ZTE中兴

ZXA10 C320
Optical Access Convergence Equipment
Maintenance Manual

Version: V2.0.0

LEGAL INFORMATION

Copyright © 2014 ZTE CORPORATION.

The contents of this document are protected by copyright laws and international treaties. Any reproduction or distribution of this document or any portion of this document, in any form by any means, without the prior written consent of ZTE CORPORATION is prohibited. Additionally, the contents of this document are protected by contractual confidentiality obligations.

All company, brand and product names are trade or service marks, or registered trade or service marks, of ZTE CORPORATION or of their respective owners.

This document is provided "as is", and all express, implied, or statutory warranties, representations or conditions are disclaimed, including without limitation any implied warranty of merchantability, fitness for a particular purpose, title or non-infringement. ZTE CORPORATION and its licensors shall not be liable for damages resulting from the use of or reliance on the information contained herein.

ZTE CORPORATION or its licensors may have current or pending intellectual property rights or applications covering the subject matter of this document. Except as expressly provided in any written license between ZTE CORPORATION and its licensee, the user of this document shall not acquire any license to the subject matter herein.

ZTE CORPORATION reserves the right to upgrade or make technical change to this product without further notice. Users may visit the ZTE technical support website http://support.zte.com.cn to inquire for related information.

The ultimate right to interpret this product resides in ZTE CORPORATION.

Revision History

Revision No.	Revision Date	Revision Reason
R1.0	2013-08-31	First edition

Serial Number: SJ-20130520170233-006

Publishing Date: 2013-08-31 (R1.0)

Contents

I

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 procedures and guidelines that support the maintenance of the ZXA10 C320.

Intended Audience

This document is intended for:

- Debugging engineer
- NM monitoring engineer
- Maintenance engineer

What Is in This Manual

This manual contains the following chapters:

Chapter	Summary
1, Safety Descriptions	Provides the safety precautions and sign description.
2, Routine Maintenance	Describes the routine maintenance at both the equipment side and the NM side.
3, Data Backup and Recovery	Describes the saving and backup of the NE data.
4, Expansion Guides	Describes the expansion flow and the processing guides for expansion failure.
5, Cutover Guides	Describes the cutover flow and the cutover restoring guides.
6, Version Upgrade Guides	Describes the version upgrading flows and upgrading failure guides.
Appendix A, Card Replacement	Describes the card replacement.

Conventions

This manual uses the following typographical conventions:

Typeface	Meaning
Italics	Variables in commands. It may also refer to other related manuals and documents.
Bold	Menus, menu options, function names, input fields, option button names, check boxes, drop-down lists, dialog box names, window names, parameters, and commands.

I

Typeface	Meaning
Constant width	Text that you type, program codes, filenames, directory names, and function names.
	Danger: indicates an imminently hazardous situation. Failure to comply can result in death or serious injury, equipment damage, or site breakdown.
	Warning: indicates a potentially hazardous situation. Failure to comply can result in serious injury, equipment damage, or interruption of major services.
	Caution: indicates a potentially hazardous situation. Failure to comply can result in moderate injury, equipment damage, or interruption of minor services.
	Note: provides additional information about a certain topic.

Chapter 1
Safety Descriptions

Table of Contents

1.1 Safety Precautions

Safety Precautions for Protection Ground

The safety precautions for protection ground are as follows:

- Connect the grounding cable first before installing the equipment. Remove the grounding cable after removing all the equipment.
- Prohibit to destroy the grounding conductor.
- Prohibit to operate on the equipment without installing the grounding conductor.
- The equipment must be connected with the protection ground perpetually. Before operating on the equipment, check the electrical connection and make sure that the equipment grounding is reliable.

Safety Precautions for Batteries

The safety precautions for the storage battery are as follows:

- Always keep the electrodes of a battery facing upward in moving a battery. Do not put it upside down or tilt it.
- Avoid short-circuit of a battery caused by metal objects. If possible, cut off the power supply of the battery before performing other operations.
- During its working, batteries will release inflammable gas, so they should be placed in the environment which is well ventilated with proper fire prevention measures taken.
- When a battery is over 60℃ in temperature, check it for any spill of acid liquid. Handle timely if there is any spill of acid liquid.
- When moving or handling a battery with leakage, be careful to protect yourself from any possible harm by the acid liquid. Use $NaHCO_3$, Na_2CO_3 or $Na_2CO_310H_2O$ to neutralize or absorb them if any spill of acid liquid is found.
- Wash with clean water if anyone touches any spill of the battery. If the situation is quite serious, take him to the hospital after washing with clean water.

The safety precautions for the li-ion battery are as follows:

- Replace with the same type of battery recommended only.
- Handle the used-up battery according to instructions only.
- Do not throw the li-ion battery into the fire.

Safety Precautions for Laser

The laser receiver and transmitter is used in the optical transmission system and the related test tools. The bared optical fiber or the connector port can transmit laser which is invisible to the naked eyes. Looking at it without any protection may hurt eyes.

The eyes are not hurt if you gaze at the bared optical fiber tips or damaged optical fiber in a distance of 150 mm. But the eyes may be hurt if you observe the bared optical fiber tip with a microscope, a magnifier or a loupe.

The safety precautions for laser are as follows:

- Only the authorized personnel with the corresponding training can perform the operation.
- Wear safety goggles while handling laser or optical fibers.
- Make sure to switch off the optical source before disconnecting the optical fiber connector.
- Prohibit to gaze at the bare optical fiber or the connector tips before the optical source is surely switched off.
- Measure the optical power in the optical fiber with an optical power meter to make sure the optical source is switched off.
- When opening the front door of the optical fiber transmission system, be careful to avoid the laser radiation.
- Prohibit to use optical instrument including the microscope, the magnifier or the loupe to observe the optical fiber connector or the optical fiber tips.

Do as follows when handling the optical fibers:

- Only the personnel with corresponding training can shear, fuse and splice the optical fiber.
- Make sure the optical fiber and optical source is disconnected before shear, fuse and splice the optical fiver. After disconnecting the optical fiber, protect all the optical fiber connectors with the optical fiber caps.

Safety Precautions for Plugging/ Unplugging Cards

The safety precautions for plugging/unplugging cards are as follows:

- Make sure that the card is compatible with the slot.
- Wear the antistatic wrist strip before operation.
- Plug in the card along sliding rail. If the card is blocked, do not shake the card to prevent any damage to the card.

1.2 Sign Descriptions

Table 1-1 lists the safety signs used in this manual. These signs remind users of the safety precautions which they have to consider during the device installation, operation and maintenance.

Table 1-1 Safety Sign and Description

Safety sign	Description
⚠	Safety precaution sign
NOTE	Note sign

The safety prompts consists of three levels: Danger, Warning and Caution. The details are as follows:

⚠ Danger!

Indicates an imminently hazardous situation, which, if not avoided, could result in death, serious injury, or serious equipment damages.

⚠ Warning!

Indicates a hazardous situation, which, if not avoided, could result in serious injuries, equipment damages or services interruption.

⚠ Caution!

Indicates a potentially hazardous situation, which, if not avoided, could result in moderate injuries, equipment damages or interruption of partial service interruption.

NOTE Note:

Indicates the notes, prompts and tips.

This page intentionally left blank.

Chapter 2
Routine Maintenance

Table of Contents

2.1 Routine Maintenance Precautions

The precautions for the routine maintenance are as follows:

- Keep the equipment room clean, and maintain normal temperature and humidity level. Take special measures to keep it dust-proof and damp-proof, and other measures against insects and rodents.
- Ensure that the primary power is stable and reliable; check the system grounding and lightning ground periodically. In particular, check the lightning protection system before and after the stormy season for the protection of the facilities.
- Establish a complete set of maintenance regulations for the equipment room to standardize the routine maintenance work. Detailed maintenance attendance log should be maintained about system operation, software version, configuration change, upgrading and troubleshooting records for fault analysis and solutions in the future.
- It is prohibited to play games, access Internet on computer terminals and set up, run, copy any software that is irrelevant to the system or apply the computer terminal for other intention.
- Configure different NM passwords for different access rights and put them under authorized management. Change the passwords periodically with only authorized personnel having the access.
- Maintenance personnel should be well trained and should have sound experience of computer networks, and will study further to improve their maintenance skills. During maintenance operations, maintenance personnel should follow the relevant manual. Wear antistatic wrist strap before touching the hardware of the equipment to avoid static discharge.
- Do not reset the equipment, load or change any data , especially the NE data unless it is necessary. Backup system configuration before any change is made on it and do not delete backup configuration files until the system is running properly (generally after a week. Timely record is necessary for any change on the data.
- Prepare a toolkit of frequently used tools and calibrate the meters regularly to ensure they are working properly. The nine tools are as follows:

  → Screw driver (Straight, Cross)

→ Signaling testers

→ Thin nose bent pliers

→ Network cable pliers

→ Multi-meters

→ AC power maintenance

→ Power extension lines and sockets

→ Telephone cables

→ Network cables

● Check standby equipment regularly to maintain inventory and label them for convenience. Store the spare components and replaced faulty component into corresponding proper places and label them for identification.

● Keep the software and documents well arranged and keep them at an easily accessible place at the time of maintenance activity.

● The equipment room should be well lightened for the maintenance tasks. In case of power failure, make necessary emergency arrangements.

● Put the contact information of ZTE Corporation local office at a noticeable place and inform the maintenance personnel of this and seek help in case of emergency. Update the contact information timely.

2.2 Equipment Routine Maintenance

2.2.1 Environment Check

Table 2-1 lists the environment check items.

Table 2-1 Environment Check

Item	Instrument and Meter	Testing Method	Reference Standard	Troubleshooting
Equipment room temperature control	Thermometer	Check and record the current value	-5℃ to 45℃ (long term) -5℃ to 5℃ (short term)	Adjust the air conditioner or other temperature control devices
Equipment room humidity	Hygrometer	Check and record the current value	5% to 95%	Adjust the air conditioner or other humidity control devices.

Item	Instrument and Meter	Testing Method	Reference Standard	Troubleshooting
Equipment room dust resistance	None	Observe the dust concentration in the equipment room	The concentration of the dust with a diameter larger than 5 μm is no more than $3×10^4$ particles/m^3. The dust particles should be non-conductive, non-magnetic, electrical or corrosive.	As it is difficult to measure the dust concentration in the equipment room in daily maintenance, the maintenance personnel must make sure the equipment is not covered with dust or polluted.
Air conditioner running status	None	Check whether the air conditioner (or other temperature and humidity adjusting devices) can work properly according to the set temperature (humidity).	Refer to the set temperature and humidity values of the equipment room.	If the air conditioner is faulty, contact the air conditioner maintenance personnel to repair it.
Storage battery	Multi-meter	Maintenance personnel measure the AC and DC voltages of the input power with a multi-meter and keep a record.	-48 V ± 15 V	If the storage battery voltage is not stable, contact the relative department for maintenance.

2.2.2 Main Device Status Check

Introduction

The check on the ZXA10 C320 running status includes the following:

- Power cable and grounding cable check
- Power supply and voltage check
- Fan running status check
- Card running states check

Power Cable and Grounding Cable Check

Table 2-2 lists the power cable and grounding cable check information.

Table 2-2 Power Cable and Grounding Check

Item	Step
Meters	None
Check method	Check whether the power cable and the grounding cable are properly connected and whether they are rusty.
Standard requirements	The power cable and the grounding cable are connected properly and they are free of rust.
Troubleshooting	If the power cable and the grounding cable are not connected properly, please reconnect or change them.

Power Supply and Voltage Check

Table 2-3 lists the power supply and voltage check information.

Table 2-3 Power Supply and Voltage Check

Item	Step
Meters	Multimeter
Check method	Maintenance personnel measure the AC and DC voltages of the input power with a multimeter and keep a record.
Standard requirements	1. The ZXA10 C320 uses –48 V power supply. The equipment room should be installed with AC/DC power transforming equipment to supply working power. The DC power voltage is allowed to fluctuate between –57 V and –38 V. 2. In order to ensure continuous working of the ZXA10 C320 device in case of the mains power failure, it is necessary to provide the uninterrupted power supply measures, such as diesel-electric set and storage battery. 3. DC power supply shall have over-voltage/current protection and indication.
Troubleshooting	When the test result is not in the standard range, please check the input power supply timely and make sure the backup power supply is in the working status.

Fans Running Status Check

Table 2-4 lists the fan running status check information.

Table 2-4 Fans Running Status Check

Item	Step
Meters	None
Check method	Check the running status of the fans with the **show fan** command. If the equipment room is at the local place, observe the fan running status directly and keep a record.
Standard requirements	The fan runs properly.
Troubleshooting	If the fan is faulty, inform the maintenance personnel to repair it.

Card Running Status Check

The LED states indicate the card running status.

Table 2-5 lists the card running states check information.

Table 2-5 Card Running States Check

Item	Step
Meters	None
Check method	Check the running status of the cards with the **show card** command. If the equipment room is at the local place, observe the fan running status directly and keep a record.
Standard requirements	The cards run properly.
Troubleshooting	If the card is faulty, inform the maintenance personnel to repair.

2.2.3 Switching and Control Card Running Status Check

The ZXA10 C320 uses the SMXA switching and control card.

Table 2-6 descriptions the indicator on the control and switching card.

Table 2-6 Indicator Description of Switching and Control card Panel

Indicator	Status	Description
PWR	LED is OFF.	The power of the equipment is not supplied from the panel, but can be supplied from the backplane.
	Green LED is ON.	The power supply from the panel is proper.
	Red LED is ON.	The power supply from the panel is proper.
RUN	LED is OFF.	The card is not powered on or CPU is not started.
	Green LED flashes slowly (0.5 Hz).	The card works properly and card type configuration is correct.
	Green LED is ON.	The card is not configured.
	Green LED flashes quickly.	The card is downloading data.
	Red LED is ON.	Card hardware failure
	Red LED flashes slowly (0.5 Hz).	The card is installed in the wrong slot.
	Yellow LED flashes slowly (0.5 Hz).	The software version of the card does not match that of the switching and control card. Auto-update is not configured on the card.
M/S	Green LED is ON.	The card is active.
	LED is OFF.	The card is standby.
HDD	Red LED is ON.	The switching and control card is operating flash. Card plug-in/plug-out is not allowed.
ACT*i* (i=1 - 2)	Green LED is ON.	The link is established.
	Green LED flashes.	The optical interface is sending and receiving data.
	LED is OFF.	The link is not established.

2.2.4 PON Interface Card Running Status Check

The ZXA10 C320 uses the GPON interface cards GTGH and GTGO.

Table 2-7 describes the indicators on the GPON interface cards.

Table 2-7 Indicator Description of GPON Interface Cards

Indicator	Status	Description
RUN	LED is OFF.	- The card is not powered ON. - The card does not match. - CPU is not started.
	Green LED is ON.	The card self-checking completes but fails to receive data from the switching and control card or NM.
	Green LED flashes quickly.	The card is downloading data from the network management server.
	Green LED flashes slowly (0.5 Hz).	The card runs properly.
	Red LED is ON.	Card hardware failure
	Red LED flashes slowly (0.5 Hz).	The card is installed in the wrong slot.
	Yellow LED flashes slowly (0.5 Hz).	The software version of the card does not match that of the switching and control card. Auto-update is not configured on the card.
ACTi/LEDi (i = 1 - 16)	LED is OFF.	- No ONU is configured on the GPON interface. - The GPON interface has no optical module installed. - The GPON interface is shutdown. - The GPON interface is TypeB protection port.
	Green LED flashes.	The GPON interface and connected ONUs work properly.
	Red LED is ON.	The GPON interface has LOS alarms.

2.2.5 P2P Interface Card Running Status Check

The ZXA10 C320 uses the FTGK P2P interface card.

Table 2-8 describes the indicators on the P2P Ethernet interface card.

