ZXA10 C320

Optical Access Convergence Equipment

Configuration Manual (CLI)

Version: V2.0.0

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	2013-08-31	First edition

Serial Number: SJ-20130520170233-005

Publishing Date: 2013-08-31 (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:

- Debugging engineer
- Maintenance 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, P2P Service Configuration	Describes P2P service configuration.
4, VLAN Configuration	Describes VLAN configuration.
5, IPTV Configuration	Describes IPTV configuration.
6, QoS Configuration	Describes QoS configuration.
7, ACL Configuration	Describes ACL configuration.
8, NTP Configuration	Describes NTP configuration.
9, STP Configuration	Describes STP configuration.
10, DHCP Configuration	Describes DHCP configuration.
11, Uplink Protection Configuration	Describes uplink protection configuration.
12, PON Protection Configuration	Describes PON protection configuration.
13, Access Security Configuration	Describes access security configuration.
14, System Security Configuration	Describes system security configuration.
15, Ethernet OAM Configuration	Describes Ethernet OAM configuration.
16, Route Protocol Configuration	Describes route protocol configuration.
17, 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 only manage the ZXA10 C320 through HyperTerminal.

- Login Through Telnet

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

- 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

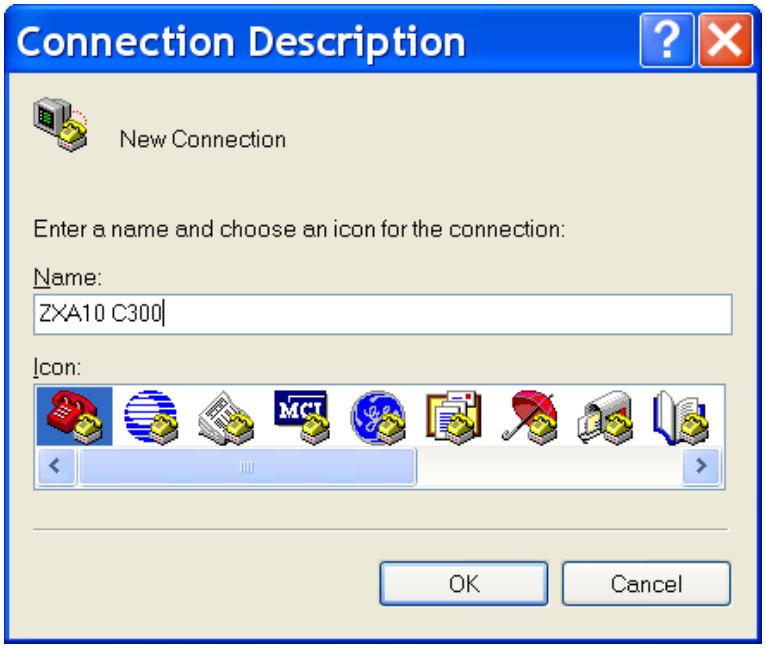
When you log in to the ZXA10 C320 through HyperTerminal, the user name and password are case-sensitive.

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, as shown in Figure 1-1.

Figure 1-1 Connection Description

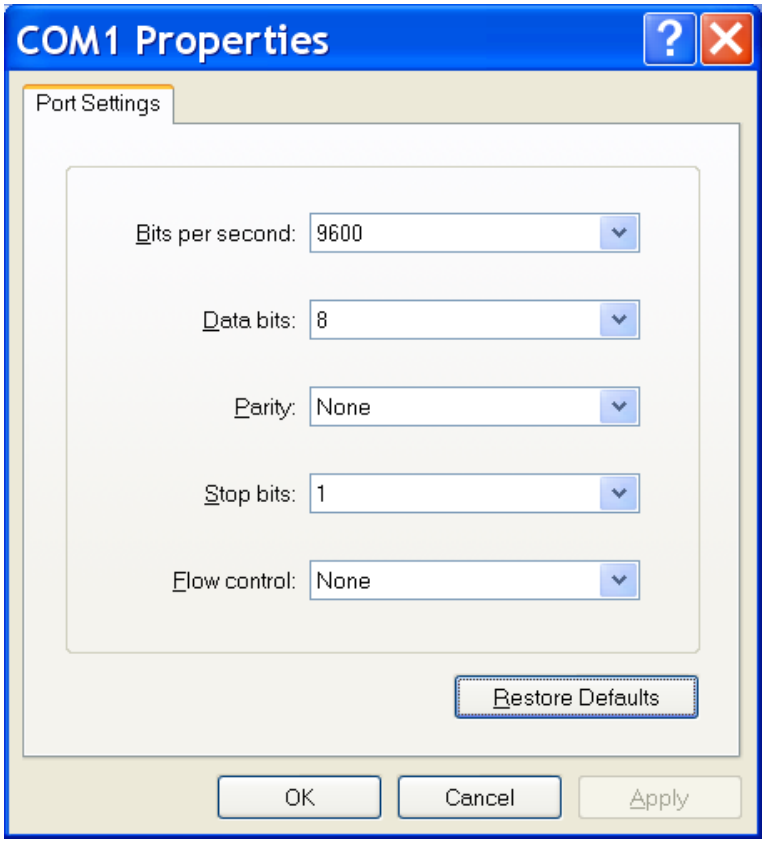


2. Fill in **Name** and click **OK**. The **Connect To** dialog box is displayed, as shown in Figure 1-2.

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**, as shown in 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 operator mode (ZXAN>). Enter the **enable** command and the password to enter administrator mode (ZXAN#), as shown below.

```
**********************************************
   Welcome to ZXAN product 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 can ping the in-band or out-of-band NM IP address.

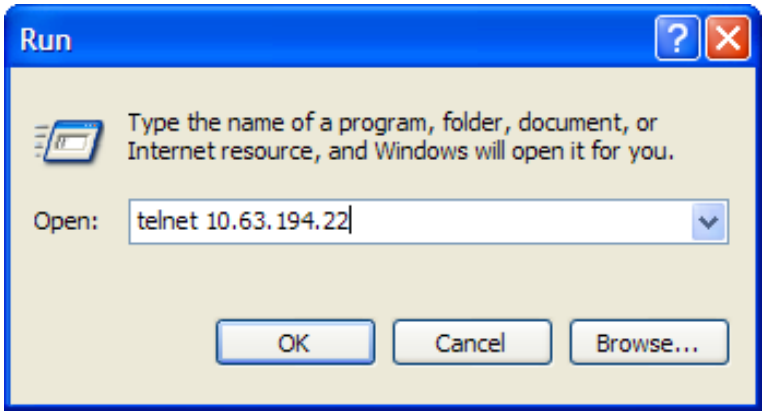
Context

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, as shown in 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 (`zte`) and password `ZTEzte123`) to enter administrator mode (`ZXAN#`), as shown below.

```
**********************************************
   Welcome to ZXAN product 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.
- The uplink daughter-card has been added. (Refer to 1.3.3 Adding a Daughter-Card.)

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 Next hop address: 10.2.1.254/24 Version: V2C Community name: public Alarm level: notifications UDP port: 162

Steps

Configure the NM on the ZXA10 C320.

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:

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:

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:

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

6. Configure the IP address of the SNMP server.

```
ZXAN(config)#snmp-server host 10.2.1.1 version 2c public enable notifications tar
get-addr-name zte target-param-name zte udp-port 162
```

7. Save the configuration data.

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

Configure the NM on the NM server.

8. Configure the static route.
   - In the Windows operating system

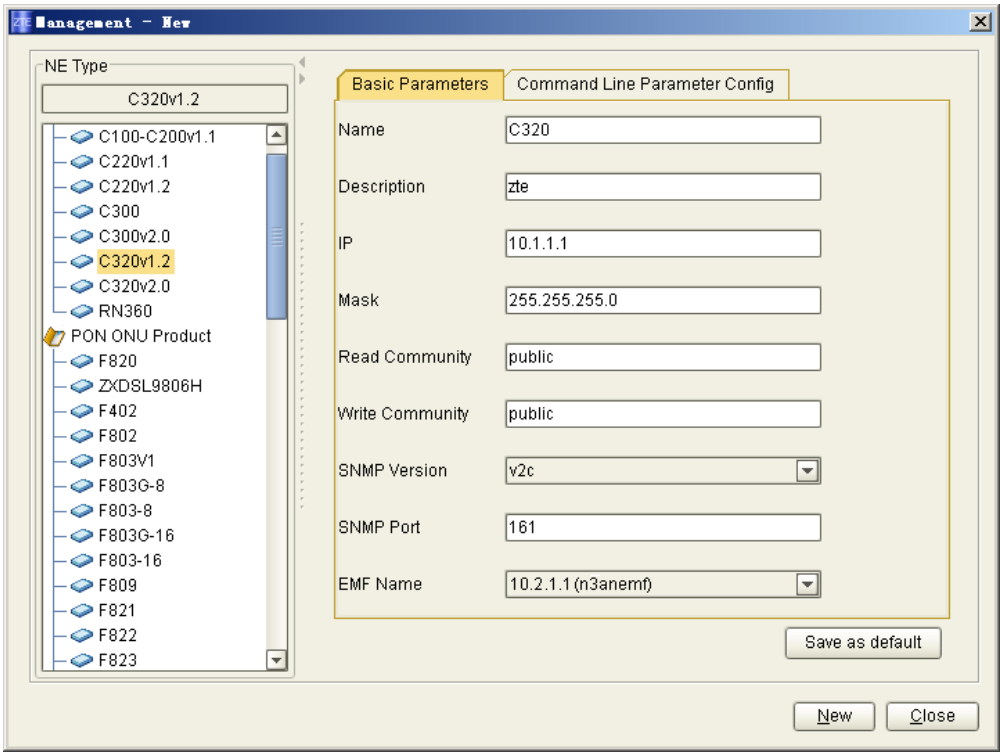
     Use the **route add 10.1.1.0 mask 255.255.255.0 10.2.1.254** command to configure the route.

     Use the **route print** command to query the route table information.
   - In the Solaris operating system

     Use the **route add 10.1.1.0 10.2.1.254** command to configure the route.

     Use the **netstat -r** command to query the route table information.
9. Log in to the NetNumen U31 NMS.
10. Create the NE.
    a. On the **Topology Management** tab, right-click the EMS server on the **NE Tree** and choose **Create Object > Add Wireline NE** to open the **Management - New** dialog box.
    b. Select the NE type from the left pane, and configure the parameters on the **Basic Parameters** tab in the right pane, see Figure 1-5.

Figure 1-5 Configure NE Parameters



c. Click **New** to confirm.

– 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 Next hop address: 10.2.1.254/24 Version: V2C Community name: public Alarm level: notifications UDP port: 162

Steps

Configure the NM on the ZXA10 C320.

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.

```
ZXAN(config)#snmp-server host 10.2.1.1 version 2c public enable notifications tar
get-addr-name zte target-param-name zte udp-port 162
```

6. Save the configuration data.

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

Configure the NM on the NM server.

7. Configure the static route.
   - In the Windows operating system

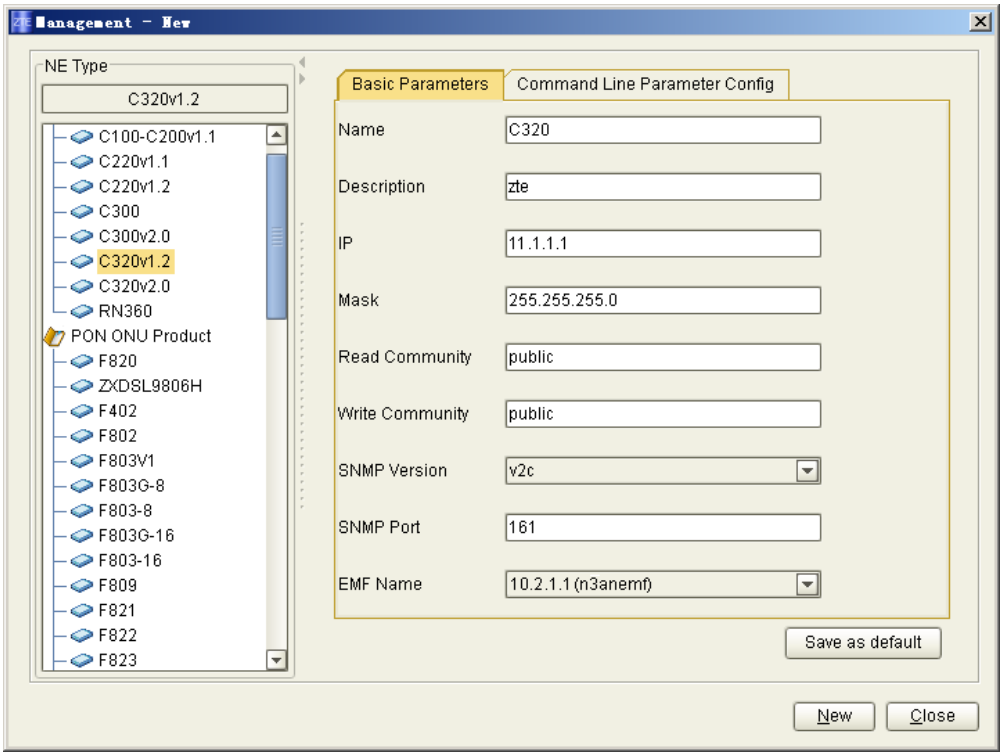
     Use the **route add 11.1.1.0 mask 255.255.255.0 10.2.1.254** command to configure the route.

