 4
EPON Service Configuration

The Ethernet Passive Optical Network (EPON) access is a flexible access technology that provides super bandwidth access in both broadband and narrowband service environments. It supports multiple rate modes and uses a single optical fiber to provide the subscriber with the voice, data, and video services.

Figure 4-1 shows the EPON service networking diagram.

Figure 4-1 EPON Service Networking Diagram

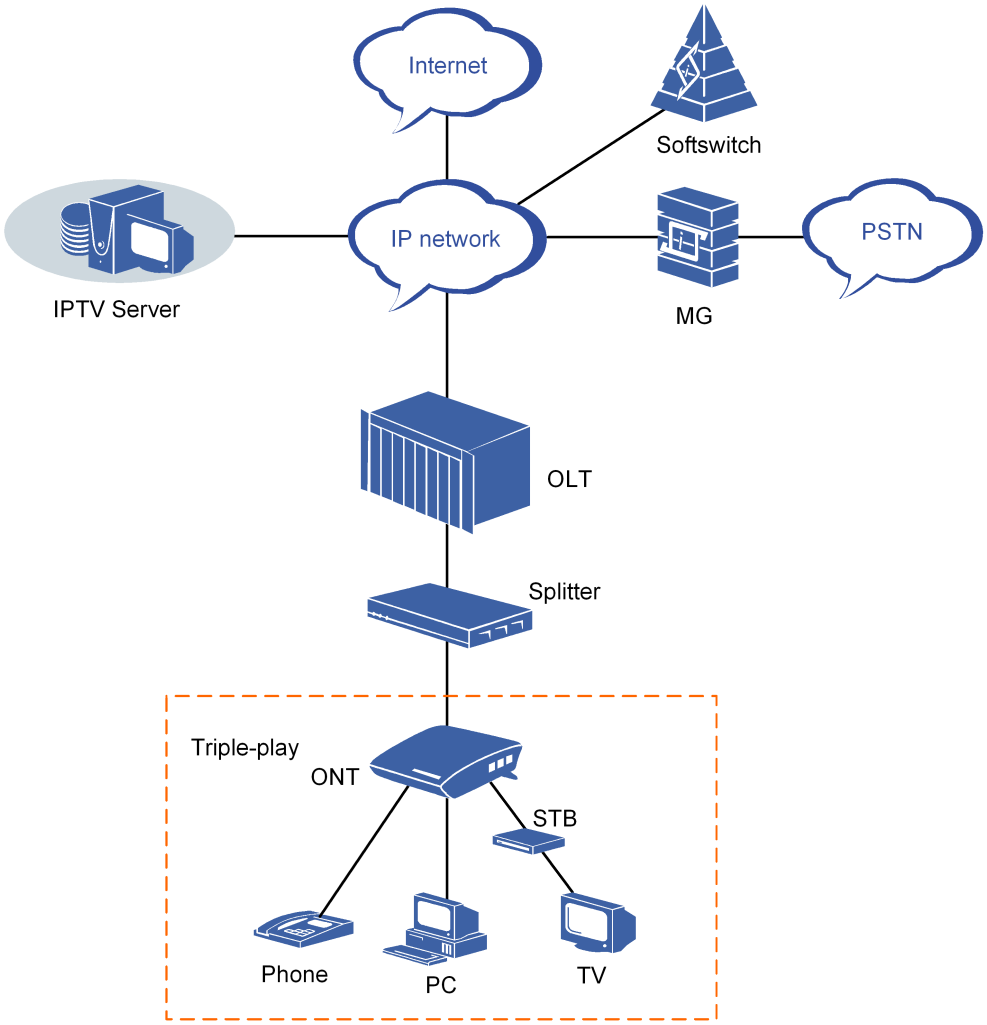


Table of Contents

4.1 Configuring the EPON ONU Type Profile

Before authenticating the EPON ONU, you need to create an ONU type profile if the ONU type does not exist.

Context

The ZXA10 C320 supports the following default EPON ONU types:

- ZTE-9806
- ZTE-D400
- ZTE-D402
- ZTE-D420
- ZTE-D421
- ZTE-D422
- ZTE-F401
- ZTE-F420
- ZTE-F425
- ZTE-F429
- ZTE-F430
- ZTE-F435
- ZTE-F500
- ZTE-F803
- ZTE-F820
- ZTE-F821
- ZTE-F822

You can use the **show onu-type epon** command to query the default EPON ONU types.

Configuration Data

Table 4-1 lists the configuration data of the EPON ONU type.

Table 4-1 Configuration Data of the EPON ONU Type

Item	Data
ONU type	ZTE-F822A

Item	Data
ONU description	24FE, 24POTS
Speed	10G (asymmetric)
Number of user ports	ETH: 24 POTS: 24
Auto-dispatch	Disable

Steps

1. In PON configuration mode, create an ONU type profile.

```
ZXAN(config)#pon
ZXAN(config-pon)#onu-type ZTE-F822A epon speed 10g-asymmetric
ZXAN(config-pon)#onu-type ZTE-F822A epon description 24FE,24POTS
```

2. Configure the user port of the ONU type.

```
ZXAN(config-pon)#onu-type-if ZTE-F822A eth_0/1-24
ZXAN(config-pon)#onu-type-if ZTE-F822A pots_0/1-24
```

3. In EPON configuration mode, disable the auto-dispatch function of the ONU type.

```
ZXAN(config)#epon
ZXAN(config-epon)#auto-dispatch-set ZTE-F822A disable
```

NOTE **Note:**

After the auto-dispatch function is enabled, the OLT will automatically deliver configurations (except VoIP configuration) to the ONU and overwrite the local configuration data on the ONU when the ONU is online.

---

4. (Optional) Query the configured ONU type profile.

```
ZXAN(config-epon)#show onu-type epon ZTE-F822A

Onu type name :         ZTE-F822A
Pon type :              epon
Description :           24FE,24POTS
Protect type:           none
Speed:                  10g-asymmetric
```

– End of Steps –

4.2 Authenticating the EPON ONU

Before configuring its services, you need to authenticate the EPON ONU that is online initially.

Prerequisite

The EPON ONU type profile has been set by default or manually.

Context

The ZXA10 C320 supports the following four ONU authentication modes:

- MAC address authentication (the default mode)

  Using the ONU PON MAC address for authentication

- Logical ID authentication

  Using the ONU logical ID for authentication

- SN authentication

  Using the ONU SN for authentication

- Hybrid authentication

  Using any of the MAC address, logical ID, or SN for authentication

In EPON configuration mode, use the **onu-authentication-mode service** command to change the ONU authentication mode.

Configuration Data

Table 4-2 lists the configuration data for EPON ONU authentication.

Table 4-2 Configuration Data for EPON ONU Authentication

Item	Data
ONU ID	1
ONU type	ZTE-F420
MAC address	00d0.d09a.46b6

Steps

1. Query the unauthenticated ONU.

```
ZXAN(config)#show onu unauthentication epon-olt_1/2/1
Onu Interface    :   epon-onu_1/2/1:1
Onu Model        :   ZTE-F420
MAC Address      :   00d0.d09a.46b6
SN               :   test1F400MAC0026EDAFCE19
LOID             :   test1F400MAC0026EDAFCE19
LOID_PSW         :   0026EDAFCE19
Online State     :   authentication deny
ExtOam State     :   complete
Software Version :   V1.1.0c_ZL2
Hardware Version :   V1.0.0
RegTime          :   2011/10/15 10:03:32
```

2. In OLT interface mode, authenticate the ONU.

```
ZXAN(config)#interface epon-olt_1/2/1
ZXAN(config-if)#onu 1 type ZTE-F420 mac 00d0.d09a.46b6
ZXAN(config-if)#exit
```

3. (Optional) Query the authenticated ONU.

```
ZXAN(config)#show onu detail-info epon-onu_1/2/1:1

Onu interface:      epon-onu_1/2/1:1
AdminState:         enable
Physical State:     online
Online State:       not register
OnuType:            ZTE-F420
SN:
MAC:                00d0.d09a.46b6
LOID:
NAME:
GeneralDescription:
SplitterNo:          1
FiberNo:            1
UserInfo:
Register time:      0000/00/00 00:00:00
Authpass time:      0000/00/00 00:00:00
Deregister time:    0000/00/00 00:00:00
FecMode:            disable
FecAbility:         unkown
LoopbackStatus:     noLoopback
OamLoopbacIgnoreRx: ignore
MAC bind mode:      disable
Onu Bind Mac:       0000.0000.0000.
```

4. In ONU interface mode, enable the ONU interface authentication protocol.

```
ZXAN(config)#interface epon-onu_1/2/1:1
ZXAN(config-if)#admin enable
```

– End of Steps –

4.3 Configuring the EPON ONU Bandwidth Profile

When configuring the bandwidth for EPON ONUs in batches, that is, ONUs use the same bandwidth configuration, you can use the bandwidth profile.

Context

Table 4-3 lists the parameters of the default bandwidth profile.

Table 4-3 Parameters of the Default Bandwidth Profile

Direction	Parameter	Value
Upstream	Maximum bandwidth (MaxBw)	100000 kbps
	Minimum bandwidth (MinBw)	10000 kbps
	Fixed bandwidth (FixBw)	0
	Fixed packet size (FixPktSize)	64 bytes
	Maximum burst size (MaxBurstSize)	45000 bytes
	Priority	0
Downstream	Maximum bandwidth (MaxBw)	100000 kbps
	Maximum burst size (MaxBurstSize)	16777215 bytes

Steps

1. In EPON configuration mode, create a bandwidth profile.

```
ZXAN(config)#epon
ZXAN(config-gpon)#onu-sla-profile profile-name create 10M
```

2. Configure the upstream and downstream bandwidths.

```
ZXAN(config-epon)#onu-sla-profile profile-set 10M upstream assured 5000 maximum
10000
ZXAN(config-epon)#onu-sla-profile profile-set 10M downstream maximum 10000
```

NOTE **Note:**

Among the upstream bandwidth configuration parameters, **assured bandwidth** and **MaxBw** are mandatory. The default values are recommended for other parameters.

Among the downstream bandwidth configuration parameters, **MaxBw** is mandatory. The system automatically calculates and sets **MaxBurstSize** according to the maximum bandwidth.

3. (Optional) Query the ONU bandwidth profile.

```
ZXAN(config-epon)#show epon onu-sla-profile 10M
ProfileName :10M
UpStream      MaxBw     MinBw     FixBw    FixPktSize MaxBurstSize Priority
              (Kbps)    (Kbps)    (Kbps)     (Bytes)    (Bytes)
--------------------------------------------------------------------------------
              10000     5000      0        64          45000       0
Downstream    MaxBw(Kbps)  MaxBurstSize(Bytes)
--------------------------------------------------------------------------------
```

```
                    10000        16777215
```

– End of Steps –

4.4 Configuring the EPON VoIP IP Profile

Using the EPON VoIP IP profile, you can configure VoIP IP addresses for EPON ONUs in batches.

Context

The ZXA10 C320 supports the following three IP address allocation modes:

- Static allocation mode
- DHCP mode
- PPPoE mode

One ONU can use only one IP address allocation mode.

The VoIP IP profile is applicable to only the static allocation mode.

Configuration Data

Table 4-4 lists the configuration data of the EPON VoIP IP profile.

Table 4-4 Configuration Data of the EPON VoIP IP Profile

Item	Data
Profile name	ip-test
Relation between voice IP and management IP	independent
IP address allocation mode	static
Gateway IP address	1.2.1.1
DNS IP address	1.1.1.1

Steps

1. In EPON configuration mode, configure the VoIP IP profile.

```
ZXAN(config)#epon
ZXAN(config-epon)#voip-ip profile ip-test relation independent mode static gateway
1.2.1.1 dns 1.1.1.1
```

2. (Optional) Query the VoIP IP profile.

```
ZXAN(config-epon)#show remote epon voip-ip profile ip-test

Voice-ip profile:                                   ip-test
relation between voice IP and MNG IP:               independent
voice ip mode:                                      static
voice ip default gateway:                           1.2.1.1
```

```
DNS :                                                    1.1.1.1
```

– End of Steps –

4.5 Configuring the EPON VoIP VLAN Profile

Using the EPON VoIP VLAN profile, you can configure VoIP VLANs for EPON ONUs in batches.

Configuration Data

Table 4-5 lists the configuration data of the EPON VoIP VLAN profile.

Table 4-5 Configuration Data of the EPON VoIP VLAN Profile

Item	Data
Profile name	vlan-test
Tag mode	Tag
VLAN ID	301
Priority	7

Steps

1. In EPON configuration mode, configure the VoIP VLAN profile.

```
ZXAN(config)#epon
ZXAN(config-epon)#voip-vlan profile vlan-test tag-mode tag cvlan 301 priority 7
```

2. (Optional) Query the VoIP VLAN profile.

```
ZXAN(config-epon)#show remote epon voip-vlan profile vlan-test

Voice-vlan profile:   vlan-test
Vlan tag mode:        tag
Cvlan:                301
Priority:             7
Svlan:                0
```

– End of Steps –

4.6 Configuring the EPON H.248 Profile

Using the EPON H.248 profile, you can configure H.248 parameters for EPON ONUs in batches.

Configuration Data

Table 4-6 lists the configuration data of the EPON H.248 profile.

Table 4-6 Configuration Data of the EPON H.248 Profile

Item	Data
Profile name	h248-test
Active server IP address	1.2.3.1
Standby server IP address	1.2.3.2
MG registration mode	Domainname

Steps

1. In GPON configuration mode, configure the SIP profile.

```
ZXAN(config)#epon
ZXAN(config-epon)#h248-profile h248-test register-server ip 1.2.3.1
ZXAN(config-epon)#h248-profile h248-test backup-register-server ip 1.2.3.2
ZXAN(config-epon)#h248-profile h248-test mg register-mode domainname
```

2. (Optional) Query the H.248 profile.

```
ZXAN(config-epon)#show remote epon h248-profile h248-test

H248protocol profile:           h248-test
   register server ip:          1.2.3.1
   port:                        2944
   backup register server ip:   1.2.3.2
   port:                        2944
   rtp link kept flag:          disable
   heartbeat mode:              h248ctc
   cycle-time(in seconds):      60
   count-time:                  3
   MG register mode:            domainname
   MG port:                     2944
```

– End of Steps –

4.7 Configuring the EPON MGCP Profile

Using the EPON MGCP profile, you can configure MGCP parameters for EPON ONUs in batches.

Configuration Data

Table 4-7 lists the configuration data of the EPON MGCP profile.

Table 4-7 Configuration Data of the EPON MGCP Profile

Item	Data
Profile name	mgcp-test

Item	Data
Active server IP address	1.2.3.1
Standby server IP address	1.2.3.2
MG registration mode	Domainname

Steps

1. In EPON configuration mode, configure the MGCP profile.

```
ZXAN(config)#epon
ZXAN(config-epon)#mgcp-profile mgcp-test register-server ip 1.2.3.1
ZXAN(config-epon)#mgcp-profile mgcp-test backup-register-server ip 1.2.3.2
ZXAN(config-epon)#mgcp-profile mgcp-test mg register-mode domainname
```

2. (Optional) Query the MGCP profile.

```
ZXAN(config-epon)#show remote epon mgcp-profile mgcp-test

MGCP protocol profile:        mgcp-test
   register server ip:        1.2.3.1
   port:                      2727
   backup register server ip: 1.2.3.2
   port:                      2727
   heartbeat mode:            mgcp
   cycle-time(in seconds):    60
   count-time:                3
   MG register mode:          domainname
   MG port:                   2427
```

– End of Steps –

4.8 Configuring the EPON SIP Profile

Using the EPON SIP profile, you can configure SIP parameters for EPON ONUs in batches.

Configuration Data

Table 4-8 lists the configuration data of the EPON SIP profile.

Table 4-8 Configuration Data of the EPON SIP Profile

Item	Data
Profile name	sip-test
Active server IP address	1.2.3.1
Standby server IP address	1.2.3.2
Outbound server IP address	1.2.3.1

Steps

1. In EPON configuration mode, configure the SIP profile.

```
ZXAN(config)#epon
ZXAN(config-epon)#sip-profile sip-test register-server ip 1.2.3.1
ZXAN(config-epon)#sip-profile sip-test backup-register-server ip 1.2.3.2
ZXAN(config-epon)#sip-profile sip-test proxy-server ip 1.2.3.1
ZXAN(config-epon)#sip-profile sip-test backup-proxy-server ip 1.2.3.2
ZXAN(config-epon)#sip-profile sip-test outbound-server ip 1.2.3.1
```

2. (Optional) Query the SIP profile.

```
ZXAN(config-epon)#show remote epon sip-profile sip-test

Sip-protocol profile:      sip-test
MG portNo:                 5060
register server ip:        1.2.3.1
port:                      5060
backup register server ip: 1.2.3.2
port:                      5060
proxy server ip:           1.2.3.1
port:                      5060
backup proxy server ip:    1.2.3.2
port:                      5060
outbound server ip:        1.2.3.1
port:                      5060
register interval:         3600
heartbeat:                 enable.
heartbeat cycle:           20
heartbeat count:           3
```

– End of Steps –

4.9 Configuring the EPON Broadband Service

After you configure the EPON broadband service, the subscriber can access the Internet.

Prerequisite

- The EPON ONU has been authenticated.
- The EPON ONU bandwidth profile has been configured.

Configuration Data

Table 4-9 lists the configuration data of the EPON broadband service.

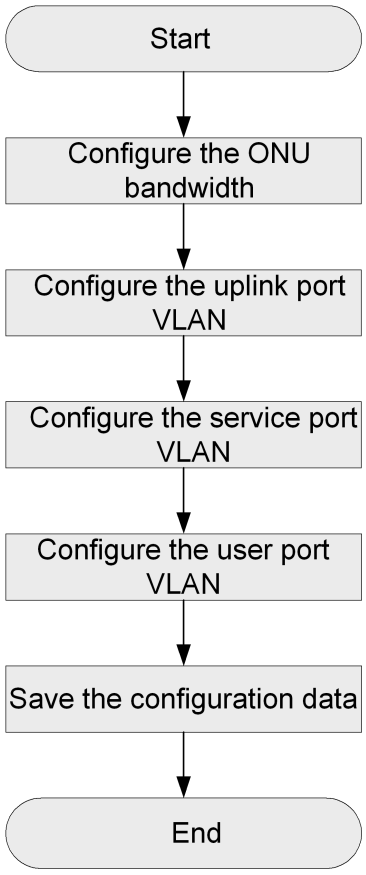
Table 4-9 Configuration Data of the EPON Broadband Service

Item	Data
Service VLAN ID	101
Uplink port	gei_1/3/1
Service port	epon-onu_1/2/1:1
Profile name	10M
User port VLAN	Port: eth_0/1 VLAN mode: tag (The upstream packet is tagged with PVID and the tag of the downstream packet is stripped.) VLAN ID: 101 Priority: 0

Configuration Flowchart

Figure 4-2 shows the configuration flowchart of the EPON broadband service.

Figure 4-2 Configuration Flowchart of the EPON Broadband Service



Steps

1. In ONU interface configuration mode, configure the ONU bandwidth.

- Specify the ONU bandwidth profile.

```
ZXAN(config)#interface epon-onu_1/2/1:1
ZXAN(config-if)#sla-profile 10M
ZXAN(config-if)#exit
```

- Modify the ONU bandwidth directly.

```
ZXAN(config)#interface epon-onu_1/2/1:1
ZXAN(config-if)#sla upstream assured 5000 maximum 10000
ZXAN(config-if)#sla downstream maximum 10000
ZXAN(config-if)#exit
```

2. In uplink interface configuration mode, configure the uplink port VLAN.

```
ZXAN(config)#interface gei_1/3/1
ZXAN(config-if)#switchport vlan 101 tag
ZXAN(config-if)#exit
```

3. In ONU interface configuration mode, configure the service port VLAN.

```
ZXAN(config)#interface epon-onu_1/2/1:1
ZXAN(config-if)#service-port 1 user-vlan 101 vlan 101
ZXAN(config-if)#exit
```

4. In ONU remote management mode, configure the user port VLAN.

```
ZXAN(config)#pon-onu-mng epon-onu_1/2/1:1
ZXAN(epon-onu-mng)#vlan port eth_0/1 mode tag vlan 101 priority 0
ZXAN(gpon-onu-mng)#end
```

5. Save the configuration data.

– End of Steps –

4.10 Configuring the EPON Multicast Service

After you configure the EPON multicast service, subscribers can receive the multicast service streams.