Table 2-8 Indicator Description of P2P Interface Card

Indicator	Status	Description
RUN	LED is OFF.	The card powers OFF or CPU is not started.
	Green LED is ON.	The card self-checking completes but fails to receive data from the switching and control card or NM.
	Green LED flashes quickly.	The card is downloading data from the main switching and control card or NM.
	Green LED flashes slowly (0.5 Hz).	The card is working properly.
	Red LED is ON.	Card hardware failure
	Red LED flashes slowly (0.5 Hz).	The card should not be inserted in this slot.
	Yellow LED flashes slowly (0.5 Hz).	The software version of the card does not match that of the switching and control card. Auto-update is not configured on the card.
LED*i* (i=1 - 48)	LED is OFF.	The optical interface is not connected or the link is not established.
	Green LED is ON.	The optical interface is connected (LINK).
	Green LED flashes.	The optical interface is sending and receiving the data (ACTIVE).

2.3 NetNumen Routine Maintenance

2.3.1 Monitoring Alarms in Real Time

To find problems during the equipment running process in time, it is recommended to check every day whether there is any critical alarm and major alarm not handled.

Prerequisites

- The NMS manages NEs properly.
- The NE alarms can be reported to the NMS normally.
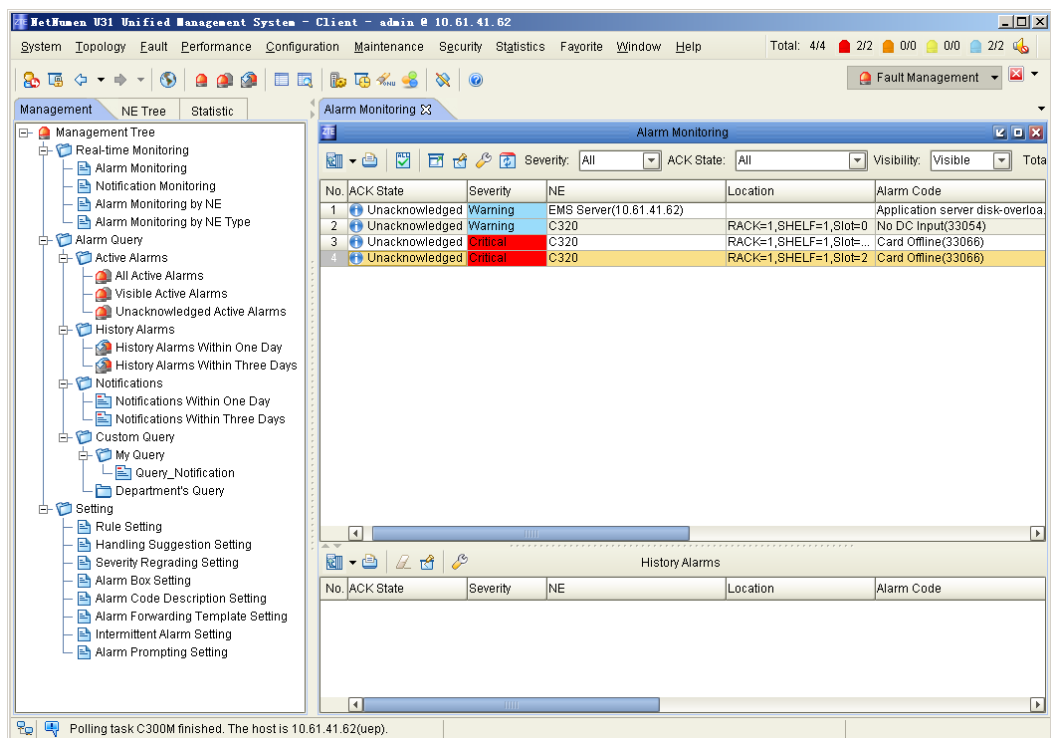
Context

Table 2-9 lists the alarm levels on the NMS.

Table 2-9 Alarm Levels

Level	Color
Critical	Red
Major	Orange
Minor	Yellow
Warning	Blue

Steps

1. In the **NetNumen U31 Unified Management System - Client** window, select **Fault > Alarm Monitoring**. The **Alarm Monitoring** view appears, see Figure 2-1.

Figure 2-1 Monitoring Alarms in Real Time

2. Double-click the alarm to be monitored. The alarm details dialogue box appears. You can view the detailed information of the alarm in the **Detail** tab, see Figure 2-2.

2-9

Figure 2-2 Detailed Alarm Messages

3. On the **Detail** tab, you can perform the following operations.
   - Click **Prev** or **Next** to view information of the previous alarm or the next alarm.
   - Click **Acknowledge**, and the **Acknowledge Alarms** dialogue box appears, see Figure 2-3. You can input information to acknowledge the alarm, and acknowledge information will be displayed on the **Detail** tab.

Figure 2-3 Acknowledge Alarms
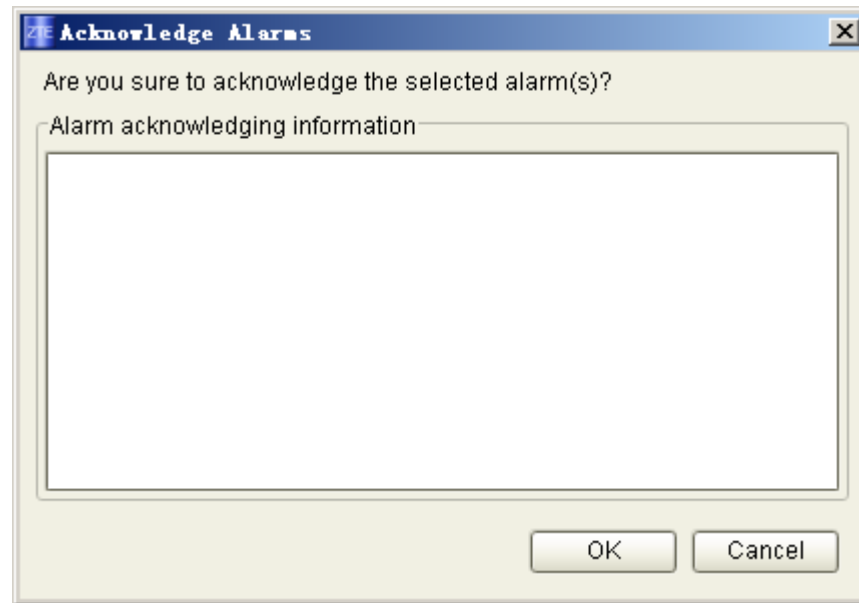
- Click **Unacknowledge**, and the **Unacknowledge Alarms** dialogue box appears. You can input unacknowledge information, and unacknowledge information will be displayed on the **Detail** tab.
- Click **Comment** to make comments for the alarm according to the actual requirement, and the comment will be displayed on the **Detail** tab.
- Click **Clear** to clear the current alarm. Users can clear some alarms that can be ignored.
- Click **Forward** to send alarm information to relevant personnel through E-mail or short message.
- Click **Export** to export detailed alarm information.
- Click **Copy** to copy all detailed alarm information on the tab to the system clipboard.

4. Click the **Handling Suggestions** tab to view the alarm handling suggestion, see Figure 2-4.

Figure 2-4 Handling Suggestions
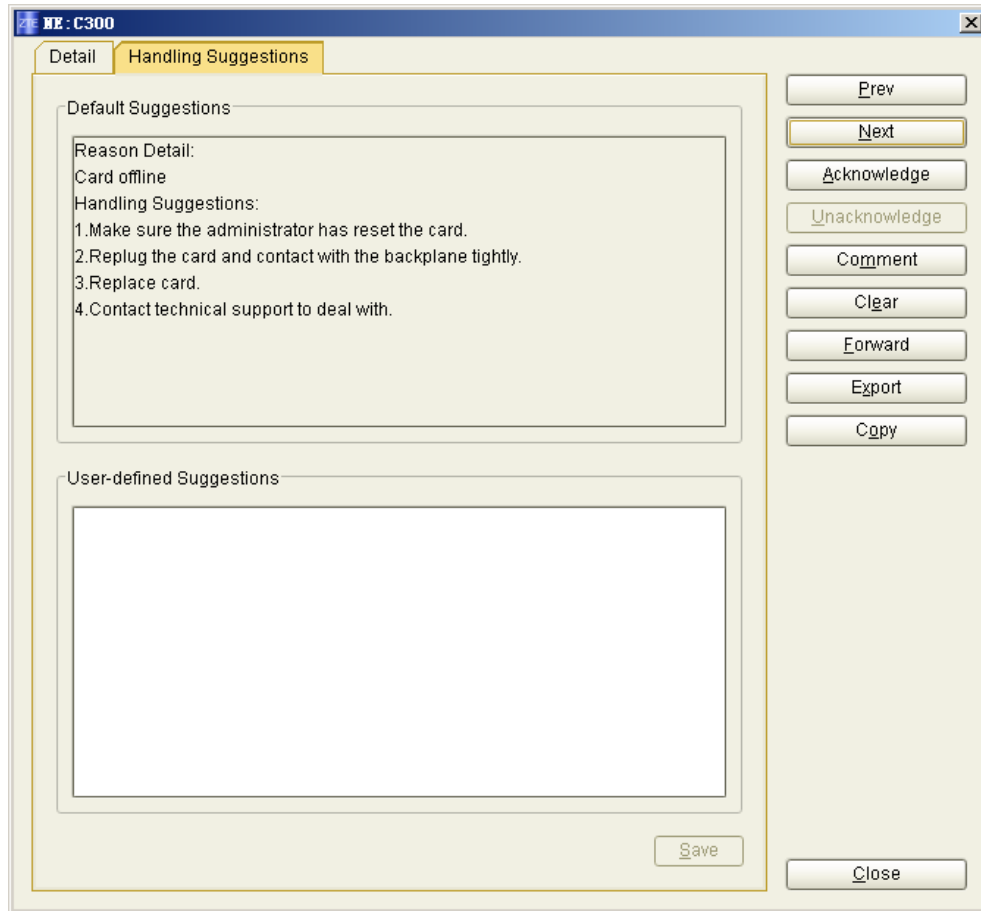
2.3.2 Checking NE Data Backup Status

ZXA10 C320 supports backing up the NE configuration files through the NMS. The NE configuration files are backed up in the specified directory of the NMS server. It is necessary to manually check whether the NE configuration files are backed up successfully.

Prerequisites

The data backup operation is completed.

Context

After the data backup operation is completed, the NE backup data is saved in the `C:\ft pdir\uni\conf\manual` directory on the network management server, see Figure 2-5. The folder name indicates the data backup date. You can decide whether to update the backup data according to the actual requirement.
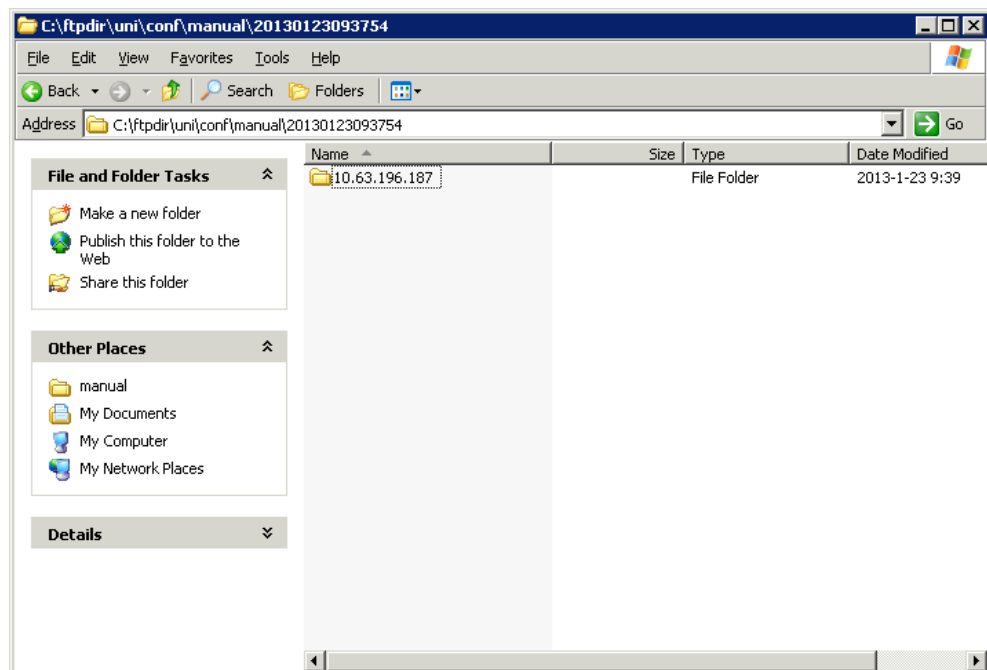
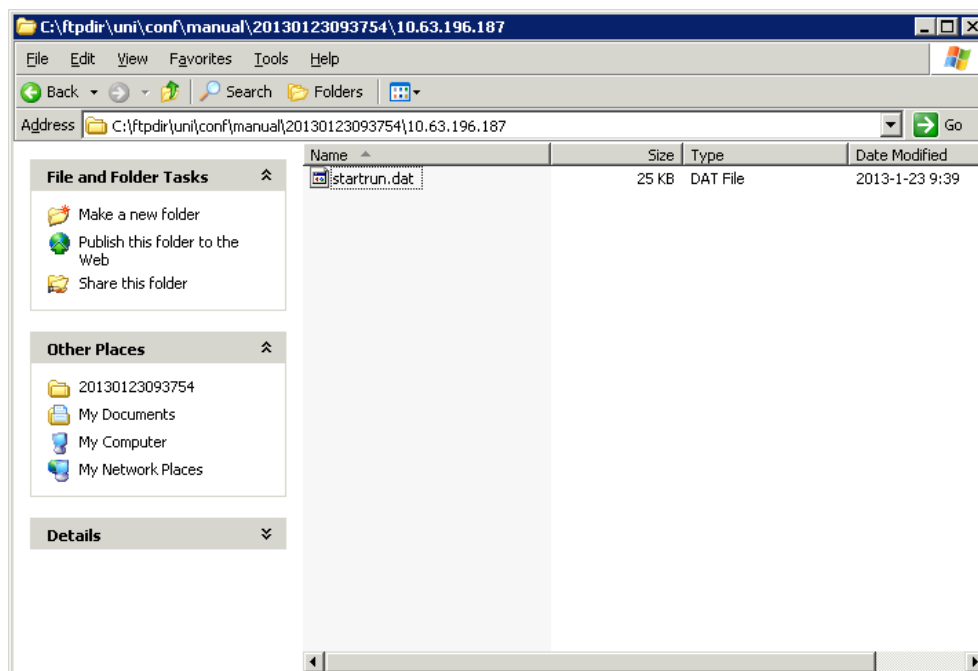**Figure 2-5 NE Data Backup Directory**
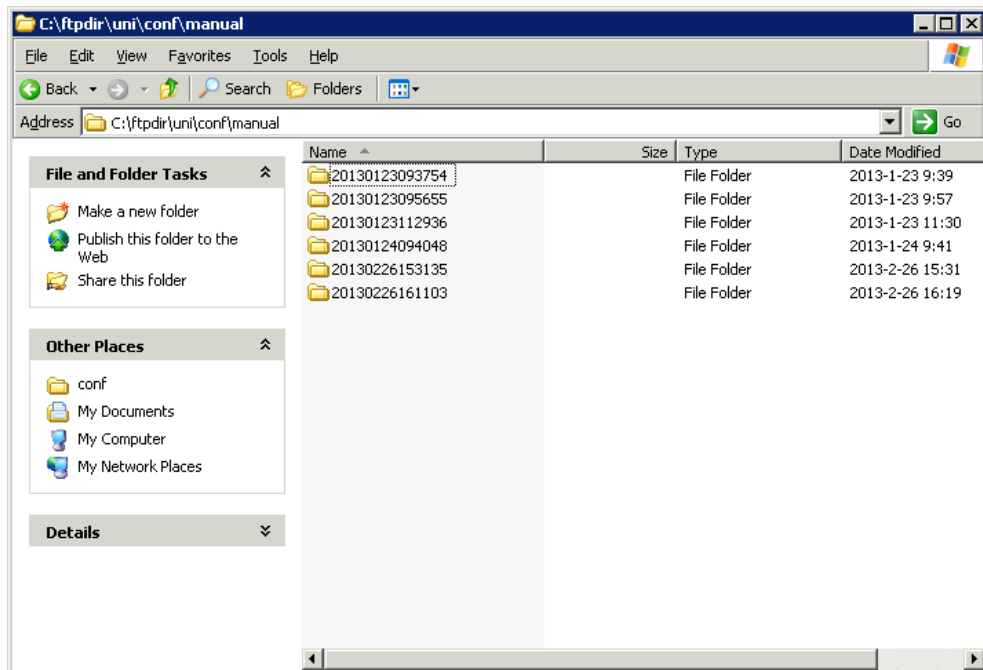
Steps

1. Under the `C:\ftpdir\uni\conf\manual` directory, double-click a folder to display its sub-folders, which are named by the NE IP address , see Figure 2-6.