     Use the **route print** command to query the route table information.
   - In the Solaris operating system

     Use the **route add 11.1.1.0 10.2.1.254** command to configure the route.

     Use the **netstat -r** command to query the route table information.
8. Log in to the NetNumen U31 NMS.
9. Create the NE.
   a. On the **Topology Management** tab, right-click the EMS server on the **NE Tree** and choose **Create Object > Add Wireline NE** to open the **Management - New** dialog box.
   b. Select the NE type from the left pane, and configure the parameters on the **Basic Parameters** tab in the right pane, see Figure 1-6.

Figure 1-6 Configure NE Parameters



c. Click **New** to confirm.

– End of Steps –

1.3 Physical Configuration

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
```

NOTE **Note:**

The ZXA10 C320 supports only one rack currently, and thus *rackno* can only be 1.

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
```

NOTE **Note:**

The ZXA10 C320 supports only one shelf currently, and thus *shelfno* can only be 1.

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  V2.0.0          INSERVICE
1    1     4    SMXA    SMXA     0     110702  V2.0.0          STANDBY
```

1.3.3 Adding a Daughter-Card

A daughter-card provides the optical Ethernet interfaces on the switching card control cards

Context

The ZXA10 C320 supports four type of uplink daughter-cards:

- UCDC/1: two GE optical interfaces
- UCDC/2: one GE optical interface and one 10GE optical interface
- UCDC/3: one GE optical interface and one 10GE optical interface
- UCDC/4: 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/3
ZXAN(config)#add-subcard slotno 4 subcardno 1 UCDC/3
```

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

```
ZXAN(config)#show subcard
ZXAN#show subcard
Rack Shelf Slot Subcard CfgType RealType Port  HardVer SoftVer      Status
------------------------------------------------------------------------------
1    1     3    1       UCDC/3  UCDC/3   3     N/A.    N/A.         INSERVICE
1    1     4    1       UCDC/3  UCDC/3   3     N/A.    N/A.         INSERVICE
```

Table 1-3 describes the status of the daughter-card.

Table 1-3 Status Description of the Daughter-Card

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

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.

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 GTGO
ZXAN(config)#add-card slotno 2 GTGO
```

3. (Optional) Query the card configuration.

```
ZXAN(config)#show card
Rack Shelf Slot CfgType RealType Port  HardVer SoftVer         Status
-------------------------------------------------------------------------------
1    1     1    GTGO    GTGOG    8     120301  V2.0.0          INSERVICE
1    1     2    GTGO    GTGOG    8     120301  V2.0.0          INSERVICE
1    1     3    SMXA    SMXA     0     110702  V2.0.0          INSERVICE
1    1     4    SMXA    SMXA     0     110702  V2.0.0          STANDBY
```

– End of Steps –

1.3.5 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 enabled.

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
```

```
Equipment PNP function is enable.
```

3. (Optional) Query the card configuration.

```
ZXAN(config)#show card
Rack Shelf Slot CfgType RealType Port  HardVer SoftVer         Status
------------------------------------------------------------------------------
1    1     1    GTGO    GTGOG    8     120301  V2.0.0          INSERVICE
1    1     2    GTGO    GTGOG    8     120301  V2.0.0          INSERVICE
1    1     3    SMXA    SMXA     0     110702  V2.0.0          INSERVICE
1    1     4    SMXA    SMXA     0     110702  V2.0.0          STANDBY
```

– End of Steps –

1.3.6 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 properly.
CONFIGING	The card is being configured.
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 properly.
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#show card
Rack Shelf Slot CfgType RealType Port  HardVer SoftVer         Status
------------------------------------------------------------------------------
1    1     1    GTGO    GTGOG    8     120301  V2.0.0          INSERVICE
1    1     2    GTGO    GTGOG    8     120301  V2.0.0          INSERVICE
```

```
1    1     3    SMXA    SMXA     0     110702  V2.0.0          INSERVICE
1    1     4    SMXA    SMXA     0     110702  V2.0.0          STANDBY
```

2. Query a certain card.

```
ZXAN#show card slotno 3
Config-Type    : SMXA      Status        : INSERVICE
Port-Number    : 0
Cpu-Alarm-Threshold : 100%
Mem-Alarm-Threshold : 100%

Real-Type      : SMXA      Serial-Number :
Phy-Mem-Size   : 1024MB    Main-CPU      : PowerPC Processor
PCB-VER        : 110702
Cpld-VER       : V1.4      Fpga-VER      :
OtherfirewareVER:

BootROM-VER    : V4.0.0    2013-06-18 15:45:06
Software-VER   : V2.0.0    2013-07-03 01:18:47
Cpu-Usage      : 28%
Mem-Usage      : 28%
Uptime         : 0 Days, 0 Hours, 2 Minutes, 7 Seconds
```

– End of Steps –

1.3.7 Delete 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 a 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#show subcard
Rack Shelf Slot Subcard CfgType RealType Port  HardVer SoftVer      Status
-------------------------------------------------------------------------------
1    1     3    1       UCDC/3  UCDC/3   3     N/A.    N/A.         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
Confirm to delete 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    GTGO    GTGOG    8     120301  V2.0.0          INSERVICE
1    1     3    SMXA    SMXA     0     110702  V2.0.0          INSERVICE
1    1     4    SMXA    SMXA     0     110702  V2.0.0          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 **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
  - → 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 25 36 50 75
```

3. Configure the high-temperature threshold.

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

4. (Optional) Query the fan configuration.

```
ZXAN(config)#show fan
Shelf                         : 1
epm                           : disable
FanControlType                : temperature-control
TemperatureThreshold          : 30  40  50  60 (deg c)
FanSpeedLevelPercent          : 25%  36%  50%  75%
HighTemperatureThreshold      : 70 (deg c)
Environment Temperature       : 61 (deg c)
HighTemperatureProtection     : Threshold  : N/A.(deg c)
                                RestartTime: N/A.(Minute)
Upper Fanboard Status         : online
All fan units actual status:
-----------------------------------------------
FanUnitId     SpeedLevel     ShiftSpeed(RPM)
-----------------------------------------------
1             3              2832
2             3              2832
-----------------------------------------------
```

– End of Steps –

1.4 System Configuration

1.4.1 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 may 7 2013
```

3. (Optional) Query the system time.

```
ZXAN#show clock
08:01:55  Mon  May 7  2013  utc
```

– End of Steps –

1.4.2 Configuring the Version Auto-Update Function

The ZXA10 C320 supports the periodic version auto-update function, that is, the ZXA10 C320 checks the consistency between the version files with the version files on the file server and updates the version files according the auto–update policy whenever there is an inconsistency.

Configuration Data

Table 1-5 lists the configuration data of auto-update function.

Table 1-5 Configuration Data of Auto-Update Function

Item	Data
File server	● IP address: 10.1.1.1 ● User name: zte ● Password: zte
Auto-update check period	● Starting time: 15:00:00, March 5, 2013 ● Interval: 24 hour
Auto-update policy	● Version backup: enable ● Version activate: enable

Steps

1. In global configuration mode, configure the version file server.

```
ZXAN(config)#file-server auto-update server-index 1 ftp ipaddress 10.1.1.1 user
zte password zte
```

2. Configure the starting time and interval of the version auto-update check period.

```
ZXAN(config)#auto-update check-period 15:00:00 mar 5 2013 interval 24
```

3. Enable the auto-backup function and card-version-update function in the auto-update process.

```
ZXAN(config)#auto-update backup enable
ZXAN(config)#auto-update activate enable
```

4. (Optional) Query the file server configuration.

```
ZXAN(config)#show file-server auto-update
ServerIndex : 1
ProtocolType: Ftp                     Server-IpAddr: 10.1.1.1
Username    : zte
Password    : ********
Path        :

ServerIndex : 2
Not configuration
```

5. (Optional) Query the auto-update check-period configuration.

```
ZXAN(config)#show auto-update check-period configure
Enable      Start-time                  Interval(hours)
-----------------------------------------------
enable      2013-03-05 15:00:00         24
```

6. (Optional) Query the auto-update configuration.

```
ZXAN#show auto-update configure
Backup          Active
--------------------------
enable           enable
```

– End of Steps –

1.4.3 Configuring the Auto-Backup Function

The ZXA10 C320 supports conditional auto-backup for configuration file, log file, and version files.

Configuration Data

Table 1-6 lists the configuration data of auto-backup function.

Table 1-6 Configuration Data of Auto-Backup Function

Item	Data
File server	● File type: all ● IP address: 10.1.1.1 ● Path: bak ● User name: zte ● Password: zte

Item	Data
Auto-backup condition	● Configuration changed: enable ● Hold-off time: 1 hour ● Maximum hold-off time: 2 hour

Steps

1. In global configuration mode, configure the backup file server.

```
ZXAN(config)#file-server auto-backup all server-index 1 ftp ipaddress 10.1.1.1
path bak user zte password zte
```

2. Configure the condition and interval of the version auto-backup check point.

```
ZXAN(config)#auto-backup condition cfg-changed hold-off-time 1 max-hold-off-time 2
```

3. Query the file server configuration.

```
ZZXAN(config)#show file-server auto-backup
FileType    : Cfg
ServerIndex : 1
ProtocolType: Ftp                       Server-IpAddr: 10.1.1.1
Username    : zte
Password    : ********
Path        : bak

FileType    : Cfg
ServerIndex : 2
Not configuration

FileType    : Log
ServerIndex : 1
ProtocolType: Ftp                       Server-IpAddr: 10.1.1.1
Username    : zte
Password    : ********
Path        : bak

FileType    : Log
ServerIndex : 2
Not configuration

FileType    : Img
ServerIndex : 1
ProtocolType: Ftp                       Server-IpAddr: 10.1.1.1
Username    : zte
Password    : ********
Path        : bak

FileType    : Img
```

```
ServerIndex : 2
Not configuration
```

4. (Optional) Query the auto-backup condition configuration.

```
ZXAN(config)#show auto-backup condition configure
Cfg-changed         Hold-off-time(hours)    Max-hold-off-time(hours)
-------------------------------------------------------
enable              1                       2
```

– End of Steps –

1.4.4 Configuring the Auto-Save Function

The ZXA10 C320 supports saving configuration automatically.

Steps

1. In global configuration mode, enable the auto-save function.

```
ZXAN(config)#auto-write enable
```

2. Configure the time for auto-save operation.

```
ZXAN(config)#auto-write 02:00:00 may 5 2013
```

3. (Optional) Query the auto-save configuration.

```
ZXAN(config)#show auto-write

auto-write global configuration:
-------------------------------------------------
auto-write enable
auto-write 02:00:00 May 5  2013
```

– 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 1-7 describes user privileges.

Table 1-7 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.

Privilege Level	Description
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

Table 1-8 describes user properties.

Table 1-8 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	8–32 characters, should contain characters from at l east three categories: lower-case, capitals, digits or special characters.
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 ZTEzte123, and the privilege is 1.

Steps

1. Add a user.

```
ZXAN(config)#username abc password Abc12345 privilege 10
```

2. (Optional) Query the user configuration.