Prerequisite

- The EPON ONU has been authenticated.
- The EPON ONU bandwidth profile has been configured.

Configuration Data

Table 4-10 lists the configuration data of the EPON multicast service.

Table 4-10 Configuration Data of the EPON Multicast Service

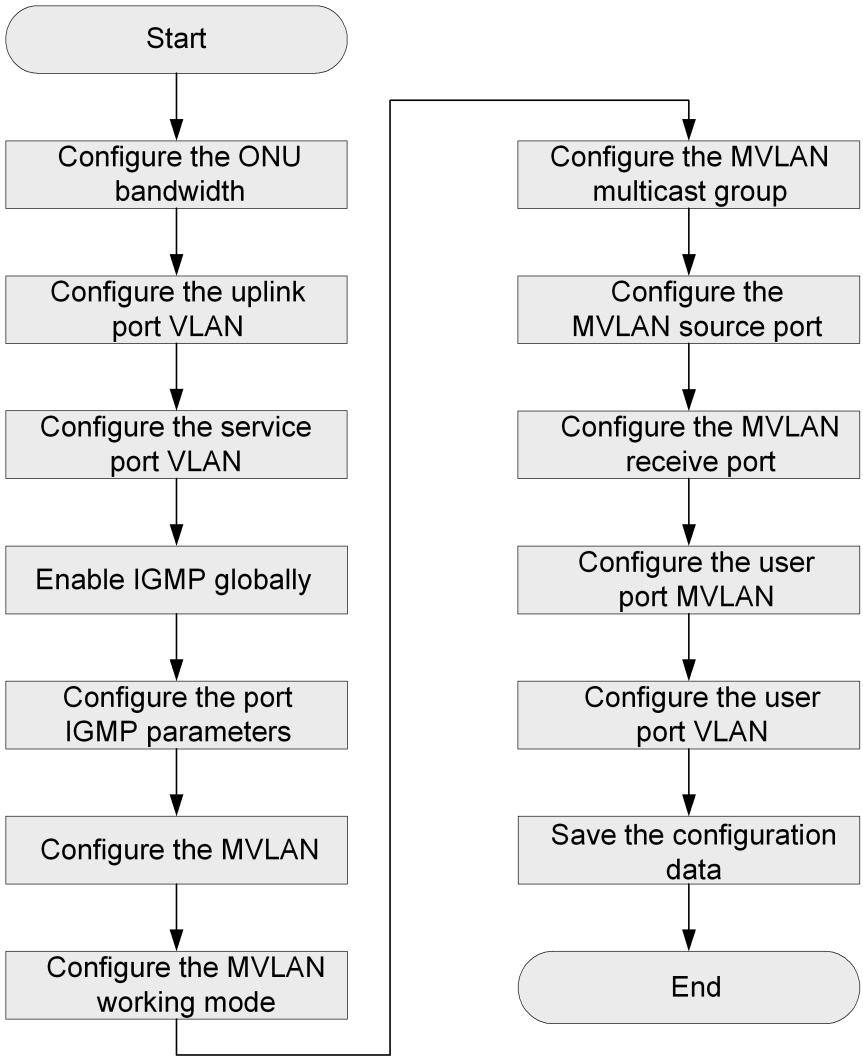
Item	Data
MVLAN ID	201
Service priority	5

Item	Data
MVLAN working mode	Proxy (default)
MVLAN multicast group	224.1.1.1 – 224.1.1.3
Uplink port	gei_1/3/1
Service port	epon-onu_1/2/1:1
Profile name	10M
User port VLAN	MVLAN ID: 201 MVLAN tag stripping: enable
User port VLAN	Port: eth_0/2 VLAN mode: tag (The untagged upstream packet is tagged with PVID.) VLAN ID: 201

Configuration Flowchart

Figure 4-3 shows the configuration flowchart of the EPON multicast service.

Figure 4-3 Configuration Flowchart of the EPON Multicast Service



Steps

1. In ONU interface configuration mode, configure the ONU bandwidth.

```
ZXAN(config)#interface epon-onu_1/2/1:1
ZXAN(config-if)#sla-profile 10M
ZXAN(config-if)#exit
```

2. In uplink interface configuration mode, configure the uplink port VLAN.

```
ZXAN(config)#interface gei_1/3/1
ZXAN(config-if)#switchport vlan 201 tag
ZXAN(config-if)#exit
```

3. In ONU interface configuration mode, configure the service port VLAN.

```
ZXAN(config)#interface epon-onu_1/2/1:1
ZXAN(config-if)#service-port 1 user-vlan 201 vlan 201
ZXAN(config-if)#exit
```

4. (Optional) Enable IGMP globally.

```
ZXAN(config)#igmp enable
```

5. Configure the port IGMP parameters.

```
ZXAN(config)#interface epon-onu_1/2/1:1
ZXAN(config-if)#igmp fast-leave enable vport 2
ZXAN(config-if)#exit
```

6. Configure the MVLAN.

```
ZXAN(config)#igmp mvlan 201
```

7. (Optional) Configure the MVLAN working mode.

```
ZXAN(config)#igmp mvlan 201 work-mode proxy
```

8. Configure the MVLAN multicast group.

```
ZXAN(config)#igmp mvlan 201 group 224.1.1.1 to 224.1.1.3
```

9. Configure MVLAN source port.

```
ZXAN(config)#igmp mvlan 201 source-port gei_1/3/1
```

10. Configure the MVLAN receive port.

```
ZXAN(config)#igmp mvlan 201 receive-port epon-onu_1/2/1:1 vport 2
```

11. In ONU remote management mode, configure the user port VLAN.

```
ZXAN(config)#pon-onu-mng epon-onu_1/2/1:1
ZXAN(epon-onu-mng)#multicast vlan port eth_0/2 add vlanlist 201
ZXAN(epon-onu-mng)#multicast vlan tag-strip port eth_0/2 enable
```

12. Configure the user port VLAN.

```
ZXAN(epon-onu-mng)#vlan port eth_0/2 mode tag vlan 201 priority 5
ZXAN(epon-onu-mng)#end
```

13. Save the configuration data.

– End of Steps –

4.11 Configuring the EPON Voice Service (H.248)

After you configure the EPON voice service, subscribers can make and answer phone calls. This section takes the H.248 protocol as an example.

Prerequisite

- The EPON ONU has been authenticated.
- The EPON ONU bandwidth profile has been configured.
- The EPON VoIP IP profile has been configured.
- The EPON VoIP VLAN profile has been configured.
- The EPON H.248 profile has been configured.

Configuration Data

Table 4-11 lists the configuration data of the EPON voice service.

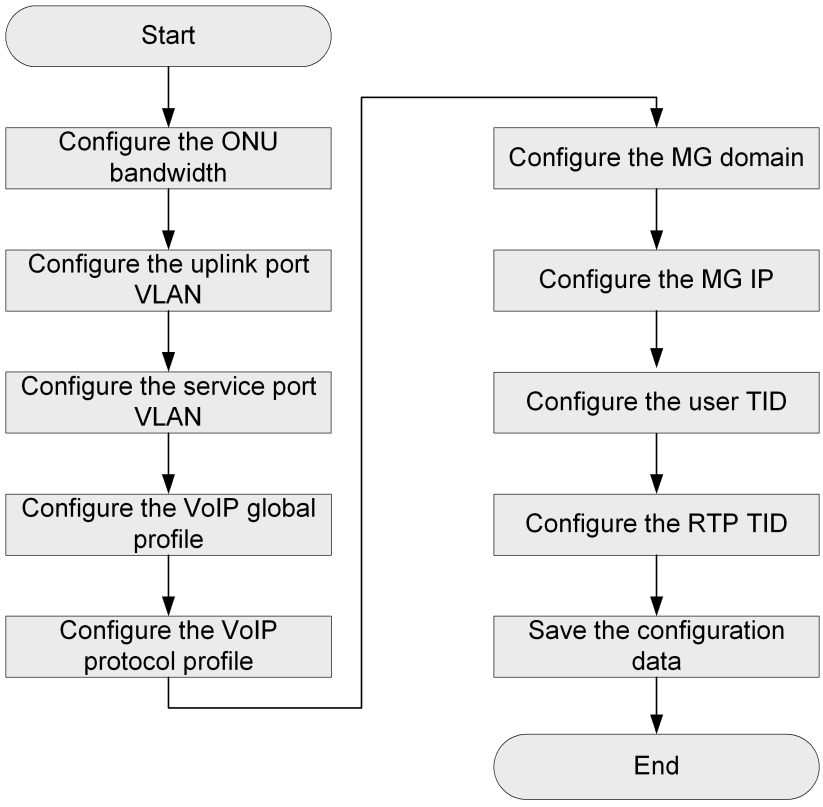
Table 4-11 Configuration Data of the EPON Voice Service

Item	Data
Service VLAN ID	301
Service priority	7
Uplink port	gei_1/3/1
Service port	epon-onu_1/2/1:1
Profile name	10M
MG	IP address: 1.2.3.4 Gateway: 1.2.3.1 Domain name: iad.zte.com.cn
VoIP global profile	IP profile: ip-test VLAN profile: vlan-test
VoIP protocol profile	Protocol type: H.248 Protocol profile: h248-test
User voice resource	User TID: USER00–USER01 RTP TID: RTPR00-RTPR001

Configuration Flowchart

Figure 4-4 shows the configuration flowchart of the EPON voice service.

Figure 4-4 Configuration Flowchart of the EPON Voice Service



Steps

1. In ONU interface configuration mode, configure the ONU bandwidth.

```
ZXAN(config)#interface epon-onu_1/2/1:1
ZXAN(config-if)#sla-profile 10M
ZXAN(config-if)#exit
```

2. In uplink interface configuration mode, configure the uplink port VLAN.

```
ZXAN(config)#interface gei_1/3/1
ZXAN(config-if)#switchport vlan 301 tag
ZXAN(config-if)#exit
```

3. In ONU interface configuration mode, configure the service port VLAN.

```
ZXAN(config)#interface epon-onu_1/2/1:1
ZXAN(config-if)#service-port 1 user-vlan 301 vlan 301
ZXAN(config-if)#exit
```

4. In ONU remote management mode, configure the VoIP global profile.

```
ZXAN(config)#pon-onu-mng epon-onu_1/2/1:1
ZXAN(epon-onu-mng)#voip-module global-profile apply ip ip-test vlan vlan-test
```

5. Configure the VoIP protocol profile.

```
ZXAN(epon-onu-mng)#voip-module protocol-profile apply h248 h248-test
```

6. Configure the MG domain name.

```
ZXAN(epon-onu-mng)#voip mg-domainname iad.zte.com.cn slot 1
```

7. Configure the MG IP address.

```
ZXAN(epon-onu-mng)#voip ip-address 1.2.3.4 mask 255.255.255.0 slot 1
```

8. Configure the user TID.

```
ZXAN(epon-onu-mng)#voip user-tid 1 beginid 1 tid-num 2 prefix USER begin-digit 0
align enable digit-length 2 slot 1
```

9. Configure the RTP TID.

```
ZXAN(epon-onu-mng)#voip rtp-tid prefix RTP begin-digit 0 align enable digit-length
2 slot 1
ZXAN(epon-onu-mng)#end
```

10. Save the configuration data.

– End of Steps –

4.12 Configuring the EPON Voice Service (SIP)

After you configure the EPON voice service, subscribers can make and answer phone calls. This section takes the SIP protocol as an example.

Prerequisite

- The EPON ONU has been authenticated.

- The EPON ONU bandwidth profile has been configured.
- The EPON VoIP IP profile has been configured.
- The EPON VoIP VLAN profile has been configured.
- The EPON SIP profile has been configured.

Configuration Data

Table 4-12 lists the configuration data of the EPON voice service.

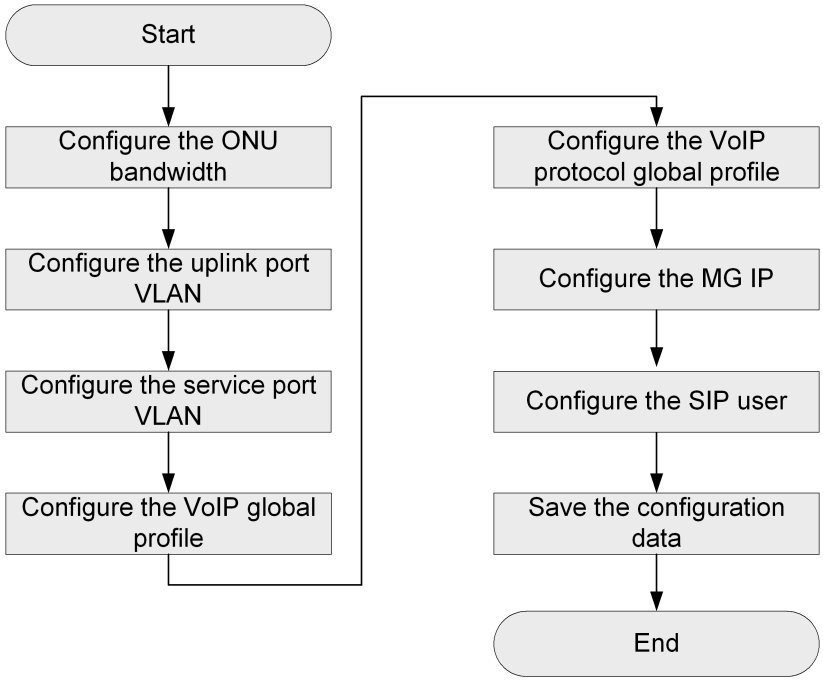
Table 4-12 Configuration Data of the EPON Voice Service

Item	Data
Service VLAN ID	301
Service priority	7
Uplink port	gei_1/3/1
Service port	epon-onu_1/2/1:1
Profile name	10M
VoIP global profile	IP profile: ip-test VLAN profile: vlan-test
VoIP protocol profile	Protocol type: SIP Protocol profile: sip-test
MG IP address	1.2.3.4
VoIP service	Port: pots_0/1 User ID: 12345 User name: 12345 Password: 12345

Configuration Flowchart

Figure 4-5 shows the configuration flowchart of the EPON voice service.

Figure 4-5 Configuration Flowchart of the EPON Voice Service



Steps

1. In ONU interface configuration mode, configure the ONU bandwidth.

```
ZXAN(config)#interface epon-onu_1/2/1:1
ZXAN(config-if)#sla-profile 10M
ZXAN(config-if)#exit
```

2. In uplink interface configuration mode, configure the uplink port VLAN.

```
ZXAN(config)#interface gei_1/3/1
ZXAN(config-if)#switchport vlan 301 tag
ZXAN(config-if)#exit
```

3. In ONU interface configuration mode, configure the service port VLAN.

```
ZXAN(config)#interface epon-onu_1/2/1:1
ZXAN(config-if)#service-port 1 user-vlan 301 vlan 301
ZXAN(config-if)#exit
```

4. In ONU remote management mode, configure the VoIP global profile.

```
ZXAN(config)#pon-onu-mng epon-onu_1/2/1:1
ZXAN(epon-onu-mng)#voip-module global-profile apply ip ip-test vlan vlan-test
```

5. Configure the VoIP protocol profile.

```
ZXAN(epon-onu-mng)#voip-module protocol-profile apply sip sip-test
```

6. Configure the MG IP address.

```
ZXAN(epon-onu-mng)#voip ip-address 1.2.3.4 mask 255.255.255.0 slot 1
```

7. Configure the SIP user.

```
ZXAN(epon-onu-mng)#voip sip-user account 12345 name 12345 password 12345 interface pots_0/1
ZXAN(epon-onu-mng)#end
```

8. Save the configuration data.

– End of Steps –

4.13 Configuring the EPON P2P Service

After you configure the EPON P2P service, certain subscribers under an EPON OLT interface can communicate with each other.

Prerequisite

The EPON broadband, multicast, or voice service is configured.

Steps

1. In OLT interface configuration mode, configure P2P mode and group.

```
ZXAN(config)#interface epon-olt_1/3/1
ZXAN(config-if)#p2p mode group
ZXAN(config-if)#p2p group 1
ZXAN(config-if)#p2p group-name 1 test-group
```

2. In ONU interface configuration mode, configure the ONU to join the P2P group.

```
ZXAN(config)#interface epon-onu_1/3/1:1
ZXAN(config-if)#join-p2p-group 1
ZXAN(config-if)#exit
ZXAN(config)#interface epon-onu_1/3/1:2
ZXAN(config-if)#join-p2p-group 1
```

3. (Optional) Query the P2P configuration.

```
ZXAN(config-if)#show p2p summary epon-olt_1/3/1
P2P mode :      GROUP

Group ID :      1
Group name :    test-group
ONU list:       1, 2
```

4. Save configuration data.

– End of Steps –

This page intentionally left blank.

Chapter 5
P2P Service Configuration

The ZXA10 C320 supports P2P service. P2P interfaces are actually Ethernet interfaces. Using the WDM technology, a P2P interface transmits and receives signals through a single optical fiber, while a traditional Ethernet interface uses two optical fibers to transmit and receiving signals. The P2P service can save a large number of optical fiber resources and thus reduce the network construction cost.

P2P service are suitable for the following scenarios.

- VIP dedicated line

  The most popular application. Because each user exclusively possesses an optical fiber, the reliable optical-layer security isolation is provided.

- Base station back-haul

  The P2P service provides connection to base stations directly or through P2P ring.

- Device interconnection

  When optical fiber resources are limited, the P2P service can be used for device interconnection.

Table of Contents

5.1 Configuring the P2P Service

The ZXA10 C320 are connected ONUs or other Ethernet devices through the P2P interface card. After you configure the P2P service, the subscribers can enjoy the data, multicast, and VoIP service.

Context

The P2P interfaces support smart VLAN configuration based on service-port.

- Adding a SVLAN to user VLANs according to user VLAN range.
- Translating user VALN to SVLAN + VLAN.
- Modifying the 802.1p priority of SVLAN.
- Adding a SVLAN to a user VLAN according to the combination, such as user VLAN + Ethernet type.

Configuration Data

Table 5-1 list the configuration data of the P2P service.

Table 5-1 P2P Service Configuration Data

Item	Data
Data service VLAN ID	CVLAN ID：101 – 124 SVLAN ID：1001
Multicast service VLAN ID	201
VoIP service VLAN ID	301
Uplink port	gei_1/3/1
Service port	gei_1/1/1
MVLAN working mode	Proxy (default)
MVLAN group	224.1.1.1 – 224.1.1.3

Steps

1. In uplink interface configuration mode, configure uplink port VLAN.

```
ZXAN(config)#interface gei_1/3/1
ZXAN(config-if)#switchport vlan 1001,201,301 tag
ZXAN(config-if)#exit
```

2. In P2P interface configuration mode, configure service port VLAN.

```
ZXAN(config)#interface gei_1/1/1
ZXAN(config-if)#service-port 1 user-vlan 101 to 124 svlan 1001
ZXAN(config-if)#service-port 2 user-vlan 201 vlan 201
ZXAN(config-if)#service-port 3 user-vlan 301 vlan 301
ZXAN(config-if)#exit
```

3. (Optional) Enable global IGMP protocol.

```
ZXAN(config)#igmp enable
```

Note:

By default, the global IGMP protocol is enabled on the ZXA10 C320.