Figure 2-6 Folder Named as NE IP Address

2. Double-click the folder. The NE backup data file is listed, see Figure 2-7.

Figure 2-7 NE Data File

2.3.3 Monitoring NMS Performance

To ensures a good running condition of the NMS server, it necessary to periodically monitor the server and database performances, and find exceptions and handle them in time.
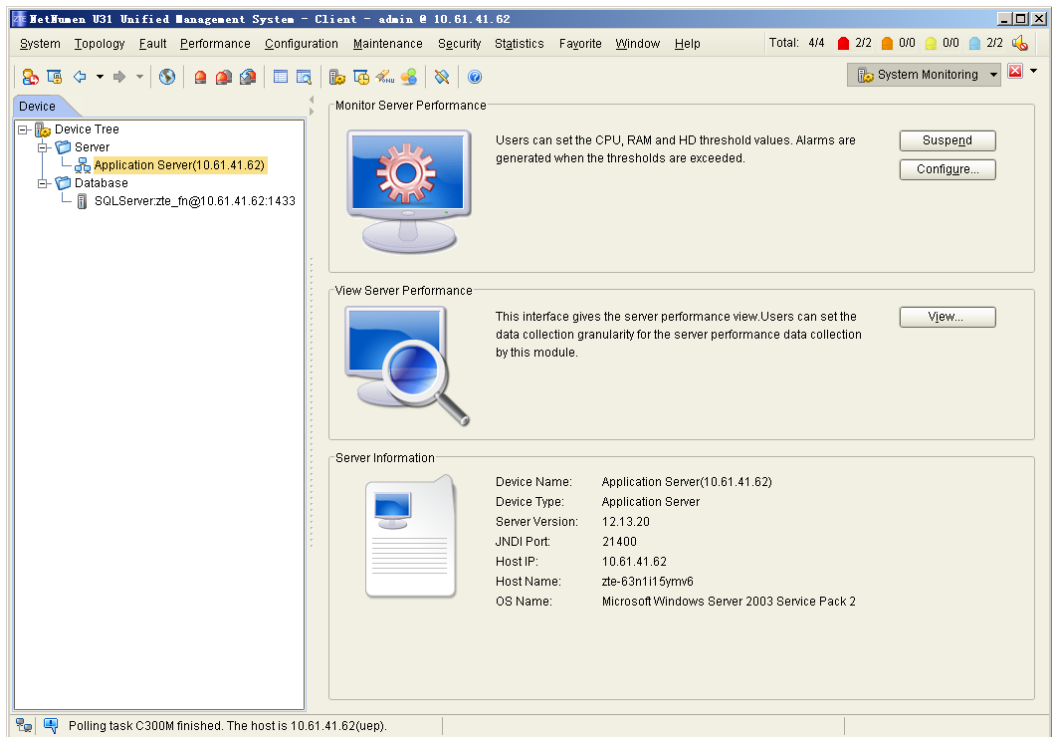
Prerequisites

The NMS manages NEs properly.

Monitoring Server Performance

1. In the **NetNumen U31 Unified Management System - Client** window, select **Maintenance > System Monitoring**. The **System Monitoring** window appears. In the left navigation tree, select **Device Tree > Server > Application Server**, see Figure 2-8.
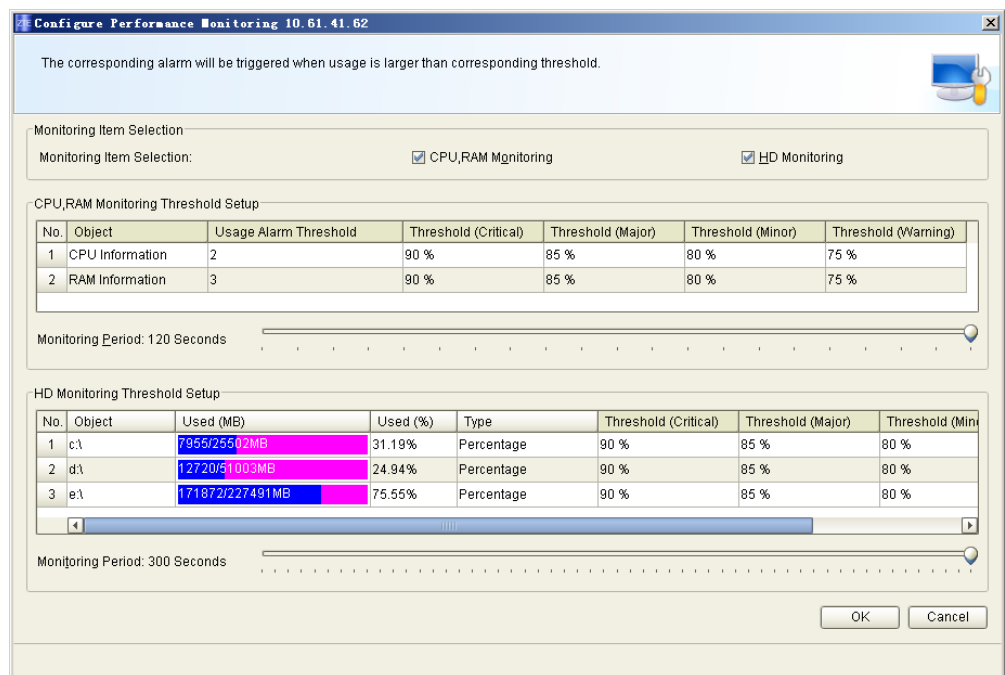
Figure 2-8 Monitoring Server Performance

2. Monitor the server performance.

   a. In the **Monitor Server Performance** pane, click **Configure**. The **Configure Performance Monitoring** dialogue box appears, see Figure 2-9.

Figure 2-9 Configure Performance Monitoring Parameters

   b. Configure the monitoring items and threshold values, and then click **OK**.

3. View the server performance.

a. In the **View Server Performance** pane, click **View**. The **View Application Server Performance** dialogue box appears, displaying the current server performance information, including hard disk information, memory information, and CPU usage, see Figure 2-10.

Figure 2-10 View Application Server Performance
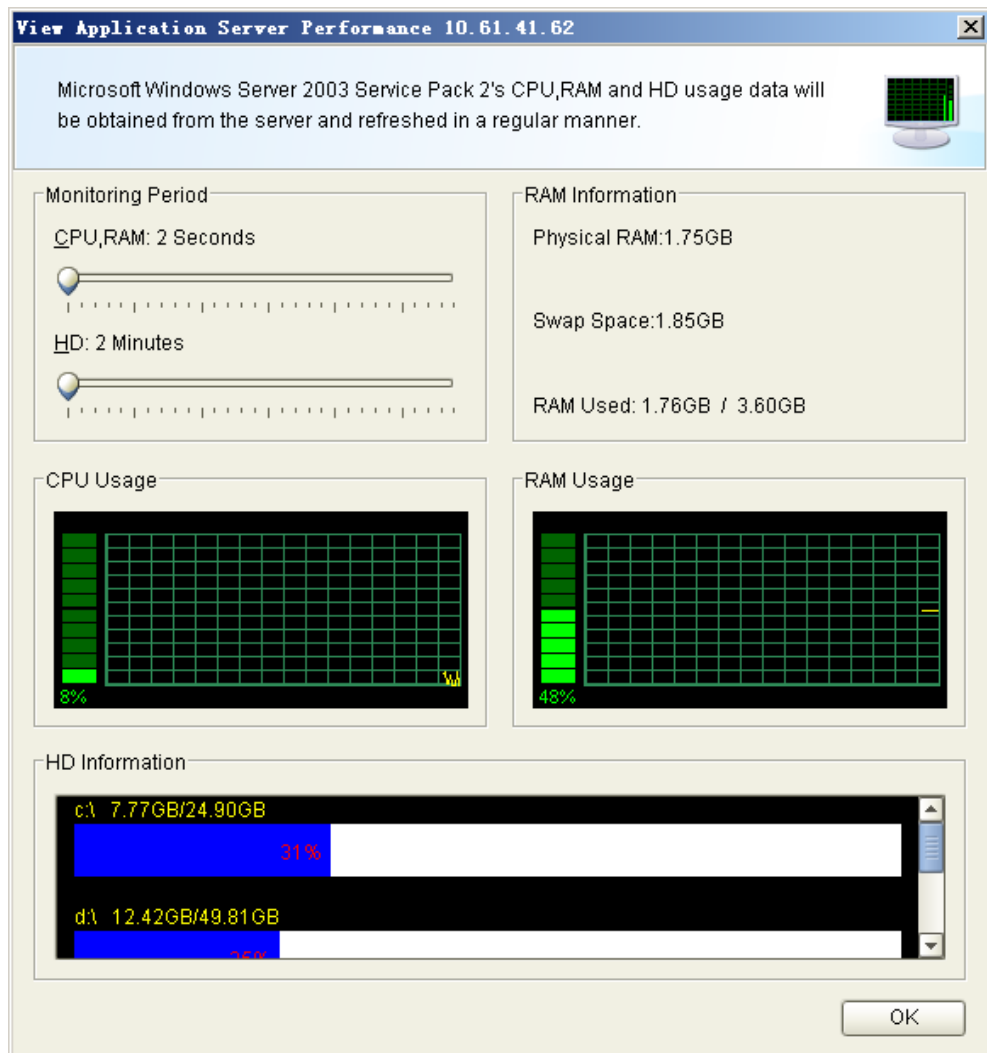
Monitoring Database Performance

1. In the **NetNumen U31 Unified Management System - Client** window, select **Maintenance > System Monitoring**. The **System Monitoring** window appears. In the left navigation tree, select **Device > Database > SQLServer**, see Figure 2-11.

Take SQL database as an example.

Figure 2-11 Monitoring Database Resource
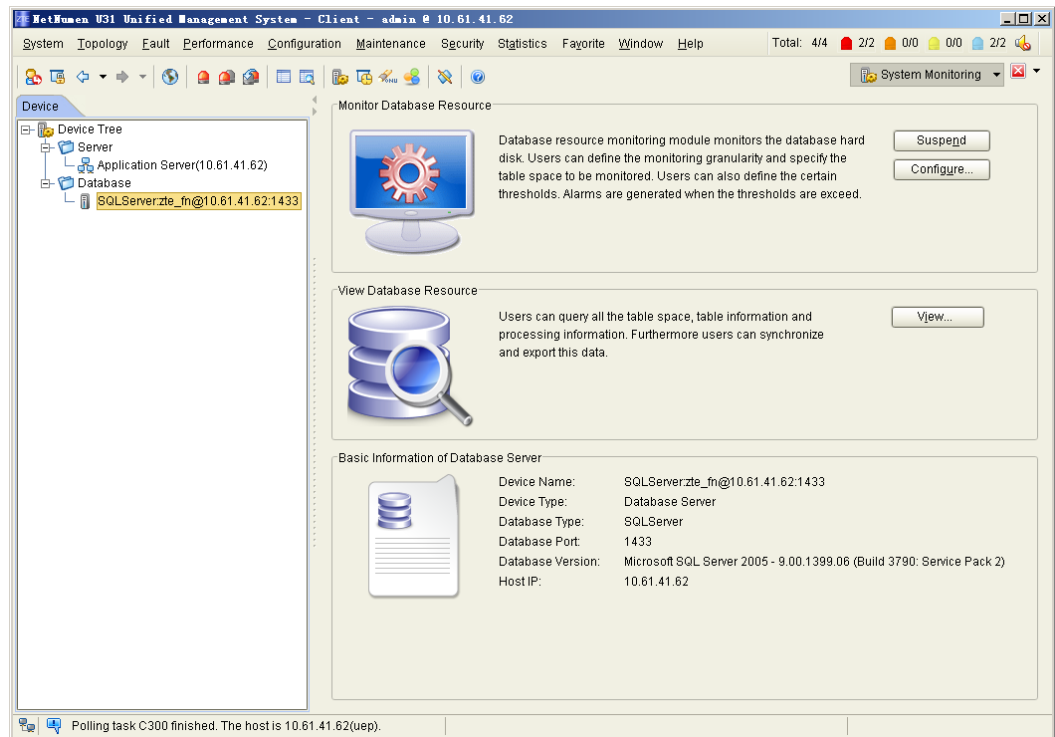
2. Monitor database resources.

    a. In the **Monitor Database Resource** pane, click **Configure**. The **Configure Database Monitoring** dialogue box appears, see Figure 2-12.

Figure 2-12 Configure Database Monitoring Parameters

b. Configure monitoring items, monitoring period, and alarm threshold value, and then click **OK**.

3. View database resources.

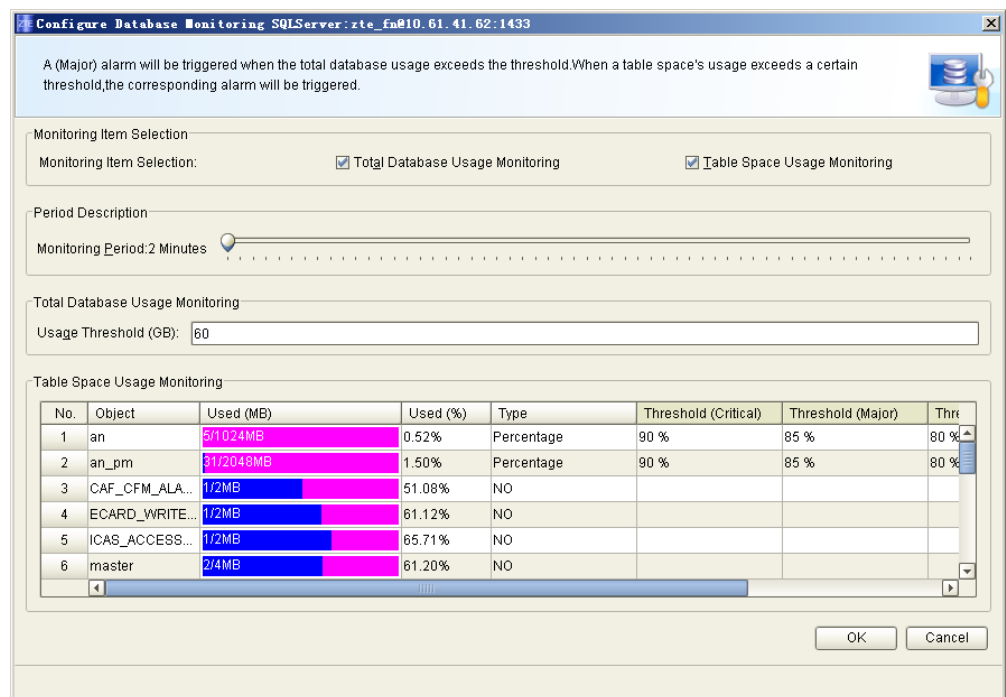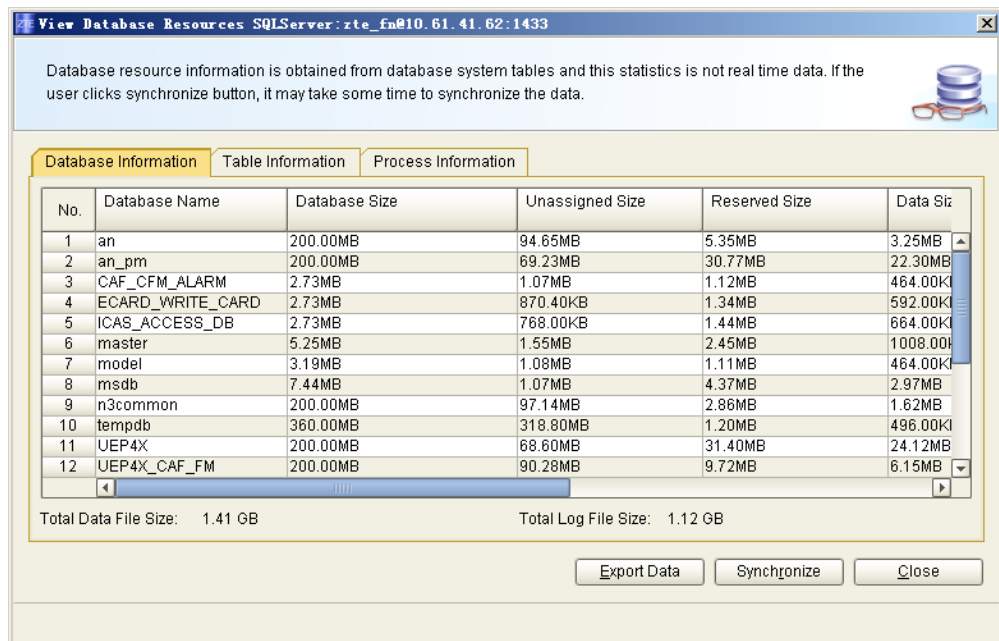a. In the **View Database Resource** pane, click **View**.   The **View Database Resources** dialogue box appears, see Figure 2-13.