```
ZXAN(config)#show username
cli user global configuration
------------------------------------------------------------------------

name     sessions  pri  OperStatus  login-begin  login-end  expire-date
------------------------------------------------------------------------
zte           16     1   Normal     00:00:00    23:59:59    2099-12-31 23:59:59
```

```
admin          16     1   Normal     00:00:00    23:59:59    2099-12-31 23:59:59
123            16     1   Normal     00:00:00    23:59:59    2099-12-31 23:59:59
abc            16    10   Normal     00:00:00    23:59:59    2099-12-31 23:59:59
```

– 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 Abcabc123 privilege 15
```

2. (Optional) Query the user configuration.

```
ZXAN(config)#show username
cli user global configuration
------------------------------------------------------------------------

name     sessions  pri  OperStatus  login-begin  login-end  expire-date
------------------------------------------------------------------------
zte            16     1   Normal     00:00:00    23:59:59    2099-12-31 23:59:59
admin          16     1   Normal     00:00:00    23:59:59    2099-12-31 23:59:59
123            16     1   Normal     00:00:00    23:59:59    2099-12-31 23:59:59
abc            16    15   Normal     00:00:00    23:59:59    2099-12-31 23:59:59
```

– 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
cli user global configuration
```

```
------------------------------------------------------------------------

name     sessions  pri  OperStatus  login-begin  login-end  expire-date
------------------------------------------------------------------------
zte           16     1   Normal     00:00:00    23:59:59    2099-12-31 23:59:59
admin         16     1   Normal     00:00:00    23:59:59    2099-12-31 23:59:59
123           16     1   Normal     00:00:00    23:59:59    2099-12-31 23:59:59
```

– 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         Host(s)              Idle        Location
   66 vty 0  zte          idle                 00:50:48    10.63.192.213
   67 vty 1  zte          idle                 00:13:27    10.63.78.129
 * 69 vty 3  abc          idle                 00:00:00    10.60.113.35
```

2. Query the TCP connections.

```
ZXAN#show tcp brief
TCB            Local Address            Foreign Address          State
410088992      10.63.192.225.23         10.60.113.35.2053        ESTAB
417166736      10.63.192.225.23         10.63.78.129.1617        ESTAB
410187888      10.63.192.225.23         10.63.192.213.3641       ESTAB
```

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

     ```
     ZXAN#clear tcp line 69
     ```

   - Disconnect the online user by IP address.

     ```
     ZXAN#clear tcp connect 10.63.192.225 23 10.63.192.213 3641
     ```

– End of Steps –

This page intentionally left blank.

Chapter 2
GPON Service Configuration

The Gigabit Passive Optical Network (GPON) access are a flexible access technologies that provide 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

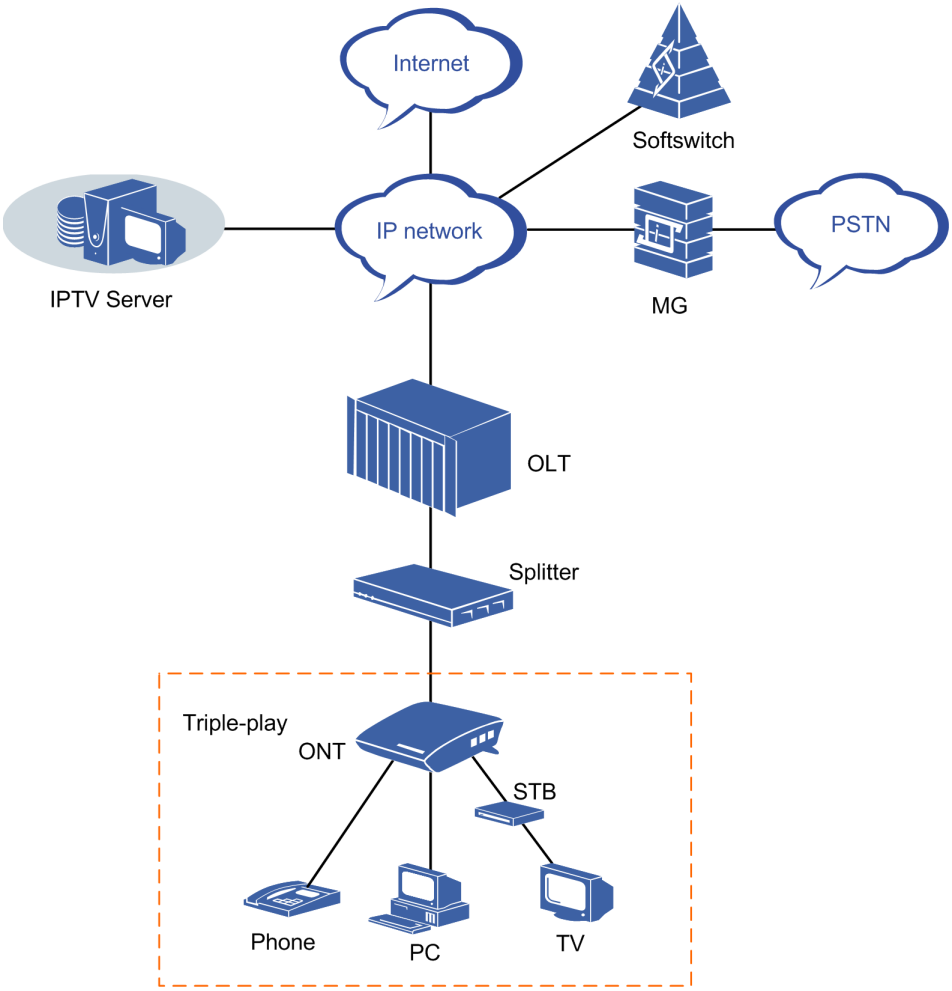


Table of Contents

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

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, you can 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	4ETH,2POTS
Maximum T-CONT	7
Maximum number of GEM ports	32
Maximum number of switch units per slot	1
Maximum number of flows per switch unit	8

Item	Data
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 4ETH,2POTS max-tcont 7
max-gemport 32 max-switch-perslot 1 max-flow-perswitch 8
```

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:          ZTE-F620
PON type:               gpon
Description:            4ETH, 4POTS
Max T-CONT:             7
Max GEM port:           32
Max switch per slot:    1
Max flow per switch:    8
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 initially.

Prerequisite

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

Context

The ZXA10 C320 supports the following ONU authentication modes:

- SN authentication

  Using the ONU SN for authentication

- Password authentication

  Using the ONU password for authentication

- SN + password authentication

  Using the ONU SN and password for authentication

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.
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

Item	Data
T-CONT bandwidth profile 3	Profile name: 10M Bandwidth type: type 3 Assured bandwidth: 5000 kbps Maximum bandwidth: 10000 kbps
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 gateway 1.2.3.1
```

2. (Optional) Query the ONU IP profile.

```
ZXAN(config-gpon)#show gpon onu profile ip
Profile name:  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 pri 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

Item	Data
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

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.

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

2. Configure the digit-map of the dial plan.

```
ZXAN(config-gpon)#onu profile dial-plan test digit-map X*.X.#|#X.*.X.##
```

3. (Optional) Query the dial plan configuration.

```
ZXAN(config-gpon)#show gpon onu profile dial-plan test
Profile name:    test
Critical timeout:4000
Partial timeout: 16000
Format:          H.248
Digit map:       X*.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 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.

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.

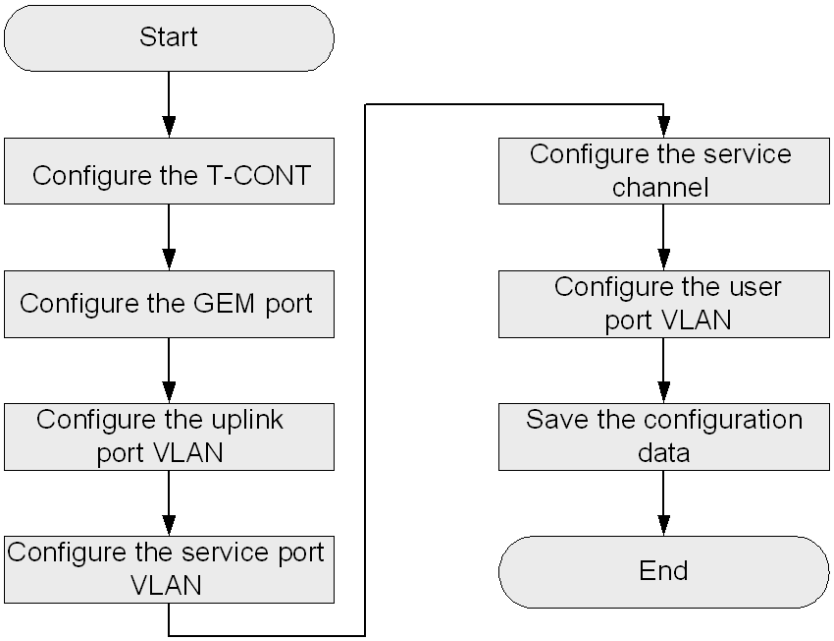
Table 2-12 Configuration Data of the GPON Broadband Service

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 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 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 **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 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 pri 0
ZXAN(gpon-onu-mng)#end
```

7. Save the configuration data.

```
ZXAN#write
```

– 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

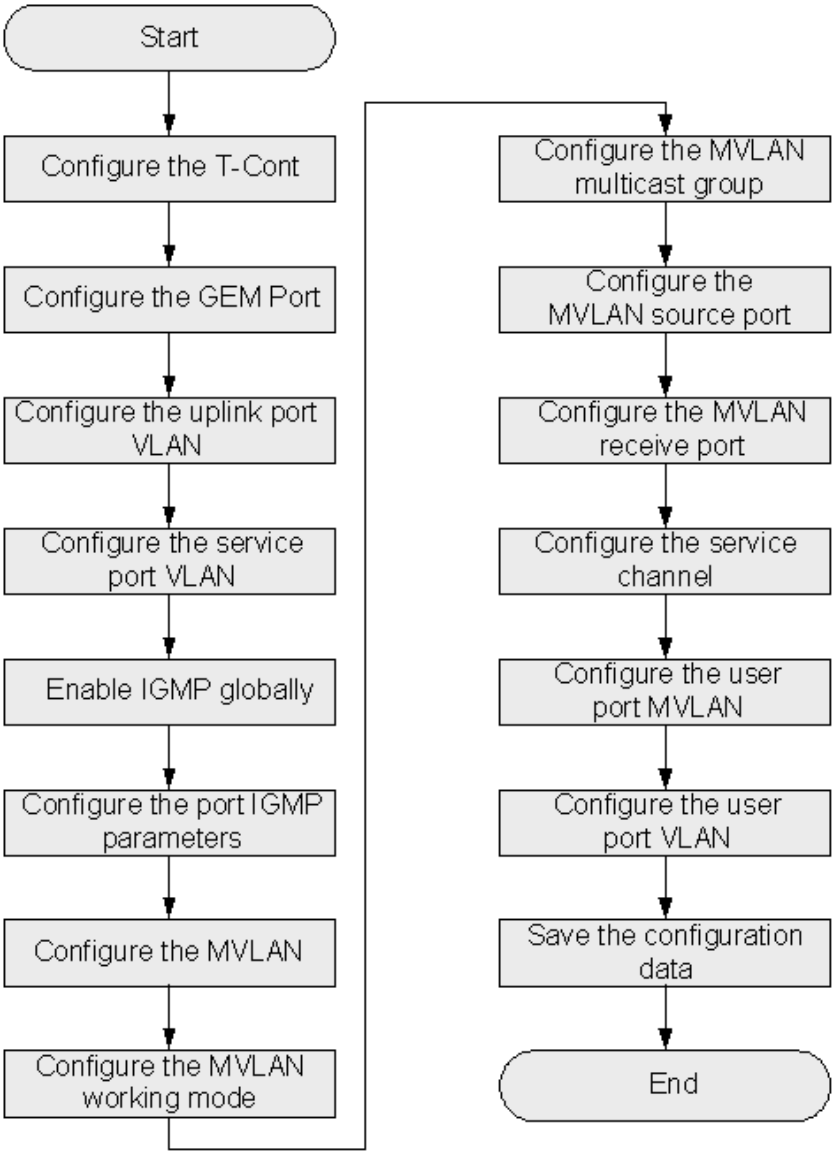
Item	Data
Multicast VLAN (MVLAN) ID	200
Service priority	5
MVLAN working mode	Proxy
MVLAN multicast group	224.1.1.1 – 224.1.1.3
Uplink port	gei_1/3/1
Service port	ONU interface: gpon-onu_1/1/1:1 Service-port ID: 2 Virtual port ID: 2
T-CONT	Index: 2 Name: T2 T-CONT bandwidth profile: 5M
GEM Port	Index: 2 Name: gemport2 T-CONT index: 2

Item	Data
Service channel	Name: mulitcast 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 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. (Optional) 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 gemport 2 cos 5 vlan 200
```

13. Configure the user port MVLAN.

```
ZXAN(gpon-onu-mng)#mvlan 200
ZXAN(gpon-onu-mng)#mvlan tag-strip eth_0/2 enable
```