---

4. Configure IGMP parameters on service port.

```
ZXAN(config)#interface gei_1/1/1
ZXAN(config-if)#igmp fast-leave enable
ZXAN(config-if)#exit
```

5. Configure the MVLAN.

```
ZXAN(config)#igmp mvlan 201
```

6. (Optional) Configure MVLAN working mode.

```
ZXAN(config)#igmp mvlan 201 work-mode proxy
```

7. Configure MVLAN multicast groups.

```
ZXAN(config)#igmp mvlan 201 group 224.1.1.1 to 224.1.1.3
```

8. Configure MVLAN source port.

```
ZXAN(config)#igmp mvlan 201 source-port gei_1/3/1
```

9. Configure MVLAN receiving port.

```
ZXAN(config)#igmp mvlan 201 receive-port gei_1/1/1
```

10. Save configuration data.

– End of Steps –

Follow-Up Action

The P2P interfaces supports the following configuration:

- QoS (see 8.1 Ethernet Interface QoS Configuration)
- DHCP (see Chapter 13 DHCP Configuration)
- Port location (see 16.1 Port Location Configuration)
- Link aggregation (see 14.1 Configuring Link Aggregation)

The DHCP configuration and port location configuration on the P2P interfaces are similar to the configuration on the PON ONU interfaces.

The QoS configuration and link aggregation configuration on the P2P interfaces are similar to the configuration on the Ethernet interfaces.

This page intentionally left blank.

Chapter 6
VLAN Configuration

VLAN is a technology that implements virtual workgroups by dividing the physical equipment in a LAN into several logical network segments. The IEEE issued the IEEE 802.1q standard in 1999 to normalize the VLAN solution.

The ZXA10 C320 supports 4094 VLANs.

Table 6-1 lists the VLAN specifications.

Table 6-1 VLAN Specifications

VLAN Type	Description
Basic VLAN	Used to isolate ports.
Service port VLAN	Used to implement VLAN translation at the ONU level.
TLS VLAN	Used to add an SVLAN to the packet to implement the Transparent LAN Service (TLS) whatever the user access mode is, or no matter whether the upstream packet has a VLAN tag, or whatever the VLAN tag is.
Cross-connection VLAN	Used to set the special channel for the user port and uplink port. The packets are forwarded in 1:1 mode according to the VLAN ID.
VLAN smart QinQ	Used to extend VLAN, adding different SVLANs according to different data streams.
VLAN translation	Used to translate user-side VLAN to network-side VLAN, adding different SVLANs according to different data streams.

Table of Contents

6.1 Configuring the Uplink Port VLAN

By configuring the uplink port VLAN, you can classify ports into different network segments logically to control the communication between ports.

Steps

1. In uplink interface configuration mode, configure the port VLAN.

```
ZXAN(config)#interface gei_1/3/1
ZXAN(config-if)#switchport vlan 2-100 tag
```

NOTE **Note:**

When you configure the uplink port VLAN, the system will automatically create the corresponding VLAN.

– End of Steps –

6.2 Configuring the Service Port VLAN

By configuring the service port VLAN on the PON ONU interface, you can implement VLAN translation at the ONU level.

Prerequisite

The ONU has been authenticated.

Context

The service port configuration supports the following applications:

- Add CVLAN + SVLAN to untagged packets
- Add SVLAN to user VLANs according to user VLAN range
- Translate user VLAN to VLAN + SVLAN
- Translate Ethernet protocol type to VLAN + SVLAN
- Translate 802.1p priority to VLAN + SVLAN
- Translate combination (user VLAN, Ethernet protocol type, and 802.1p priority) to VLAN + SVLAN
- Modify SVLAN 802.1p priority
- TLS VLAN

Steps

1. In ONU interface configuration mode, configure the service port VLAN.

```
ZXAN(config)#interface epon-onu_1/2/1:1
ZXAN(config-if)#service-port 1 vport 1 user-vlan 7 vlan 8 svlan 9
ZXAN(config-if)#service-port 2 vport 1 other-all tls-vlan 501
```

2. (Optional) Query the configured service port VLAN.

```
ZXAN(config-if)#show service-port interface epon-onu_1/2/1:1
Interface epon-onu_1/2/1:1
Sport Vport BeginVid EndVid OuterVid InnerVid UserPrio Dscp Etype  Filter Vlan C
os SVlan SCos Tls  Mode Ingress Egress  Queue Status Enable
--------------------------------------------------------------------------------
```

```
-------------------------------------------------------------
1     1     7         7       --       --       --       --   --     --     8    -
-  9     --    --    1:1  --       --       --     --     YES
2     1     --        --      --       --       --       --   --     --     --   -
-  --    --    501   --    --       --       --     --     YES
Sport total number:
2
```

– End of Steps –

6.3 Configuring the Cross-Connection VLAN

By configuring the cross-connection VLAN, you can implement 1:1 VLAN forwarding.

Context

The cross-connection VLAN is a special channel for a user port and an uplink port. When the cross-connection VLAN is configured, packets are forwarded in 1:1 mode according to the VLAN ID but not forwarded in MAC + VLAN mode.

1:1 VLAN exchange is implemented in the following two modes:

- SVLAN
- CVLAN + SVLAN dual tags

Steps

1. In uplink interface configuration mode, configure the port VLAN.

```
ZXAN(config)#interface gei_1/3/1
ZXAN(config-if)#switchport vlan 5 tag
ZXAN(config-if)#exit
```

2. In ONU interface configuration mode, configure the service port VLAN.

```
ZXAN(config)#interface gpon-onu_1/1/1:1
ZXAN(config-if)#service-port 1 vport 1 user-vlan 3 svlan 5
ZXAN(config-if)#exit
```

3. In VLAN configuration mode, configure the VLAN to the cross-connection VLAN.

```
ZXAN(config)#vlan 5
ZZXAN(config-vlan)#xconnect enable cvlan 3
```

4. (Optional) Query the cross-connection VLAN configuration.

```
ZXAN(config-vlan)#show vlan-xconnect detail
User-Port                    Uplink-Port  Svlan  Cvlan
-------------------------------------------------------
gpon-onu_1/1/1:1 vport 1     gei_1/3/1   5      3
```

– End of Steps –

6.4 Configuring the VLAN Smart QinQ

By configuring the VLAN smart QinQ, you can add different external VLAN tags to different service streams to classify service streams.

Context

The service streams of the ZXA10 C320 smart QinQ are classified based on the following items:

- CoS Priority of the service stream
- User CVLAN range
- Ethernet type of the service stream
- CVLAN + CoS
- CVLAN + Ethernet type

For GPON service, it is recommended to implement VLAN smart QinQ by the service-port VLAN, not the VLAN smart QinQ on the GPON OLT interface.

Steps

1. In global configuration mode, enable the global smart QinQ function.

```
ZXAN(config)#vlan-smart-qinq enable
```

2. In OLT interface configuration mode, enable the smart QinQ function on the interface.

```
ZXAN(config)#interface epon-olt_1/2/1
ZXAN(config-if)#vlan-smart-qinq enable
ZXAN(config-if)#exit
```

NOTE **Note:**

Before enable the smart QinQ function on the OLT interface, you need to clear all service–port and switchport entries on all ONU interfaces under the OLT port.

---

3. Configure the VLAN smart QinQ rule.

```
ZXAN(config)#vlan-smart-qinq ingress-port epon-olt_1/2/1 cvlan 200 to 299 svlan
4000 newcos 6
ZXAN(config)#vlan-smart-qinq ingress-port epon-olt_1/2/1 ether-type 0x8863 svlan
1000
```

4. In uplink interface configuration mode, configure the port VLAN.

```
ZXAN(config)#interface gei_1/3/1
ZXAN(config-if)#switchport vlan 1000,4000 tag
ZXAN(config-if)#exit
```

5. (Optional) Query the smart QinQ rule.

```
ZXAN(config)#show vlan-smart-qinq
```

```
smart-qinq item num(used): 2
Ingress-Port      Begin- End-   EType  Cos Svlan NewCos GroupId Status
                  Vid    Vid
------------------------------------------------------------------------
epon-olt_1/2/1    200    299    ----   --  4000  6      --      OK
epon-olt_1/2/1    ----   ----   0x8863 --  1000  --     --      OK
```

– End of Steps –

6.5 Configuring the VLAN Translation

By configuring the VLAN translation entries, you can convert user-side VLANs to network-side VLANs to classify service streams. By default, the VLAN translation is in 1:1 mode, which means one user-side VLAN is converted to one network-side VLAN

Context

For GPON service, it is recommended to implement VLAN translation by the service-port VLAN, not the VLAN translation on the GPON OLT interface.

Steps

1. In global configuration mode, configure the VLAN translation entries.
   a. Configure 1:1 VLAN translation.

      ```
      ZXAN(config)#vlan-translate ingress-port epon-olt_1/2/1 user-vlan 101 vlan
      201 1:1
      ```

   b. Configure N:1 VLAN translation.

      ```
      ZXAN(config)#vlan-translate ingress-port epon-olt_1/2/1 user-vlan 102 vlan
      202 N:1
      ZXAN(config)#vlan-translate ingress-port epon-olt_1/2/1 user-vlan 103 vlan
      202 N:1
      ```

   c. Configure 1:1 VLAN translation and add SVLAN.

      ```
      ZXAN(config)#vlan-translate ingress-port epon-olt_1/2/1 user-vlan 100 vlan
      200 svlan 300 1:1
      ```

   d. Configure N:1 VLAN translation and add SVLAN.

      ```
      ZXAN(config)#vlan-translate ingress-port epon-olt_1/2/1 user-vlan 105 vlan
      205 svlan 305 N:1
      ZXAN(config)#vlan-translate ingress-port epon-olt_1/2/1 user-vlan 106 vlan
      205 svlan 305 N:1
      ```

Note:

Before configuring VLAN translation entries on the OLT interface, you need to clear all service–port and switchport entries on all ONU interfaces under the OLT port.

2. In uplink interface configuration mode, configure interface VLAN.

```
ZXAN(config)#interface gei_1/3/2
ZXAN(config-if)#switchport vlan 201,202,300,305 tag
ZXAN(config-if)#exit
```

3. (Optional) Query VLAN translation configuration.

```
ZXAN(config)#show vlan-translate
Ingress-Port      User-Vlan Vlan  Svlan TransMode
-------------------------------------------------------------------------------
epon-olt_1/2/1    100       200   300     1:1
epon-olt_1/2/1    101       201   --      1:1
epon-olt_1/2/1    102       202   --      N:1
epon-olt_1/2/1    103       202   --      N:1
epon-olt_1/2/1    105       205   305     N:1
epon-olt_1/2/1    106       205   305     N:1
```

– End of Steps –

6.6 Configuring the VLAN Translation for Broadcast Traffic

After you configure the VLAN translation on Broadcast LLID or GEM port, the ZXA10 C320 can process the VLAN for the downstream traffic on broadcast LLID and broadcast GEM port.

Context

The VLAN configuration on service-port, switchport, or PON OLT interface are only valid for the traffic on unicast LLID and unicast GEM port, but not the downstream traffic on broadcast LLID and broadcast GEM port.

- For the EPON interface cards, only downstream multicast, broadcast, and flooding traffic are transmitted on the broadcast LLIDs, all other downstream traffic and all upstream traffic are transmitted on the unicast LLIDs.
- For the GPON interface cards, only downstream multicast traffic are transmitted on the broadcast GEM ports, all other downstream traffic and all upstream traffic are transmitted on the unicast GEM ports.

Steps

1. Configure the global MVLAN translation entry.

```
ZXAN(config)#mvlan-translate 4000 to 3006
```

2. Configure processing rule for SCB VLAN on the EPON OLT interface.
   - Remove the VLAN tag from SCB downstream traffic.

```
ZXAN(config)#vlan-scb-action interface epon-olt_1/2/1 vlan-remove 4094
```

   - Configure the VLAN translation rule for SCB downstream traffic.

```
ZXAN(config)#vlan-scb-action interface epon-olt_1/2/1 vlan-translate svlan 10
vlan 20 user-vlan 30
```

– End of Steps –

This page intentionally left blank.

Chapter 7
IPTV Configuration

The secondary duplication of the Internet Protocol Television (IPTV) layer-2 multicast service is implemented on the OLT and ONU. The related configuration information is as follows:

- Configurations of the basic OLT service parameters

  The basic parameters of layer-2 multicast control includes multicast VLAN, source port, receive port, and multicast program address. The multicast VLAN is the VLAN that carries the multicast data. The source port is the uplink port that connects the multicast source. The receive port is the ONU interface that connects the multicast subscriber. The multicast program address consists of the group address and source address.

- Configuration of the OLT multicast protocol mode

  The ZXA10 C320 supports the IPv4 and IPv6 multicast dual protocol stack so it can be flexibly configured to accept/drop packets of various protocols. Three working modes (Snooping/Router/Proxy) can be configured based on the multicast VLAN.

- Configuration of ONU user rights

  Based on the ITU-T G984.4 standard, the OLT configures the multicast right profile to the ONU via the OMCI interface. The ONU runs the IGMP Snooping protocol, and implements the user right control according to the local multicast right table.

Service Description

As the streaming media such as the multimedia video and data warehouse appear in the IP network, the multicast application gradually becomes the new service demand. The multicast service is applicable to the streaming media, tele-education, video conference, video multicast (Web TV), network game, data copy, and any other point-to-multipoint data transmission application.

Service Specifications

ZXA10 C320 has the carrier-class multicast operation capacity. It supports multicast protocols and controllable multicast and supports a full set of protocols from the subscriber to the network. Hence, it provides a basis for the broadband multicast value-added service and multicast service management. The ZXA10 C320 provides operational and manageable controllable multicast service, supports the Internet Group Management Protocol (IGMP) v1/v2/v3, and supports the IGMP snooping, IGMP proxy, and IGMP router modes.

- Supports the IGMP v1/v2/v3.

- Supports Multicast Listener Discovery (MLD) v1/v2.
- Supports IGMP Snooping/Proxy/Router.
- Supports MLD Snooping/Proxy.
- Supports 8K multicast entries.
- Supports 256 multicast VLANs.
- Supports Channel Access Control (CAC).
- Supports channel preview.
- Supports Call Detail Record (CDR).

Table of Contents

7.1 Configuring the IGMP MVLAN

The IGMP MVLAN is the VLAN that carries the IGMP multicast data, which includes the service VLAN, source port, receive port, and multicast group.

Configuration Data

Table 7-1 lists the configuration data of the IGMP MVLAN.

Table 7-1 Configuration Data of the IGMP MVLAN

Item	Data
IGMP	Enable
Span VLAN function	Enable
MVLAN ID	200
MVLAN working mode	Proxy
MVLAN host version	IGMPv3
IGMP packet processing mode	IGMPv1: drop IGMPv2: drop IGMPv3: accept
Multicast group IP address	224.1.1.1–224.1.1.3
Multicast source port	gei_1/3/1
Multicast receive port	ONU interface: gpon-onu_1/1/1:1 Virtual port ID: 2

Steps

1. Enable IGMP globally.

```
ZXAN(config)#igmp enable
```

2. Enable IGMP span VLAN function.

```
ZXAN(config)#igmp span-vlan enable
```

3. Configure the IGMP packet processing mode.

```
ZXAN(config)#igmp version-mode v1 drop
ZXAN(config)#igmp version-mode v2 drop
ZXAN(config)#igmp version-mode v3 accept
```

4. Configure the MVLAN.

```
ZXAN(config)#igmp mvlan 200
```

5. Configure the MVLAN working mode.

```
ZXAN(config)#igmp mvlan 200 work-mode proxy
```

6. Configure the MVLAN host version.

```
ZXAN(config)#igmp mvlan 200 host-version v3
```

7. Configure the MVLAN multicast group.

```
ZXAN(config)#igmp mvlan 200 group 224.1.1.1 to 224.1.1.3
```

8. Configure MVLAN source port.

```
ZXAN(config)#igmp mvlan 200 source-port gei_1/3/1
```

9. Configure the MVLAN receive port.

```
ZXAN(config)#igmp mvlan 200 receive-port gpon-onu_1/1/1:1 vport 2
```

10. (Optional) Query the IGMP global configuration.

```
ZXAN(config)#show igmp
IGMP global parameters:
-----------------------------------------------------
IGMP is globally enable.
IGMP log is disable.
Snooping aging time is 300 seconds.
Span vlan is enable.
Bandwidth control is disable.
Host tracking is disable.
Robustness variable is 2.
General query interval is 125(second).
Query max response time is 100(0.1second).
Last member query interval is 10(0.1second).
Last member query count is 2.
Unsolicited report interval is 10 seconds.
Non match group is forward.
Intermode status is disable.
Prejoin interval is 120(second).
Igmp version-mode v1 is drop.
Igmp version-mode v2 is drop.
Igmp version-mode v3 is accept.
```

```
General query gemport mode is unicast.
```

11. (Optional) Query the MVLAN.

```
ZXAN(config)#show igmp mvlan

Total Num is 1.
Total Receive-Port Num is 1.
VID Status  Mode     Host IP         GroupFilter MaxGroups ActGroups HostVersion

------------------------------------------------------------------------------
200  enable  proxy    192.168.2.14    enable      4096      0         v3

ZXAN(config)#show igmp mvlan 200
Protocol packet's priority is 0 (in proxy/router mode)
Act Port is 0
Cvlan is 0
Source Port
----------------------------
gei_1/3/1

Receive Port
----------------------------
gpon-onu_1/1/1:1:2

Group
----------------------------
224.1.1.1 - 224.1.1.3
```

– End of Steps –

7.2 Configuring the MLD MVLAN

The MLD MVLAN is the VLAN that carries the MLD multicast data, which includes the service VLAN, source port, receive port, and multicast group.

Configuration Data

Table 7-2 lists the configuration data of the MLD MVLAN.

Table 7-2 Configuration Data of the MLD MVLAN

Item	Data
MLD	Enable
Span VLAN function	Enable
MVLAN ID	200
MVLAN working mode	Proxy

Item	Data
MVLAN host version	MLDv1
Multicast group IP address	ff1e::0101–ff1e::0103
Multicast source port	gei_1/3/1
Multicast receive port	ONU interface: gpon-onu_1/1/1:1 Virtual port ID: 2

Steps

1. Enable MLD globally.

```
ZXAN(config)#mld enable
```

2. Enable MLD span VLAN function.

```
ZXAN(config)#mld span-vlan enable
```

3. Configure the MVLAN.

```
ZXAN(config)#mld mvlan 200
```

4. Configure the MVLAN working mode.

```
ZXAN(config)#mld mvlan 200 work-mode proxy
```

5. Configure the MVLAN host version.

```
ZXAN(config)#mld mvlan 200 host-version v1
```

6. Configure the MVLAN multicast group.

```
ZXAN(config)#mld mvlan 200 group ff1e::0101 to ff1e::0103
```

7. Configure MVLAN source port.

```
ZXAN(config)#mld mvlan 200 source-port gei_1/3/1
```

8. Configure the MVLAN receive port.

```
ZXAN(config)#mld mvlan 200 receive-port gpon-onu_1/1/1:1 vport 2
```

9. (Optional) Query the MLD global configuration.

```
ZXAN(config)#show mld
MLD global parameters:
-----------------------------------------------------
Mld is globally enable.
Mld log is disable.
Snooping aging time is 300 seconds.
Span vlan is enable.
Bandwidth control is disable.
Host tracking is disable.
Robustness variable is 2.
General query interval is 125(second).
Query max response time is 100(0.1second).
Last member query interval is 10(0.1second).
Last member query count is 2.
```

```
Unsolicited report interval is 10 seconds.
Non match group is forward.
Intermode status is disable.
Prejoin interval is 120(second).
```

10. (Optional) Query the MVLAN.

```
ZXAN(config)#show mld mvlan

Total Num is 1.
Total Receive-Port Num is 1.
VID Status  Mode     Host IP         GroupFilter MaxGroups ActGroups HostVersion

------------------------------------------------------------------------------
200  enable  proxy    fe80::c0a8:20e  enable      4096      0         v1

ZXAN(config)#show mld mvlan 200
Protocol packet's priority is 0 (in proxy/router mode)
Act Port is 0
Cvlan is 0
Source Port
----------------------------
gei_1/3/1

Receive Port
----------------------------
gpon-onu_1/1/1:1:2

Group
----------------------------
ff1e::101 - ff1e::103
```

– End of Steps –

7.3 Configuring the IPTV Package

By configuring the IPTV package, you can manage the access right of the IPTV channel.