Figure 2-13 View Database Resources

b. The **View Database Resources** dialogue box displays the database information, table information, and process information. Click the desired tab to display the corresponding information.

c. (Optional) Click **Export Data** to save the database information of the current tab to the local drive as a file.

d. (Optional) Click **Synchronize** and the system will synchronize the data and display the latest database information.

2.3.4 Detecting Virus

Perform this procedure to detect virus.

Prerequisites

Before virus check, make sure that antivirus software has been installed on the server.

Context

Virus may cause problems or even paralysis of the server. Thus it is necessary to perform virus check periodically on the server.

2-18

Checking Methods

- Scan the system every week.

  The virus scan tools such as Norton Antivirus or MacAfee are recommended. They can scan virus periodically and update periodically.

- Do not use the floppy disk drive or CD drive to perform read or write operations which are irrelevant to maintenance.
- Make sure the floppy disk or CD is free of virus if you have to use it on the PC.

Result

No virus exists or virus is killed.

This page intentionally left blank.

ZTE Proprietary and Confidential

Chapter 3
Data Backup and Recovery

Table of Contents

3.1 Configuring FTP Services

FTP accounts refer to the FTP users that access the NMS. They are used for the FTP transmission of the configuration file and version file between the NEs and NMS. For example, the configuration data backup policy needs to back up the configuration files in FTP mode. The NMS server works as the FTP server to provide the FTP services.

There is a default FTP server on the NetNumen. There is no need to modify the configuration for NE routine maintenance. If it is required to modify the FTP account, the FTP server configuration should be modified.

Prerequisites

- The network management server is running properly.
- The **NetNumen U31 Unified Management System-Console** window is closed.

Steps

1. Open the **NetNumen U31 Unified Management System-Configuration Center** window.

   Take Windows operating system as an example.

   Select **Start > Programs > NetNumen U31 Unified Management System > U31 Config Center**. The **NetNumen U31 Unified Management System-Configuration Center** window appears.

2. In the left navigation tree, select **Configuration Center > Product Configuration > Wireline Common Configuration > FTP/SFTP Service** to display the FTP/SFTP configuration parameters in the right pane, see Figure 3-1.

   When the NMS server works as the FTP server, different NE has different FTP main directory, user name and password.

   If **Use Outside FTP Server** is selected, make sure all the users in the list are configured for the FTP services.

3-1

Figure 3-1 FTP/SFTP Configuration Parameters
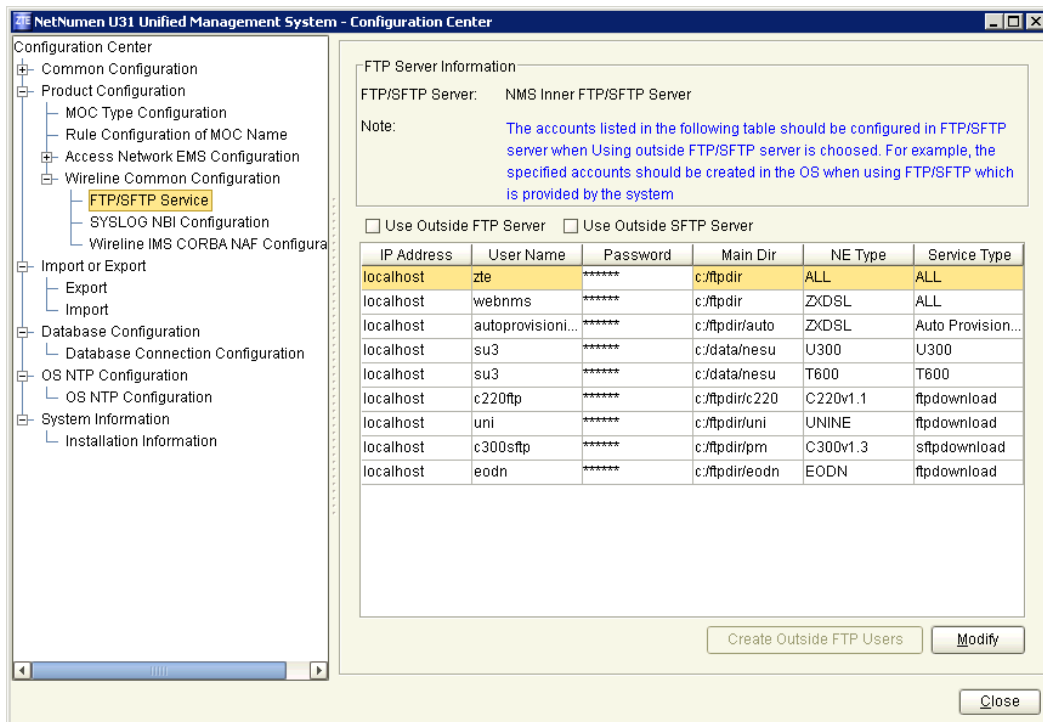
NOTE **Note:**

● Windows: It is recommended to use the FTP service provided by the NMS Server.

● Solaris: It is recommended to use the FTP service provided by Solaris.

3. Configure the FTP parameters.

a. Select one NE type, and click **Modify**. The **Modify FTP/SFTP User** dialogue box appears, see Figure 3-2.

Figure 3-2 Modify FTP/SFTP User Dialogue Box

Note:

● When you are uploading or downloading the version files, the NMS lists all the files under the FTP user directory according to the settings on the configuration center, and then sends commands to the NE. If the path defined in **NetNumen U31 Unified Ma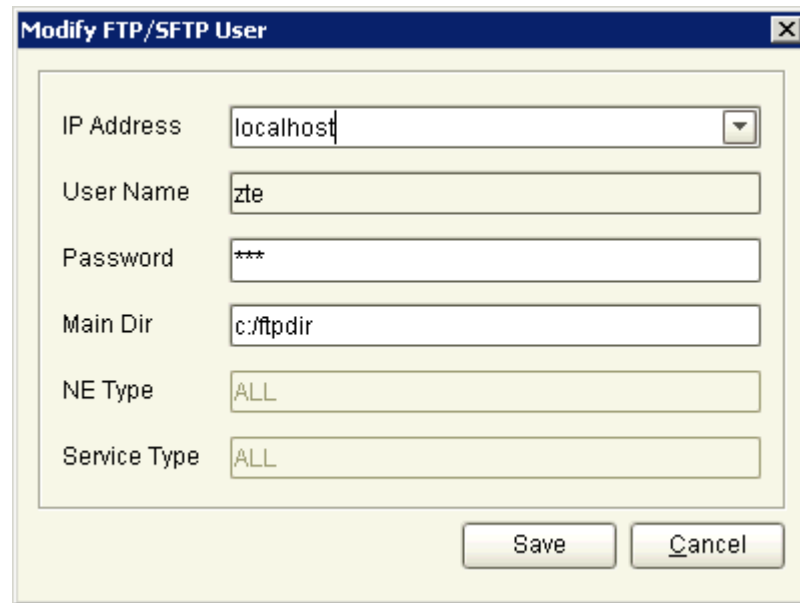nagement System-Configuration Center** window is inconsistent with that corresponds to the FTP user, the version file cannot be uploaded or downloaded.

● When multiple IP addresses are configured on the NMS Server, you need to change the IP address of the FTP user and select the IP address that connects to the NE device, to ensure correct FTP operations.

b. Modify the FTP server parameters, and then click **Save**.

4. In the **NetNumen U31 Unified Management System-Configuration Center** window, click **Close**.

3.2 NE Data Saving

3.2.1 Saving NE Data in Real Time

ZXA10 C320 supports saving NE data to the Flash through NMS.

Prerequisites

The NMS manages NEs properly.

3-3

Steps

1. In the topology view of the **NetNumen U31 Unified Management System - Client** window, right-click the ZXA10 C320 NE, and select **System Management > Save Configuration Data**. The **Save Configuration Data** dialogue box appears.
2. Click **Save**, and the system starts to save the data.
3. The system shows it is successful to save the data. Click **Close**.

3.2.2 Saving NE Data Periodically

ZXA10 C320 supports the configuration of the NE data periodical saving policy through the NMS, and the system executes the policy to save the NE data periodically.
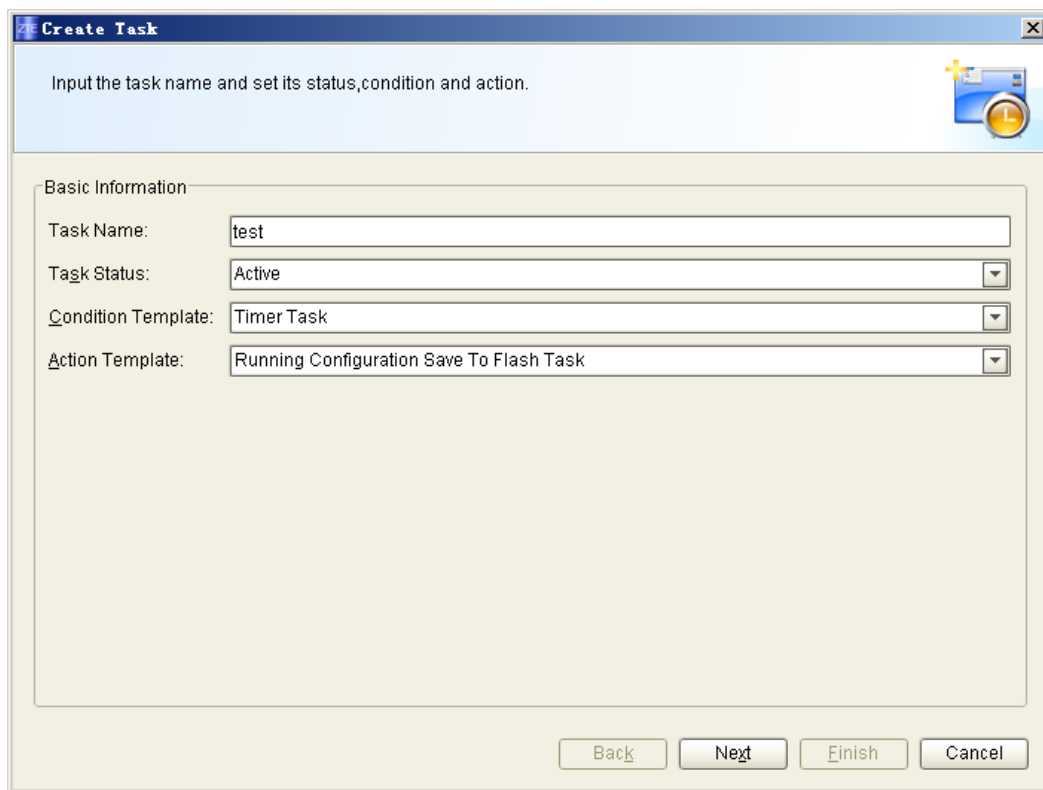
Prerequisites

The NMS manages NEs properly.

Steps

1. In the **NetNumen U31 Unified Management System - Client** window, select **Maintenance > Task Management**. The **Task Management** view appears.
2. In the left navigation tree, select **Task Management > Access Network Task > Running Configuration Save To Flash Task** to open the corresponding policy configuration window, see Figure 3-3.

Figure 3-3 Running Configuration Save To Flash Task Window
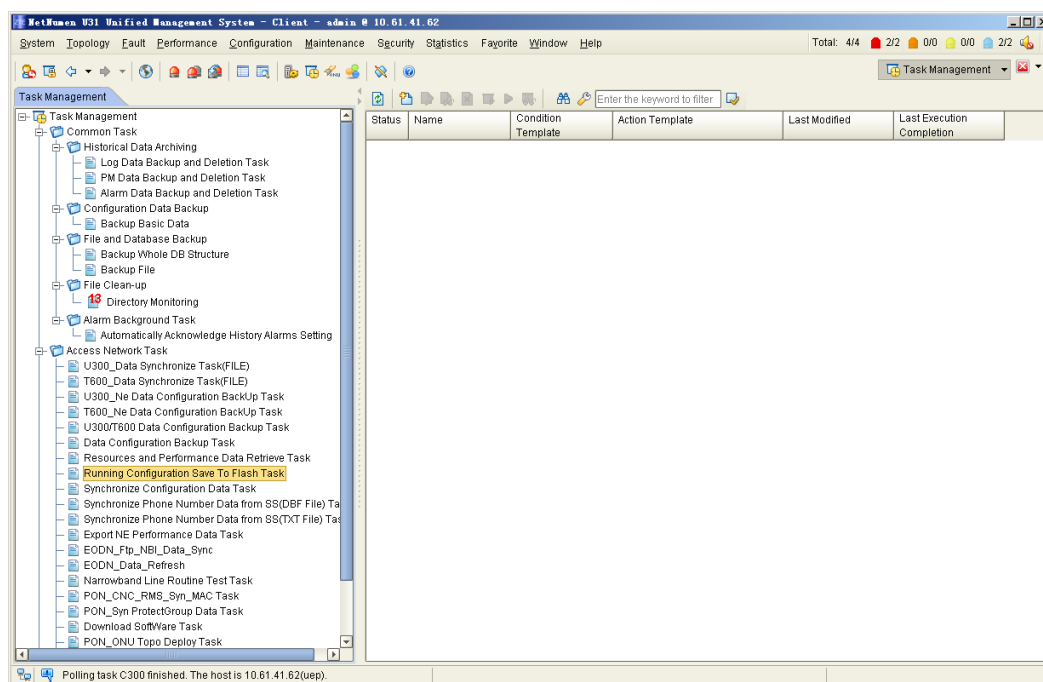
3. Click to open the **Create Policy** window. Specify the policy name, policy status, condition template, and action template, see Figure 3-4. Click **Next**.

