ZXUAS 10800E

Carrier Class BRAS

User Manual (Volume I)

Version 2.8.01

ZTE CORPORATION
ZTE Plaza, Keji Road South,
Hi-Tech Industrial Park,
Nanshan District, Shenzhen,
P. R. China
518057
Tel: (86) 755 26771900 800-9830-9830
Fax: (86) 755 26772236
URL: http://support.zte.com.cn
E-mail: doc@zte.com.cn

Revision History

Date	Revision No.	Serial No.	Reason for Issue
Jan. 5, 2008	R1.0	sjzl20080610	First edition

ZTE CORPORATION
Values Your Comments & Suggestions!

Your opinion is of great value and will help us improve the quality of our product documentation and offer better services to our customers.

Please fax to (86) 755-26772236 or mail to Documentation R&D Department, ZTE CORPORATION, ZTE Plaza, A Wing, Keji Road South, Hi-Tech Industrial Park, Shenzhen, P. R. China 518057.

Thank you for your cooperation!

<table>
<tr><td>Document Name</td><td colspan="3">ZXUAS 10800E (V2.8.01) Carrier Class BRAS User Manual (Volume I)</td></tr>
<tr><td>Product Version</td><td>V2.8.01</td><td>Document Revision Number</td><td>R1.0</td></tr>
<tr><td>Serial No.</td><td>sjzl20080610</td><td>Equipment Installation Date</td><td></td></tr>
<tr><td rowspan="3">Your evaluation of this documentation</td><td colspan="3">Presentation:
(Introductions, Procedures, Illustrations, Completeness, Level of Detail, Organization, Appearance)
☐ Good ☐ Fair ☐ Average ☐ Poor ☐ Bad ☐ N/A</td></tr>
<tr><td colspan="3">Accessibility:
(Contents, Index, Headings, Numbering, Glossary)
☐ Good ☐ Fair ☐ Average ☐ Poor ☐ Bad ☐ N/A</td></tr>
<tr><td colspan="3">Intelligibility:
(Language, Vocabulary, Readability & Clarity, Technical Accuracy, Content)
☐ Good ☐ Fair ☐ Average ☐ Poor ☐ Bad ☐ N/A</td></tr>
<tr><td>Your suggestions for improvement of this documentation</td><td colspan="3">Please check the suggestions which you feel can improve this documentation:
☐ Improve the overview/introduction ☐ Make it more concise/brief
☐ Improve the Contents ☐ Add more step-by-step procedures/tutorials
☐ Improve the organization ☐ Add more troubleshooting information
☐ Include more figures ☐ Make it less technical
☐ Add more examples ☐ Add more/better quick reference aids
☐ Add more detail ☐ Improve the index
☐ Other suggestions
_____
_____
_____
_____
_____
Please feel free to write any comments on an attached sheet.</td></tr>
<tr><td colspan="4">If you wish to be contacted regarding your comments, please complete the following:</td></tr>
<tr><td>Name</td><td></td><td>Company</td><td></td></tr>
<tr><td>Postcode</td><td></td><td>Address</td><td></td></tr>
<tr><td>Telephone</td><td colspan="2"></td><td>E-mail</td></tr>
</table>

This page is intentionally blank.

Contents

This Page is intentionally blank.

About This Manual

Purpose

This manual provides procedures and guidelines that support the operation of ZXUAS 10800E (V2.8.01) Carrier Class BRAS.

Intended Audience

This manual is intended for engineers and technicians who perform operation activities on ZXUAS 10800E (V2.8.01) Carrier Class BRAS.

What Is in This Manual

This manual contains the following chapters:

TABLE 1 CHAPTER SUMMARY

Chapter	Summary
Chapter 1 Safety Instructions	This chapter describes the safety instructions and signs.
Chapter 2 System Introduction	This chapter covers brief introduction of software/hardware structure of ZXUAS 10800E Carrier Class BRAS.
Chapter 3 Structure and Principles	This chapter describes structure and principles of ZXUAS 10800E Carrier Class BRAS.
Chapter 4 Usage and Operation	This chapter describes configuration methods, command modes and use of command lines of ZXUAS 10800E Carrier Class BRAS.
Chapter 5 System Management	This topic covers brief introduction about system management of ZXUAS 10800E Carrier Class BRAS.
Chapter 6 Interface Configuration	This chapter describes interface configuration on ZXUAS 10800E Carrier Class BRAS.

Chapter	Summary
Chapter 7 BRAS Service	This chapter describes basic concepts and configuration of BRAS access features.
Chapter 8 PPPoX Configuration	This chapter describes PPPoX and configuration on ZXUAS 10800E.
Chapter 9 IPoX Configuration	This chapter describes IPoX and configuration on ZXUAS 10800E.
Chapter 10 DHCP Configuration	This chapter describes DHCP and configuration on ZXUAS 10800E.
Chapter 11 RADIUS Configuration	This chapter describes RADIUS protocol and configuration on ZXUAS 10800E.
Chapter 12 BRAS Security Configuration	This chapter describes BRAS security and configuration on ZXUAS 10800E.
Chapter 13 Network Management Configuration	This chapter describes NTP, SNMP RMON and system log, and related configuration on ZXUAS 10800E.