Prerequisite

The MVLAN has been configured.

Configuration Data

Table 7-3 lists the configuration data of the IPTV package.

Table 7-3 Configuration Data of the IPTV Package

Item	Data
IPTV channel	Name: stv Multicast group IP address 224.1.1.1
IPTV package	Name: pkg1 Channel: stv Right: watch

Steps

1. Configure the IPTV channel.

```
ZXAN(config)#iptv channel mvlan 200 group 224.1.1.1 name stv
```

2. Create the IPTV package.

```
ZXAN(config)#iptv package name pkg1
```

3. Configure the channel in the IPTV package.

```
ZXAN(config)#iptv package pkg1 channel stv watch
```

4. (Optional) Query the IPTV channel.

```
ZXAN(config)#show iptv channel
Total channel number  :1
------------------------------------------------------------------
ID      mvlan     group                                    name
------------------------------------------------------------------
0       200       224.1.1.1                                STV
```

5. (Optional) Query the IPTV package.

```
ZXAN(config)#show iptv package pkg1
Package name: PKG1
Total channel number: 1
------------------------------------------------------------------------------
Ip-address                          Mvlan   Right    Id   Name
------------------------------------------------------------------------------
224.1.1.1                           200     Watch    0    STV
```

– End of Steps –

7.4 Configuring the Port IPTV Right

By configuring the IPTV right for port, you can apply the IPTV package to the subscriber port to implement the access control of the IPTV channel.

Prerequisite

- The MVLAN has been configured.
- The IPTV package has been configured.

Context

The ZXA10 C320 supports 2-level CAC.

- When the CAC function is enabled globally, the subscriber port IPTV right takes effect and only the subscriber who subscribes the package can access the channel in the package.
- When the global CAC function is disabled, the subscriber port IPTV right does not take effect and subscribers in the MVLAN can access the channel in the MVLAN.

By default, the global CAC function is disabled.

Steps

1. Enable the CAC function globally.

```
ZXAN(config)#iptv cac enable
```

2. In ONU interface configuration mode, configure the port right.

```
ZXAN(config)#interface gpon-onu_1/1/1:1
ZXAN(config-if)#iptv package pkg1
ZXAN(config-if)#exit
```

3. (Optional) Query the IPTV global configuration.

```
ZXAN(config)#show iptv control
CAC      : enable
SMS      : 192.168.0.119
```

4. (Optional) Query the IPTV port configuration.

```
ZXAN(config)#show iptv interface gpon-onu_1/1/1:1
auth-mode : auth
right-mode: package
cdrstatus : enable
service   : IN_SERVICE
```

– End of Steps –

Chapter 8
QoS Configuration

Service Description

Quality of Service (QoS) provides different service qualities to meet different requirements of various applications, for example, providing dedicated bandwidth, reducing the packet loss ratio and reducing packet transmission delay/jitter. Via flexible configuration and application of the QoS attributes, the carrier can provide effective differentiated services and implement and assure the committed service quality.

Service Specifications

The ZXA10 C320 supports the following QoS operations:

- Precedence remarking
- Queue scheduling
- Queue mapping
- Traffic shaping

Table of Contents

8.1 Ethernet Interface QoS Configuration

This section includes the following topics:

- Configuring the Default CoS
- Configuring DSCP to CoS Remarking
- Configuring the Drop Precedence
- Configuring DSCP Remarking
- Configuring Queue Scheduling
- Configuring Traffic Shaping
- Configuring the Mapping Relation From CoS to Local Queues

8.1.1 Configuring the Default CoS

When the default CoS is configured, the Ethernet interface adds the default CoS to the untagged packet.

Steps

1. In Ethernet interface mode, configure the default Class of Service (CoS).

```
ZXAN(config)#interface gei_1/3/1
ZXAN(config-if)#qos cos default-cos 5
```

2. (Optional) Query the QoS configuration on the interface.

```
ZXAN(config-if)#show qos interface gei_1/3/1
  qos cos default-cos 5
```

– End of Steps –

8.1.2 Configuring DSCP-CoS Remarking

Using the DSCP-to-CoS remarking profile, you can remark the packet CoS priority according to the its DSCP value.

Steps

1. In global configuration mode, configure the DSCP-to-CoS remarking profile.

```
ZXAN(config)#qos dscp-to-cos-profile test 3 to 6
```

2. In Ethernet interface mode, apply the DSCP-to-CoS remarking profile.

```
ZXAN(config)#interface gei_1/3/1
ZXAN(config-if)#qos cos dscp-remark test
```

3. Configure trust Differentiated Services Code Point (DSCP) on the interface.

```
ZXAN(config-if)#qos trust dscp
```

4. (Optional) Query the QoS configuration on the interface.

```
ZXAN(config-if)#show qos interface gei_1/3/1
  qos cos default-cos 5 qos cos dscp-remark TEST qos trust dscp
```

5. (Optional) Query the CoS remarking profile.

```
ZXAN(config-if)#show qos dscp-to-cos-profile test
------------------------------------------------------------
profile name   : TEST
profile detail :
------------------------------------------------------------
 dscp list  0  1  2  3  4  5  6  7  8  9  10 11 12 13 14 15
 cos value  0  0  0  6  0  0  0  0  1  1  1  1  1  1  1  1
------------------------------------------------------------
 dscp list  16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
 cos value  2  2  2  2  2  2  2  2  3  3  3  3  3  3  3  3
------------------------------------------------------------
 dscp list  32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47
 cos value  4  4  4  4  4  4  4  4  5  5  5  5  5  5  5  5
------------------------------------------------------------
 dscp list  48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63
 cos value  6  6  6  6  6  6  6  6  7  7  7  7  7  7  7  7
profile used by:
```

```
gei_1/3/1
```

– End of Steps –

8.1.3 Configuring the Drop Precedence

Using the DSCP-to-drop profile, you can remark the packet drop precedence according to the its DSCP value.

Steps

1. In global configuration mode, configure the drop precedence profile.

```
ZXAN(config)#qos dscp-to-drop-profile test 3 to 2
```

2. In Ethernet interface mode, apply the drop precedence profile.

```
ZXAN(config)#interface gei_1/3/1
ZXAN(config-if)#qos drop-procedence test
```

3. Configure trust DSCP on the interface.

```
ZXAN(config-if)#qos trust dscp
```

4. (Optional) Query the QoS configuration on the interface.

```
ZXAN(config-if)#show qos interface gei_1/3/1
  qos drop-procedence TEST
  qos trust dscp
```

5. (Optional) Query the drop precedence profile.

```
ZXAN(config-if)#show qos dscp-to-drop-profile test
------------------------------------------------------------------
profile name   : TEST
profile detail :
------------------------------------------------------------------
 dscp list  0  1  2  3  4  5  6  7  8  9  10 11 12 13 14 15
 drop value 0  0  0  2  0  0  0  0  0  0  0  0  0  0  0  0
------------------------------------------------------------------
 dscp list  16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
 drop value 0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0
------------------------------------------------------------------
 dscp list  32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47
 drop value 0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0
------------------------------------------------------------------
 dscp list  48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63
 drop value 0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0
profile used by:
gei_1/3/1
```

– End of Steps –

8.1.4 Configuring DSCP Remarking

Using the DSCP remark profile, you can remark the packet DSCP priority according to the its original DSCP value.

Steps

1. In global configuration mode, configure the DSCP remarking profile.

```
ZXAN(config)#qos dscp-to-dscp-profile test 3 to 13
```

2. In Ethernet interface mode, apply the DSCP remarking profile.

```
ZXAN(config)#interface gei_1/3/1
ZXAN(config-if)#qos dscp dscp-remark test
```

3. Configure trust DSCP on the interface.

```
ZXAN(config-if)#qos trust dscp
```

4. (Optional) Query the QoS configuration on the interface.

```
ZXAN(config-if)#show qos interface gei_1/3/1
  qos dscp dscp-remark TEST
  qos trust dscp
```

5. (Optional) Query the DSCP remarking profile.

```
ZXAN(config)#show qos dscp-to-dscp-profile test
------------------------------------------------------------------
profile name   : TEST
profile detail :
------------------------------------------------------------------
 dscp list   0  1  2  3  4  5  6  7  8  9  10 11 12 13 14 15
 dscp value  0  1  2  13 4  5  6  7  8  9  10 11 12 13 14 15
------------------------------------------------------------------
 dscp list   16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
 dscp value  16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
------------------------------------------------------------------
 dscp list   32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47
 dscp value  32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47
------------------------------------------------------------------
 dscp list   48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63
 dscp value  48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63
profile used by:
gei_1/3/1
```

– End of Steps –

8.1.5 Configuring Queue Scheduling

Using the profile, you can implement queue scheduling on the Ethernet interface.

Steps

1. In global configuration mode, configure the queue scheduling profile.

```
ZXAN(config)#qos queue-block-profile test queue0 2 0 queue1 3 0
```

NOTE **Note:**

In a queue scheduling profile, the queue of which the queue weight is 0 should be configured at the end.

2. In Ethernet interface mode, apply the queue scheduling profile.

```
ZXAN(config)#interface gei_1/3/1
ZXAN(config-if)#qos queue-block-profile test
```

3. (Optional) Query the QoS configuration on the interface.

```
ZXAN(config)#show qos interface gei_1/3/1
  qos queue-block-profile TEST
```

4. (Optional) Query the QoS queue scheduling profile.

```
ZXAN(config-if)#show qos queue-block-profile test
-------------------------------------------------------------
profile name   : TEST
profile detail :
----------------------------------------
  queue-number :  8
  queue-id     :  0  1  2  3  4  5  6  7
  queue-weight :  2  3  0  0  0  0  0  0
  queue-depth  :  0  0  0  0  0  0  0  0
----------------------------------------
profile used by:
gei_1/3/1
```

– End of Steps –

8.1.6 Configuring Traffic Shaping

By implementing traffic shaping, you can set the packet rate to match that of the receiving device, to avoid congestion or packet discarding.

Context

Traffic shaping controls the rate of the output packets so that the packets are sent at a constant rate.

By default, traffic shaping is disabled.

Steps

1. In Ethernet interface mode, configure traffic shaping.

```
ZXAN(config)#interface gei_1/3/1
ZXAN(config-if)#qos traffic-shape rate-limit 1280 bucket-size 512
```

2. (Optional) Query the QoS configuration on the interface.

```
ZXAN(config)#show qos interface gei_1/3/1
  qos traffic-shape rate-limit 1280 bucket-size 512
```

– End of Steps –

8.1.7 Configuring the Mapping Relation From CoS to Local Queues

This section describes how to configure the mapping relation from the Ethernet packet CoS to local queues.

Steps

1. In global configuration mode, configure the mapping relation from CoS to local queues.

```
ZXAN(config)#qos eth-cos-local-map cos0 7 cos1 5 cos2 2 cos3 3 cos4 4 cos5 5
cos6 6 cos7 7
```

2. (Optional) Query the mapping relation from CoS to local queues.

```
ZXAN(config)#show qos eth-cos-local-map
-----------------------------------
cos value  0  1  2  3  4  5  6  7
queue ID   7  5  2  3  4  5  6  7
```

– End of Steps –

8.2 OLT Interface QoS Configuration

This section includes the following topics:

- Configuring Queue Scheduling
- Configuring Queue Mapping
- Configuring Traffic Shaping
- Configuring the Traffic Profile

8.2.1 Configuring Queue Scheduling

Using the profile, you can implement queue scheduling on the OLT interface.

Steps

1. In global configuration mode, configure the queue scheduling profile.

```
ZXAN(config)#qos queue-block-profile test queue0 2 12 queue1 3 12
```

2. In OLT interface configuration mode, apply the queue scheduling profile.

```
ZXAN(config)#interface gpon-olt_1/1/1
ZXAN(config-if)#qos queue-block-profile test
```

3. (Optional) Query the QoS queue scheduling profile.

```
ZXAN(config-if)#show qos queue-block-profile test
-------------------------------------------------
profile name   : TEST
profile detail :
---------------------------------------
  queue-number :  8
  queue-id     :  0  1  2  3  4  5  6  7
  queue-weight :  2  3  0  0  0  0  0  0
  queue-depth  :  12 12 0  0  0  0  0  0
---------------------------------------
profile used by:
gpon-olt_1/1/1
```

– End of Steps –

8.2.2 Configuring Queue Mapping

Using the profile, you can implement queue mapping on the OLT interface.

Steps

1. In global configuration mode, configure the queue map profile.

```
ZXAN(config)#qos queue-map-profile test cos-queue-type cos0 2
```

2. In OLT interface configuration mode, apply the queue map profile.

```
ZXAN(config)#interface gpon-olt_1/1/1
ZXAN(config-if)#qos queue-map-profile test
```

3. (Optional) Query the QoS queue mapping profile.

```
ZXAN(config-if)#show qos queue-map-profile test
-------------------------------------------------------
profile name   : TEST
profile detail :
---------------------------------------
  queue-map    :  cos-queue-type
  queue-number :  8
  cos-value    :  0  1  2  3  4  5  6  7
  cos-queue-map:  2  1  2  3  4  5  6  7
---------------------------------------
profile used by:
gpon-olt_1/1/1
```

– End of Steps –

8.2.3 Configuring Traffic Shaping

By implementing traffic shaping, you can set the packet rate to match that of the receiving device, to avoid congestion or packet discarding.

Context

Traffic shaping controls the rate of the output packets so that the packets are sent at a constant rate.

By default, traffic shaping is disabled.

Steps

1. In EPON OLT interface mode, configure traffic shaping.

```
ZXAN(config)#interface epon-olt_1/6/1
ZXAN(config-if)#qos traffic-shape rate-limit 1280 bucket-size 1000
```

2. (Optional) Query the QoS configuration on the interface.

```
ZXAN(config-if)#show qos interface epon-olt_1/6/1
  qos traffic-shape rate-limit 1280 bucket-size 1000
```

– End of Steps –

8.2.4 Configuring the Traffic Profile

Using the profile, you can limit the traffic on the GPON OLT interface.

Steps

1. In global configuration mode, configure the traffic profile.

```
ZXAN(config)#traffic-profile test ip cir 10240 cbs 1000 pir 20480 pbs 1000
```

2. In OLT interface configuration mode, apply the traffic profile.

```
ZXAN(config)#interface gpon-olt_1/1/1
ZXAN(config-if)#traffic-profile test direction egress
```

3. (Optional) Query the QoS traffic profile.

```
ZXAN(config-if)#show traffic-profile test
-----------------------------------------------------------------
profile name                : TEST
profile detail              :
-----------------------------------------------------------------
 basic traffic type         : ip
 committed information rate : 10240 kbps
 committed burst size       : 1000 kbytes
 peak information rate       : 20480 kbps
 peak burst size            : 1000 kbytes
 discard mode               : low priority first
 color mode                 : blind
```

```
---------------------------------------------------------------
profile used by :
gpon-olt_1/1/1 egress
```

– End of Steps –

8.3 ONU Interface QoS Configuration

This section includes the following topics:

- Configuring the Trust Precedence
- Configuring the Default CoS
- Configuring CoS Remarking
- Configuring DSCP to CoS Remarking
- Configuring the Default Egress CoS
- Configuring Egress CoS Remarking
- Configuring Egress DSCP to CoS Remarking
- Configuring CoS Filtering
- Configuring Queue Scheduling
- Configuring Queue Mapping
- Configuring the Traffic Profile

8.3.1 Configuring the Trust Precedence

This section describes how to configure the ONU virtual port (vport) to trust CoS or DSCP priority of packets.

Context

When the vport trusts CoS or DSCP priority, there are two cases:

- When the vport trusts CoS priority, the CoS in packets is marked in the override > cos-remark > trust order based on the ingress CoS.
- When the vport trusts DSCP priority, the CoS is marked according to the configured DSCP-to-CoS mapping relation.

Steps

1. In ONU interface configuration mode, configure the trust precedence of the vport.

```
ZXAN(config)#interface gpon-onu_1/1/1:1
ZXAN(config-if)#qos trust dscp vport 1
ZXAN(config-if)#qos trust cos vport 2
```

2. (Optional) Query the QoS configuration on the interface.

```
ZXAN(config-if)#show qos interface gpon-onu_1/1/1:1
  qos trust dscp vport 1
```

NOTE **Note:**

CoS is the default configuration of the interface and is not displayed.

– End of Steps –

8.3.2 Configuring the Default CoS

When the default CoS is configured, the ONU virtual port (vport) adds the default CoS to the untagged packet.

Context

When the default CoS is configured on a virtual port, the override operation is optional.

- With the override operation: the CoS in all packets (including untagged packets) is modified to the default CoS.
- Without the override operation: Only the CoS in untagged packets is modified to the default CoS.

Steps

1. In ONU interface configuration mode, configure the default CoS.

```
ZXAN(config)#interface gpon-onu_1/1/1:1
ZXAN(config-if)#qos cos default-cos 5 override vport 1
ZXAN(config-if)#qos cos default-cos 5 vport 2
```

2. (Optional) Query the QoS configuration on the interface.

```
ZXAN(config-if)#show qos interface gpon-onu_1/1/1:1
  qos cos default-cos 5 override vport 1
  qos cos default-cos 5 vport 2
```

– End of Steps –

8.3.3 Configuring CoS Remarking

Using the CoS remark profile, you can remark packet's CoS priority according to its CoS value on the ONU virtual port (vport).

Context

When the vport trusts CoS and the default CoS is not configured with the override operation, the CoS in packets is modified according to the mapping relation in the profile after the CoS remarking profile is configured.

Steps

1. In global configuration mode, configure the CoS remarking profile.

```
ZXAN(config)#qos cos-to-cos-profile test cos0 3
```

2. In ONU interface configuration mode, apply the CoS remarking profile.

```
ZXAN(config)#interface gpon-onu_1/1/1:1
ZXAN(config-if)#qos cos cos-remark test vport 1
ZXAN(config-if)#qos trust cos vport 1
```

3. (Optional) Query the QoS configuration on the interface.

```
ZXAN(config-if)#show qos interface gpon-onu_1/1/1:1
  qos cos cos-remark TEST vport 1
```

– End of Steps –

8.3.4 Configuring DSCP to CoS Remarking

Using the DSCP-to-CoS remarking profile, the ONU virtual port (vport) modifies packet's CoS priority according to its DSCP value.

Context

When the vport trusts DSCP, the CoS in packets is modified according to the mapping relation in the profile after the DSCP remarking profile is configured.

Steps

1. In global configuration mode, configure the DSCP-to-CoS remarking profile.

```
ZXAN(config)#qos dscp-to-cos-profile test 12 to 3
```

2. In ONU interface configuration mode, apply the DSCP-to-CoS remarking profile.

```
ZXAN(config)#interface gpon-onu_1/1/1:1
ZXAN(config-if)#qos cos dscp-remark test vport 1
ZXAN(config-if)#qos trust dscp vport 1
```

3. (Optional) Query the QoS configuration on the interface.

```
ZXAN(config-if)#show qos interface gpon-onu_1/1/1:1
  qos trust dscp vport 1
  qos cos dscp-remark TEST vport 1
```

– End of Steps –

8.3.5 Configuring the Default Egress CoS

When the default CoS is configured, the ONU virtual port (vport) adds the default egress CoS to the untagged packet.

Context

When the default CoS is configured on a vport, the override operation is optional.

- With the override operation: the CoS in all packets on the vport is modified to the default egress CoS.
- Without the override operation: the vport transparently transmits all packets.

Steps

1. In ONU interface configuration mode, configure the default CoS.

```
ZXAN(config)#interface gpon-onu_1/1/1:1
ZXAN(config-if)#qos egress-cos default-cos 5 override vport 1
```

2. (Optional) Query the QoS configuration on the interface.

```
ZXAN(config-if)#show qos interface gpon-onu_1/1/1:1
  qos egress-cos default-cos 5  override vport 1
```

– End of Steps –

8.3.6 Configuring Egress CoS Remarking

Using the CoS remark profile, you can remark packet's egress CoS priority according to its CoS value on the ONU virtual port (vport).