Figure 3-4 Specifying the Policy Basic Information

4. Specify the plan type, task start time, execution time, and duration, see Figure 3-5. Click **Next**.

Figure 3-5 Specifying the Policy Time Condition
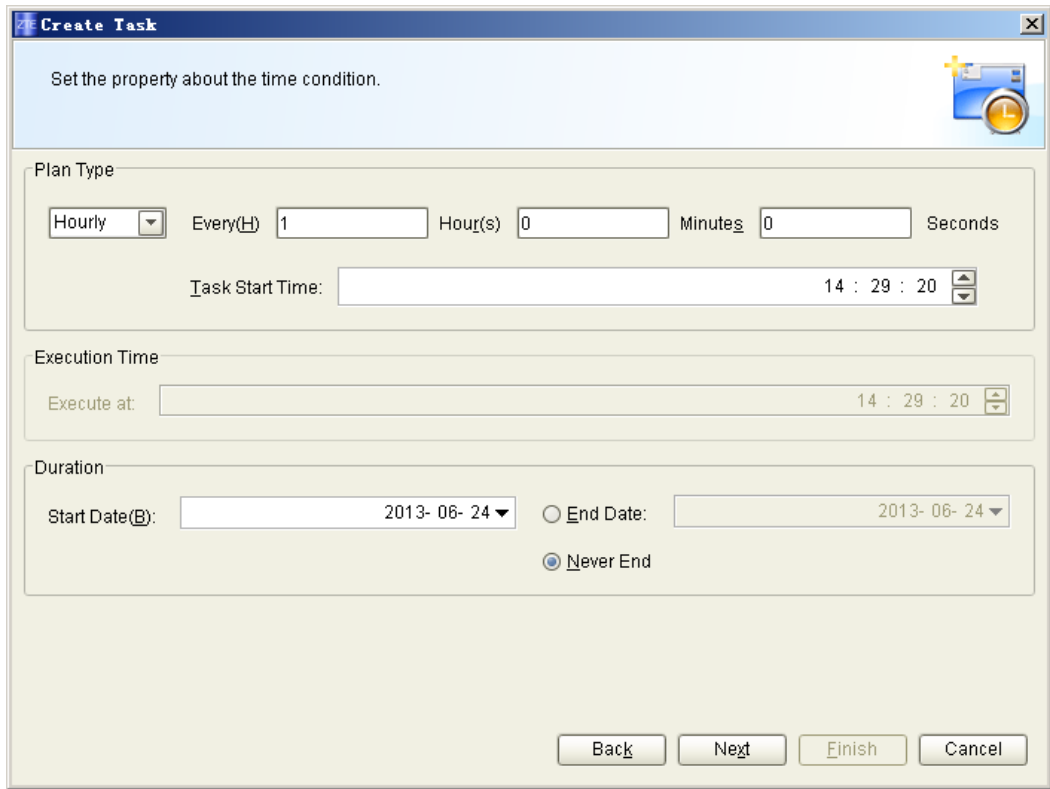
5. Specify the NE type to execute the policy, see Figure 3-6.

Figure 3-6 Specifying the NE Type for the Policy
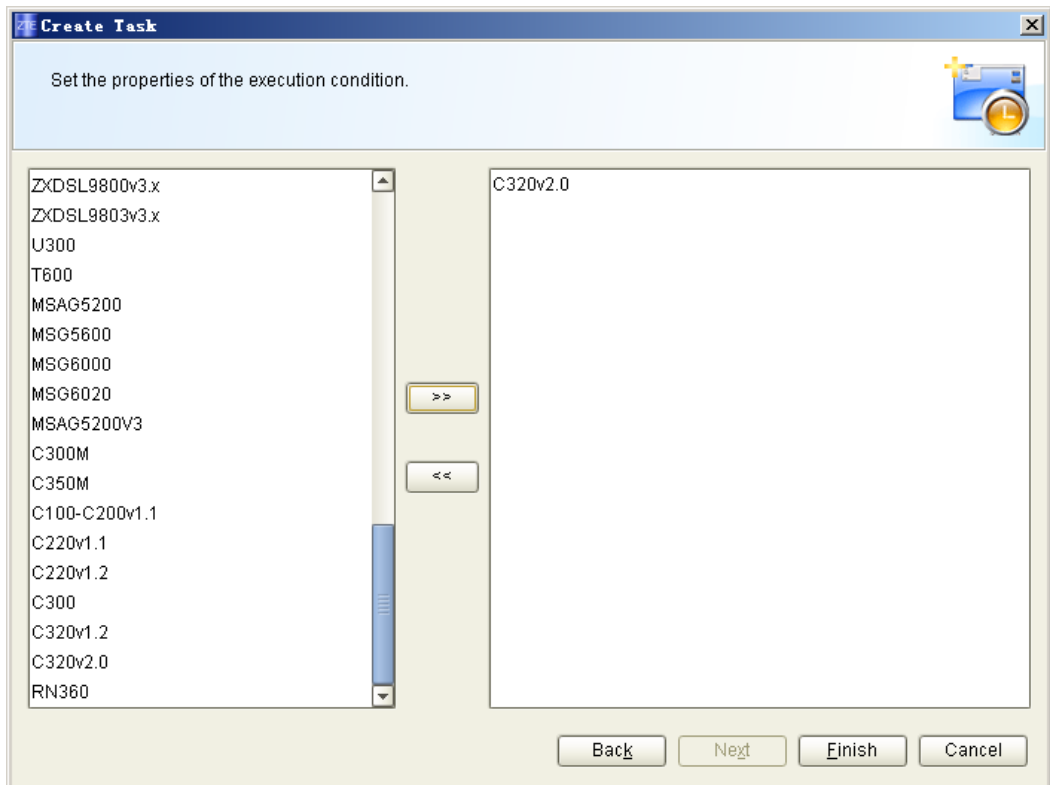
6. Click **Finish** to finish creating the policy.

3.3 NE Data Backup

3.3.1 Backing Up NE Data in Real Time

ZXA10 C320 supports backing up the NE data to the specified directory of the NMS server. The backup data can be restored in case there is any data loss or error.

Prerequisites

The NMS manages NEs properly.

Steps

1. Open the **Backup/Restore Configuration File** window.

   In the **NetNumen U31 Unified Management System - Client** window, right-click the ZXA10 C320 NE and select **System Management > Backup/Restore NE Configuration Data**. The **Backup/Restore Configuration File** window appears, see Figure 3-7.

   Figure 3-7 Backup/Restore Configuration File Window
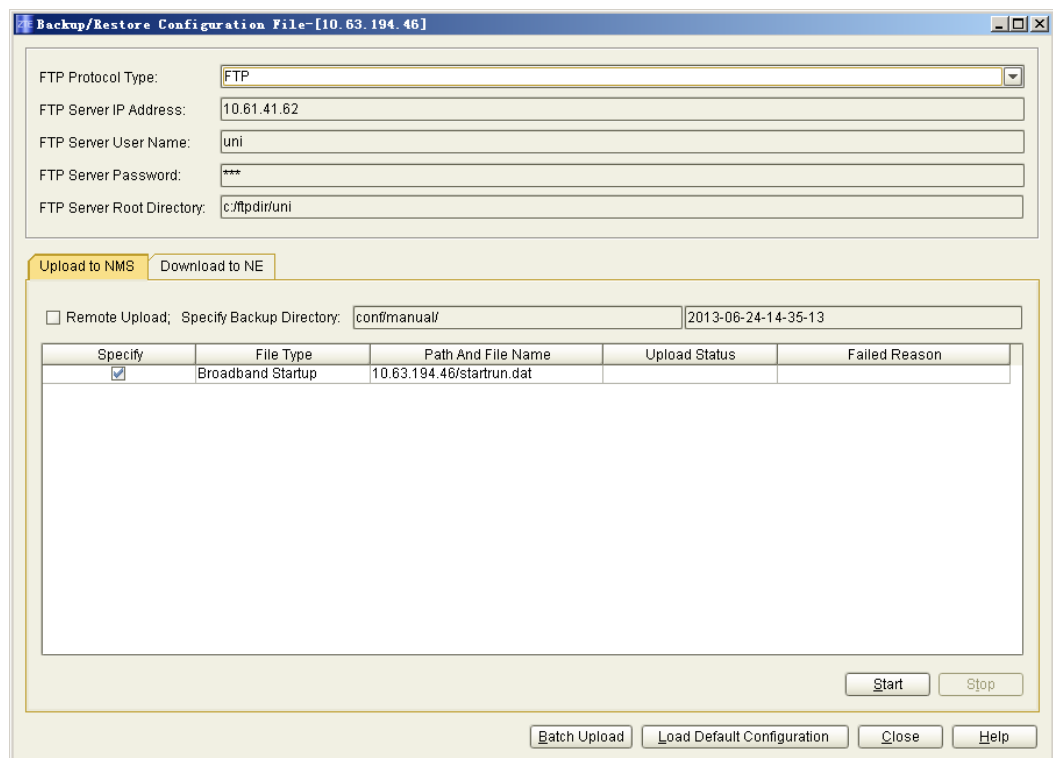
2. Back up the NE configuration files to the specified directory of the NMS server.

   a. On the **Upload to NMS** tab, select the files to upload, and then click **Start** to back up the NE configuration files to the backup directory of the FTP server.

NOTE **Note:**

- Select **Remote Upload**, and upload the NE configuration files to the root directory of the FTP server
- Click **Batch Upload** to back up the NE configuration files of multiple NEs.

b. After the uploading, the **Upload Status** column shows whether the upload process is successful or not.

3.3.2 Backing up NE Data Periodically

ZXA10 C320 supports the configuration of the NE data periodical backup policy through the NMS, and the system executes the policy to back up the NE data periodically.

Prerequisites

The NMS manages NEs properly.

Steps

1. Open the **Task Management** view.

    In the **NetNumen U31 Unified Management System - Client** window, select **Maintenance > Task Management**.

2. Configure the policy parameters to backup the NE data.

    a. In the left navigation tree, select **Task Management > Access Network Task > Data Configuration Backup Task** to open the corresponding policy configuration window, see Figure 3-8.

Figure 3-8 Data Configuration Backup Task Window
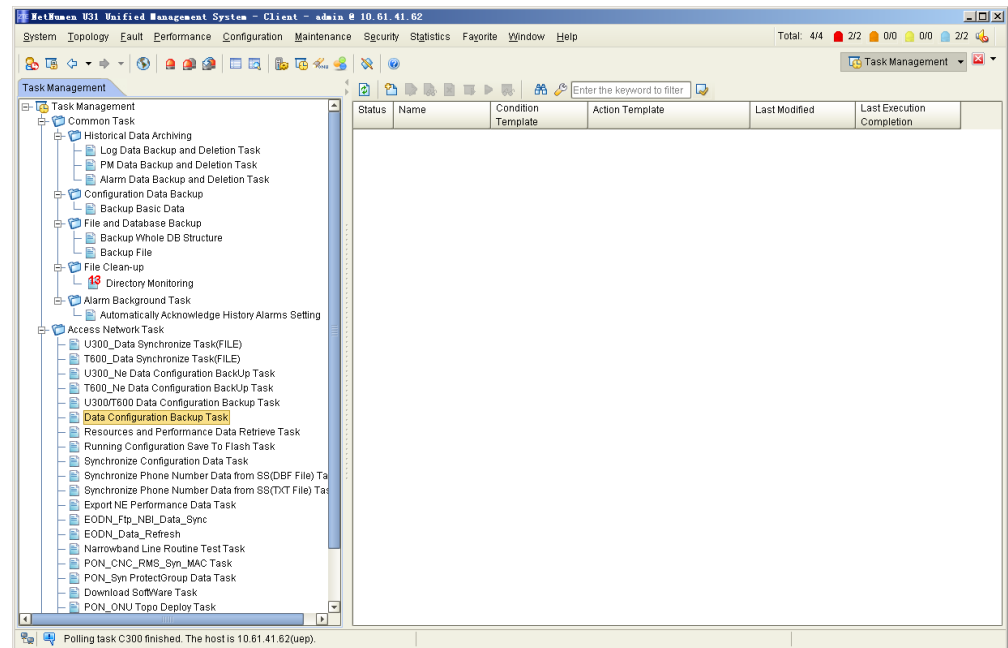
b. Click ![icon] to open the **Create Policy** window. Specify the policy name, policy status, condition template, and action template, see Figure 3-9. Click **Next**.

**Figure 3-9 Specifying the Policy Basic Information**

c. Specify the plan type, task start time, execution time, and duration, see Figure 3-10. Click **Next**.

3-9

Figure 3-10 Specifying the Policy Time Condition
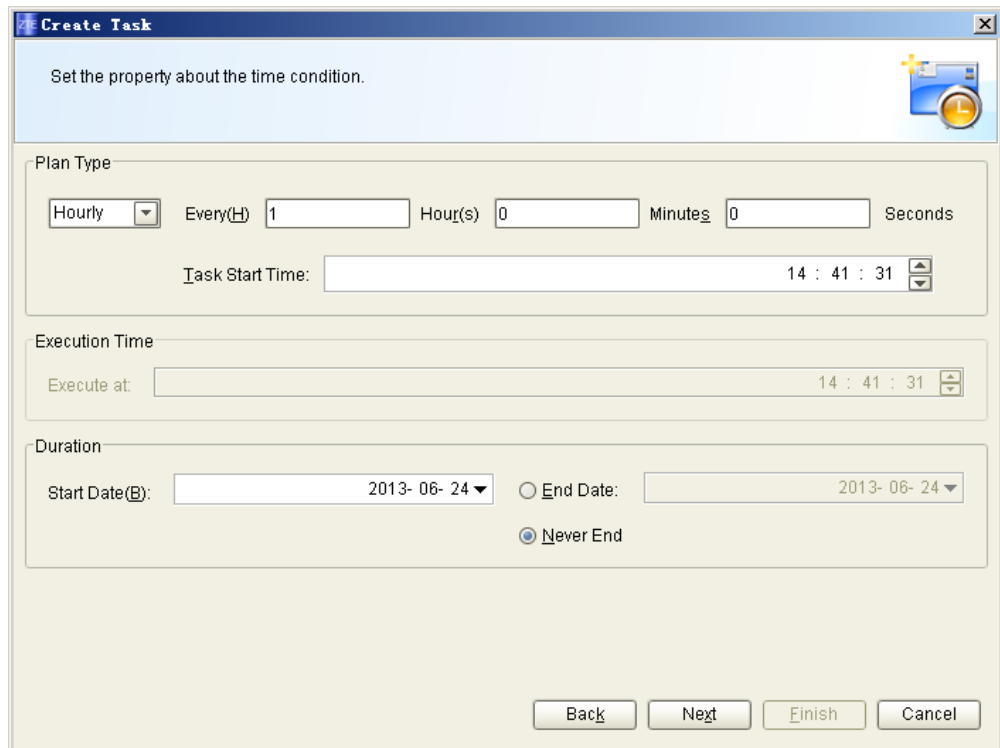
d. Specify the NE type to execute the policy, see Figure 3-11. The **Home Directory** shows the directory to save the backup data in the NMS server.