14. Configure the user port VLAN.

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

15. Save the configuration data.

```
ZXAN#write
```

– 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

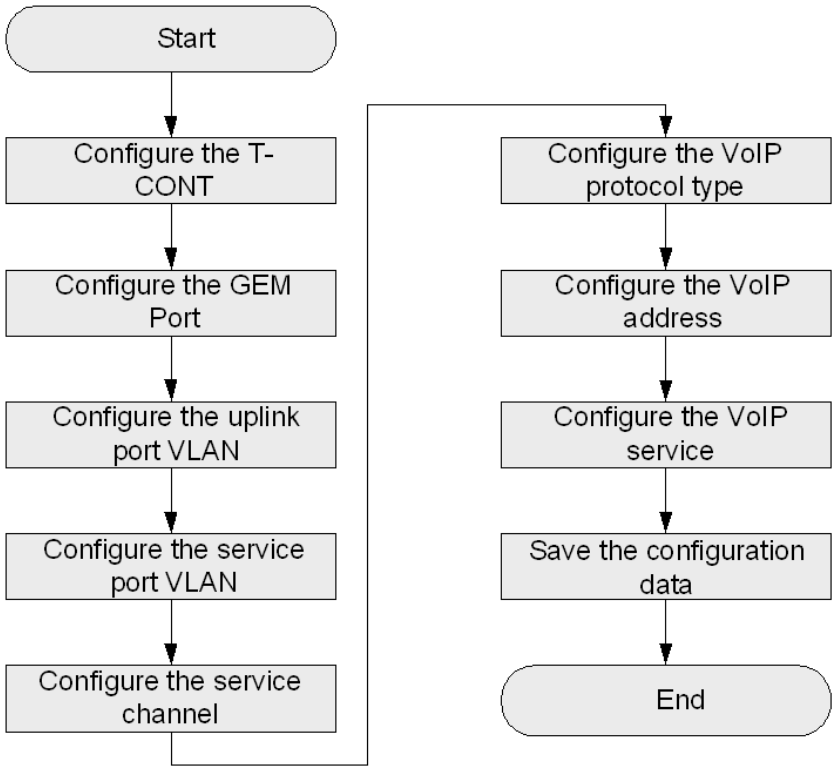
Item	Data
Service VLAN ID	300
Service priority	7
Uplink port	gei_1/3/1
Service port	ONU interface: gpon-onu_1/1/1:1 Service-port ID: 3 Virtual port ID: 3
T-CONT	Index: 3 Name: voip T-CONT bandwidth profile: 2M
GEM Port	Index: 3 Name: gemport3 T-CONT index: 3
Service channel	Name: voip-sip GEM port index: 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 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 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.

```
ZXAN#write
```

– 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.

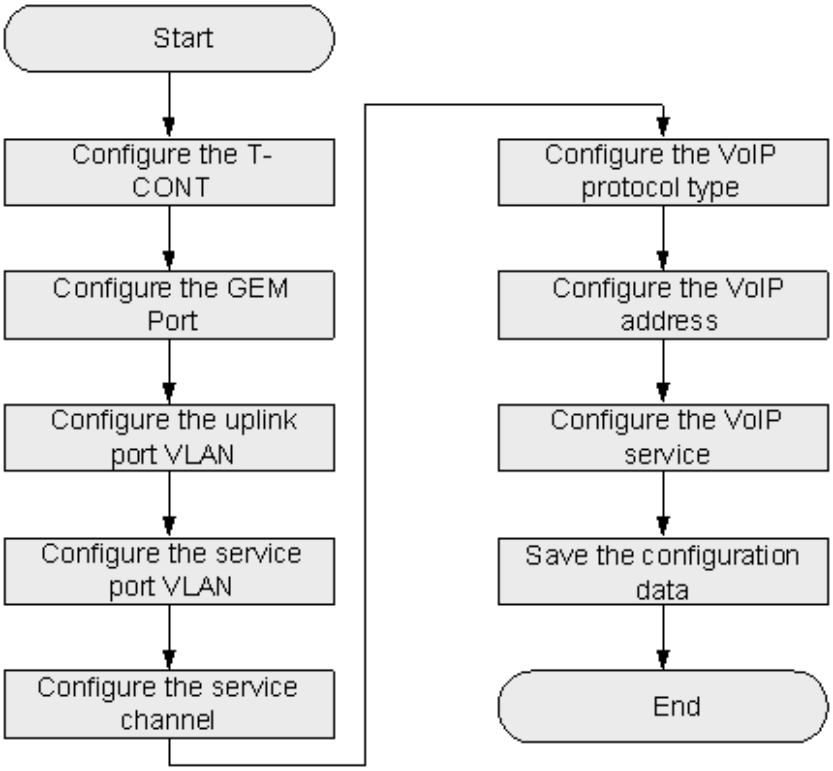
Table 2-15 Configuration Data of the GPON Voice Service

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 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 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:

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 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.

```
ZXAN#write
```

– End of Steps –

This page intentionally left blank.

Chapter 3
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

3.1 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 3-1 list the configuration data of the P2P service.

Table 3-1 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:

- DHCP (refer to Chapter 10 DHCP Configuration)
- Port identification (refer to 13.1 Port Identification Configuration)
- QoS (refer to 6.1 Ethernet Interface QoS Configuration)
- Link aggregation (refer to 11.1 Configuring Link Aggregation)

The DHCP configuration and port identification 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 4
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 4-1 lists the VLAN specifications.

Table 4-1 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.

Table of Contents

4.1 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:

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

– End of Steps –

4.2 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 gpon-onu_1/1/1:1
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 gpon-onu_1/1/1:1
Interface gpon-onu_1/1/1:1
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 –

4.3 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 global configuration mode, configure the uplink port VLAN.

```
ZXAN(config)#vlan-translate ingress-port gei_1/3/1 user-outer-vlan 5 user-inner
-vlan 3 vlan 3 svlan 5
```

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-vlan5)#xconnect enable cvlan 3
```

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

```
ZXAN(config-vlan5)#show vlan-xconnect detail
User-Port                  Uplink-Port  Svlan  Cvlan  Status
-----------------------------------------------------------
gpon-onu_1/1/1:1 vport 1   gei_1/3/1      5      3    --
```

– End of Steps –

This page intentionally left blank.

Chapter 5
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

5.1 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 5-1 lists the configuration data of the IGMP MVLAN.

Table 5-1 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
MVLAN packet processing mode	IGMPv1: drop IGMPv2: drop IGMPv3: accept
Multicast group IP address	224.1.1.1–224.1.1.3
Multicast source IP address	10.1.1.1
Multicast source port	gei_1/3/1
Multicast receive port	ONU interface: gpon-onu_1/1/1:1 Virtual port ID: 1

Steps

1. 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
```

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 200 vlan 200
ZXAN(config-if)#exit
```

3. Enable IGMP globally.

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

4. Enable IGMP span VLAN function.

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

5. Configure the MVLAN.

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

6. Configure the MVLAN packet processing mode.

```
ZXAN(config)#igmp mvlan 200 version-mode v1 drop
ZXAN(config)#igmp mvlan 200 version-mode v2 drop
ZXAN(config)#igmp mvlan 200 version-mode v3 accept
```

7. Configure the MVLAN working mode.

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

8. Configure the MVLAN host version.

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

9. Configure the MVLAN multicast group.

```
ZXAN(config)#igmp mvlan 200 group 224.1.1.1 to 224.1.1.3 source 10.1.1.1 prejoin
enable
```

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 1
```

12. (Optional) Query the IGMP global configuration.

```
ZXAN(config)#show igmp
IGMP global parameters:
---------------------------------------
IGMP is globally enable.
Span vlan is enable.
Host tracking is disable.
IGMP log is disable.
General query gemport mode is unicast.
Prejoin interval is 120(second).
```

13. (Optional) Query the MVLAN.

```
ZXAN(config)#show igmp mvlan

Total Num is 1.
VID  Status Work-mode  GroupFilter Filter-mode ActGroups HostVersion
------------------------------------------------------------------------

200  enable proxy      disable     asmssm      0         v3

ZXAN(config)#show igmp mvlan 200
Protocol packet's priority is 0 (in proxy/spr mode)
Act Port is 0.
Host ip is 192.168.2.14.
Proxy ip is 192.168.2.14.
Igmp v1 mode  is drop.
Igmp v2 mode  is drop.
Igmp v3 mode  is accept.
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 1(second).
Startup query interval is 30(second).
Startup query count is 2.
Snooping aging time is 300(second).
-------------------------------------------------------------------------------
Source Port        HostCompatibleMode   HostConfigMode   V1TimeOut   V2TimeOut
-------------------------------------------------------------------------------

gei_1/3/1            v3                   v3                0           0

Receive Port
----------------------------

gpon-onu_1/1/1:1:1


SSM Group Range
----------------------------

232.0.0.0 mask 255.0.0.0
```

– End of Steps –

5.2 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 5-2 lists the configuration data of the MLD MVLAN.

Table 5-2 Configuration Data of the MLD MVLAN

Item	Data
MLD	Enable
Span VLAN function	Enable
MVLAN ID	200
MVLAN working mode	Proxy
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: 1

Steps

1. 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
```

2. 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 200 vlan 200
ZXAN(config-if)#exit
```

3. Enable MLD globally.

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

4. Enable MLD span VLAN function.

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

5. Configure the MVLAN.

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

6. Configure the MVLAN working mode.

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

7. Configure the MVLAN host version.

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

8. Configure the MVLAN multicast group.

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

9. Configure MVLAN source port.

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

10. Configure the MVLAN receive port.

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

11. (Optional) Query the MLD global configuration.

```
ZXAN(config)#show mld
MLD global parameters:
-----------------------------------------------
MLD is globally enable.
Span vlan is disable.
Host tracking is disable.
MLD log is disable.
General query gemport mode is unicast.
Prejoin interval is 120(second).
```

12. (Optional) Query the MVLAN.

```
ZXAN(config)#show mld mvlan

Total Num is 1.
VID  Status Work-mode  GroupFilter Filter-mode ActGroups HostVersion
------------------------------------------------------------------------------

200  enable proxy      disable     asmssm      0         v1

ZXAN(config)#show mld mvlan 200
Protocol packet's priority is 0 (in proxy/spr mode)
Act Port is 0.
Host ip is fe80::c0a8:20e.
Proxy ip is fe80::c0a8:20e.
mld v1 mode  is accept.
mld v2 mode  is accept.
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 1(second).
Startup query interval is 30(second).
Startup query count is 2.
Snooping aging time is 300(second).
------------------------------------------------------------------------------
Source Port           HostCompatibleMode   HostConfigMode   V1TimeOut
```

```
------------------------------------------------------------------------------

gei_1/3/1            v1                   v1                   0

Receive Port
----------------------------

gpon-onu_1/1/1:1:1



SSM Group Range
----------------------------

FF3x:: mask fff0:ffff:ffff:ffff:ffff:ffff::
```

– End of Steps –

5.3 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 5-3 lists the configuration data of the IPTV package.

Table 5-3 Configuration Data of the IPTV Package

Item	Data
IPTV channel	Name prefix: stv Group IP address: 224.1.1.1–224.1.1.3 Source IP address: 10.1.1.1
IPTV package	Name: pkg1 Channel 0: stv001 (watch) Channel 1: stv002 (watch) Channel 2: stv003 (preview)

Steps

1. Configure the IPTV channel.

```
ZXAN(config)#iptv channel mvlan 200 group 224.1.1.1 to 224.1.1.3 source-address
10.1.1.1 prename stv
```

2. Create the IPTV package.

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

3. (Optional) Query the IPTV channel.

```
ZXAN(config)#show iptv channel
Total channel number  :3
-------------------------------------------------------------------------
ID      mvlan     group           source          name
-------------------------------------------------------------------------

0       200       224.1.1.1       10.1.1.1        STV001
1       200       224.1.1.2       10.1.1.1        STV002
2       200       224.1.1.3       10.1.1.1        STV003
```

4. Configure the channel in the IPTV package.

```
ZXAN(config)#iptv package pkg1 channel stv001 watch
ZXAN(config)#iptv package pkg1 channel stv002 watch
ZXAN(config)#iptv package pkg1 channel stv003 preview
```

5. (Optional) Query the IPTV package.

```
ZXAN(config)#show iptv package pkg1
Package name: PKG1
Total channel number: 3
-------------------------------------------------------------------------
Group            Source          Mvlan   Right    Id   Name
-------------------------------------------------------------------------

224.1.1.1        10.1.1.1        200     watch    0    STV001
224.1.1.2        10.1.1.1        200     watch    1    STV002
224.1.1.3        10.1.1.1        200     preview  2    STV003
```

– End of Steps –

5.4 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 –

This page intentionally left blank.