Context

When the vport trusts CoS and the default CoS is not configured with the override operation, the CoS in packets is modified according to the mapping relation in the profile after the egress CoS remarking profile is configured.

Steps

1. In global configuration mode, configure the CoS remarking profile.

```
ZXAN(config)#qos cos-to-cos-profile test cos0 3
```

2. In ONU interface configuration mode, apply the CoS remarking profile.

```
ZXAN(config)#interface gpon-onu_1/1/1:1
ZXAN(config-if)#qos egress-cos cos-remark test vport 1
ZXAN(config-if)#qos trust cos vport 1
```

3. (Optional) Query the QoS configuration on the interface.

```
ZXAN(config-if)#show qos interface gpon-onu_1/1/1:1
  qos egress-cos cos-remark TEST vport 1
```

– End of Steps –

8.3.7 Configuring Egress DSCP to CoS Remarking

Using the DSCP-to-CoS remarking profile, you can remark packet's egress CoS priority according to its DSCP value on the ONU virtual port (vport).

Context

When the vport trusts DSCP, the CoS in packets is modified according to the mapping relation in the profile after the egress DSCP remarking profile is configured.

Steps

1. In global configuration mode, configure the DSCP-to-CoS remarking profile.

```
ZXAN(config)#qos dscp-to-cos-profile test 12 to 3
```

2. In ONU interface configuration mode, apply the DSCP-to-CoS remarking profile.

```
ZXAN(config)#interface gpon-onu_1/1/1:1
ZXAN(config-if)#qos egress-cos dscp-remark test vport 1
ZXAN(config-if)#qos trust dscp vport 1
```

3. (Optional) Query the QoS configuration on the interface.

```
ZXAN(config-if)#show qos interface gpon-onu_1/1/1:1
  qos trust dscp vport 1
  qos egress-cos dscp-remark TEST vport 1
```

– End of Steps –

8.3.8 Configuring CoS Filtering

When CoS filtering is configured on the ONU virtual port (vport), only those packets are forwarded whose CoS is the same as the default CoS of the vport.

Steps

1. In ONU interface configuration mode, configure the default CoS.

```
ZXAN(config)#interface gpon-onu_1/1/1:1
ZXAN(config-if)#qos cos default-cos 5 vport 1
ZXAN(config-if)#qos cos-filter enable vport 1
```

2. (Optional) Query the QoS configuration on the interface.

```
ZXAN(config-if)#show qos interface gpon-onu_1/1/1:1
  qos cos-filter enable vport 1
  qos cos default-cos 5 vport 1
```

– End of Steps –

8.3.9 Configuring Queue Scheduling

Using the queue block profile, you can implement queue scheduling on the ONU virtual port (vport).

Steps

1. In global configuration mode, configure the queue block profile.

```
ZXAN(config)#qos queue-block-profile test queue0 2 12 queue1 3 12
```

2. In ONU interface configuration mode, apply the queue block profile.

```
ZXAN(config)#interface gpon-onu_1/1/1:1
ZXAN(config-if)#qos queue-block-profile test vport 1
```

3. (Optional) Query the QoS queue block profile.

```
ZXAN(config-if)#show qos queue-block-profile test
-------------------------------------------------------------------------
profile name   : TEST
profile detail :
---------------------------------------
  queue-number :  8
  queue-id     :  0  1  2  3  4  5  6  7
  queue-weight :  2  3  0  0  0  0  0  0
  queue-depth  :  12 12 0  0  0  0  0  0
---------------------------------------
profile used by:
gpon-onu_1/1/1:1:1
```

– End of Steps –

8.3.10 Configuring Queue Mapping

Using the queue map profile, you can implement queue mapping on the ONU virtual port (vport).

Steps

1. In global configuration mode, configure the queue map profile.

```
ZXAN(config)#qos queue-map-profile test cos-queue-type cos0 2
```

2. In ONU interface configuration mode, apply the queue map profile.

```
ZXAN(config)#interface gpon-onu_1/1/1:1
ZXAN(config-if)#qos queue-map-profile test vport 1
```

3. (Optional) Query the QoS queue map profile.

```
ZXAN(config-if)#show qos queue-map-profile test
---------------------------------------------------------------
profile name   : TEST
profile detail :
---------------------------------------
  queue-map    :  cos-queue-type
  queue-number :  8
  cos-value    :  0  1  2  3  4  5  6  7
  cos-queue-map:  2  1  2  3  4  5  6  7
---------------------------------------
profile used by:
```

```
gpon-onu_1/1/1:1:1
```

– End of Steps –

8.3.11 Configuring the Traffic Profile

Using the traffic profile, you can limit the traffic of the GPON ONU virtual port (vport).

Steps

1. In global configuration mode, configure the traffic profile.

```
ZXAN(config)#traffic-profile test ip cir 10240 cbs 1000 pir 20480 pbs 1000
```

2. In ONU interface configuration mode, apply the traffic profile.

```
ZXAN(config)#interface gpon-onu_1/1/1:1
ZXAN(config-if)#traffic-profile test vport 1 direction egress
```

3. (Optional) Query the QoS traffic profile.

```
ZXAN(config-if)#show traffic-profile test
-------------------------------------------------------------------
profile name                : TEST
profile detail              :
-------------------------------------------------------------------
 basic traffic type         : ip
 committed information rate : 10240 kbps
 committed burst size       : 1000 kbytes
 peak information rate      : 20480 kbps
 peak burst size            : 1000 kbytes
 discard mode               : low priority first
 color mode                 : blind
-------------------------------------------------------------------
profile used by :
gpon-olt_1/1/1 egress
gpon-onu_1/1/1:1 vport 1 egress
```

– End of Steps –

This page intentionally left blank.

Chapter 9
ACL Configuration

The network devices use the Access Control List (ACL) to filter the data packets and control the policy routes and special flows. ACL sets a series of matching rules to identify the objects to be filtered, and permits or denies the corresponding data packet to pass through according to the preset policies.

An ACL can contain one or more rules. These rules enable the device to permit or deny the matching traffic according to specific parameters. An ACL compares the traffic with each rule till it finds a matched rule. The last rule in an ACL is an implicit deny rule. When no rule is configured in an ACL, the default rule is an implicit permit rule.

One interface supports only one ACL.

The ZXA10 C320 supports the following four types of ACLs:

- Standard ACL

  The standard ACL is only matched by the source IP address.

- Extended ACL

  The extended ACL is matched by the source IP address, destination IP address, IP protocol type, TCP/UDP source/destination port number, ICMP type, IGMP type, DSCP, ToS, and IP priority.

- Layer-2 ACL

  The layer-2 ACL is matched by the source MAC address, destination MAC address, source VLAN ID, layer-2 Ethernet protocol type, and 802.1p priority value.

- Hybrid ACL

  The hybrid ACL is matched by the source MAC address, destination MAC address, source VLAN ID, source IP address, destination IP address, TCP/UDP source/destination port number, including all the matching fields of the preceding three types.

- IPv6 hybrid ACL

  It is the IPv6-based hybrid ACL.

Table of Contents

9.1 Configuring a Standard ACL

This section describes how to configure a standard ACL and apply it to an Ethernet interface.

Configuration Data

Table 9-1 lists the configuration data of the standard ACL.

Table 9-1 Configuration Data of the Standard ACL

Item	Data
Time range	Name: worktime Range: 09:00:00–17:00:00 Day: working-day
ACL number	3
Rule 1	Action: deny Source address: 168.1.1.1/24 Time range: worktime
Rule 2	Permit any traffic
Interface	gei_1/3/1

Steps

1. (Optional) In global configuration mode, configure the ACL time range.

```
ZXAN(config)#time-range worktime 09:00:00 to 17:00:00 working-day
```

2. Create a standard ACL.

```
ZXAN(config)#acl standard number 3
ZXAN(config-std-acl)#
```

NOTE **Note:**

The standard ACL number ranges from 1 to 99. The standard ACL can be applied to the Ethernet interface only.

---

3. Configure the ACL rules.

```
ZXAN(config-std-acl)#rule 1 deny 168.1.1.1 0.0.0.255 time-range worktime
ZXAN(config-std-acl)#rule 2 permit any
ZXAN(config-std-acl)#exit
```

Note:

Each standard ACL supports up to 127 rules.

If the time range is not configured, the rule is always effective.

4. In Ethernet interface configuration mode, apply the ACL.

```
ZXAN(config)#interface gei_1/3/1
ZXAN(config-if)#ip access-group 3 in
```

5. (Optional) Query the ACL configuration.

```
ZXAN(config-if)#show acl 3
acl standard number 3
  rule 1 deny 168.1.1.0 0.0.0.255 time-range worktime
  rule 2 permit any
```

6. (Optional) Query the interface bound with the ACL.

```
ZXAN(config-if)#show access-list bound
Interface                       Direction Type   Status      Acl number/name

gei_1/3/1                       in        V4STD  successful  3
```

– End of Steps –

9.2 Configuring an Extended ACL

This section describes how to configure an extended ACL and apply it to an Ethernet interface.

Configuration Data

Table 9-2 lists the configuration data of the extended ACL.

Table 9-2 Configuration Data of the Extended ACL

Item	Data
ACL number	101
Rule 1	Action: deny Source address: 192.168.1.0/24 Protocol type: TCP, Telnet
Rule 2	Permit any TCP and telnet traffic
Interface	gei_1/3/1

Steps

1. In global configuration mode, create an extended ACL.

```
ZXAN(config)#acl extended number 101
ZXAN(config-ext-acl)#
```

Note:

The extended ACL number ranges from 100 to 199. An extended ACL can be applied to an Ethernet interface only.

2. Configure the ACL rules.

```
ZXAN(config-ext-acl)#rule 1 deny tcp 192.168.1.0 0.0.0.255 eq telnet any
ZXAN(config-ext-acl)#rule 2 permit tcp any eq telnet any
ZXAN(config-ext-acl)#exit
```

Note:

Each extended ACL supports up to 1024 rules.

If the time range is not configured, the rule is always effective.

3. In Ethernet interface configuration mode, apply the ACL.

```
ZXAN(config)#interface gei_1/3/1
ZXAN(config-if)#ip access-group 101 in
```

4. (Optional) Query the ACL configuration.

```
ZXAN(config-if)#show acl 101
acl extend number 101
  rule 1 deny tcp 192.168.1.0 0.0.0.255 eq telnet any
  rule 2 permit tcp any eq telnet any
```

5. (Optional) Query the interface bound with the ACL.

```
ZXAN(config-if)#show access-list bound
Interface                       Direction Type   Status      Acl number/name

gei_1/3/1                       in        V4EXT  successful  101
```

– End of Steps –

9.3 Configuring a Layer-2 ACL

This section describes how to configure a layer-2 ACL and apply it to an Ethernet interface.

Configuration Data

Table 9-3 lists the configuration data of the layer-2 ACL.

Table 9-3 Configuration Data of the Layer-2 ACL

Item	Data
ACL number	200
Rule 1	Action: deny Source MAC address: 0000.0000.0001 Protocol type: any
Rule 2	Permit any traffic
Interface	gei_1/3/1

Steps

1. In global configuration mode, create a layer-2 ACL.

```
ZXAN(config)#acl link number 200
ZXAN(config-link-acl)#
```

NOTE **Note:**

The layer ACL number ranges from 200 to 299. A layer-2 ACL can be applied to the Ethernet interface and EPON-OLT interface.

2. Configure the ACL rules.

```
ZXAN(config-link-acl)#rule 1 deny any ingress 0000.0000.0001 0000.0000.0000
egress any
ZXAN(config-link-acl)#rule 2 permit any
ZXAN(config-link-acl)#exit
```

NOTE **Note:**

Each layer-2 ACL supports up to 4096 rules.

If the time range is not configured, the rule is always effective.

3. In Ethernet interface configuration mode, apply the ACL.

```
ZXAN(config)#interface gei_1/3/1
ZXAN(config-if)#ip access-group 200 in
```

4. (Optional) Query the ACL configuration.

```
ZXAN(config-if)#show acl 200
```

```
acl link number 200
  rule 1 deny any ingress 0000.0000.0001 0000.0000.0000 egress any
  rule 2 permit any ingress any egress any
```

5. (Optional) Query the interface bound with the ACL.

```
ZXAN(config-if)#show access-list bound
Interface                       Direction Type    Status      Acl number/name

gei_1/3/1                       in        V4LVL2 successful  200
```

– End of Steps –

9.4 Configuring a Hybrid ACL

This section describes how to configure a hybrid ACL and apply it to an Ethernet interface.

Configuration Data

Table 9-4 lists the configuration data of the hybrid ACL.

Table 9-4 Configuration Data of the Hybrid ACL

Item	Data
ACL number	300
Rule 1	Action: deny IP protocol type: any Source address: any Destination address: any Ethernet protocol type: ARP
Rule 2	Action: deny IP protocol type: any Source MAC address: 0000.0000.0001 Destination IP address 192.168.1.0/24 Ethernet protocol type: any
Rule 3	Permit any traffic
Interface	gei_1/3/1

Steps

1. In global configuration mode, create a hybrid ACL.

```
ZXAN(config)#acl hybrid number 300
ZXAN(config-hybd-acl)#
```

NOTE **Note:**

The hybrid ACL number ranges from 300 to 399. A hybrid ACL is applied to the Ethernet interface and PON-ONU interface.

2. Configure the ACL rules.

```
ZXAN(config-hybd-acl)#rule 1 deny any any any arp
ZXAN(config-hybd-acl)#rule 2 deny any any 192.168.1.0 0.0.0.255 ip ingress 0000.
0000.0001 0000.0000.0000 egress any
ZXAN(config-hybd-acl)#rule 3 permit any any any any
ZXAN(config-hybd-acl)#exit
```

NOTE **Note:**

Each hybrid ACL supports up to 127 rules.

If the time range is not configured, the rule is always effective.

3. In Ethernet interface configuration mode, apply the ACL.

```
ZXAN(config)#interface gei_1/3/1
ZXAN(config-if)#ip access-group 300 in
```

4. (Optional) Query the ACL configuration.

```
ZXAN(config-if)#show acl 300
acl hybrid number 300
  rule 1 deny any any any arp ingress any egress any
  rule 2 deny any any 192.168.1.0 0.0.0.255
ip ingress 0000.0000.0001 0000.0000.0000 egress any
  rule 3 permit any any any any ingress any egress any
```

5. (Optional) Query the interface bound with the ACL.

```
ZXAN(config-if)#show access-list bound
Interface                       Direction Type   Status      Acl number/name

gei_1/3/1                       in        V4HYBD successful  300
```

– End of Steps –

9.5 Configuring an IPv6 Hybrid ACL

This section describes how to configure an IPv6 hybrid ACL and apply it to an Ethernet interface.

Configuration Data

Table 9-5 lists the configuration data of the IPv6 hybrid ACL.

Table 9-5 Configuration Data of the IPv6 Hybrid ACL

Item	Data
ACL number	600
Rule 1	Action: deny IP protocol type: TCP Source address: any Destination address: any Traffic class: 7 Ethernet protocol type: any
Rule 2	Action: deny Protocol type: any Source address: 00:00::00:22/128 Destination address: any Ethernet protocol type: any CoS priority: 3
Rule 3	Permit any traffic
Interface	gei_1/3/1

Steps

1. In global configuration mode, create an IPv6 hybrid ACL.

```
ZXAN(config)#acl6 hybrid number 600
ZXAN(config-hybd-acl6)#
```

NOTE **Note:**

The IPv6 hybrid ACL number ranges from 600 to 699. An IPv6 hybrid ACL can be applied to an Ethernet interface and PON-OLT interface.

2. Configure the ACL rules.

```
ZXAN(config-hybd-acl6)#rule 1 deny tcp any any traffic-class 7 any
ZXAN(config-hybd-acl6)#rule 2 deny any 00:00::00:22/128 any any cos 3
ZXAN(config-hybd-acl6)#rule 3 permit any any any any
ZXAN(config-hybd-acl6)#exit
```

Note:

Each IPv6 hybrid ACL supports up to 127 rules.

If the time range is not configured, the rule is always effective.

3. In Ethernet interface configuration mode, apply the ACL.

```
ZXAN(config)#interface gei_1/3/1
ZXAN(config-if)#ip access-group 600 in
```

4. (Optional) Query the ACL configuration.

```
ZXAN(config-if)#show acl 600
Acl6 hybrid number 600
 rule 1 deny tcp any any traffic-class 7 any
 rule 2 deny any ::22/128 any any cos 3 ingress any egress any
 rule 3 permit any any any any ingress any egress any
```

5. (Optional) Query the interface bound with the ACL.

```
ZXAN(config-if)#show access-list bound
Interface                       Direction Type   Status      Acl number/name

gei_1/3/1                       in        V6HYBD successful  600
```

– End of Steps –

This page intentionally left blank.

Chapter 10
ONU Version Upgrade

The ZXA10 C320 supports two modes of upgrading ONU versions:

- Manual mode
- Task mode

Before using the Customer Premises Equipment (CPE) upgrading function, make sure that whether the ONU type and version supports CPE upgrade.

- EPON ONU

  F460B and F420 supports CPE upgrade.

- GPON ONU

  All ONU supporting OMCI supports CPE upgrade.

Table of Contents

10.1 Configuring FTP Parameters

Before downloading version files, you need configure FTP parameters on the ZXA10 C320.

Steps

1. In out-of-band interface mode, configure the FTP server IP address.

```
ZXAN(config)#interface mng1
ZXAN(config-if)#boot-server 10.3.1.1
```

2. Configure the username and pasword of the FTP server.

```
ZXAN(config-if)#boot-username gpon
ZXAN(config-if)#boot-password gpon
```

3. (Optional) Query the FTP configuration.

```
ZXAN(config)#show interface mng1
mng running information
 ip address      : 10.3.1.2
 mask            : 255.255.255.0
 boot-server     : 10.3.1.1
 boot-username   : gpon
```

```
 boot-password   : ****
 config-filename : startrun.dat
 imgfile-location: local
 inband-mac      : 00d0.d043.3832
 outband-mac     : 00d0.d043.3831
 admin-status    : no shutdown

mng configuration information
 ip address      : 10.3.1.2
 mask            : 255.255.255.0
 boot-server     : 10.3.1.1
 boot-username   : gpon
 boot-password   : ****
 config-filename : startrun.dat
 imgfile-location: local
 inband-mac      : 00d0.d043.3832
 outband-mac     : 00d0.d043.3831
 admin-status    : no shutdown
```

– End of Steps –

10.2 Downloading the Version File

Before upgrading the ONU version, you need to download the version file to the ZXA10 C320.

Prerequisite

The FTP server is started on the maintenance PC.

Steps

1. Download the ONU version file.

```
ZXAN#download onuver f62xp2t4.bin
```

2. (Optional) Query the ONU version file.

```
ZXAN#dir onuver
Directory of /flash/onuver/
attribute   size       date         time       name
-rwx        5993232    SEP-08-2011  07:30:30   f601.bin
-rwx        9956800    OCT-26-2011  12:36:34   f62xp2t4.bin
-rwx        1644       NOV-04-2011  13:48:48   cfg.xml
Current directory 3 files total
Total disk size: 126664704 bytes (26910720 bytes free)
```

– End of Steps –

10.3 Upgrading the ONU Version Manually

For individual ONU or a small batch ONUs, you can upgrade the version manually.

Prerequisite

The ONU version file is downloaded.

Context

The manual operation can only upgrade the version of online ONUs.

If the version of an ONU is not upgraded after the manual operation, check whether the ONU is online.

Steps

1. Upgrade the version of a specific ONU.

```
ZXAN#cpe update-and-reboot f62xp2t4.bin gpon-olt_1/1/1 1
```

2. Upgrade the version of a specific ONU type.

```
ZXAN#cpe update-and-reboot f62xp2t4.bin type ZTE-F660
```

3. (Optional) Query the version upgrade status.

```
ZXAN(config)#show cpe update-status gpon-olt_1/1/1 1
gpon-onu_1/1/1: 1
Taskname   : Manual
Action     : Update-and-reboot
Status     : Success
Progress   : 100%
Failreason : None
Committime : 2011-11-18 10:50:47
```

4. (Optional) Query the ONU version information.

```
ZXAN#show cpe information gpon-olt_1/1/1 1
gpon-onu_1/1/1: 1
CpeVendorName :
CpeType       : ZTE-F622
Region 1
Vertag        : V1.0.0P2T3S_Z
Commited      : No
Activated     : No
Valid         : Yes
Region 2
Vertag        : V1.0.0P2T5S_L
Commited      : Yes
Activated     : Yes
```

```
Valid         : Yes
```

– End of Steps –

10.4 Creating an Version Upgrade Task

Using the version upgrade task, you can upgrade the version of ONUs in batches.