Figure 3-11 Specifying NE Type for the Policy
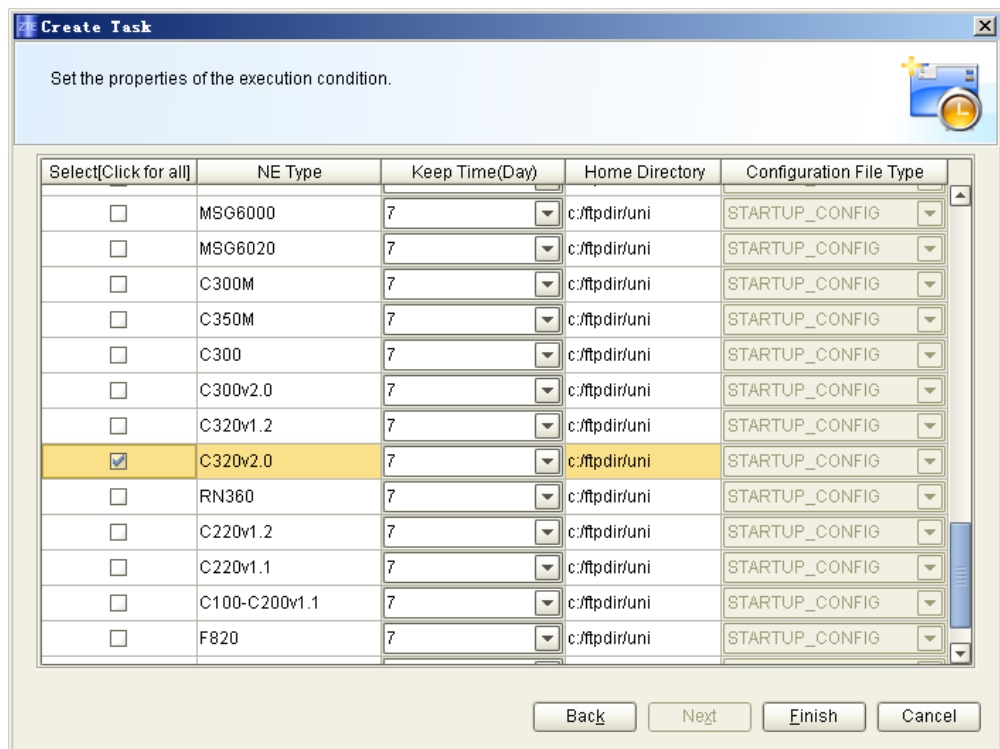
e.   Click **Finish** to finish creating the policy.

3.4 Restoring NE Data

ZXA10 C320 supports restoring the specified NE data. This implementation of the operation must be approved by the operator, and carried out cautiously. Incorrect operations might cause error data and affect the services.

Prerequisites

● The NE data is backed up.
● The NMS manages NEs properly.

Steps

1. Open the **Backup/Restore Configuration File** window.

   In the **NetNumen U31 Unified Management System - Client** window, right-click the ZXA10 C320 NE and select **System Management > Backup/Restore NE Configuration Data**. The **Backup/Restore Configuration File** window appears.

2. Download files to NE.

   a.   On the **Download to NE** tab, select the files to download, and click **Start** to download the files to the NE.

   b.   After downloading, the **Download Status** column shows the downloading process is successful, see Figure 3-12.

   Figure 3-12 Downloading Files to NE
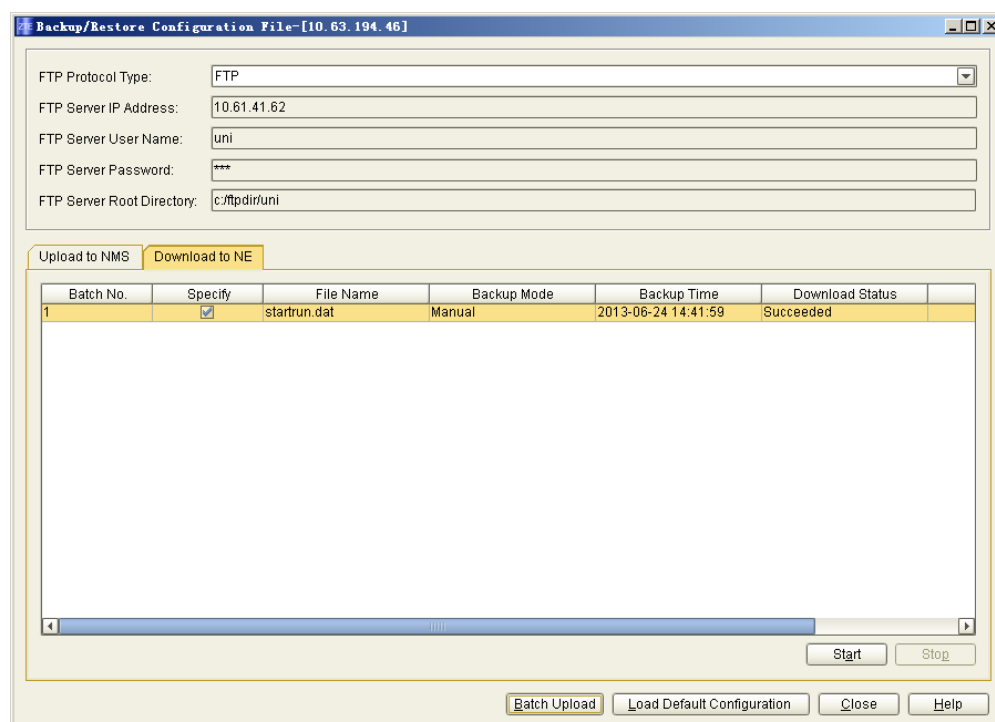
3.5 Performing Active/Standby Card Changeover

ZXA10 C320 can be equipped with two control and switching cards in active/standby mode. When the active control and switching card is faulty, you can perform the active/standby card changeover, and the standby control and switching card takes the responsibility of service control and data processing. In this way, you can ensure the related services are normal.

Prerequisites

The standby card is working normally.

Steps

1. In the **NetNumen U31 Unified Management System - Client** window, right-click the ZXA10 C320 NE and select **System Management > Reset/Swap Card**. The **Reset/Swap Card** dialogue box appears, see Figure 3-13.

   Figure 3-13 Reset/Swap Card Dialogue Box
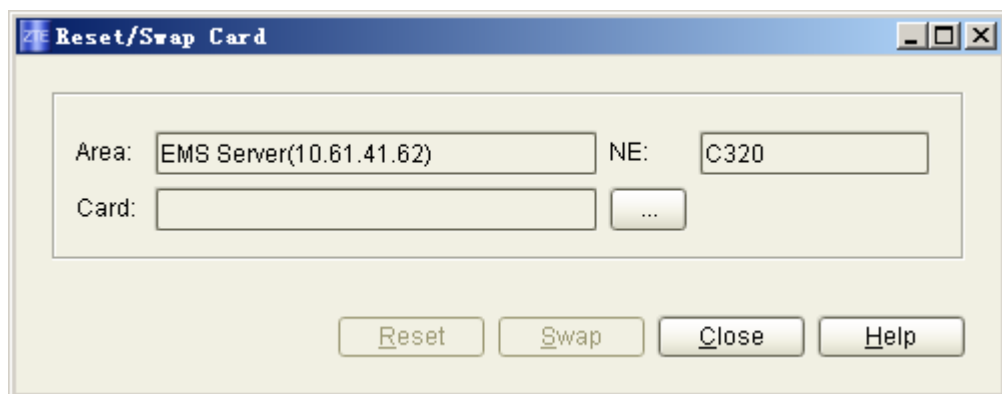
2. Click [...]. The **Select Card** dialogue box appears, see Figure 3-14. Select the control and switch card, and click **OK**.

Figure 3-14 Select Card Dialogue Box
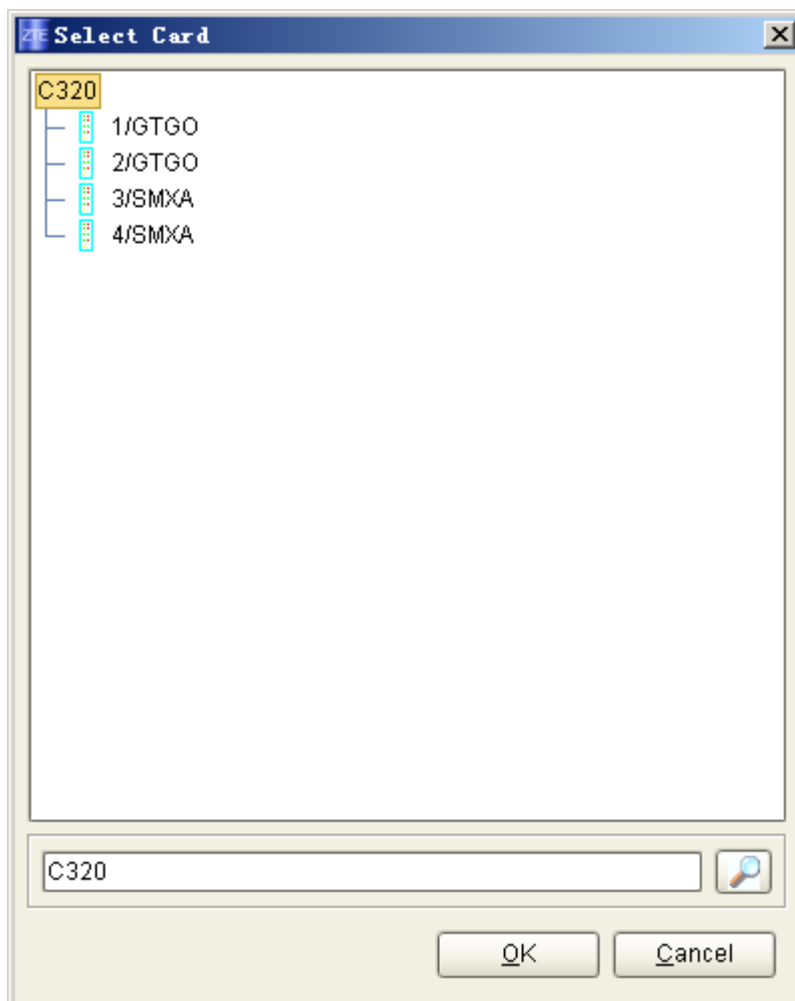
3. In the **Reset/Swap Card** dialogue box, click **Swap**.
4. The **Confirm** dialogue box appears. Click **Yes** to start active/standby card change-over.

This page intentionally left blank.

Chapter 4
Expansion Guides

Expansion Definition

Expansion is to expand the system capacity on the basis of the existing hardware resources and software resources in order to meet the operator's requirements for service expansion.

Expansion Flow

Figure 4-1 shows the expansion flowchart.

Figure 4-1 Expansion Flowchart
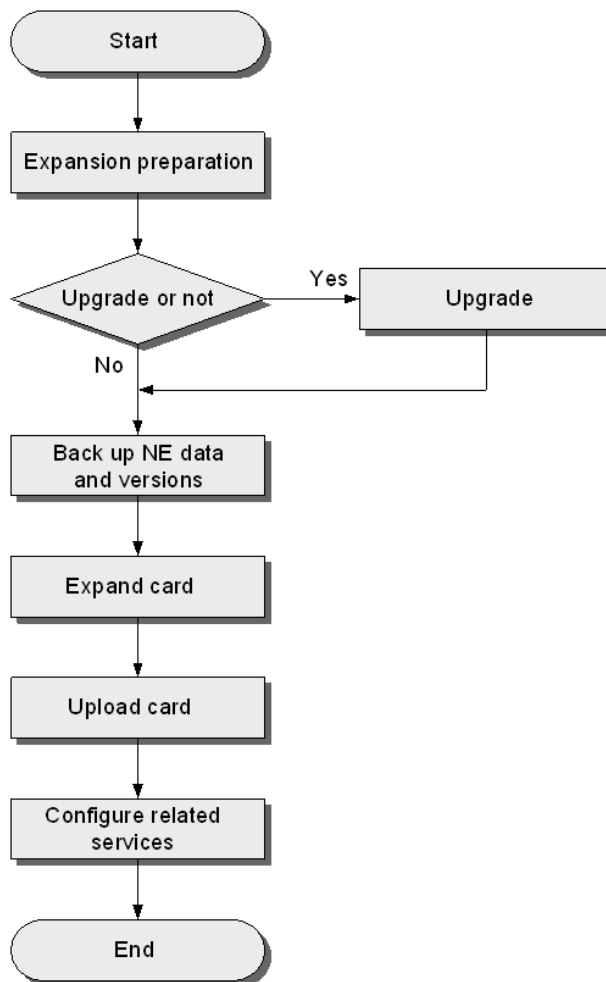
Before the expansion, make sure that the optical resources are enough for the expansion. If the resources are not sufficient, negotiate with the operator. Otherwise, the service can not be available even the expansion is completed.

To expand the capacity, perform the following steps:

1. Confirm the NE version.

   If the NE version is compatible, perform the next step directly. If the NE version needs to be upgraded, upgrade the NE version first.

2. Back up NE data and the software versions.
3. Expand a card.

   Cooperate with the operator' personnel and the construction personnel to install the device and give necessary installation guidance. Pay attention not to damage the pins on the backplane or other components.

NOTE
Note:

You need to wear the anti-static wrist strap.

You need to be more careful with the fiber pigtail and power.

---

4. Upload a card.

   If you are at the locale, you can connect the device through the serial port. Use the command to add a card. If you are not on site, you can add a card on the NMS remotely.

5. Lay out the fiber tails by cooperating with the operators' personnel and the construction personnel. If the site is not available for expansion, the operators can arrange other time for the layout.
6. Configure the related services as required.

Processing Guides for Expansion Failure

If the card fails to work properly after expansion, perform the following steps:

1. Pull out the card, and add it once more.
2. If the card still fails to work, change another slot and insert the card again.
3. If the card still fails to work, replace the card. If the new card can work, the previous card is faulty. Return the faulty card for repair.

NOTE
Note:

Before performing these operations, you need to make sure that your operations will not affect the service. You cannot restart the NE or perform any operation which may affect the service if you have not obtained the technical support or the approval from the service provider.

Chapter 5
Cutover Guides

Cutover Definition

Cutover is to replace a device which is currently running in the network with a new one in the period with the minimum service traffic. The service is transmitted to the new one smoothly. Cutover is often used to handle faults, update devices, promote new services, and optimize the network structure.

NOTE **Note:**

If the service cannot be transmitted from the old device to the new one, it is necessary to switch the service back to the old device immediately and ensure the service can be restored in a certain period.

Cutover Flow

Figure 5-1 shows the cutover flowchart.

Figure 5-1 Cutover Flowchart
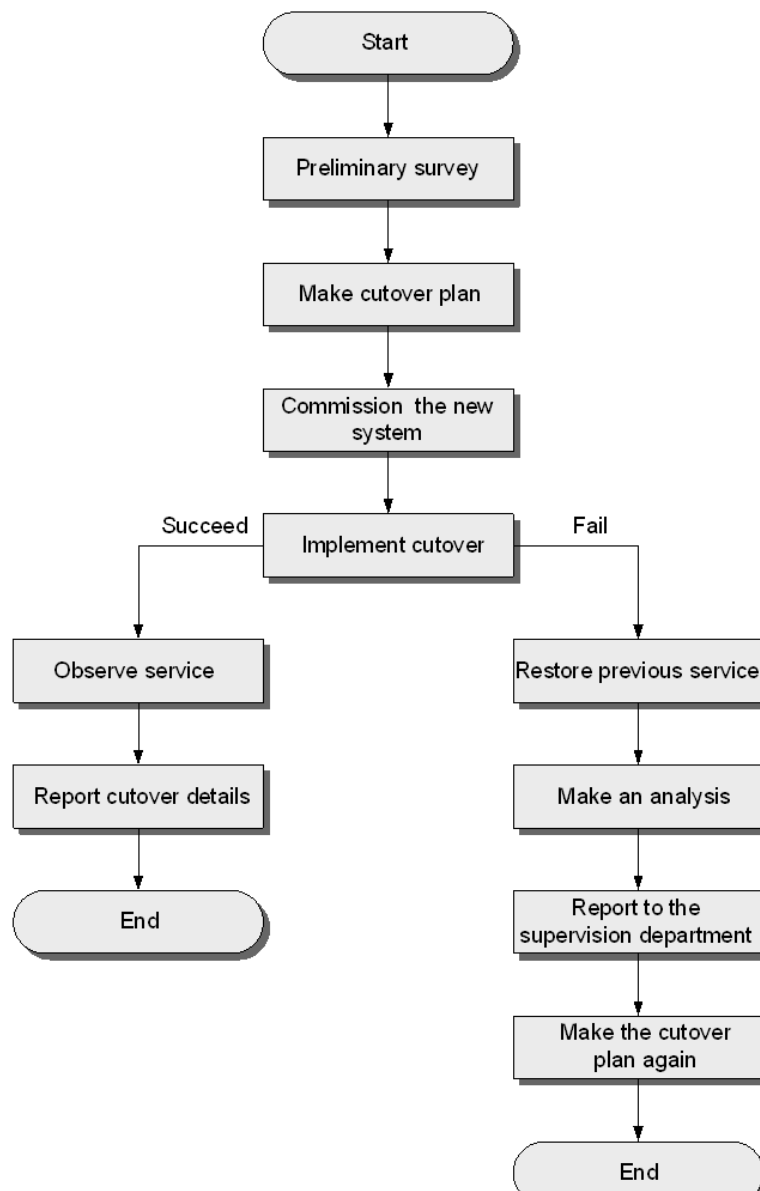
Make the following preparations before the cutover:

● Arrange the personnel properly.