Chapter 6
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

6.1 Ethernet Interface QoS Configuration

6.1.1 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 –

6.1.2 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 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 –

6.1.3 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 –

6.1.4 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 –

6.1.5 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:

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-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 –

6.1.6 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 –

6.1.7 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 –

6.2 OLT Interface QoS Configuration

6.2.1 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)#show qos queue-block-profile test
-------------------------------------------------------------------
profile name    : TEST
profile detail  :
-------------------------------------------------------------------
 queue-number   :  8
 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 –

6.2.2 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
  queue-map:      2  1  2  3  4  5  6  7
----------------------------------------
profile used by:
gpon-olt_1/1/1
```

– End of Steps –

6.2.3 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
```

– End of Steps –

6.3 ONU Interface QoS Configuration

6.3.1 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 –

6.3.2 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 –

6.3.3 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 –

6.3.4 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 –

6.3.5 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 –

6.3.6 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 –

6.3.7 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 –

6.3.8 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 –

6.3.9 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-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 –

6.3.10 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 –

6.3.11 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
gpon-onu_1/1/1:1:1
```

– End of Steps –

Chapter 7
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.

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

7.1 Configuring a Standard ACL

This section describes how to configure a standard ACL and apply it to an Ethernet interface.

Configuration Data

Table 7-1 lists the configuration data of the standard ACL.

Table 7-1 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:

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 –

7.2 Configuring an Extended ACL

This section describes how to configure an extended ACL and apply it to an Ethernet interface.

Configuration Data

Table 7-2 lists the configuration data of the extended ACL.

Table 7-2 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 –

7.3 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 7-3 lists the configuration data of the layer-2 ACL.

Table 7-3 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 –

7.4 Configuring a Hybrid ACL

This section describes how to configure a hybrid ACL and apply it to an Ethernet interface.

Configuration Data

Table 7-4 lists the configuration data of the hybrid ACL.

Table 7-4 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 –

7.5 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 7-5 lists the configuration data of the IPv6 hybrid ACL.

Table 7-5 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 8
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

8.1 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 priority 1
```

3. Configure the source IP address of NTP packets for the time synchronization request.

```
ZXAN(config)#ntp source mng1
```

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 5
```

6. (Optional) Query the NTP running status.

```
ZXAN(config)#show ntp status
Clock is unsynchronized , stratum 16, no reference clock
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**16
reference time is 0.0 (0)
clock offset is 0.00 msec, root delay is 0.00  msec
root dispersion is 0.00  msec, peer dispersion is 0.00 msec
server in use is 0:1.2.1.1
```

– End of Steps –

This page intentionally left blank.

Chapter 9
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 IEEE 802.1d 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 IEEE 802.1w 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 IEEE 802.1s 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

9.1 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 10
DHCP Configuration

DHCP

DHCP enables a host on the network to obtain an IP address that ensures its proper communication and the relevant configuration information from a DHCP server.

IPv6 DHCP

Dynamic Host Configuration Protocol for IPv6 (IPv6 DHCP) assigns address parameters to hosts, which include IPv6 prefix, IPv6 addresses, and other network configuration parameters.

DHCP Applications

The ZXA10 C320 supports the following DHCP applications:

- DHCP snooping (including IPv6 DHCP snooping)

  The ZXA10 C320 snoops on the DHCP communication process of the specified ONU in the specified VLAN to record the user IP/MAC relationship of the specified ONU.

  Through DHCP snooping, the administrator can implement IP source-guard according to the IP/MAC binding table.

- DHCP server

  The ZXA10 C320 works as a DHCP server to allocate IP addresses for users.

- DHCP client (including IPv6 DHCP client)

  The ZXA10 C320 works as a DHCP client. It requires an IP address from the specified DHCP server, so that users can access it through SNMP.

Table of Contents

10.1 Configuring DHCP Snooping

After you configure 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 10-1 lists the configuration data of an DHCP snooping.

Table 10-1 Configuration Data of DHCP Snooping

Item	Data
Global DHCP	● Status: enable ● Option 82: enable
DHCP VLAN ID	200
Uplink interface:	gei_1/3/1
Service interface	gpon-onu_1/1/1:1 (virtual port 1)

Steps

1. In Ethernet 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
```

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

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

3. Enable DHCP snooping on the VLAN.

```
ZXAN(config)#ip dhcp snooping vlan 200
```

4. Enable the global DHCP Option 82 processing.

```
ZXAN(config)#dhcpv4-l2-relay-agent vlan 200 enable
```

5. (Optional) Query the DHCP snooping VLAN configuration.

```
ZXAN(config)#show ip dhcp snooping vlan
DHCP snooping state on vlans
Vlan     State
------------------------------
200      enable
```

– End of Steps –

10.2 Configuring DHCP Server

After you configure the DHCP server function, the ZXA10 C320 can work as a DHCP server to allocate IP addresses to subscribers.

Configuration Data

Table 10-2 lists the configuration data of the DHCP server.

Table 10-2 Configuration Data of DHCP Server

Item	Data
Global DHCP status	enable
IP address pool	• Name: ippool1 • Range: 10.10.1.3–10.10.1.254
DHCP IP address pool	• Name: dhcppool1 • IP pool: ippool1 • DNS IP address: 10.10.1.2 • IP address lease period: infinite • Default route: 10.10.1.254
DHCP policy	• Name: dhcppy • Priority: 1 • DHCP IP address pool: dhcppool1
DHCP server	• IP address: 10.10.1.1 • Mode: server • Policy: dhcppy

Steps

1. Enable the global DHCP function.

```
ZXAN(config)#ip dhcp enable
```

2. Configure the IP address pool for DHCP clients.

```
ZXAN(config)#ip pool ippool1
ZXAN(config-ip-pool)#range 10.10.1.3 10.10.1.254 255.255.255.0
ZXAN(config-ip-pool)#exit
```

3. Apply the IP address pool to the DHCP IP address pool.

```
ZXAN(config)#ip dhcp pool dhcppool1
ZXAN(config-dhcp-pool)#ip-pool ippool1
```

4. Configure the lease time of the IP addresses.

```
ZXAN(config-dhcp-pool)#lease-time infinite
```

5. Configure the DHCP DNS server.

```
ZXAN(config-dhcp-pool)#dns-server 10.10.1.2
```

6. Configure the default route.

```
ZXAN(config-dhcp-pool)#default-router 10.10.1.254
ZXAN(config-dhcp-pool)#exit
```

7. Configure the DHCP policy.

```
ZXAN(config)#ip dhcp policy dhcppy 1
ZXAN(config-dhcp-policy)#dhcp-pool dhcppool1
ZXAN(config-dhcp-policy)#exit
```

8. In management interface mode, configure the DHCP mode and policy.

```
ZXAN(config)#interface mng1
ZXAN(config-if)#ip address 10.10.1.1 255.255.255.0
ZXAN(config-if)#ip dhcp mode server
ZXAN(config-if)#ip dhcp policy dhcppy
ZXAN(config-if)#exit
```

9. Configure the route.

```
ZXAN(config)#ip route mng 0.0.0.0 0.0.0.0 10.10.1.254
```

10. Query the DHCP server clients.

```
ZXAN(config)#show ip dhcp server user
Current online users are 0
Index MAC addr       IP addr         State    Expiration
```

– End of Steps –

10.3 Configuring DHCP Client

The ZXA10 C320 can work as a client to acquire an IP address from a DHCP server.

Configuration Data

Table 10-3 lists the configuration data of the DHCP client.

Table 10-3 Configuration Data of DHCP Client

Item	Data
Global DHCP	Enable
DHCP client	• VLAN ID: 100 • IP address mode: DHCP • Client ID: vlan100 • Class ID: c300 • Hostname: zxan
Uplink interface	gei_1/3/1

Steps

1. Enable the global DHCP function.

```
ZXAN(config)#ip dhcp enable
```

2. Configure the response packet type that is requested by the DHCP client.

```
ZXAN(config)#ip dhcp client broadcast-flag
```

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

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

4. Enter the VLAN interface mode, enable the DHCP client in the VLAN.

```
ZXAN(config)#interface vlan 100
ZXAN(config-if-vlan100)#ip address dhcp
```

5. Configure the DHCP client parameters in the VLAN.

```
ZXAN(config-if-vlan100)#ip dhcp client client-id vlan100
ZXAN(config-if-vlan100)#ip dhcp client class-id c300
ZXAN(config-if-vlan100)#ip dhcp client hostname zxan
ZXAN(config-if-vlan100)#end
ZXAN#
```

6. (Optional) In the administrator mode, configure the DHCP client to obtain IP address again.

```
ZXAN#renew dhcp vlan 100
```

7. (Optional) In the administrator mode, configure the DHCP client to release addresses.

```
ZXAN#release dhcp vlan 100
```

– End of Steps –

This page intentionally left blank.

Chapter 11
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

Table of Contents

11.1 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. 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-smartgroup1)#
```

2. Configure load balancing mode.

```
ZXAN(config-smartgroup1)#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 LACP mode.

```
ZXAN(config-smartgroup1)#smartgroup mode 802.3ad
```

NOTE **Note:**

The ZXA10 C320 supports two LACP modes:

- On (default): LACP static aggregation mode.
- 802.3ad: LACP dynamic negotiation mode

---

4. Configure the VLAN for the smartgroup.

```
ZXAN(config-smartgroup1)#switchport vlan 100 tag
ZXAN(config-smartgroup1)#exit
```

5. Configure the VLAN for uplink ports.

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

6. (Optional) Query VLAN properties of the smartgroup and uplink ports.

```
ZXAN(config)#show vlan port smartgroup1
PortMode      Pvid  CPvid Tpid/mode   TLSStatus TLSVlan  ProtEn   PrioEn
------------------------------------------------------------------------
hybrid>=0     1     0     0x8100/PORT disable   0        disable  disable
UntaggedVlan:
1
TaggedVlan:
100
ZXAN(config)#show vlan port gei_1/3/1
PortMode      Pvid  CPvid Tpid/mode   TLSStatus TLSVlan  ProtEn   PrioEn
------------------------------------------------------------------------
hybrid>=0     1     0     0x8100/PORT disable   0        disable  disable
UntaggedVlan:

TaggedVlan:
100
ZXAN(config)#show vlan port gei_1/3/3
PortMode      Pvid  CPvid Tpid/mode   TLSStatus TLSVlan  ProtEn   PrioEn
------------------------------------------------------------------------
hybrid>=0     1     0     0x8100/PORT disable   0        disable  disable
UntaggedVlan:

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.

7. In uplink interface configuration mode, add the port to the aggregation group and set port aggregation mode to active.

```
ZXAN(config)#interface gei_1/3/1
```

```
ZXAN(config-if)#smartgroup 1 mode active
```

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.

8. Configure the timeout mode of the port.

```
ZXAN(config-if)#lacp timeout long
```

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.

9. 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
```

10. (Optional) Query the smartgroup status.

```
ZXAN(config-if)#show lacp internal
Smartgroup:1    Switch attribute:TRUE    Mode:802.3ad
Flag *--Loop is TRUE
Actor       Agg       LACPDUs  Port     Oper    Port  RX            Mux
Port        State     Interval Priority Key     State Machine       Machine
--------------------------------------------------------------------------------
gei_1/3/1   inactive  30       32768    0x100   0x45  port-disabled defaulted
gei_1/3/3   inactive  30       32768    0x100   0x45  port-disabled defaulted
```

– End of Steps –

11.2 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_1/3/2
```

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_1/3/2 : down
```

– End of Steps –

Chapter 12
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

12.1 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 12-1 lists the PON protection configuration data.

Table 12-1 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_
1/5/2 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 13
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 identification
- MAC address anti-spoofing
- ARP anti-spoofing
- IP source guard
- Split horizon
- MFF
- ARP proxy

Table of Contents

13.1 Port Identification Configuration

The system provides the port identification mechanism to improve network security and prevent user accounts from being stolen. The system implements port identification through the following techniques:

- DHCPv4 Layer-2 Relay Agent
- PPPoE Intermediate Agent
- DHCPv6 Layer-2 Relay Agent
- NDP LIO

13.1.1 Configuring the Port Identification

Port-identification is to define the format and content of the Circuit ID (CID) and Remote ID (RID).

Context

When subscribers access the Internet in PPPoE Intermediate Agent, DHCPv4 Layer-2 Relay Agent, DHCPv6 Layer-2 Relay Agent, or NDP Line Identification Option (LIO) mode, the system uses the corresponding agent to locate port. The system sends the packets with port information to authentication servers to bind subscribers accounts and circuits.

Configuration Data

Table 13-1 lists the configuration data of port identification.