Prerequisite

The ONU version file is downloaded.

Context

The ZXA10 C320 supports maximum 31 tasks to upgrade version for different ONU types. These tasks can work concurrently without interference. The auto upgrade task can upgrade the version of offline ONUs.

The ZXA10 C320 supports conflict detection on version upgrade tasks. Two conflicted task cannot be configured simultaneously.

When the following item of two tasks are the same:

- Service type
- Vendor name
- Equipment type

ONU ranges cannot be the same. Otherwise, these two tasks conflict.

Steps

1. In global configuration mode, create the ONU version upgrade task.

```
ZXAN(config)#cpe task test
ZXAN(cpe-task)#
```

2. Configure the version file.

```
ZXAN(cpe-task)#version-file f62xp2t4.bin
```

3. Configure the version tag and match rule.

```
ZXAN(cpe-task)#match-vertag Below V1.0.0P2T5S_L
```

4. Configure the service type.

```
ZXAN(cpe-task)#service-type GPON
```

5. Configure the vendor name

```
ZXAN(cpe-task)#vendor-name ZTEG
```

6. Configure the ONU type.

```
ZXAN(cpe-task)#equipment-type ZTE-F622
```

7. Configure the ONU range.

```
ZXAN(cpe-task)#range port gpon-olt_1/1/1
```

8. Configure the upgrade action.

```
ZXAN(cpe-task)#action Update-and-reboot
```

9. Configure the upgrade mode.

```
ZXAN(cpe-task)#mode Both
```

10. Add the upgrade task.

```
ZXAN(cpe-task)#task add
```

11. (Optional) Query the version upgrade task.

```
ZXAN(cpe-task)#show cpe task
Taskname    : test
Status      : Working          VerFile      : f62xp2t4.bin
ImageSize   : 5993232          EquType      : ZTE-F622
ServiceType: Gpon              VendorName   : ZTEG
Mode        : Both             VerBase      : V1.0.0P2T5S_L
ImgLocation: Local             Rule         : Below
Limitation:  64                Action       : Update-and-reboot
RangeType   : Port
gpon-olt_1/1/1
```

– End of Steps –

This page intentionally left blank.

Chapter 11
NTP Configuration

The Network Time Protocol (NTP) is a protocol for synchronizing the time of different network members. The devices that support NTP periodically exchange NTP packets to synchronize their clocks.

Table of Contents

11.1 Configuring NTP

The ZXA10 C320 works in NTP client mode and synchronizes its time with the NTP server.

Steps

1. In global configuration mode, enable NTP.

```
ZXAN(config)#ntp enable
```

2. Configure the NTP server.

```
ZXAN(config)#ntp server 1.2.1.1
```

3. Configure the source IP address of NTP packets for the time synchronization request.

```
ZXAN(config)#ntp source 10.1.1.1
```

NOTE **Note:**

The source IP address of NTP packets is the in-band or out-of-band NM IP address of the ZXA10 C320.

---

4. Configure the alarm threshold of the NTP time synchronization offset value.

```
ZXAN(config)#ntp alarm-threshold 10
```

5. Configure the NTP synchronization poll interval.

```
ZXAN(config)#ntp poll-interval 50
```

6. (Optional) Query the NTP running status.

```
ZXAN(config)#show ntp status
  Clock is unsynchronized.
  stratum is 16
  no reference clock
```

```
reference time is:
 01:50:19  Fri  Aug 12  2011  utc
clock offset is 0.00
delay is 0.00
root dispersion is 0.00
peer dispersion is 0.00
server in use is 1.2.1.1
```

– End of Steps –

Chapter 12
STP Configuration

The ZXA10 C320 supports the following three Spanning Tree Protocol (STP) modes:

- Single Spanning Tree Protocol (SSTP)
- Rapid Spanning Tree Protocol (RSTP)
- Multiple Spanning Tree Protocol (MSTP)

SSTP Mode

SSTP complies with the IEEE802.1d standard. It is compatible with STP, RSTP and MSTP. The bridge in SSTP mode can interwork with the bridge in RSTP and MSTP modes.

RSTP Mode

RSTP complies with the IEEE802.1w standard. RSTP provides faster convergence than SSTP. When the network topology changes, the port state of the redundant switch port can be quickly changed from Discard to Forward in a point-to-point connection condition.

MSTP Mode

MSTP complies with the IEEE802.1s standard. MSTP is added with the concepts of instance and VLAN mapping. SSTP and RSTP modes can be considered as a special MSTP instance, in which case, the instance is 0. The MSTP mode provides fast convergence and load balancing for VLAN.

In SSTP and RSTP modes, the VLAN concept does not exist, and each port has only one state. Namely, the port has the same forwarding state in different VLANs.

In MSTP mode, multiple spanning-tree instances can exist, and a port has different forwarding states in different VLANs. Multiple sub-tree instances can be generated in the Multiple Spanning Tree (MST) region to realize load balancing.

MSTP is applied to the redundant network. MSTP can not only provide fast convergence but also distribute flows of different VLANs to the respective paths, which provides a good load sharing mechanism for redundant links.

Table of Contents

12.1 Configuring STP

The ZXA10 C320 supports MSTP and is compatible with SSTP and RSTP. It also supports MSTP ring networking. By default, the ZXA10 C320 uses the MSTP mode. Any one of

the modes is compatible and interconnected with the other two modes. This topic takes MSTP as an example.

Steps

1. In global configuration mode, enable STP.

```
ZXAN(config)#spanning-tree enable
```

2. Configure STP protocol mode.

```
ZXAN(config)#spanning-tree mode mstp
```

3. (Optioanl) Configure the MST key and digest.

```
ZXAN(config)#spanning-tree mst hmd5-key cisco 0x13ac06a62e47fd51f95d2ba243cd0346
ZXAN(config)#spanning-tree mst hmd5-digest cisco 0x13ac06a62e47fd51f95d2ba243cd0346
```

NOTE **Note:**

The MSTP packet formats of the Cisco/Huawei devices may not follow the IEEE standard strictly. When the ZXA10 C320 interworks with the Cisco/Huawei devices in the same region, the KEY and DIGEST values are mandatory.

---

4. In MST configuration mode, configure the MST version number and name.

```
ZXAN(config)#spanning-tree mst configuration
ZXAN(config-mstp)#revision 10
ZXAN(config-mstp)#name zte
```

5. Create the MSTP instance.

   The ZXA10 C320 has only instance 0 that is the common and internal spanning tree (CIST) in SSTP and RSTP modes. In MSTP mode, instance 0 exists by default and cannot be deleted.

   The devices in the same MST region should meet all the following four requirements:

   - The MST names are the same.
   - The MST version numbers are the same.
   - The INS-VLAN mapping tables are the same.
   - The devices are connected physically.

```
ZXAN(config-mstp)#instance 1 vlans 10-20
ZXAN(config-mstp)#exit
```

6. Configure the priority of the local bridge.

```
ZXAN(config)#spanning-tree mst instance 1 priority 4096
```

7. In uplink interface configuration mode, configure the port VLAN.

```
ZXAN(config)#interface gei_1/3/1
ZXAN(config-if)#switchport vlan 10 tag
```

8. (Optional) Query the MSTP configuration.

```
ZXAN(config-if)#show spanning-tree mst configuration
spanning-tree           : [enable]
mode                    : [MSTP]
CISCO    Hmd5-key       : 0x13ac06a62e47fd51f95d2ba243cd0346
CISCO    Hmd5-digest    : 0x13ac06a62e47fd51f95d2ba243cd0346
HUAWEI   Hmd5-key       : 0x00000000000000000000000000000000
HUAWEI   Hmd5-digest    : 0x00000000000000000000000000000000
BPDU   Hmd5-digest      : 0x6cab52e9278d2d221c83bfdff1a4da72
Name                    : [zte]
Revision                : 10
Instance   Vlans mapped
--------   ------------------------------------------------------------
0          1-9,21-4094

1          10-20
```

9. (Optional) Query the instance configuration.

```
ZXAN(config-if)#show spanning-tree instance 1

MST01
  Spanning tree enabled protocol MSTP
  RegRootID: Priority       4097;   Address  00d0.d043.3832
             Hello-Time     2  sec;  Max-Age  20 sec
             Forward-Delay  15 sec;


  BridgeID:  Priority       4097;   Address  00d0.d043.3832
             Hello-Time     2  sec;  Max-Age  20 sec
             Forward-Delay  15 sec;  Max-Hops  20
             Message-Age    0 sec;   RemainHops  20

Interface   Prio.Nbr
Name        Port ID     Cost      Sts         Role        LinkType  Bound
--------------------------------------------------------------------------------
gei_1/3/1  128.42      20000     Discard     Designated  p2p       MSTP
```

– End of Steps –

This page intentionally left blank.

Chapter 13
DHCP Configuration

The ZXA10 C320 supports the following three Dynamic Host Configuration Protocol (DHCP) applications:

- DHCP snooping
- DHCP server
- DHCP relay

The ZXA10 C320 can either work as the DHCP server or DHCP relay to forward the DHCP message. The two applications, however, cannot be used simultaneously on one VLAN interface.

Table of Contents

13.1 Configuring DHCP Snooping

After you configure DHCP snooping, the ZXA10 C320 will set up and maintain a DHCP snooping binding table to filter out the untrusty DHCP messages.

Context

After being configured with DHCP snooping, the ZXA10 C320 will intercept the DHCP interaction process on the specified user port, extract the IP address and MAC address, and set up the DHCP snooping binding table that is the basis of IP source guard.

Configuration Data

Table 13-1 lists the DHCP snooping configuration data.

Table 13-1 DHCP Snooping Configuration Data

Item	Data
Global DHCP	enable
Global DHCP snooping	enable
Global DHCP option 82	enable
VLAN ID	100
DHCP snooping user port	ONU interface: gpon-onu_1/1/1:1 Virtual port ID: 1

Item	Data
Uplink port	gei_1/3/1

Steps

1. In uplink interface configuration mode, configure the port VLAN.

```
ZXAN(config)#interface gei_1/3/1
ZXAN(config-if)#switchport vlan 100 tag
ZXAN(config-if)#exit
```

2. In global configuration mode, enable the DHCP function.

```
ZXAN(config)#ip dhcp enable
```

3. Enable DHCP snooping globally.

```
ZXAN(config)#ip dhcp snooping enable
```

4. Enable DHCP snooping in the VLAN.

```
ZXAN(config)#ip dhcp snooping vlan 100
```

5. Enable global DHCP option 82.

```
ZXAN(config)#dhcp-option82 enable
```

6. In ONU interface configuration mode, configure the interface VLAN and enable DHCP snooping.

```
ZXAN(config)#interface gpon-onu_1/1/1:1
ZXAN(config-if)#service-port 1 vport 1 user-vlan 100 vlan 100
ZXAN(config-if)#ip dhcp snooping enable vport 1
ZXAN(config-if)#exit
```

7. (Optional) Query the DHCP snooping VLAN.

```
ZXAN(config)#show ip dhcp snooping vlan
DHCP snooping state on vlans
Vlan     State
------------------------------
100     enable
```

– End of Steps –

13.2 Configuring DHCP Server

After being configured with the DHCP server function, the ZXA10 C320 can work as the DHCP server to allocate IP addresses to subscribers.

Configuration Data

Table 13-2 lists the DHCP server configuration data.

Table 13-2 DHCP Server Configuration Data

Item	Data
Global DHCP snooping	enable
VLAN ID	100
DHCP server	IP address: 10.10.1.1 DNS IP address: 10.10.1.2 Gateway IP address: 10.10.1.1
IP address pool	Name: zte Range: 10.10.1.3–10.10.1.254
IP address lease time	90s

Steps

1. In global configuration mode, enable global DHCP.

```
ZXAN(config)#ip dhcp enable
```

2. Configure the IP address pool of the DHCP server.

```
ZXAN(config)#ip local pool zte 10.10.1.3 10.10.1.254 255.255.255.0
```

3. Configure the IP address lease time.

```
ZXAN(config)#ip dhcp server leasetime 90
```

4. Configure the DNS IP address of the DHCP server.

```
ZXAN(config)#ip dhcp server dns 10.10.1.2
```

5. In layer-3 VLAN interface mode, configure the IP address.

```
ZXAN(config)#interface vlan 100
ZXAN(config-if)#ip address 10.10.1.1 255.255.255.0
```

6. Configure the working mode and gateway IP address of the VLAN interface.

```
ZXAN(config-if)#ip dhcp mode server
ZXAN(config-if)#ip dhcp server gateway 10.10.1.1
```

NOTE **Note:**

When the DHCP server is directly connected with the client subnet, the default gateway IP address is the IP address of the VLAN interface.

---

7. Configure the IP address pool.

```
ZXAN(config-if)#peer default ip pool zte
```

8. Query the user information on the DHCP server.

```
ZXAN(config-if)#show ip dhcp server user vlan 100
Current online users are 0.
```

```
Index MAC addr       IP addr         State    Expiration
```

– End of Steps –

13.3 Configuring DHCP Relay

When the DHCP client and DHCP server do not work in the same network segment, the DHCP relay is required. The ZXA10 C320 can work as the DHCP relay to forward user's DHCP request to the specified DHCP server.

Context

The ZXA10 C320 supports the DHCP relay and DHCP proxy functions. The DHCP proxy mode is the extension of the DHCP relay mode, which can quickly detect whether a user is offline.

You can configure the DHCP server for DHCP relay function in the following two ways:

- Disable Option 60, and configure the IP address of the DHCP server on the VLAN interface.
- Enable Option 60, and configure the mapping relation between the Option 60 character string and DHCP server IP address. The ZXA10 C320 determines the DHCP server to be used according to the Option field in the user request packet.

Configuration Data

Table 13-3 lists the DHCP relay configuration data.

Table 13-3 DHCP Relay Configuration Data

Item	Data
Global DHCP	enable
Network layer-3 interface	VLAN ID: 200 IP address: 10.1.1.2
User layer-3 interface	VLAN ID: 100 IP address: 10.10.1.1
DHCP server	Option 60 character string: zte IP address: 10.1.1.1

Steps

1. In global configuration mode, enable global DHCP.

```
ZXAN(config)#ip dhcp enable
```

2. Configure the network layer-3 interface.

```
ZXAN(config)#interface vlan 200
ZXAN(config-if)#ip address 10.1.1.2 255.255.255.0
ZXAN(config-if)#exit
```

3. Configure the user layer-3 interface.

```
ZXAN(config)#interface vlan 100
ZXAN(config-if)#ip address 10.10.1.1 255.255.255.0
```

4. Configure working mode of the VLAN interface and IP address of DHCP relay agent.

```
ZXAN(config-if)#ip dhcp mode relay
ZXAN(config-if)#ip dhcp relay agent 10.10.1.1
ZXAN(config-if)#exit
```

NOTE **Note:**

The DHCP relay agent and VLAN interface have the same IP address.

---

5. Configure the IP address of DHCP relay server.
   - Disable Option 60.

```
ZXAN(config)#interface vlan 100
ZXAN(config-if)#ip dhcp relay server 10.1.1.1
ZXAN(config-if)#exit
```

   - Enable Option 60.
     i. In global configuration mode, configure the mapping relation between the option 60 character string and DHCP server IP address.

```
ZXAN(config)#ip dhcp relay server vclass-id zte 10.1.1.1 standard
```

     ii. In layer-3 VLAN interface mode, configure the DHCP packet to be forwarded according to the Option 60 character string.

```
ZXAN(config)#interface vlan 100
ZXAN(config-if)#ip dhcp helper-address policy vclass-id
ZXAN(config-if)#exit
```

```
ZXAN(config)#ip dhcp relay server vclass-id zte 10.1.1.1 standard
```

6. (Optional) Query the user information on the DHCP relay.

```
ZXAN(config)#show ip dhcp relay user vlan 100
Current online users are 0.
Index MAC addr    IP addr   Server addr  User Port  State Expiration
```

– End of Steps –

This page intentionally left blank.

Chapter 14
Uplink Protection Configuration

The ZXA10 C320 adopts the dual uplink protection mechanism to ensure the service stability. When the physical connection between the ZXA10 C320 and upper-layer equipment is broken and the services are interrupted, the device will automatically switch the services to the standby line to restore the services quickly.

The ZXA10 C320 supports the following uplink protection modes:

- Link aggregation
- UAPS
- ZESS

Table of Contents

14.1 Configuring Link Aggregation

This section describes how to configure link aggregation to implement load balancing and protection on the uplink port.

Prerequisite

Before this operation, make sure that:

- Link aggregation has been configured on the opposite end.
- Port rate and VLAN properties on the opposite end are the same as that on the ZXA10 C320.

Context

The ZXA10 C320 supports two link aggregation modes.

- Static aggregation

  In static aggregation mode, multiple physical ports are directly added to a trunk group to form a logical port. This mode is simple but not suitable for observing the status of the link aggregation port.

- Link Aggregation Control Protocol (LACP)

In LACP mode, multiple physical ports are dynamically aggregated into a trunk group to form a logical port, thus to balance the load of the egress/ingress flow among the member ports. Aggregation is automatically generated to obtain the maximum bandwidth.

The ZXA10 C320 link aggregation function complies with the following rules:

- The link aggregation function supports up to eight trunk groups, and each trunk group contains up to eight member ports.
- The inter-interface card aggregation is supported, and the member ports can be located on any interface card.
- Member ports must operate in full duplex mode, and the working rates and VLAN attributes must be consistent.

The logical port formed by link aggregation on the ZXA10 C320 is called smartgroup. A smartgroup has the same default VLAN attributes as a common Ethernet port.

Steps

1. In global configuration mode, create a smartgroup.

```
ZXAN(config)#interface smartgroup1
ZXAN(config-if)#
```

2. Configure the load balancing mode.

```
ZXAN(config-if)#smartgroup load-balance src-dst-mac
```

NOTE **Note:**

The ZXA10 C320 supports six load balancing modes that are based on source IP, destination IP, source/destination IPs, source MAC, destination MAC, and source/destination MACs respectively. The default mode is based on source/destination MACs.

3. Configure the VLAN for the smartgroup.

```
ZXAN(config-if)#switchport vlan 100 tag
ZXAN(config-if)#switchport default vlan 200
ZXAN(config-if)#exit
```

4. (Optional) Query VLAN properties of the smartgroup and uplink ports.

```
ZXAN(config)#show vlan port smartgroup1
PortMode    Pvid  CPvid Tpid/mode   TLSStatus TLSVlan
-------------------------------------------------
hybrid      1     0     0x8100/PORT disable   0
UntaggedVlan:
200
TaggedVlan:
```

```
100
ZXAN(config)#show vlan port gei_1/3/1
PortMode    Pvid  CPvid Tpid/mode   TLSStatus TLSVlan
-------------------------------------------------
hybrid      1     0     0x8100/PORT disable   0
UntaggedVlan:
200
TaggedVlan:
100
ZXAN(config)#show vlan port gei_1/3/3
PortMode    Pvid  CPvid Tpid/mode   TLSStatus TLSVlan
-------------------------------------------------
hybrid      1     0     0x8100/PORT disable   0
UntaggedVlan:
200
TaggedVlan:
100
```

NOTE **Note:**

Before adding ports to a smartgroup, you need to make sure that the VLAN configuration and switchport mode of member ports should be consistent with the that of the smartgroup.