→ Considering the large traffic of the ZXA10 C320, it is recommended to arrange two groups of personnel. One group goes to the locale for on-site operation. The other group stays at the operator's NMS center for support.

→ The personnel from the operator's related departments, such as transmission department, power supply department, and the related upper-layer equipment provider, also need to be on site. If they cannot be on site, they need to provide technical support in time.

● Prepare enough spare parts.

5-2

The previous device needs to be powered off and removed. If the cutover fails, the service will be restored to the previous system. A fault may occur when the previous system is powered on again. Therefore, it is necessary to prepare enough spare parts for the previous system.

- Back up data.

  Backup the data on the previous system, ensuring that the data is the latest.

Perform the following steps to carry out the cutover:

1. Preliminary survey
   - Communicate with the technicians from other related equipment manufacturers. Make sure the purpose and the significance of the cutover. Cutover is not the best choice if there are other easier methods to deal with the existing problems.
   - Do the on-site survey thoroughly. Confirm that the conditions for hardware installation, the optical line resources (for uplink and downlink) and the upper-layer device resources are sufficient.
   - Fully know about the detailed networking situation of the cutover service.
   - Specify the related departments and supervisors for each node in the network concerned.

⚠ **Caution!**

Any unauthorized or illegal operation is not allowed. The execution of any plan and the processing of unexpected events must be implemented with the formal approval of the operator and the technical support.

2. Make cutover plan.

   a. Draft a cutover plan according to the network situation of actual services.

   b. Urge the operator's supervision department to organize the related departments and their supervisors at each node in the network to attend a meeting for discussing the draft. Record all the opinions from every department and the related precautions for actual operation in detail.

   c. Work out the start and end time of installing the new device, debugging software and testing the system. Decide the time for cutover.

   d. After determining the cutover plan, apply for the approval of the higher authority.

3. Commission new system.

   a. Perform the commissioning work on the new system.

   b. Implement the simulated test according to the features of the online services to ensure that the online services can run properly after being transit to the new equipment.

4. Implement cutover.

a. Determine the time of starting the cutover.

b. Inform the R&D department and the customer service department of the specific time and other related events for cutover to get timely technical support in case of any unexpected fault.

c. Remind the operator to notify each branch office where the lower-layer ONU locates of the specific cutover time. Therefore, they can timely inform the users of the service interruption in a certain period, and the terminal users can make the corresponding preparations to avoid any loss.

Work After Cutover

If the cutover succeeds, confirm the following:

- Ping the ZXA10 C320 from the NMS. Check whether it succeeds.
- Check whether the port status and traffic are normal.
- Check whether the ONU is already online.
- Check whether the MAC address of the user can be learnt.

Observe the service running status after the cutover succeeds. Report the cutover details to the supervision department. Keep the previous equipment on site. The service can be restored to the previous system in case of any accident.

If the cutover fails, restore the service back to the previous system in the specified period. Send the faults, alarms and data to the technical engineers for analysis.

Processing Guides for Cutover Failure

- Precautions

  → In principle, the service interruption must be within the period that the service provider permits.

  → It is recommended to restore the services to the previous system if the cutover cannot be finished in the planned period due to unexpected reason.

  → The cutover cannot have influence on the network security and online services. Do not cut over all NEs at one time.

- Restoring Process

  → Observe LED status on cards and take a record.

  → Observe alarms on NMS and record alarms, especially service alarms. Avoid the same fault when restoring services.

  → Power on the previous system and have a check. Restore services after the system works properly.

  → Restore the services in sequence.

5-4

Chapter 6
Version Upgrade Guides

Table of Contents

6.1 Version Upgrade Instructions

Version Information

Table 6-1 lists the version files of the ZXA10 C320 cards.

Table 6-1 Version Files of ZXA10 C320 Cards

Card	BOOT Version	Software Version	Firmware Version
SMXA	SMXA.BT	SMXA.MVR	SMXA.FW
GTGOE	GTGOE.BT	GTGOE.MVR	GTGOE.FW
GTGOG	GTGOG.BT	GTGOG_LX.MVR	GTGOG.FW
GTGHG	GTGHG.BT	GTGHG_LX.MVR	GTGHG.FW
FTGKB	FTGKB.BT	FTGKB_LX.MVR	FTGKB.FW

Upgrading Precautions

The upgrading precautions are as follows:

- Because upgrading requires many cables, please be careful to connect each cable to the card properly, including the pins and directions.
- Abide by the upgrading flow to upgrade the BOOT chip. Upgrade the uplink card and the user card first, and then upgrade the main control card. If the BOOT chip of the main control is upgraded first, the BOOT files of other cards cannot be upgraded.
- Save and back up the data before upgrading.
- When upgrading BOOT chips, do not unplug the card with the power ON. Turn OFF the card first, thus to avoid the BOOT chips being burnt.

Upgrading Tools

- Laptop and upgrading program
- Crossover network cables

● Configuration serial port cable
● Upgrading software, such as FTP software.

Upgrading Preparations

The preparation for upgrading includes the following:

1. Make sure that the card status is proper.
2. Connect the **CLI** interface on the active control and switching card in the ZXA10 C320 to the laptop serial port. Keep the default values for the serial port configuration.
3. Use a cross cable to connect the **10/100M** interface on the active control and switching card with the computer network port (unplug the standby control and switching card first).
4. Configure the IP addresses of the debugging computer and the ZXA10 C320 in the same network segment. Ping the ZXA10 C320 address on the computer and if it succeeds, that means that the network connectivity is good. Otherwise, please close the firewall of the debugging computer and check the data configuration of the ZXA10 C320.
5. Configure the FTP software **Wftpd32.exe**.

   a. Copy the **Wftpd32.exe** file to the FTP server.

   b. Run the **Wftpd32.exe** program. The **No log file open** window appears, see Figure 6-1.

Figure 6-1 No Log File Open Dialogue Box
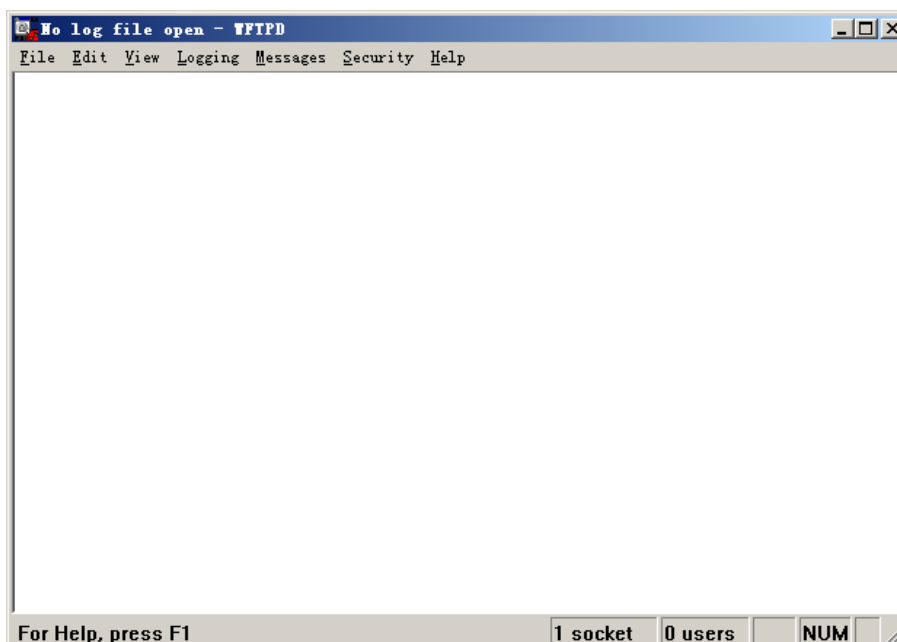
   c. Select **Security > Users/rights...** The **User/Rights Security** dialogue box appears, see Figure 6-2.

6-2

Figure 6-2 User/Rights Security Dialogue Box
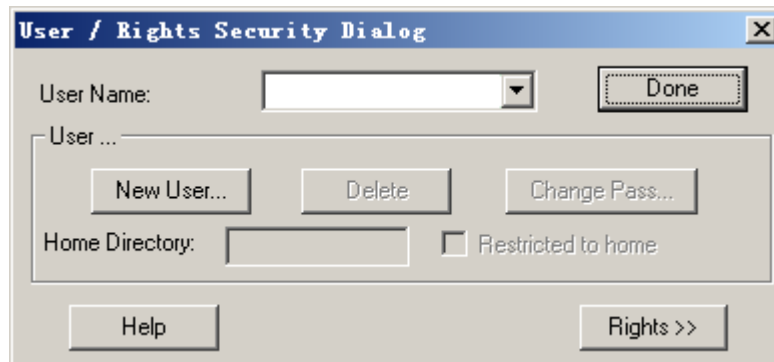
d. In the **User/Rights Security** dialogue box, click **New User...**. The **New User** dialogue box appears, see Figure 6-3.

Figure 6-3 New User Dialogue Box
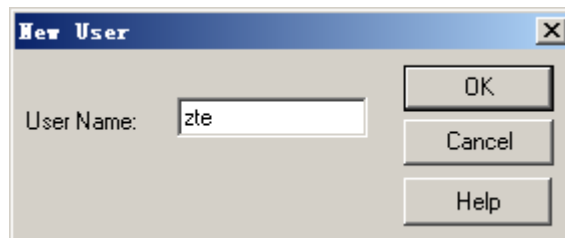
e. Set the **User Name** and click **OK**. The **Change Password** dialogue box appears, see Figure 6-4.

Figure 6-4 Change Password Dialogue Box

f. Set the password and click **OK**.

g. In the **User/Rights Security** dialogue box, enter `D:\` as the root directory in the **Home Directory** text box, see Figure 6-5.

6-3

Figure 6-5 User/Rights Security Dialogue Box
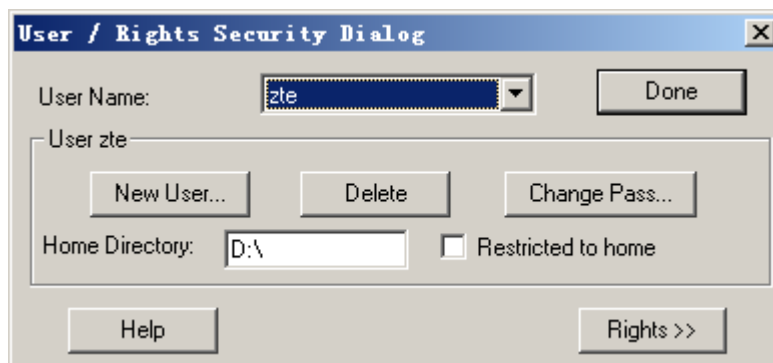
    h.   Click **Done**. The configuration is completed.

6.   Back up the NE data.

```
ZXAN#file upload cfg-startup startrun.dat ftp ipaddress 10.1.1.1 path \cfg
user zte password zte
```

7.   Back up the NE version files.

```
ZXAN#file upload version * ftp ipaddress 10.1.1.1 path \version user zte
password zte
```

8.   Configure the user name and the password of the FTP server on the ZXA10 C320.

```
ZXAN(config)#file-server boot-server ftp ipaddress 10.1.1.1 user zte
password zte
```

NOTE **Note:**

The user name and password should be the same as that configured in the **Wftpd32** software.

---

9.   Save the version files necessary for upgrading under home directory specified in the **Wftpd32** software.

6.2 Upgrading Versions

The ZXA10 C320 supports upgrading the version though the NMS and CLI mode.

This procedure introduces how to upgrade the version in CLI mode.

Prerequisite

- The version files for upgrading are saved under the specified directory when the FTP tool is configured.
- The FTP services on the ZXA10 C320 device have been configured.
- The NE data of the ZXA10 C320 device has been backed up.

● The NE to be upgraded must not have any major alarm, otherwise it may influence the upgrade. If there is any, clear the fault first and then upgrade the NE.

Steps

1. Download version files.

```
ZXAN#file download version smxa.bt        //Download a file.
Downloading from host(10.1.1.1)
Transfering file SMXA.BT ...
........Successfully
Synchronizing file smxa.bt to slave board...
.............Successfully

ZXAN#file download version *        //Download all version files.
```

2. (Optional) Synchronize version file to the active control and switching card to the standby control and switching card.

```
ZXAN#file sync version
```

NOTE
Note:

If the standby card is in the standby status, the version is automatically synchronized to the standby card.

---

3. View downloaded version files.

```
ZXAN#show version-saved master
PhyLoc FileName   VerType VerTag        BuildTime        Length   Active
--------------------------------------------------------------------------------

1/1/4  bsp.mvr    MVR     v1.0          2012-09-27 10:16:13 1212669
1/1/4  gtghg.bt   BT      V4.0.0        2013-01-30 16:54:16 524288
1/1/4  gtghg.fw   FW      V2.0.0P1      2013-09-23 01:14:49 78842
1/1/4  gtghg.mvr  MVR     V2.0.0P1      2013-09-23 01:14:48 4939176
1/1/4  gtgoe.bt   BT      V1.2.0P1      2012-10-24 14:17:00 387020
1/1/4  gtgoe.fw   FW      V2.0.0P1      2013-09-23 01:52:53 4298811
1/1/4  gtgoe.mvr  MVR     V2.0.0P1      2013-09-23 01:52:53 1886523
1/1/4  gtgog.bt   BT      V4.0.0        2013-03-05 14:11:46 524288
1/1/4  gtgog.fw   FW      V2.0.0P1      2013-09-23 02:11:58 59946
1/1/4  gtgog.mvr  MVR     V2.0.0P1      2013-09-23 02:11:57 5193224
1/1/4  etgo.fw    FW      V2.0.0P1      2013-09-21 23:25:49 1427718
1/1/4  etgo.mvr   MVR     V2.0.0P1      2013-09-21 23:25:48 5009999
1/1/4  etgod.bt   BT      V1.2.0        2012-06-14 15:52:36 249604
1/1/4  pm.fw      FW      V2.0.0P1      2013-09-22 22:22:22 934
1/1/4  smxa.bt    BT      V4.0.0        2013-09-13  9:34:23 524288
```