Table 13-1 Configuration Data of Port Identification

Item	Data
Port-Identification global	● Master identifier type: access-node-name ● Access node name: ZXA10–C300 ● Slave identifier: ZTE
Port-Identification interface	● Interface: gpon-onu_1/1/1:1 ● Virtual port: 1 ● Remote ID status: enable ● Remote ID name: REMOTE-ID

Steps

1. Configure access node master identifier type.

```
ZXAN(config)#port-identification access-node-id-type access-node-name
```

2. Configure the access node name.

```
ZXAN(config)#port-identification access-node-name ZXA10-C300
```

3. Configure the access node slave identifier.

```
ZXAN(config)#port-identification access-node-slave-id ZTE
```

4. Enter GPON-ONU interface mode, and configure the remote ID field.

```
ZXAN(config)#interface gpon-onu_1/1/1:1
ZXAN(config-if)#port-identification sub-option remote-id enable vport 1
ZXAN(config-if)#port-identification sub-option remote-id name REMOTE-ID vport 1
ZXAN(config-if)#exit
```

5. (Optional) Query the global configuration of port identification.

```
ZXAN(config)#show port-identification global
access-node-name      : ZXA10-C300
access-node-id-type   : access-node-name
access-node-slave-id  : ZTE
rackno    : 1
shelfno   : 1
```

6. (Optional) Query the interface configuration of port identification.

```
ZXAN(config)#show port-identification port gpon-onu_1/1/1:1 vport 1
```

```
Port              : gpon-onu_1/1/1:1  vport 1
Cid-Format        : CHINA-TELECOM-PON
Rid-status        : Enable
Rid-name          : REMOTE-ID
Rid-Format        :
Access-Loop-Tag   : REMOTE-ID
```

– End of Steps –

13.1.2 Configuring the DHCPv4 Layer-2 Relay Agent (DHCPv4L2RA)

When DHCPv4L2RA is enabled, the ZXA10 C320 adds DHCPv4L2RA Option 82 field to the upstream DHCP packets.

Context

The DHCPv4L2RA Option 82 field contains CID and RID, which includes the shelf number, slot number, and port number.

- Only when DHCPv4L2RA is enabled, the Option 82 field can be added/stripped to/from the DHCP packets.
- When DHCPv4L2RA is disabled, the ZXA10 C320 transparently transmits or directly forwards the DHCP packets without any processing.

The global DHCPv4L2RA function and VLAN DHCPv4L2RA function are mutually exclusive.

Configuration Data

Table 13-2 lists the configuration data of the DHCPv4L2RA.

Table 13-2 Configuration Data of DHCPv4L2RA

Item	Data
DHCPv4L2RA global	Enable
DHCPv4L2RA interface	• Interface: gpon-onu_1/1/1:1 • Virtual port: 1 • DHCPv4L2RA status: enable • Policy: trust and replace

Steps

1. Enable the global DHCPv4L2RA.

```
ZXAN(config)#dhcpv4-l2-relay-agent enable
```

2. In GPON-ONU interface mode, enable DHCPv4L2RA on the interface.

```
ZXAN(config)#interface gpon-onu_1/1/1:1
ZXAN(config-if)#dhcpv4-l2-relay-agent enable vport 1
```

3. Configure the DHCPv4L2RA policy on the interface.

```
ZXAN(config-if)#dhcpv4-l2-relay-agent trust true replace vport 1
```

4. (Optional) Query either the global DHCPv4L2RA status or DHCPv4L2RA status on vlan.

```
ZXAN(config)#show dhcpv4-l2-relay-agent global
dhcpv4-l2-relay-agent status : enable
```

5. (Optional) Query the interface DHCPv4L2RA configuration.

```
ZXAN(config)#show dhcpv4-l2-relay-agent port gpon-onu_1/1/1:1 vport 1
Onu                 Vport  dhcpv4-l2-relay-agent status   Trust    Policy
gpon-onu_1/1/1:1    1      enable                         true     replace
```

– End of Steps –

Result

When the subscriber sends DHCP protocol packets, the system adds the following fields to the packets:

```
Circuit-id:  ZXA10-C300/ZTE eth 5/1/1/0/1:10
Remote-id :  REMOTE-ID
//where, 10 is the original user VLAN.
```

13.1.3 Configuring the PPPoE Intermediate Agent (PPPoE-IA)

When PPPoE-IA is enabled, the ZXA10 C320 adds port information to the upstream PPPoE-IA packets.

Context

When users access the Internet in PPPoE mode, the ZXA10 C320 uses PPPoE-IA to locate port. The system carries the user information in the PPPoE-IA discovery packets to report to the BRAS for user authentication, and thus binding the user account and circuit.

The global PPPoE-IA function and VLAN PPPoE-IA function are mutually exclusive.

Configuration Data

Table 13-3 lists the configuration data of PPPoE-IA.

Table 13-3 Configuration Data of PPPoE-IA

Item	Data
PPPoE-IA global	Enable
PPPoE-IA interface	● Interface: gpon-onu_1/1/1:1 ● Virtual port: 1 ● PPPoE-IA status: enable ● Policy: trust and replace

Steps

1. Enable the global PPPoE-IA.

```
ZXAN(config)#pppoe-intermediate-agent enable
```

2. In GPON-ONU interface mode, enable PPPoE-IA on the interface.

```
ZXAN(config)#interface gpon-onu_1/1/1:1
ZXAN(config-if)#pppoe-intermediate-agent enable vport 1
```

3. Configure the PPPoE-IA policy on the interface.

```
ZXAN(config-if)#pppoe-intermediate-agent trust true replace vport 1
```

4. (Optional) Query either the global DHCPv4L2RA status or DHCPv4L2RA status on VLAN.

```
ZXAN(config)#show pppoe-intermediate-agent global
pppoe-intermediate-agent status : enable
```

5. (Optional) Query the interface PPPoE-IA configuration.

```
ZXAN(config)#show pppoe-intermediate-agent port gpon-onu_1/1/1:1 vport 1
Onu                 Vport       Pppoe-intermediate-agent status   Trust    Policy
gpon-onu_1/1/1:1    1           enable                            true     replace
```

– End of Steps –

Result

When the subscriber sends PPPoE protocol packets, the system adds the following fields to the packets:

```
Circuit-id:  ZXA10-C300/ZTE eth 5/1/1/0/1:10
Remote-id :  REMOTE-ID
//where, 10 is original user VLAN.
```

13.1.4 Configuring the DHCPv6 Layer-2 Relay Agent (DHCPv6L2RA)

When DHCPv6L2RA is enabled, the ZXA10 C320 adds DHCPv6L2RA Option 18 and Option 37 fields to the upstream DHCP packets.

Context

The option 18 field includes CID , and the option 37 field includes RID, which provides the physical information such as the shelf number, slot number, and port number.

- Only when DHCPv6L2RA is enabled, the option 18 field and option 37 field can be added/stripped to/from DHCPv6 packets. For option 37, the remote ID status should be enabled and remote ID name should be configured in addition.
- When DHCPv6L2RA is disabled, the system transparently transmits or directly forwards DHCPv6 packets without any processing.

The global DHCPv6L2RA function and VLAN DHCPv6L2RA function are mutually exclusive.

Configuration Data

Table 13-4 lists the configuration data of DHCPv6L2RA.

Table 13-4 Configuration Data of DHCPv6L2RA

Item	Data
DHCPv6L2RA VLAN	● VLAN: 100 ● Status: enable
DHCPv6L2RA interface	● Interface: gpon-onu_1/1/1:1 ● Virtual port: 1 ● DHCPv6L2RA status: enable

Steps

1. Enable DHCPv6L2RA on VLAN.

```
ZXAN(config)#dhcpv6-l2-relay-agent vlan 100 enable
//VLAN 100 is the service vlan after vlan-translation.
```

2. In GPON-ONU interface mode, configure DHCPv6L2RA on the virtual port.

```
ZXAN(config)#interface gpon-onu_1/1/1:1
ZXAN(config-if)#dhcpv6-l2-relay-agent enable vport 1
ZXAN(config-if)#exit
```

3. (Optional) Query either the global DHCPv6L2RA status or DHCPv6L2RA status on VLAN (mutually exclusive).

```
ZXAN(config)#show dhcpv6-l2-relay-agent vlan all
vlan total  : 1
vlan list   : 100
```

4. (Optional) Query the interface configuration of DHCPv6L2RA.

```
ZXAN(config)#show dhcpv6-l2-relay-agent port gpon-onu_1/1/1:1 vport 1
Port               Pvc dhcpv6-l2-relay-agent status   Trust    Policy
gpon-onu_1/1/1:1   1   enable                         false    add
```

– End of Steps –

Result

When the subscriber sends DHCPv6 protocol packets, the system adds the following fields to the packets:

```
Option 18:  ZXA10-C300/ZTE eth 5/1/1/0/1:10
Option 37:  REMOTE-ID
//where, 10 is original user VLAN.
```

13.1.5 Configuring the NDP Line Identification Option (NDP-LIO)

When NDP-LIO is enabled, the ZXA10 C320 adds LIO field to the upstream NDP packets.

Context

The LIO field includes CID, and provides the information such as the shelf number, slot number, and port number.

- Only when NDP-LIO is enabled, the LIO field can be added/stripped to/from the NDP packets.
- When NDP-LIO is disabled, the system transparently transmits or directly forwards the NDP packets without any processing.

The global NDP-LIO function and VLAN NDP-LIO function are mutually exclusive.

Configuration Data

Table 13-5 lists the configuration data of NDP-LIO.

Table 13-5 Configuration Data of NDP-LIO

Item	Data
NDP-LIO VLAN	• VLAN: 100 • Status: enable
NDP-LIO interface	• Interface: gpon-onu_1/1/1:1 • Virtual port: 1 • NDP-LIO status: enable • Policy: trust and replace

Steps

1. Enable NDP-LIO on VLAN.

```
ZXAN(config)#ndp-lio vlan 100 enable
//VLAN 100 is the service vlan after vlan-translation.
```

2. In GPON-ONU interface mode, configure NDP-LIO on the virtual port.

```
ZXAN(config)#interface gpon-onu_1/1/1:1
ZXAN(config-if)#ndp-lio enable vport 1
ZXAN(config-if)#ndp-lio trust true replace vport 1
ZXAN(config-if)#exit
```

3. (Optional) Query either the global NDP-LIO status or NDP-LIO status on vlan.

```
ZXAN(config)#show ndp-lio vlan all
vlan total  : 1
vlan list   : 100
```

4. (Optional) Query the interface configuration of NDP-LIO.

```
ZXAN(config)#show ndp-lio port gpon-onu_1/1/1:1 vport 1
Onu                Vport          ndp-lio status      Trust    Policy
gpon-onu_1/1/1:1   1              enable              true     replace
```

– End of Steps –

Result

When the subscriber sends NDP protocol packets, the system adds the following LIO field to the packets:

```
Circuit-id: ZXA10-C300/ZTE eth 5/1/1/0/1:10
//where, 10 is original user VLAN.
```

13.2 MAC Address Anti-Spoofing Configuration

The ZXA10 C320 supports the MAC address anti-spoofing function to prevent malicious MAC address spoofing, which affects the network security.

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.

13.2.1 Configuring the User Port MAC Address Anti-Spoofing

User-port MAC address anti-spoofing prevents malicious MAC address spoofing between user ports.

Context

The user-port MAC address anti-spoofing has the following features:

- When one MAC address is learnt by one user port, the address cannot be learnt by other user ports.
- Once there is a MAC move event at the first time, the system will generate a notification including the MAC address, VLAN, move-to-port and move-from-port.
- The notification report interval of the same MAC move events can be configured.

Steps

1. Enable global MAC address anti-spoofing function.

   ```
   ZXAN(config)#security mac-anti-spoofing enable
   ```

2. Enable MAC move notification control.

   ```
   ZXAN(config)#security mac-move-report enable
   ```

3. (Optional) Configure the notification report interval of the same MAC move log.

   ```
   ZXAN(config)#security mac-move-report interval 30
   ```

4. (Optional) Query the configuration of MAC address anti-spoofing.

```
ZXAN(config)#show security mac-anti-spoofing configuration
mac-move-report :enable
mac-move-report interval:30[minutes]
mac-anti-spoofing :enable
uplink-protect    :disable
```

5. (Optional) Query the MAC move log.

```
ZXAN#show security mac-move-log
Flag *--macMove is forbidden by system.
the total mac-move-log num:2
--------------------------------------------------------------------------
mac-address   vlan  cfgMacProtect  moveToPort     moveToIfId    moveCount
index trapFlag detector queryPort   moveFromPort  moveFromIfId trapCount
--------------------------------------------------------------------------
0002.0304.0506 100  UNNEED  inner-port_1/2/1     unknown(0)           1

 1   SENDED    MP   UNNEED  inner-port_1/3/1     unknown(0)           1

--------------------------------------------------------------------------
0002.0304.0507 100  UNNEED  inner-port_1/2/2     unknown(0)           1

 2   *SENDED   MP   UNNEED  inner-port_1/3/1     unknown(0)           1
```

– End of Steps –

13.2.2 Configuring the Service Gateway MAC Anti-Spoofing

Service gateway MAC address anti-spoofing prevents malicious MAC address spoofing between user ports and permits MAC address learning between uplink ports.

Context

The ZXA10 C320 supports the following features by service gateway MAC anti-spoofing:

- A MAC address learnt by a user port can be learnt by an uplink port as well.
- The same MAC address cannot be learnt by two user ports.
- The same MAC address can be learnt by multiple uplink ports.