5. In uplink interface configuration mode, add the port to the aggregation group and set the port aggregation mode to active.

```
ZXAN(config)#interface gei_1/3/1
ZXAN(config-if)#smartgroup 1 mode active
```

NOTE **Note:**

The ZXA10 C320 supports the following three port aggregation modes:

- On: Static aggregation trunk. The two ends of the aggregation need to be set to the on mode.
- Active: LACP active negotiation mode
- Passive: LACP passive negotiation mode

It is recommended that you set the port at one end to the active aggregation mode, and set the port at the other end to the passive aggregation mode, or set ports at both ends to the active aggregation mode.

6. Configure the timeout mode of the port.

```
ZXAN(config-if)#lacp timeout long
```

NOTE **Note:**

The ZXA10 C320 supports the following two LACP timeout modes:

- Long (default): The adjacent port sends a LACPDU packet every 30s.
- Short: The adjacent port sends a LACPDU packet every second.

The LACP timeout mode is valid only when the port is in active or passive aggregation mode.

---

7. Configure other port in the aggregation group.

```
ZXAN(config)#interface gei_1/3/3
ZXAN(config-if)#smartgroup 1 mode active
ZXAN(config-if)#lacp timeout long
```

8. (Optional) Query the smartgroup status.

```
ZXAN(config-if)#show lacp internal
Smartgroup:1    System priority:32768    Load-balance:src-dst-mac
Flag *--LOOP is TRUE
Actor      Agg     LACPDUs  Port     Oper    Port  RX           Mux          Sub
Port       State   Interval Priority Key     State Machine      Machine      Group
--------------------------------------------------------------------------------
gei_1/3/1  unselected 30    32768    0x1     0x5   N/A          N/A           N/A
gei_1/3/3  unselected 30    32768    0x1     0x5   N/A          N/A           N/A
```

– End of Steps –

14.2 Configuring UAPS

This section describes how to configure UAPS to implement automatic protection switchover of the uplink port.

Context

The ZXA10 C320 supports the uplink automatic protection switching (UAPS) function. The system periodically checks the working status of the uplink port. When the system detects that the link of the working port is disconnected or the link is not available due to link quality degradation, it switches the services to the standby port automatically and without interrupting the services.

Steps

1. In global configuration mode, create a UAPS group.

```
ZXAN(config)#uaps-group 1
ZXAN(cfg-uaps-1)#
```

2. Configure the active/standby ports of the UAPS group.

```
ZXAN(cfg-uaps-1)#port master-port gei_1/3/1 slave-port gei_1/3/3
```

NOTE **Note:**

The configuration data on the active port and standby port should be consistent.

3. Enable active/standby auto-switch for the UAPS group.

```
ZXAN(cfg-uaps-1)#revertive enable
```

4. Configure the UAPS group protection time.

```
ZXAN(cfg-uaps-1)#protect-time 400
```

If the UAPS group implements switchover once, it does not implement switchover again during the protection time.

5. Configure the port attribute of the UAPS group.

```
ZXAN(cfg-uaps-1)#switch-type common-port
```

NOTE **Note:**

The ZXA10 C320 supports the following two port attributes:

- Common-port: common port
- Trunking-port: link aggregation port

6. (Optional) Query the UAPS group configuration.

```
ZXAN(cfg-uaps-1)#show uaps groupid 1
Revertive control         :   enable
PortLight  control        :   disable
Protect-time              :   400s
Next-hop                  :   0.0.0.0
Bfd next_hop              :   0.0.0.0
Link-type                 :   normal
Link-detect-retry         :   5
Link-detect-interval      :   3
Link status               :   connected or NA
Bfd  Link status          :   connected or NA
Switch-type               :   common port
Master ports status       :   forwarding
                              gei_1/3/1 : down
```

```
Slave ports status        :   block
                              gei_1/3/3 : down
```

– End of Steps –

14.3 Configuring ZESS

This section describes how to configure the ZESS to implement VLAN protection on the uplink port.

Context

The ZTE Ethernet Smart Switch (ZESS) aims to protect VLAN services. Two links (one active and one standby) are configured between the ZXA10 C320 and uplink equipment. When the active link is faulty, the ZXA10 C320 switches to the backup link immediately.

Steps

1. Configure VLANs on the active uplink port.

```
ZXAN(config)#interface gei_1/3/1
ZXAN(config-if)#switchport vlan 11-20 tag
ZXAN(config-if)#exit
```

2. Configure VLANs on the backup uplink port.

```
ZXAN(config)#interface gei_1/3/2
ZXAN(config-if)#switchport vlan 11-20 tag
ZXAN(config-if)#exit
```

3. Configure the MSTP instance.

```
ZXAN(config)#spanning-tree enable
ZXAN(config)#spanning-tree mst configuration
ZXAN(config-mstp)#instance 1 vlans 11-20
ZXAN(config-mstp)#exit
```

4. Configure the ZESS protection instance.

```
ZXAN(config)#zess domain 1 protect-instance 1
```

5. Configure the active and backup ports.

```
ZXAN(config)#zess domain 1 member primary gei_1/3/1 secondary gei_1/3/2
```

6. (Optional) Enable the revertive function.

```
ZXAN(config)#zess domain 1 mode revertive
```

7. (Optional) Query the ZESS configuration.

```
ZXAN(config)#show zess domain 1

DomainId:    1  ProtectInstance:  1
  State:  down             Mode:  revertive
```

```
Port :  gei_1/3/1(P)      PortState:   forward / up
Port :  gei_1/3/2(S)      PortState:   block   / up
Preup:  2   (s)           ChangeTimes :   0
```

– End of Steps –

This page intentionally left blank.

Chapter 15
PON Protection Configuration

The ZXA10 C320 uses the active/standby switchover mechanism and PON port protection mechanism to guarantee stable operation of services. When the backbone fiber connection between the ZXA10 C320 and ONU is broken and the services are interrupted, the device will automatically switch the services to the standby PON port to restore the services quickly.

The ZXA10 C320 supports the following four types of PON protection:

- Type A

  Type B is the backbone fiber redundancy protection. It backs up the backbone fiber between the PON port and splitter.

- Type B

  Type B is the OLT-side redundancy protection. It backs up the OLT PON ports and the backbone fiber between the PON port and splitter. The splitter OLT-side has two input ports and two output ports. This protection mode can recover the service on the OLT side only.

- Type C

  Type C is the OLT-side and ONU-side redundancy protection, It backs up the OLT PON port, ONU (dual optical modules), splitter, and all the fibers. In this mode, the fault at any point can be rectified via the active/standby switchover.

- Type D

  Type D is the OLT-side and ONU-side redundancy protection, also known as full duplex protection. It backs up the OLT PON port, ONU (dual PON ports), splitter, and all the fibers. In this mode, the fault at any point can be rectified via the active/standby switchover.

Table of Contents

15.1 Configuring PON Port Protection

This section describes how to configure type-B PON protection to implement dual PON port backup protection.

Context

The ZXA10 C320 supports the following three PON port switchover modes:

- Force

  The service is switched to the specified PON port unconditionally. The service can be switched from the protection port to the working port (p2w) or from the working port to the protection port (w2p) forcedly.

- Alarm-triggered (default)
- Manual

  The service needs to be switched manually. Switchover in p2w or w2p mode is supported.

The priorities of the three modes in descending order are force, alarm-triggered, and then manual.

Configuration Data

Table 15-1 lists the PON protection configuration data.

Table 15-1 PON Protection Configuration Data

Item	Data
PON protection group	zte
Working PON port	1/1/1
Protection PON port	1/1/2
Protection type	Type B
Protection mode	revertive
Restoring time	120s

Steps

1. In PON configuration mode, clear the configuration data on the protection PON port.

```
ZXAN(config)#pon
ZXAN(config-pon)#clear gpon-olt_1/1/2
```

2. Create a PON protection group.

```
ZXAN(config-pon)#protection group zte workpon gpon-olt_1/1/1 protectpon gpon-olt_
1/1/2 typeB
```

3. Configure the attributes of the PON protection group.

```
ZXAN(config-pon)#protection prop group zte mode revertive wtr 120
```

4. (Optional) Switch the PON port by forced.

```
ZXAN(config-pon)#protection switch-command group zte force w2p
```

5. (Optional) Query the PON protection group.

```
ZXAN(config-pon)#show protection group information zte
```

```
Name :                      zte
System model:               self-contained
Peer host IP:               N/A
Protection type :           typeB
Work channel interface :    gpon-olt_1/1/1
Protect channel interface:  gpon-olt_1/1/2
Protection mode:            revertive
Time to restore(s):         120
Active channel:             protect-channel
Alarm request:
  Work channel:             OLTSF
  Protect channel:          OLTSF
External request:           force-switch-to-protection-request
```

– End of Steps –

This page intentionally left blank.

Chapter 16
Access Security Configuration

Access security configuration can assure the safety of subscriber accounts, prevent illegal users from accessing the device, and illegal user-side packets from attacking the device.

The ZXA10 C320 supports the following access security features:

- Port location
- IP Source Guard
- MAC address anti-spoofing
- ARP anti-spoofing
- ARP proxy
- MFF

Table of Contents

16.1 Port Location Configuration

The ZXA10 C320 provides the user port location mechanism to improve network security and prevent user accounts from being stolen.

User port location uses the Option field of the protocol to transmit the user location information (namely, physical line information of the user access) during the protocol interaction process for Authentication, Authorization, and Accounting (AAA).

16.1.1 Configuring User Port Location

When the ZXA10 C320 uses the PPPoE+/DHCP Option 82/DHCPv6 Option 18 modes to locate the user port, circuit ID and remote ID need to be configured. The ZXA10 C320 supports port location configuration based on either a virtual port (vport) or a service port (sport).

Steps

1. In global configuration mode, enable DHCP option 82.

```
ZXAN(config)#dhcp-option82 enable
```

2. Configure the access node identifier.

```
ZXAN(config)#port-location access-node-identifier hostname
```

3. Configure the host name.

```
ZXAN(config)#port-location hostname ZXA10-C320
```

4. In ONU interface configuration mode, enable remote ID.

```
ZXAN(config)#interface gpon-onu_1/1/1:1
ZXAN(config-if)#port-location sub-option remote-id enable vport 1
```

5. Configure the remote ID name.

```
ZXAN(config-if)#port-location sub-option remote-id name REMOTE-ID vport 1
```

6. Configure the circuit ID format.

```
ZXAN(config-if)#port-location format china-telecom vport 1
```

7. (Optional) Query the global configuration of port location.

```
ZXAN(config-if)#show port-location global
identifier : hostname
rackno     : 0
frameno    : 0
hostname   : ZXA10-C320
flex-syn-stat : disable
```

8. (Optional) Query the port location configuration on the interface.

```
ZXAN(config-if)#show port-location port gpon-onu_1/1/1:1 vport 1
Onu               Vport Cid-Format     Rid-status Rid-name    Ft-cid
gpon-onu_1/1/1:1  1     china-telecom  enable     REMOTE-ID
```

– End of Steps –

16.1.2 Configuring PPPoE+

After you configure PPPoE+, the ZXA10 C320 labels the upstream PPPoE packets with 0x0105.

Prerequisite

User port location has been configured.

Context

When users access the Internet in PPPoE+ mode, the ZXA10 C320 uses the PPPoE+ Intermediate Agent mode to locate the port. The ZXA10 C320 carries the user port information in the PPPoE+ discovery packets to report to the BRAS for user authentication, and thus binding the user account and circuit.

Steps

1. In global configuration mode, enable global PPPoE+.

```
ZXAN(config)#pppoe-plus enable
```

2. In ONU interface configuration mode, enable PPPoE+ on the interface.

```
ZXAN(config)#interface gpon-onu_1/1/1:1
ZXAN(config-if)#pppoe-plus enable vport 1
```

3. Configure the PPPoE+ policy on the interface.

```
ZXAN(config-if)#pppoe-plus trust true replace vport 1
```

4. (Optional) Query the global PPPoE+ configuration.

```
ZXAN(config-if)#show pppoe-plus global
pppoe-plus status : enable
```

5. (Optional) Query the PPPoE+ configuration on the interface.

```
ZXAN(config-if)#show pppoe-plus port gpon-onu_1/1/1:1 vport 1
Onu                Vport          Pppoe-plus status   Trust    Policy
gpon-onu_1/1/1:1   1              enable              true     replace
```

– End of Steps –

16.1.3 Configuring DHCP Option 82

After you configure DHCP Option 82, the ZXA10 C320 adds the Option 82 field to the upstream DHCP packets.

Prerequisite

User port location has been configured.

Context

The Option 82 field includes the circuit ID, remote ID, and sub-option90 (optional) fields and provides information such as the shelf number, slot number, port number, VPI, and VCI.

- After DHCP Option 82 is enabled, the ZXA10 C320 can add/strip the Option 82 ield to/from the DHCP packets.
- When DHCP option 82 is disabled, the ZXA10 C320 transparently transmits or directly forwards the DHCP packets without any processing.

Steps

1. In global configuration mode, enable global DHCP Option 82.

```
ZXAN(config)#dhcp-option82 enable
```

2. In ONU interface configuration mode, enable DHCP Option 82 on the interface.

```
ZXAN(config)#interface gpon-onu_1/1/1:1
ZXAN(config-if)#dhcp-option82 enable vport 1
```

3. Configure the DHCP Option 82 policy on the interface.

```
ZXAN(config-if)#dhcp-option82 trust true replace vport 1
```

4. Enable the DHCP snooping function on the interface.

```
ZXAN(config-if)#ip dhcp snooping enable vport 1
```

5. (Optional) Query the global DHCP Option 82 configuration.

```
ZXAN(config)#show dhcp-option82 global
option82 status : enable
```

6. (Optional) Query the DHCP Option 82 configuration on the interface.

```
ZXAN(config)#show dhcp-option82 port gpon-onu_1/1/1:1 vport 1
Onu                Vport  Option82 status   Trust    Policy
gpon-onu_1/1/1:1   1      enable            true     replace
```

– End of Steps –

16.1.4 Configuring DHCPv6 Option 18

After you configure DHCPv6 Option 18, the ZXA10 C320 adds the Option 18 and Option 37 fields to the upstream DHCPv6 packets.

Prerequisite

User port location has been configured.

Context

The option 18 field includes circuit ID, and the option 37 field includes remote ID. The two fields provides information such as the shelf number, slot number, port number, VPI, and VCI.

- After DHCPv6 option 18 is enabled, the ZXA10 C320 can add/strip the Option 82 field or Option 37 field to/from the DHCPv6 packets.
- When DHCPv6 option 18 is disabled, the ZXA10 C320 transparently transmits or directly forwards the DHCPv6 packets without any processing.

Steps

1. In global configuration mode, enable global DHCPv6 option 18.

```
ZXAN(config)#dhcp6-option18 enable
```

2. Configure the working mode of global DHCPv6 option 18.

```
ZXAN(config)#dhcp6-work-mode l2_mode
```

3. In ONU interface configuration mode, enable DHCPv6 Option 18.

```
ZXAN(config)#interface gpon-onu_1/1/1:1
ZXAN(config-if)#dhcp6-option18 enable vport 1
```

4. Configure the DHCPv6 Option 18 policy.

```
ZXAN(config-if)#dhcp6-option18 trust true replace vport 1
```

5. (Optional) Query the global DHCP Option 18 configuration.

```
ZXAN(config-if)#show dhcp6-option18 global
option18 status : enable
ZXAN(config-if)#show dhcp6-work-mode global
dhcp6 work mode : l2_mode
```

6. (Optional) Query the DHCP Option 18 configuration on the interface.

```
ZXAN(config-if)#show dhcp6-option18 port gpon-onu_1/1/1:1 vport 1
Onu                Vport  Option18 status   Trust    Policy
gpon-onu_1/1/1:1   1      enable            true     replace
```

– End of Steps –

16.2 Configuring IP Source Guard

This section describes how to configure IP source guard based on the service port to prevent illegal users from accessing the Internet.

Context

The ZXA10 C320 supports IPv4 and IPv6 IP source guard.

- The legal IPv4 users are managed through either the DHCP snooping table or static IPv4 addresses.
- The legal IPv6 users are managed through static IPv6 addresses.

Steps

1. In global configuration mode, enable global IP source guard.

```
ZXAN(config)#ip-service ip-source-guard enable
```

2. In PON ONU interface configuration mode, configure the service port VLAN.

```
ZXAN(config)#interface gpon-onu_1/1/1:1
ZXAN(config-if)#service-port 1 vport 1 user-vlan 100 vlan 100
```

3. Enable IP source guard on the service port.

```
ZXAN(config-if)#ip-service ip-source-guard enable sport 1
```

4. Configure the IP address of the IPv4 and IPv6 static access user.

```
ZXAN(config-if)#ip-service ip-fixed-user 1.1.1.2 vlan 100 sport 1
ZXAN(config-if)#ip-service ipv6-fixed-user 1:2::1 ipv6-mask 128 mac-address 0000.
0000.0001 vlan 100 sport 1
```

5. (Optional) Query the global IP source guard configuration.

```
ZXAN(config-if)#show ip-service ip-source-guard
global ip-source-guard status :enable
```

6. (Optional) Query the configuration of the IPv4 and IPv6 static access user.

```
ZXAN(config-if)#show ip-service user interface gpon-onu_1/1/1:1
Port                Sport  IP-addr      MAC-addr        Vlan     Source
```

```
gpon-onu_1/1/1:1    1      1.1.1.2      0000.0000.0000  100      fixed-user

ZXAN(config-if)#show ip-service ipv6-user interface gpon-onu_1/1/1:1
Port                Sport  IPv6-addr    Mask MAC-addr        Vlan    Source
gpon-onu_1/1/1:1    1      1:2::1            0000.0000.0001  100     fixed-user
```

– End of Steps –

16.3 Configuring MAC Address Anti-Spoofing

This section describes how to configure MAC address anti-spoofing to prevent malicious MAC address spoofing.

Context

The ZXA10 C320 MAC address anti-spoofing function has the following features:

- This function constrains the user port that learns the MAC address. When one MAC address is learnt by one user port, the address cannot be learnt by other user ports. Thus, the same MAC address cannot float between different ports.
- Once a user port is detected trying MAC address spoofing, an alarm message including the port and MAC address will be reported.
- This function supports uplink port protection. A user port MAC address can float to an uplink port, whereas an uplink port address cannot float to a user port. A MAC address can float between uplink ports, thus to protect the gateway MAC address of the uplink ports.

Steps

1. In global configuration mode, enable MAC address anti-spoofing.

```
ZXAN(config)#security mac-anti-spoofing enable
```

2. Enable MAC address spoofing trap.

```
ZXAN(config)#security mac-spoofing-trap enable
```

3. Enable uplink port protection of MAC address anti-spoofing.

```
ZXAN(config)#security mac-anti-spoofing uplink-protect enable
```

4. (Optional) Query the MAC address anti-spoofing configuration.

```
ZXAN(config)#show security configuration
mac-spoofing-trap :enable
mac-anti-spoofing :enable
uplink-protect    :enable
the total uplink-protect-mac num:0
```

5. (Optional) Query the MAC address spoofing log.

```
ZXAN(config)#show security mac-spoofing-log
```

```
the total mac-spoofing-log num:0
```

– End of Steps –

16.4 Configuring ARP Anti-Spoofing

The ZXA10 C320 supports Address Resolution Protocol (ARP) anti-spoofing on both network side and user side.

Context

User-side ARP anti-spoofing is determined based on the ARP entry added by DHCP and the fixed ARP entry of the static IP access user.

If the source IP address of the received ARP packets and the VLAN exist in the ARP table, the ZXA10 C320 checks whether the MAC addresses are the same. If they are different, the ZXA10 C320 considers the packet as an ARP spoofing behavior and discards it.

Network-side ARP anti-spoofing is based on the static gateway MAC address of the VLAN.

Steps

1. In global configuration mode, enable ARP anti-spoofing.

```
ZXAN(config)#ip-service arp-anti-spoofing enable
```

2. Configure ARP anti-spoofing in the VLAN.

```
ZXAN(config)#ip-service arp-anti-spoofing vlan 100 direction all
```

3. (Optional) Query the ARP anti-spoofing configuration.

```
ZXAN(config)#show ip-service arp-anti-spoofing
Arp Anti-Spoofing status:Enabled.
vlan       direction
----------------------
 100       all
```

– End of Steps –

16.5 Configuring ARP Proxy

This section describes how to configure ARP proxy to implement interworking between subscribers under the same PON port.