6-5

```
1/1/4    smxa.fw      FW      V2.0.0P1          2013-09-23 07:34:25 492068
1/1/4    smxa0.mvr    MVR     V2.0.0P1          2013-09-12 07:02:00 13984601  0
1/1/4    smxa1.mvr    MVR     V2.0.0P1          2013-09-23 07:34:16 13989282  1


ZXAN#show version-saved slave
PhyLoc FileName    VerType VerTag          BuildTime        Length    Active
--------------------------------------------------------------------------------


1/1/3    bsp.mvr      MVR     v1.0            2012-09-27 10:16:13 1212669
1/1/3    gtghg.bt     BT      V4.0.0          2013-01-30 16:54:16 524288
1/1/3    gtghg.fw     FW      V2.0.0P1        2013-09-23 01:14:49 78842
1/1/3    gtghg.mvr    MVR     V2.0.0P1        2013-09-23 01:14:48 4939176
1/1/3    gtgoe.bt     BT      V1.2.0P1        2012-10-24 14:17:00 387020
1/1/3    gtgoe.fw     FW      V2.0.0P1        2013-09-23 01:52:53 4298811
1/1/3    gtgoe.mvr    MVR     V2.0.0P1        2013-09-23 01:52:53 1886523
1/1/3    gtgog.bt     BT      V4.0.0          2013-03-05 14:11:46 524288
1/1/3    gtgog.fw     FW      V2.0.0P1        2013-09-23 02:11:58 59946
1/1/3    gtgog.mvr    MVR     V2.0.0P1        2013-09-23 02:11:57 5193224
1/1/3    etgo.fw      FW      V2.0.0P1        2013-09-21 23:25:49 1427718
1/1/3    etgo.mvr     MVR     V2.0.0P1        2013-09-21 23:25:48 5009999
1/1/3    etgod.bt     BT      V1.2.0          2012-06-14 15:52:36 249604
1/1/3    pm.fw        FW      V2.0.0P1        2013-09-22 22:22:22 934
1/1/3    smxa.bt      BT      V4.0.0          2013-09-13  9:34:23 524288
1/1/3    smxa.fw      FW      V2.0.0P1        2013-09-23 07:34:25 492068
1/1/3    smxa0.mvr    MVR     V2.0.0P1        2013-09-23 07:34:16 13989282  1
1/1/3    smxa1.mvr    MVR     V2.0.0P1        2013-09-12 07:02:00 13984601  0
```

4.　Upgrade versions.

```
ZXAN#update-boot slotno 1
...................................................[Successfully]
ZXAN#update-boot slotno 2
.....................................................................
...............................[Successfully]
ZXAN#update-boot slotno 3
...........................................................[Successfully]
ZXAN#update-boot slotno 4
.......................................[Successfully]
```

5.　Save the configuration and reboot the NE.

```
ZXAN#write
Building configuration...
..[OK]
ZXAN#reboot
Confirm to reboot? [yes/no]:y
```

6.　View running versions.

```
ZXAN#show version-running
PhyLoc  FileType  VerType  VerTag     BuildTime           VerLength
-----------------------------------------------------------------------------
1/1/1   ETGO      MVR      V2.0.0P1   2013-09-21 23:25:48 5009999
1/1/1   PM        FW       V2.0.0P1   2013-09-22 22:22:22 934
1/1/1   ETGOD     BT       V1.2.0     2012-06-14 15:52:36 249604
1/1/2   GTGOE     FW       V2.0.0P1   2013-09-23 01:52:53 4298811
1/1/2   PM        FW       V2.0.0P1   2013-09-22 22:22:22 934
1/1/2   GTGOE     MVR      V2.0.0P1   2013-09-23 01:52:53 1886523
1/1/2   GTGOE     BT       V1.2.0P1   2012-10-24 14:17:00 387020
1/1/3   SMXA      MVR      V2.0.0P1   2013-09-23 07:34:16 13989282
1/1/3   SMXA      BT       V4.0.0     2013-09-13  9:34:23 524288
1/1/4   SMXA      MVR      V2.0.0P1   2013-09-23 07:34:16 13989282
1/1/4   SMXA      BT       V4.0.0     2013-09-13  9:34:23 524288
```

7. Check the equipment running status.

8. Check the service running status.

– End of Steps –

6.3 Upgrading Patches

The ZXA10 C320 supports updating the patches though the NMS and CLI mode.

This procedure introduces how to upgrade the patches in CLI mode.

Prerequisite

- The patch files for updating are saved under the specified directory when the FTP tool is configured.
- The FTP services on the ZXA10 C320 device have been configured.
- The NE data of the ZXA10 C320 device has been backed up.
- The NE to be upgraded must not have any major alarm, otherwise it may influence the upgrade. If there is any, clear the fault first and then upgrade the NE.

Context

The following upgrading steps are applicable for both local upgrading and remote upgrading.

Patch upgrading focuses on the service card or the control and switching card, and is irrelevant to the slot number.

Steps

Upgrade the patch file for the service card.

1. Download the patch file. (Take the GTGOE card as the example.)

> **NOTE** **Note:**
>
> Before the upgrading patch, you need to make sure that the service card is in INSERVICE status.

```
ZXAN##file download patch GTGOEV120P1T6_r2.pat
```

2. Upgrade the patch file.

```
ZXAN#patch active GTGOEV120P1T6_r2.pat
```

3. (Optional) Restart the card.

```
ZXAN#reset slotno 1
```

> **NOTE** **Note:**
>
> After the upgrading patch, it is usually not necessary to restart the card. About the card restarting, you can refer to the corresponding upgrade note for details.

Upgrade the patch for the control and switching card.

4. Download the patch file.

```
ZXAN##file download patch SMXAV120P1T6_r0.pat
```

5. Upgrade the patch file.

```
ZXAN#patch active SMXAV120P1T6_r0.pat
```

Check the patch details and the service running status.

6. Check the running versions.

```
ZXAN#show patch-running
```

7. Check the equipment running status.

8. Check the service running status.

– End of Steps –

6.4 Testing Upgrading Results

Perform this procedure to test upgrading result.

Prerequisite

Before the operation, make sure that the upgrading of all the cards are complete.

Context

The test content includes the following:

- Narrowband service
- Broadband service
- NM management
- ONU management

To test update result, perform the following steps:

Steps

1. To test the narrowband service, perform the following steps:
   - Test whether the H.248 interface status is compatible with that prior to upgrading.
   - Test whether the user's fax service is proper.
   - Test whether the voice service is proper.
   - Test whether the POTS service, and the intelligent public telephone service is proper.
2. To test the broadband services, perform the following steps:
   - Test whether the broadband dialling is proper.
   - Test whether the web page opening, the e-mail sending and receiving and the download rate are proper.
   - Test whether the IPTV service is proper.
3. Test the NM functions.

   The NM connection is proper and the NM can synchronize and configure the data properly.

4. Test the ONU management.
   - All the ONUs are online and they can be successfully registered.
   - The ONU data can be delivered properly.

6.5 Upgrading Failure Guides

If the upgrading fails, the system automatically use the original version software.

Please record the prompts for upgrading failure, and then report them to the technical support.

Obtain ZTE technical support in the following ways:

- Technical support website: http://support.zte.com.cn
- E-mail address: 800@zte.com.cn
- Contact the local ZTE office.

This page intentionally left blank.

Appendix A
Card Replacement

Table of Contents

A.1 Card Replacement Precautions

When replacing the card, pay attention to the following:

- Do not look close without any protection or directly at the optical interface to avoid any hurt to the eyes during the operation.
- Plug/unplug the card (partially seated) carefully and slowly and make sure that the card does not collide the shelf or the next cards.
- One hand helps while the other hand is plugging/unplugging cards to avoid any damage.
- Plug/unplug only one card once. Prohibit to plug/unplug several cards once.
- Please observe the specifications while employing tools to plug/unplug the cards to avoid any damage to the cards.
- Pay attention to the ESD protection, and handle the cards carefully before the cards are placed outside the shelf. Put the card horizontally with its side which cannot be damaged easily down. Make sure the horizontal plane is clear of other things.
- Do not put the cards in the humid place or expose them to the sunshine directly. Make sure the surroundings does not do any harm to the cars.
- While moving several cards, do not pile the cards together to move them with the protection of antistatic bags only. Make sure to move only one card once.

A.2 Replacing Switching and Control Card

Context

- Precautions

    Pay attention to the following precautions while replacing the switching and control card:

    → Make an antistatic preparation.

    → Generally, the maintenance personnel can only replace the faulty switching and control card. Prohibit to replace the switching and control card in running status.

A-1

→ Recommend to replace the card during 00:00 to 05:00 with the minimum traffic.

→ Make sure that the service data has already been backed up.

→ Make sure that the new switching and control card is intact.

→ Be careful to avoid any short circuit caused by metal objects, including misplace of tools or screws dropped into the shelf.

→ Align the switching and control card to the guide rail and carefully push it in along the rail to connect accurately with the backplane.

- Tools

  The following are tools for replacing the switching and control card:

  → Antistatic wrist strap

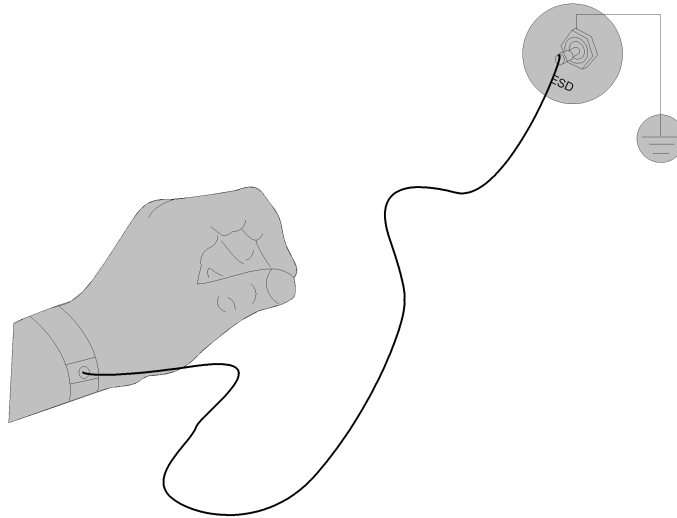 → Screwdriver

  → Antistatic bag

- Preparations

  The preparations are as follows:

  → Back up the current configuration data.

  → Back up the system configuration file.

  → Confirm whether the new switching and control card is the same as the original one in type.

  → Record the cable positions, and check whether the labels on the cables are correct, clear and tidy. If the labels are not visible, make a new label to prevent any mistake on connecting cables.

To replace the switching and control card, perform the following steps:

Steps

1. Wear the antistatic wrist strap, as shown in Figure A-1.

Figure A-1 Wear the Antistatic Wrist Strap

2. Remove the cables connected to the switching and control card.

3. Use the screwdriver to unfasten the screws on the switching and control card in the anti-clockwise direction.

4. Unclasp the lever on the switching and control card to separate the switching and control card from the back plane.

5. Grasp the lever and pull the switching and control card out along the guide rail steadily.

NOTE
Note:

You should gently pull the switching and control card out of the backplane along the guide rail to avoid any damage on the components of other card.

6. Put the switching and control card replaced into the antistatic bag and label it for maintenance with the note of its name and fault.

7. Pull the new switching and control card out of the antistatic bag, and check it. Make sure that the card is intact.

8. Pull the lever on the new switching and control card outward. Plug in the card and push it in along the guide rail steadily.

9. Gently push in the new switching and control card till the contact point of the lever and the shelf. Press the lever inward and push the switching and control card into the shelf with the working force between the lever and the position pin on the shelf, till the switching and control card lever is parallel to the panel.

10. Fasten the screws with the screwdriver in the clockwise direction to fix the card.

11. Connect the cables to the new switching and control card according to the recorded order.

Result

The switching and control card is replaced successfully.

Follow-up Actions

The follow-up actions includes the following:

● Observe the LED status of the new card. The switching and control card runs properly if the RUN LED is green and flashing.

● View whether the switching and control card type is correct and the status is normal through command lines. The switching and control card runs properly if it is in INSERVICE status.

● View whether the card version is correct through the command line. If it is not correct, download the correct version.

● Save the existing configuration data.

● Restore the previous backup configuration data to the system.

● Query the system alarms, notifications and events. Confirm there is no exceptional alarms, notifications and events.

A.3 Replacing Service Cards

Context

● Precautions

Pay attention to the following precautions while replacing the service cards:

→ Replacing the service cards cause causes the interruption of service carried on the card.

→ Make an antistatic preparation.

→ Recommend to replace the card during 00:00 to 05:00 with the minimum traffic.

→ Be careful to avoid any short circuit caused by metal objects, including misplace of tools or screws dropped into the shelf.

→ Make sure that the new switching and control card is intact.

→ Be careful to avoid any short circuit caused by metal objects, including misplace of tools or screws dropped into the shelf.

→ Align the switching and control card to the guide rail and carefully push it in along the rail to connect accurately with the backplane.

→ Removing the service cards which is loading program may cause the damage on the service cards program. Therefore, make sure that the service cards is not loading program before it is replaced.

● Tools

The following are tools for replacing the service cards:

→ Antistatic wrist strap

→ Screwdriver

→ Antistatic bag

A-4

● Preparations

The preparations are as follows:

→ Check and record the card type, and make sure that the new card is the same as the original one in type.

→ Record the cable positions, and check whether the labels on the cables are correct, clear and tidy. If the labels are not visible, make a new label to prevent any mistakes on connecting cables.

To replace the service cards, perform the following steps:

Steps

1. Wear the antistatic wrist strap, as shown in Figure A-2.

Figure A-2 Wear the Antistatic Wrist Strap
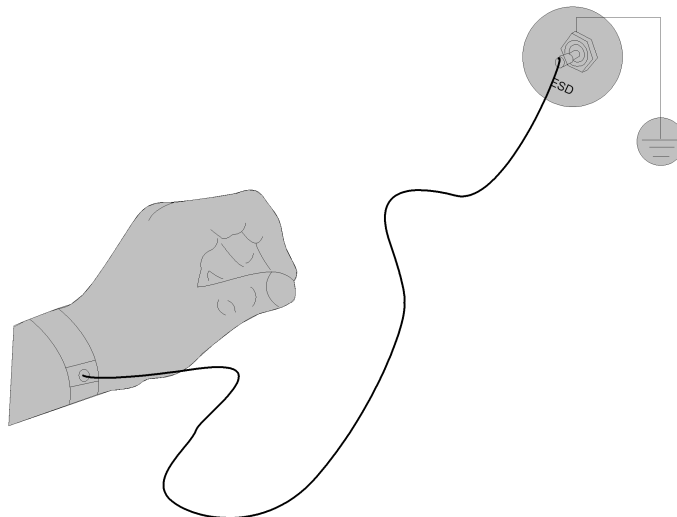
2. Remove the cables connected to the service card.
3. Use the screwdriver to unfasten the screws on the card in the anti-clockwise direction.
4. Pull the lever on the card outward to separate the service card from the back plane.
5. Grasp the lever and pull the card out along the guide rail steadily.

NOTE **Note:**

You should gently pull the card out of the shelf along the guide rail to avoid any damage on other cards.

---

6. Put the card replaced into the antistatic bag and label it for maintenance with the note of its name and fault.
7. Pull the new card out of the antistatic bag, and check it. Make sure that the card is intact.

A-5

NOTE **Note:**

You should not touch the circuit card surface.

8. Pull the lever on the new card outward. Plug the card in and push it in along the guide rail.
9. Gently push in the new card till the contact point of the lever and the shelf. Press the lever inward and push the card into the shelf with the working force between the lever and the position pin on the shelf, till the card lever is parallel with the panel.
10. Fasten the screws with the screwdriver in the clockwise direction to fix the card.
11. Connect the cables to the new service card according to the recorded order.

Result

The service cards are replaced successfully.

Follow-up Actions

The follow-up actions includes the following:

● Observe the LED status of the new card. The switching and control card runs properly if the RUN LED is green and flashing.
● View whether the switching and control card type is correct and the status is normal through command lines. The switching and control card runs properly if it is in INSERVICE status.
● View whether the card version is correct through the command line. If it is not correct, download the correct version.
● Save the existing configuration data.
● Restore the previous backup configuration data to the system.
● Query the system alarms, notifications and events. Confirm there is no exceptional alarms, notifications and events.

Glossary

AC
  - Access Control

CPU
  - Central Processing Unit

DC
  - Direct Current

ESD
  - Electrostatic Discharge

FTP
  - File Transfer Protocol

IPTV
  - Internet Protocol Television

LED
  - Light Emitting Diode

LOS
  - Loss of Signal

MAC
  - Media Access Control

NE
  - Network Element

NM
  - Network Management

NMS
  - Network Management System

ONU
  - Optical Network Unit