Steps

1. Enable global MAC address anti-spoofing function.

```
ZXAN(config)#security mac-anti-spoofing enable
```

2. Enable MAC address anti-spoofing function with uplink protection.

```
ZXAN(config)#security mac-anti-spoofing uplink-protect enable
```

3. (Optional) Query the configuration of MAC address anti-spoofing.

```
ZXAN(config)#show security mac-anti-spoofing configuration
```

```
mac-move-report :enable
mac-move-report interval:30[minutes]
mac-anti-spoofing :enable
uplink-protect    :enable
```

4. (Optional) Query the MAC move log.

```
ZXAN#show security mac-move-log
Flag *--macMove is forbidden by system.
the total mac-move-log num:2
--------------------------------------------------------------------------
mac-address    vlan  cfgMacProtect  moveToPort     moveToIfId    moveCount
index trapFlag detector queryPort   moveFromPort  moveFromIfId trapCount
--------------------------------------------------------------------------
0002.0304.0506 100   UNNEED  inner-port_1/2/1     unknown(0)           1

 1    SENDED    MP    UNNEED  inner-port_1/3/1     unknown(0)           1

--------------------------------------------------------------------------
0002.0304.0507 100   UNNEED  inner-port_1/2/2     unknown(0)           1

 2    *SENDED   MP    UNNEED  inner-port_1/3/1     unknown(0)           1
```

– End of Steps –

13.3 Configuring the ARP Anti-Spoofing

The ARP anti-spoofing prevents the ARP spoofing on user side.

Context

The ZXA10 C320 supports user-side ARP anti-spoofing function, which is implemented based on the following ARP entries:

- The ARP entries inserted by the DHCP module
- The ARP entries of DHCP snooping static binding item configured by the IP source Guard module

ARP anti-spoofing function is based on both VLAN and service port. Only when the ARP anti-spoofing functions on both VLAN and service port are enabled, the system can implement ARP anti-spoofing on ARP packets with the specific VLAN tag.

When receiving an ARP packet, the ZXA10 C320 compares the packet with the known ARP entries. If the source IP address of the received ARP packet 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.

The ARP anti-spoofing function can be configured with up to 256 VLANs.

Configuration Data

Table 13-6 lists the configuration data of the ARP anti-spoofing.

Table 13-6 Configuration Data of ARP Anti-Spoofing

Item	Data
ARP anti-spoofing status	Enable
VLAN ID	200
Direction	User port

Steps

1. Enable the global ARP anti-spoofing function.

```
ZXAN(config)#ip-service arp-anti-spoofing enable
```

2. Configure the ARP anti-spoofing function on the VLAN.

```
ZXAN(config)#ip-service arp-anti-spoofing vlan 200 direction user-port
```

3. (Optional) Query the configuration of ARP anti-spoofing.

```
ZXAN(config)#show ip-service arp-anti-spoofing
Arp Anti-Spoofing status: Enabled
vlan       direction
 200       user-port
```

– End of Steps –

13.4 Configuring the Split Horizon

When user communication control is enabled, only subscribers in the specific VLAN and SVLAN can communicate with each other.

Context

The ZXA10 C320 supports the following split horizon features:

- Subscriber separation/intercommunication
- Subscriber intercommunication based on SVLAN and CVLAN

Steps

1. Enable the user communication control function.

```
ZXAN(config)#security user-communication control enable
```

2. Configure the intercommunication VLANs.

```
ZXAN(config)#security user-communication svlan 300 cvlan 200
```

3. (Optional) Query the configuration of intercommunication VLANs.

```
ZXAN(config)#show security user-communication
usercommunication item:
```

```
Svlan    Cvlan
-------------
300      200
```

– End of Steps –

13.5 Configuring the IP Source Guard

The IP source guard based on the service port prevents illegal users from accessing the Internet.

Context

IP source guard supports IP/MAC anti-spoofing and access security management based on the service port.

The ZXA10 C320 supports IP source guard on both IPv4 and IPv6.

- The legal IPv4 subscribers are managed through either the DHCP snooping table or static IP addresses.
- The legal IPv6 subscribers are managed through either the NDP snooping/DHCPv6 snooping, or static IP addresses.

Configuration Data

Table 13-7 lists the configuration data of the IP source guard.

Table 13-7 Configuration Data of IP Source Guard

Item	Data
Global IP source guard	Enable
Interface IP source guard	● Interface: gpon-onu_1/1/1:2 (virtual port 1) ● Service port: 1 ● IP source guard: enable
Maximum IP address number	● IPv4: 2 ● IPv6: 4
IPv4 DHCP snooping static binding	IP address: 1.1.1.1
IPv6 DHCP snooping static binding	● IPv6 address: 2001::ff01 ● IPv6-mask: 128 ● MAC address: 2365.1498.2369

Steps

1. Enable the IP source guard function.

   ```
   ZXAN(config)#ip-source-guard enable
   ```

2. In GPON-ONU interface mode, configure the maximum IPv4 and IPv6 subscriber binding entries on the ONU interface.

```
ZXAN(config)#interface gpon-onu_1/1/1:2
ZXAN(config-if)#ip-source-guard ip-limit ipv4 2 ipv6 4
```

3. Configure the service port VLAN.

```
ZXAN(config-if)#service-port 1 vport 1 user-vlan 100 vlan 200
```

4. Enable the IP source guard on the service port.

```
ZXAN(config-if)#ip-source-guard enable sport 1
```

5. Configure the IPv4 DHCP snooping static binding.

```
ZXAN(config-if)#ip dhcp snooping binding 1.1.1.2 sport 1
```

6. Configure the IPv6 DHCP snooping static binding.

```
ZXAN(config-if)#ipv6 dhcp snooping binding mac-address 2365.1498.2369 2001::ff01
ipv6-mask 128 sport 1
```

7. (Optional) Query the IP source guard status.

```
ZXAN(config)#show ip-source-guard
global ip-source-guard status :enable
```

8. (Optional) Query the IPv4 DHCP snooping static binding.

```
ZXAN(config-if)#show ip dhcp snooping static port gpon-onu_1/1/1:2
Port                Sport  IP-addr      MAC-addr
gpon-onu_1/1/1:2    1      1.1.1.2      0000.0000.0000
```

9. (Optional) Query the IPv6 DHCP snooping static binding.

```
ZXAN(config-if)#show ipv6 dhcp snooping static port gpon-onu_1/1/1:2
Port                Sport  IPv6-addr      Mask MAC-addr
gpon-onu_1/1/1:2    1      2001::ff01     128  2365.1498.2369
```

– End of Steps –

13.6 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 the data traffic between subscribers to prevent malicious attacks.

Steps

1. 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 –

13.7 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-vlan100))#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-vlan100))#ip proxy-arp
```

– End of Steps –

Chapter 14
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

14.1 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.

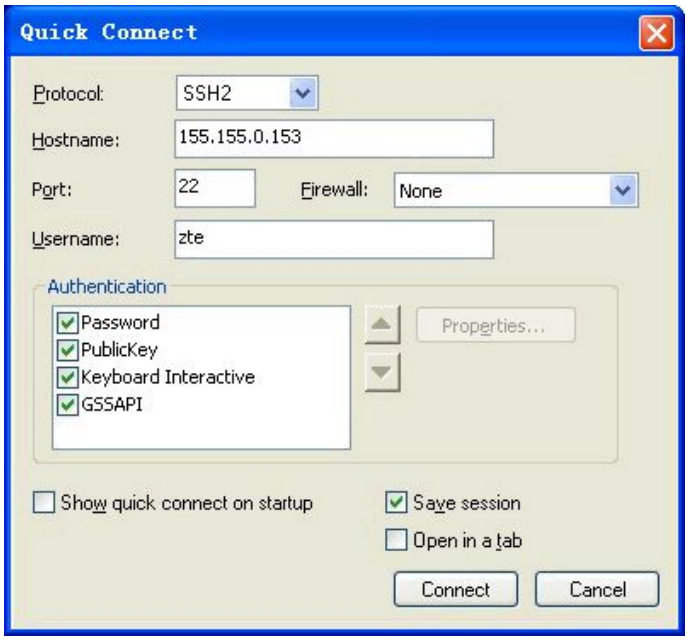
```
ZXAN(config)#show ssh
SSH configuration:
  SSH enable-flag configuration : enable
  SSH version                   : ver2.0
  SSH only configuration        : disable
  SSH init server key           : not initialized
  SSH auth mode                 : local
  SSH auth type                 : pap
```

– End of Steps –

Follow-Up Action

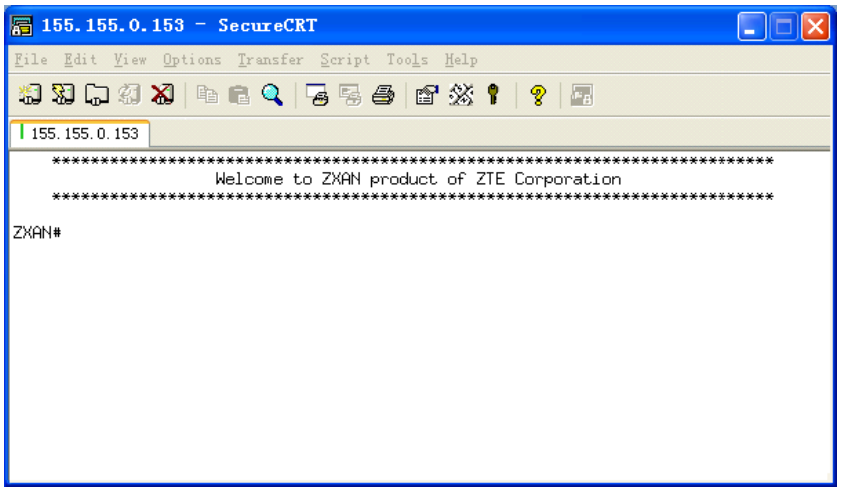
1. In a Windows OS, run the SSH client software (SecureCRT, for example). The **Quick Connect** dialog box opens, as shown in Figure 14-1.

Figure 14-1 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, as shown in Figure 14-2.

Figure 14-2 SSH Login Window



NOTE **Note:**

The hostname is the in-band/out-of-band NM IP address of the ZXA10 C320.

14.2 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 two login modes:

- Telnet
- SSH

Steps

1. Configure telnet user authentication type.

```
ZXAN(config)#user-authentication-type aaa
```

2. Configure telnet user authorization type.

```
ZXAN(config)#user-authorization-type aaa
```

3. Configure SSH server authentication mode.

```
ZXAN(config)#ssh server authentication mode aaa
```

4. Enable TACACS+.

```
ZXAN(config)#tacacs enable
```

5. Configure TACACS+ server.

- In-band NM mode (The ZXA10 C320 is connected to the TACACS+ server through the in-band NM channel.)

```
ZXAN(config)#tacacs-server host 1.2.2.3
```

- Out-of-band NM mode (The ZXA10 C320 is connected to the TACACS+ server through the out-of-band NM channel.)

```
ZXAN(config)#tacacs-server host vrf mng 1.2.2.3
```

6. Configure TACACS+ server group.
   - In-band NM mode

```
ZXAN(config)#aaa group-server tacacs+ zte
ZXAN(config-sg)#server 1.2.2.3
ZXAN(config-sg)#exit
```

   - Out-band NM mode

```
ZXAN(config)#aaa group-server tacacs+ zte
ZXAN(config-sg)#server vrf mng 1.2.2.3
ZXAN(config-sg)#exit
```

7. Configure the authorization, authentication, and accounting group.

```
ZXAN(config)#aaa authentication login default group zte
ZXAN(config)#aaa authorization exec default group zte
ZXAN(config)#aaa accounting commands 10 default stop-only group zte
```

– End of Steps –

14.3 Configuring RADIUS

RADIUS ensures data safety of the ZXA10 C320 by implementing safety authentication and authorization for remote users who access the ZXA10 C320.

Context

RADIUS supports two login modes:

- Telnet
- SSH

Steps

1. Configure telnet user authentication type.

```
ZXAN(config)#user-authentication-type aaa
```

2. Configure telnet user authorization type.

```
ZXAN(config)#user-authorization-type aaa
```

3. Configure SSH server authentication mode.

```
ZXAN(config)#ssh server authentication mode aaa
```

4. Configure the RADIUS server group.

```
ZXAN(config)#aaa group-server radius-authen 1
ZXAN(config-authgrp-1)#
```

5. Configure the RADIUS server.

```
ZXAN(config-authgrp-1)#server 1 2.2.2.3 key zteRad
```

6. (Optional) Configure the route.

```
ZXAN(config-authgrp-1)#ip mng
ZXAN(config-authgrp-1)#exit
```

NOTE **Note:**

When the ZXA10 C320 is connected to the RADIUS server through the in-band NM channel, you can skip this step.

7. Configure the authentication group.

```
ZXAN(config)#aaa authentication login default rds-group 1
```

8. Configure the authorization group.