Context

By default, the ZXA10 C320 services on different ONUs under the same PON port are isolated. When a service, such as VoIP, requires interworking between the subscribers under the same PON port, the ZXA10 C320 uses the ARP proxy function to achieve interworking between the subscribers in the same VLAN and same network segment under the same PON port.

Steps

1. In layer-3 VLAN interface mode, configure the layer-3 interface IP address.

```
ZXAN(config)#interface vlan 100
ZXAN(config-if)#ip address 10.1.1.1 255.255.255.0
```

NOTE **Note:**

The VLAN is the user VLAN. The IP address should be in the same network segment as that of the interworking device.

2. Enable ARP proxy on the layer-3 interface.

```
ZXAN(config-if)#ip proxy-arp
ZXAN(config-if)#exit
```

– End of Steps –

16.6 Configuring MFF

This section describes how to configure MFF to implement layer-3 interworking between subscribers and prevent malicious attacks.

Context

The MAC forced forwarding (MFF) function prohibits interworking between two subscribers in the same subnet and forcedly forwards the upstream flows of the subscribers to the gateway. The gateway then forwards the flows to implement layer-3 interworking between subscribers. The gateway can analyze flows between subscribers to prevent malicious attacks.

Steps

1. In global configuration mode, enable MFF.

```
ZXAN(config)#ip-service mac-forced-forwarding enable
```

2. Configure the gateway IP address of the MFF VLAN.

```
ZXAN(config)#ip-service mac-forced-forwarding vlan 100 gateway 10.1.1.1
```

3. (Optional) Query the global MFF configuration.

```
ZXAN(config)#show ip-service mac-forced-forwarding
Mac-Forced Forwarding status:Enabled.
```

4. (Optional) Query the gateway information of the MFF VLAN.

```
ZXAN(config)#show ip-service gateway
Vlan  Gateway IP      Gateway MAC        Type
------------------------------------------------------------
```

```
100    10.1.1.1        00d0.d0c7.0561     dynamic-600s
```

– End of Steps –

This page intentionally left blank.

Chapter 17
System Security Configuration

System security configuration can prevent illegal network-side packets from attacking devices, thus to ensure stable running of the devices.

The ZXA10 C320 supports the following system security features:

- Secure Shell (SSH)
- Terminal Access Controller Access-Control (TACACS+)
- Remote Authentication Dial In User Service (RADIUS)
- Management ACL
- Control panel safety

Table of Contents

17.1 Configuring SSH

SSH can replace Telnet to implement secure remote login.

Prerequisite

The SSH client software has been installed.

Context

SSH can encrypt the data during transmission to prevent the "intermediate" attacks. In addition, SSH compresses the data to be transmitted, thus increasing the transmission speed. When the SSH client communicates with the SSH server, the user name and password are encrypted, thus to prevent the password from being intercepted.

The ZXA10 C320 supports the SSH server function.

Steps

1. In global configuration mode, enable SSH server.

```
ZXAN(config)#ssh server enable
```

2. Configure the SSH server protocol version.

```
ZXAN(config)#ssh server version 2
```

3. Configure the SSH server authentication mode.

```
ZXAN(config)#ssh server authentication mode local
```

4. Configure the SSH server authentication type.

```
ZXAN(config)#ssh server authentication type pap
```

5. (Optional) Query the SSH configuration.

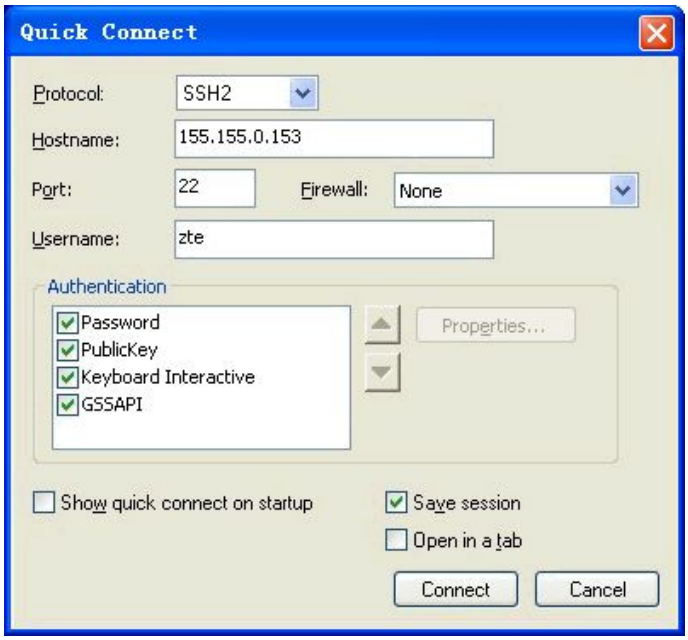
```
ZXAN(config)#show ssh
SSH configuration:
  SSH enable-flag configuration : enable
  SSH version                   : ver2.0
  SSH only configuration        : disable
  SSH init server key           : disable
  SSH auth radius isp-groupid   : 0
  SSH auth mode                 : local
  SSH auth type                 : pap
```

– End of Steps –

Follow-Up Action

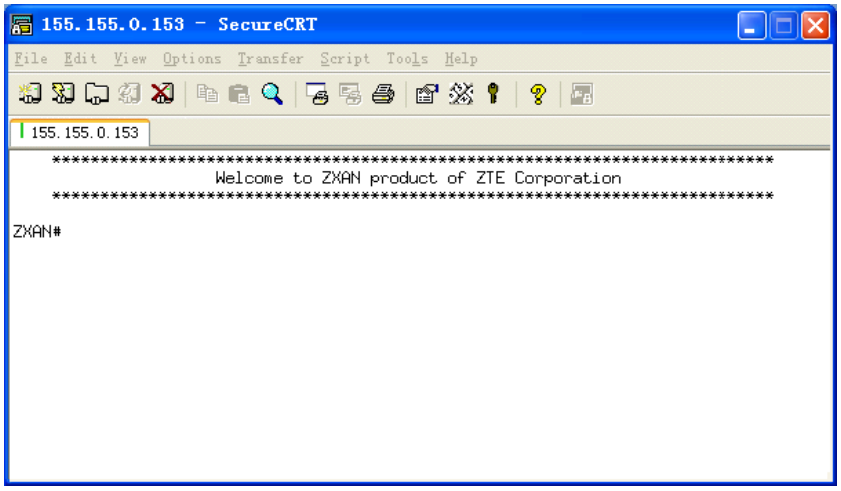
1. In a Windows OS, run the SSH client software (SecureCRT, for example). The **Quick Connect** dialog box opens, as shown in Figure 17-1.

Figure 17-1 Quick Connect Dialog Box



2. In the **Quick Connect** dialog box, select **Protocol**, type **Hostname** and **Username**, and then click **Connect**. The login window opens, see Figure 17-2.

Figure 17-2 SSH Login Window



NOTE **Note:**

The hostname is the in-band/out-of-band NM IP address of the ZXA10 C320.

17.2 Configuring TACACS+

TACACS+ ensures data safety of the ZXA10 C320 by implementing safety authentication and authorization for remote subscribers who access the ZXA10 C320.

Context

TACACS+ supports the following two login modes:

- Telnet
- SSH

Steps

1. Configure the login authentication type and login authorization type to TACACS+.

```
ZXAN(config)#login-authentication-type tacacs+
ZXAN(config)#login-authorization-type tacacs+
```

2. Configure the TACACS+ server.

```
ZXAN(config)#tacacs enable
ZXAN(config)#tacacs-server host 10.1.1.1 timeout 25 key zte
```

3. Configure the homing group of the TACACS+ server.

```
ZXAN(config)#aaa group-server tacacs+ zte_tac
ZXAN(config-sg)#server 10.1.1.1
ZXAN(config-sg)#exit
```

4. Configure the AAA authentication group, authorization group, and accounting group.

```
ZXAN(config)#aaa authentication login default group zte_tac
ZXAN(config)#aaa authorization exec default group zte_tac
ZXAN(config)#aaa accounting commands 15 default stop-only group zte_tac
```

5. (Optional) Configure the SSH server authentication mode to TACACS+.

NOTE **Note:**

When logging in through Telnet, you can skip this step.

```
ZXAN(config)#ssh server enable
ZXAN(config)#ssh server authentication mode tacacs+
```

– End of Steps –

17.3 Configuring RADIUS

RADIUS ensures data safety of the ZXA10 C320 by implementing safety authentication and authorization for remote subscribers who access the ZXA10 C320.

Context

RADIUS supports the following two login modes:

- Telnet
- SSH

Steps

1. Configure the login authentication mode to RADIUS, using authentication group 1.

```
ZXAN(config)#login-authentication-type radius 1
```

2. Configure the RADIUS authentication group.

```
ZXAN(config)#radius authentication-group 1
ZXAN(config-authgrp-1)#server 1 10.1.1.1 key zte
ZXAN(config-authgrp-1)#exit
```

3. (Optional) Configure the SSH server authentication mode to RADIUS.

NOTE **Note:**

When logging in through Telnet, you can skip this step.

```
ZXAN(config)#ssh server enable
```

```
ZXAN(config)#ssh server authentication mode radius
ZXAN(config)#ssh server authentication type chap
ZXAN(config)#ssh server authentication ispgroup 1
```

– End of Steps –

17.4 Configuring Management ACL

After you configure the management ACL, accessing the ZXA10 C320 in Telnet/SNMP mode can be restricted.

Context

The management ACL is a standard ACL, which controls the source IP address of the received IP packets. The management ACL restricts users' access to the ZXA10 C320 NM module.

Steps

1. Create a standard ACL.

```
ZXAN(config)#acl standard number 10
ZXAN(config-std-acl)#
```

2. Configure the ACL rules.

```
ZXAN(config-std-acl)#rule 1 deny 1.1.1.10 0.0.0.0
ZXAN(config-std-acl)#rule 2 permit 1.1.1.0 0.0.0.255
ZXAN(config-std-acl)#exit
```

3. Apply the ACL.

```
ZXAN(config)#line telnet access-class 10
```

– End of Steps –

17.5 Configuring Control Panel Safety

After you configure control panel safety, the ZXA10 C320 can limit the protocol packet rate and prevent DoS packet attacks.

Context

Control panel safety includes the following three functions:

- Rate limit of protocol packets

  Different rate limits are set for packets of different protocols.

- Rate limit of CPU queue packets

  Packet rate limits for eight queues of the exchange chip can be set separately. When the packet rate of a certain queue is too high, a corresponding rate limit can be set to reduce the impact on the CPU.

- Black list

  When the number of packets sent to the CPU by a user in one polling period (5s by default) exceeds the threshold, the ZXA10 C320 considers that the user implements a DoS attack on the NE and includes the user into the black list. Then packets sent by the user will be dropped till the user stops the attack.

Steps

1. Enter control panel mode, and configure packet limit.

```
ZXAN(config)#control-panel
ZXAN(control-panel)#packet-limit dhcp 20
ZXAN(control-panel)#packet-limit arp 50
```

2. Configure the rate limit of CPU queue packets.

```
ZXAN(control-panel)#cpu queue 1 25
```

3. Enable anti-DoS.

```
ZXAN(control-panel)#anti-dos enable
```

4. Enable the anti-DoS drop function.

```
ZXAN(control-panel)#anti-dos drop enable
```

5. Configure the threshold of the black list.

```
ZXAN(control-panel)#anti-dos limit-num 20
```

6. Configure the polling time of the black list.

```
ZXAN(control-panel)#anti-dos blocking-time 10
```

7. (Optional) Query the black list.

```
ZXAN(control-panel)#show control-panel anti-dos black-table
----------------------------MP  BLACK TABLE-------------------------------------
mac-address     vlan       port              onu-sn        state     PktIn  Drop


----------------------------NP  BLACK-TABLE-------------------------------------
mac-address          port              onu-sn         state     PktIn     Drop
-------------------------------------------------------------------------------
```

– End of Steps –

Chapter 18
Route Protocol Configuration

Besides static route, the ZXA10 C320 supports the following routing protocols:

- OSPF
- BGP

Table of Contents

18.1 Configuring the Static Route

This section describes how to implement the static route of the ZXA10 C320 by configuring the next hop address to the destination network segment.

Context

Static route is the route info added into the routing table by the network administrator via the configuration command. You can using static route with a few configurations to avoid using dynamic routing. In the case that multiple routers and multiple paths exist, however, dynamic routing is recommended.

Steps

1. In global configuration mode, configure the static route.

```
ZXAN(config)#ip route 10.1.1.0 255.255.255.0 1.1.1.2
```

– End of Steps –

18.2 Configuring the OSPF Protocol

This section describes how to implement the ZXA10 C320's access to the adjacent router by configuring the OSPF protocol.

Context

OSPF is an Interior Gateway Protocol (IGP), used to determine the route in a single Autonomous System (AS). OSPF is a link-state routing protocol. It overcomes the weaknesses of RIP and other distance vector protocol.

OSPF version 1 is defined in RFC1131. OSPF version 2 is defined in RFC2328. The ZXA10 C320 supports OSPF version 2.

Steps

1. In global configuration mode, enable OSPF.

```
ZXAN(config)#router ospf 1
ZXAN(config-router)#
```

2. Configure the network segment of the interface.

```
ZXAN(config-router)#network 10.1.1.0 0.0.0.255 area 0
```

– End of Steps –

18.3 Configuring the BGP

This section describes how to implement the ZXA10 C320's access to the adjacent router by configuring the BGP.

Context

BGP is an inter-AS routing protocol. It involves a table of IP networks or 'prefixes' which designates network reachability among AS. BGP is a path vector protocol, or a variant of a Distance-vector routing protocol. BGP does not involve traditional IGP metrics, but routing decisions are made based on path, network policies, and/or rule-sets. For this reason, it is more appropriately termed a reachability protocol rather than routing protocol.

Steps

1. In global configuration mode, enable BGP.

```
ZXAN(config)#router bgp 1
ZXAN(config-router)#
```

2. Configure the BGP neighbor.

```
ZXAN(config-router)#neighbor 1.1.1.1 remote-as 2
```

3. Advertise the network using BGP.

```
ZXAN(config-router)#network 30.1.1.0 255.255.255.0
```

– End of Steps –

Chapter 19
Clock Configuration

In a synchronization network, synchronization network connections that can transport different synchronization levels transmits synchronization information. Each synchronization network connection consists of one or more synchronization link connection(s), Each synchronization link connection is provided by a synchronized PDH trail, SDH multiplex section trail, or IEEE 802.3 physical media trail.

Partial synchronization trail signal contain a communication channel that can transmit the SSM, TM, or ESMC of the quality-level identifier. This quality-level identifier can be used to select the input reference signal of the highest synchronization level from a set of nominated synchronization references.

Table of Contents

19.1 Configuring the Synchronous Ethernet Clock

The ZXA10 C320 supports the synchronous Ethernet clock and can provide the synchronous Ethernet clock for the ONU via the PON port.

Configuration Data

Table 19-1 lists the configuration data of the synchronous Ethernet clock.

Table 19-1 Configuration Data of the Synchronous Ethernet Clock

Item	Data
Clock source port	1/3/1
Clock type	SYNCE
Priority	1
Clock SSM value	QL-SEC
PON port	1/1/1

Steps

1. Query the current clock source.

```
ZXAN(config)#show clock source active
interface :1/3/0
type      :internal
ssm-ql    :qlsec
status    :free_run
```

```
warning   :none
operation :none
```

2. In clock configuration mode, configure the clock source.

```
ZXAN(config)#clock
ZXAN(config-clock)#source 1/3/1 type syncE priority 1
```

NOTE **Note:**

When multiple clock sources are configured, the system will select one clock source according to the following criteria:

- The clock status is proper.
- The clock priority is the highest.
- The clock quality is the best.
- The clock is configured earlier.

Priority range is defined from 1 to 250. 1 is defined as the highest priority.

---

3. Configure the SSM value of the clock source.

```
ZXAN(config-clock)#ssm-set 1/3/1 qlsec
```

4. (Optional) Enable the ESMC on the uplink port.

```
ZXAN(config-clock)#switch esmc set 1/3/1
```

5. Configure the SSM value sent by the PON port .

```
ZXAN(config-clock)#ssm-send 1/1/1 qlsec
```

6. Enable the ESMC on the PON port.

```
ZXAN(config-clock)#switch esmc set 1/1/1
```

7. (Optional) Switch the clock source.

```
ZXAN(config-clock)#switch force set 1/3/1
```

8. (Optional) Query the clock configuration.

```
ZXAN(config-clock)#show clock config
interface   type      priority  ssm     mode      status    remarks
.....................................................................
1/3/1       syncE     1         qlsec   -         primary   source
clock source count: 1;
wtr 5 minutes ;   holdofftime 300 ms; QL-enable
external-clock: unbalance
```

9. (Optional) Query the clock source alarms.

```
ZXAN(config-clock)#show clock source alarm
interface   type      priority  ssm-received alarm
.....................................................................
```

```
1/3/1       syncE     1          qlsec         none
```

– End of Steps –

This page intentionally left blank.

Figures

This page intentionally left blank.

Tables

Glossary

AAA
- Authentication, Authorization and Accounting

ACL
- Access Control List

ARP
- Address Resolution Protocol

AS
- Autonomous System

BGP
- Border Gateway Protocol

BRAS
- Broadband Remote Access Server

CAC
- Channel Access Control

CDR
- Call Detail Record

CLI
- Command Line Interface

CPE
- Customer Premises Equipment

CVLAN
- Customer Virtual Local Area Network

CoS
- Class of Service

DHCP
- Dynamic Host Configuration Protocol

DSCP
- Differentiated Services Code Point

DoS
- Denial of Service

EPON
- Ethernet Passive Optical Network

ESMC
- Ethernet Synchronization Message Channel

GEM
- GPON Encapsulation Method

GPON
- Gigabit Passive Optical Network

ICMP
- Internet Control Message Protocol

IGMP
- Internet Group Management Protocol

IGP
- Interior Gateway Protocol

IP
- Internet Protocol

IPTV
- Internet Protocol Television

IPv4
- Internet Protocol version 4

IPv6
- Internet Protocol Version 6

LACP
- Link Aggregation Control Protocol

LAN
- Local Area Network

LLID
- Logical Link Identifier

MAC
- Media Access Control

MFF
- MAC-Forced Forwarding

MG
- Media Gateway

MGC
- Media Gateway Controller

MLD
- Multicast Listener Discovery

MST
- Multiple Spanning Tree

MSTP
- Multiple Spanning Tree Protocol

MVLAN
- Multicast Virtual Local Area Network

NE
- Network Element

NM
- Network Management

NMS
- Network Management System

NTP
- Network Time Protocol

OLT
- Optical Line Terminal

OMCI
- ONT Management Control Interface

ONU
- Optical Network Unit

OSPF
- Open Shortest Path First

P2P
- Point to Point

PDH
- Plesiochronous Digital Hierarchy

PON
- Passive Optical Network

PPPoE
- Point to Point Protocol over Ethernet

PnP
- Plug and Play

QoS
- Quality of Service

RADIUS
- Remote Authentication Dial In User Service

RSTP
- Rapid Spanning Tree Protocol

RTP
- Real-time Transport Protocol

SCB
- Single Copy Broadcast

SDH
- Synchronous Digital Hierarchy

SIP
- Session Initiation Protocol

SSH
- Secure Shell

SSM
- Synchronization Status Message

SSTP
- Single Spanning Tree Protocol

STP
- Spanning Tree Protocol

SVLAN
- Service Virtual Local Area Network

TACACS+
- Terminal Access Controller Access-Control System Plus

TCP
- Transmission Control Protocol

TID
- Terminal Identification

TLS
- Transport Layer Security

TM
- Timing Marker

ToS
- Type of Service

UAPS
- Uplink Auto Protection Switching

UNI
- User Network Interface

VLAN
- Virtual Local Area Network

VoIP
- Voice over Internet Protocol