```
ZXAN(config)#aaa authorization exec default rds-group 1
```

– End of Steps –

14.4 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 –

14.5 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-number 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 –

This page intentionally left blank.

Chapter 15
Ethernet OAM Configuration

The ZXA10 C320 supports service layer OAM function, which includes link continuity check, port loopback detection, link trace, and alarm notification.

Table of Contents

15.1 Configuring the CCM Function

CCM is used to ensures the continuity between MPs in an MA.

Context

A MEG End Point (MEP) sends Continuity Check Message (CCM) packets periodically, which ensures the continuity of Maintenance Points (MPs) in the corresponding Maintenance Association (MA). The MPs that receive the packets need not to respond.

Configuration Data

Table 15-1 list the configuration data of the CCM function.

Table 15-1 Configuration Data of CCM Function

Item	Data
MD	● Session ID: 1 ● Name: md1 ● Level: 3
MA	● Session ID: 1 ● Name: ma1 ● Protection mode: VLAN protection ● Primary VLAN ID: 100
Local MEP	● Session ID: 1 ● MEP ID: 1 ● Direction: down
Remote MEP	● Session ID: 2 ● MEP ID: 2 ● Remote MAC address: 00d0.d058.6958
Uplink interface	gei_1/3/1

NOTE **Note:**

The remote MAC address of the remote MEP is the in-band MAC address of the local MEP.

Steps

1. Enable the CFM function.

```
ZXAN(config)#cfm enable
```

2. Create the Ethernet OAM MD.

```
ZXAN(config)#cfm create md session 1 name md1 level 3
```

3. Create the Ethernet OAM MA.

```
ZXAN(config-md1)#create ma session 1 format icc-based name ma1
```

4. Configure the MA protection mode.

```
ZXAN(config-md1-ma1)#protect vlan
```

NOTE **Note:**

Only VLAN protection mode is valid.

5. Configure the MA primary VLAN.

```
ZXAN(config-md1-ma1)#primary vlan 100
```

NOTE **Note:**

In the Ethernet OAM MDs of the same level, primary VLAN of MAs is unique.

6. Configure CCM interval.

```
ZXAN(config-md1-ma1)#ccm timer-interval 2
```

Note:

The ZXA10 C320 supports seven intervals:

- 1: 3.3 ms
- 2: 10 ms
- 3: 100 ms
- 4: 1 s
- 5: 10 s
- 6: 1 min
- 7: 10 min

7. Create local Ethernet OAM MEP.

```
ZXAN(config-md1-ma1)#create mep session 1 1 direction down
```

8. Assign local MEP to the uplink port.

```
ZXAN(config-md1-ma1)#assign mep 1 to interface gei_1/3/1
```

9. Enable the MEP.

```
ZXAN(config-md1-ma1)#mep 1 state enable
```

10. Configure the remote MEP.

```
ZXAN(config-md1-ma1)#create rmep session 2 2 remote-mac 00d0.d058.6958
```

11. Enable the CCM-send function on local MEP.

```
ZXAN(config-md1-ma1)#mep 1 ccm-send unicast enable
```

12. Configure the uplink port VLAN of local MEP.

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

– End of Steps –

Result

If the ZXA10 C320 receives error CCM packets or does not receive any CCM packets, there will be a CCM alarm information on the NMS. You can query the CCM alarm information using the **show cfm mp all md 1 ma 1 detail** command.

15.2 Configuring the LBM Function

The Ethernet LBM, which is an optional OAM function, is used to check the bidirectional continuity between an MEP and an MIP, or between an MEP to one or multiple MEPs.

Configuration Data

Table 15-2 list the configuration data of the Loopback Message (LBM) function.

Table 15-2 Configuration Data of LBM Function

Item	Data
MD	● Session ID: 1 ● Name: md1 ● Level: 3
MA	● Session ID: 1 ● Name: ma1 ● Protection mode: VLAN protection ● Primary VLAN ID: 100
Local MEP	● Session ID: 1 ● MEP ID: 1 ● Direction: down
Remote MEP	● Session ID: 2 ● MEP ID: 2 ● Remote MAC address: 00d0.d058.6958
Uplink interface	gei_1/3/1

NOTE **Note:**

The remote MAC address of the remote MEP is the in-band MAC address of the local MEP.

Steps

1. Enable the CFM function.

```
ZXAN(config)#cfm enable
```

2. Create the Ethernet OAM MD.

```
ZXAN(config)#cfm create md session 1 name md1 level 3
```

3. Create the Ethernet OAM MA.

```
ZXAN(config-md1)#create ma session 1 format icc-based name ma1
```

4. Configure the MA protection mode.

```
ZXAN(config-md1-ma1)#protect vlan
```

NOTE **Note:**

Only VLAN protection mode is valid.

5. Configure the MA primary VLAN.

```
ZXAN(config-md1-ma1)#primary vlan 100
```

NOTE **Note:**

In the Ethernet OAM MDs of the same level, primary VLAN of MAs is unique.

6. Create local Ethernet OAM MEP.

```
ZXAN(config-md1-ma1)#create mep session 1 1 direction down
```

7. Assign local MEP to the uplink port.

```
ZXAN(config-md1-ma1)#assign mep 1 to interface gei_1/3/1
```

8. Enable the MEP.

```
ZXAN(config-md1-ma1)#mep 1 state enable
```

9. Configure the remote MEP.

```
ZXAN(config-md1-ma1)#create rmep session 2 2 remote-mac 00d0.d058.6958
```

10. Configure the uplink port VLAN of local MEP.

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

11. In administrator mode, carry out the LBM function.

```
ZXAN#cfm lbm check unicast md 1 ma 1 smep-id 1 dmep-id 2
```

– End of Steps –

Result

In the CLI window, a message shows that whether the destination MEP (or MIP) is reachable.

15.3 Configuring the LTM Function

The LTM function is used to trace the link between two MEPs.

Context

When you carry out the Link Trace Message (LTM) function on an MEP, the MEP sends LTM packets to trace the path to the destination MAC address. MIPs forward the messages until the messages arrive the destination MEP or the messages cannot be forwarded any more. When MPs on the path receive the LTM packets, each MP responds to the source MEP with an LTR message. When the destination is an MIP, the MIP does not forward the LTM anymore.

Steps

1. Enable the CFM function.

```
ZXAN(config)#cfm enable
```

2. Create the Ethernet OAM MD.

```
ZXAN(config)#cfm create md session 1 name md1 level 3
```

3. Create the Ethernet OAM MA.

```
ZXAN(config-md1)#create ma session 1 format icc-based name ma1
```

4. Configure the MA protection mode.

```
ZXAN(config-md1-ma1)#protect vlan
```

NOTE **Note:**

Only VLAN protection mode is valid.

---

5. Configure the MA primary VLAN.

```
ZXAN(config-md1-ma1)#primary vlan 100
```

NOTE **Note:**

In the Ethernet OAM MDs of the same level, primary VLAN of MAs is unique.

---

6. Create local Ethernet OAM MEP.

```
ZXAN(config-md1-ma1)#create mep session 1 1 direction down
```

7. Assign local MEP to the uplink port.

```
ZXAN(config-md1-ma1)#assign mep 1 to interface gei_1/3/1
```

8. Enable the MEP.

```
ZXAN(config-md1-ma1)#mep 1 state enable
```

9. Configure the remote MEP.

```
ZXAN(config-md1-ma1)#create rmep session 2 2 remote-mac 00d0.d058.6958
```

10. Configure the uplink port VLAN of local MEP.

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

11. In the administrator mode, carry out the LTM function.

```
ZXAN#cfm ltm md 1 ma 1 smep-id 1 dmep-id 2
```

– End of Steps –

Result

In the CLI window, a message shows the MEP (or MIP) path and whether the destination MEP is reachable.

This page intentionally left blank.

Chapter 16
Route Protocol Configuration

Besides static route, the ZXA10 C320 supports the following routing protocols:

- OSPF
- BGP

Table of Contents

16.1 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 –

16.2 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 –

16.3 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 17
Clock Configuration

Clock Synchronization

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.

IEEE 1588

IEEE 1588, also known as the PTP, is a protocol for frequency and time of day distribution, which is based on timestamp information exchange in a master-slave hierarchy, , whereby the timing information is originated at a grandmaster clock that is usually traceable to a PRC or UTC.

Similar to NTP, PTP nonetheless offers higher accuracy, with HW-based timestamping support and fractional nanosecond precision.

Table of Contents

17.1 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 17-1 lists the configuration data of the synchronous Ethernet clock.

Table 17-1 Configuration Data of the Synchronous Ethernet Clock

Item	Data
Clock source port	1/3/1
Clock type	SYNCE

Item	Data
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 –

17.2 Configuring PTP Slave Clock

The ZXA10 C320 works as the PTP slave clock to transmit PTP clock signals to downlink ONUs.

Prerequisite

A reliable PTP source clock exits in the network.

Configuration Data

Table 17-2 lists configuration data of the PTP slave clock configuration.

Table 17-2 PTP Slave Clock Configuration Data

Item	Data
PTP slave	IP address: 192.168.2.11 Packet type: unicast Step mode: one-step Delay request interval: -4
PTP source	IP address: 192.168.2.1
PTP VLAN ID	100
ONU interface	gpon-onu_1/1/1:1

Steps

1. In PTP configuration mode, configure the PTP slave clock.

```
ZXAN(config)#ptp
ZXAN(config-ptp)#ptp slave ip 192.168.2.11 packet-type unicast step-mode one-
step interval -4
```

2. Configure the PTP source.

```
ZXAN(config-ptp)#ptp-source ip 192.168.2.1
```

NOTE **Note:**

When the PTP packet type is multicast, there is no need to configure the PTP source.

3. Enable the 1PPS+TOD function on the ONU interface.

```
ZXAN(config)#interface gpon-onu_1/1/1:1
ZXAN(config-if)#1pps-tod enable
ZXAN(config-if)#exit
```

4. Bind the PTP VLAN.

```
ZXAN(config)#vlan 100
ZXAN(config-vlan100)#1588-bind
ZXAN(config-vlan100)#exit
```

5. (Optional) Query the PTP configuration.

```
ZXAN(config)#show time ptp
Slot/                       Hybrid Multi  Two-
port Mode  Domain addr      -Mode  cast   Step  Status Interval   Utc     Layer2
.....................................................................................
3/1  slave 0 192.168.2.11    syn-hyb   n     n freerun  -4 1970-01-01 00:35:02 n
ptp configure count: 1
```

6. (Optional) Query the PTP source configuration.

```
ZXAN(config)#show time ptp-source
addr               adjust  Layer2
.............................
192.168.2.1         0      n
time source count: 1
```

– End of Steps –

Figures

This page intentionally left blank.

Tables

Glossary

ACL
- Access Control List

ARP
- Address Resolution Protocol

AS
- Autonomous System

BGP
- Border Gateway Protocol

BRAS
- Broadband Remote Access Server

CAC
- Channel Access Control

CCM
- Continuity Check Message

CDR
- Call Detail Record

CFM
- Connectivity Fault Management

CLI
- Command Line Interface

CVLAN
- Customer Virtual Local Area Network

CoS
- Class of Service

DHCP
- Dynamic Host Configuration Protocol

DNS
- Domain Name System

DSCP
- Differentiated Services Code Point

DoS
- Denial of Service

EPON
- Ethernet Passive Optical Network

ESMC
- Ethernet Synchronization Message Channel

GPON
- Gigabit Passive Optical Network

HW
- High speed data Way

ICMP
- Internet Control Message Protocol

IEEE
- Institute of Electrical and Electronics Engineers

IGMP
- Internet Group Management Protocol

IGP
- Interior Gateway Protocol

IP
- Internet Protocol

IPTV
- Internet Protocol Television

LACP
- Link Aggregation Control Protocol

LAN
- Local Area Network

LBM
- Loopback Message

MA
- Maintenance Association

MAC
- Media Access Control

MD
- Maintenance Domain

MEP
- MEG End Point

MFF
- MAC-Forced Forwarding

MGC
- Media Gateway Controller

MIP
- MEG Intermediate Point

MLD
- Multicast Listener Discovery

MST
- Multiple Spanning Tree

MSTP
- Multiple Spanning Tree Protocol

MVLAN
- Multicast Virtual Local Area Network

NDP
- Neighbor Discovery Protocol

NE
- Network Element

NM
- Network Management

NMS
- Network Management System

NTP
- Network Time Protocol

OLT
- Optical Line Terminal

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

PRC
- Premium Rate Calls

PTP
- Precision Time Protocol

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

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
- Transparent LAN Service

TM
- Timing Marker

ToS
- Type of Service

UAPS
- Uplink Auto Protection Switching

UTC
- Universal Time Coordinated

VLAN

- Virtual Local Area Network

VoIP

- Voice over Internet Protocol