Related Documentation

The following documentation is related to this manual:

- ZXUAS 10800E (V2.8.01) Carrier Class BRAS Hardware Installation Manual
- ZXUAS 10800E (V2.8.01) Carrier Class BRAS User Manual (Volume II)
- ZXUAS 10800E (V2.8.01) Carrier Class BRAS Command Manual

Conventions

Typographical Conventions

ZTE documents employ the following typographical conventions.

TABLE 2 TYPOGRAPHICAL CONVENTIONS

Typeface	Meaning
Italics	References to other Manuals and documents.
“Quotes”	Links on screens.
Bold	Menus, menu options, function names, input fields, radio button names, check boxes, drop-down lists, dialog box names, window names.
CAPS	Keys on the keyboard and buttons on screens and company name.
`Constant width`	Text that you type, program code, files and directory names, and function names.

Typeface	Meaning
[ ]	Optional parameters.
{ }	Mandatory parameters.
|	Select one of the parameters that are delimited by it.

How to Get in Touch

The following sections provide information on how to obtain support for the documentation and the software.

Customer Support

If you have problems, questions, comments, or suggestions regarding your product, contact us by e-mail at support@zte.com.cn. You can also call our customer support center at (86) 755 26771900 and (86) 800-9830-9830.

Documentation Support

ZTE welcomes your comments and suggestions on the quality and usefulness of this document. For further questions, comments, or suggestions on the documentation, you can contact us by e-mail at doc@zte.com.cn; or you can fax your comments and suggestions to (86) 755 26772236. You can also browse our website at http://support.zte.com.cn, which contains various interesting subjects like documentation, knowledge base, forum and service request.

This page is intentionally blank.

Chapter 1

Safety Instructions

Overview

Introduction This chapter describes the safety instructions and signs.

Contents This chapter includes the following topics.

Safety Introduction

In order to operate the equipment in a proper way, follow these instructions:

- Only qualified professionals are allowed to perform installation, operation and maintenance due to the high temperature and high voltage of the equipment.
- Observe the local safety codes and relevant operation procedures during equipment installation, operation and maintenance to prevent personal injury or equipment damage. Safety precautions introduced in this manual are supplementary to the local safety codes.
- ZTE bears no responsibility in case of universal safety operation requirements violation and safety standards violation in designing, manufacturing and equipment usage.

Safety Description

Contents deserving special attention during ZXUAS 10800E configuration are explained in the following example:

Note: This function is disabled by default.

Chapter 2

System Introduction

Overview

Introduction This chapter covers brief introduction of software/hardware structure of ZXUAS 10800E Carrier Class BRAS.

Contents This chapter includes the following topics.

Product Overview

Introduction With the increase of Internet services in exponential order and the widely application of multimedia, service providers have to face the following problems.

- How to meet different access requirements of different users.
- How to manage the users and develop services.
- How to improve network utilization.

With the rich development experience, ZTE designs ZXUAS 10800E carrier class BRAS (Broadband Remote Access Server). It adopts modularization structure, which provides multiple types of service interfaces, supporting 10G high-speed links and excellent service ability. The key system module adopts 1:1 redundancy structure, ensuring the security of system. Combined with effective software technology, high-speed network processor can identify internal users, ensure information security and prevent service attacks. ZXUAS 10800E also provides different bandwidth, QoS and ACL for different services.

For individuation value additional services, flexible accounting policy is indispensable. ZXUAS 10800E is the first choice for building convergence and access network, and it is the basic platform of integrated services.

The structure of ZXUAS 10800E Carrier Class BRAS fully loaded is shown in Figure 1.

FIGURE 1 ZXUAS 10800E CARRIER CLASS BRAS

Functions

System Design

ZXUAS 10800E Carrier Class BRAS integrates IP routing and switching technologies, current broadband network technologies. In aspect of system design, routing engine and forwarding engine are separated, partial forwarding table is divorced from global routing table and fast hardware is adopted to realize the packet header processing, routing, and forwarding of the IP packets.

Interface Cards

ZXUAS 10800E Carrier Class BRAS adopts CROSSBAR switching structure to enhance data communication speed among respective interface units. It is a new-generation BRAS with extremely large capacity. The following interface cards are supported.

- BRAS 24-port gigabit Ethernet interface card (BT-24GE-SFP)
- BRAS 10-port gigabit SFP interface card (BT-10x1GE-SFP)
- BRAS 1-port 10 gigabit XFP LAN interface card (BT-1x10GE-LAN-XFP)
- BRAS 1-port 10 gigabit XFP WAN interface card (BT-1x10GE-WAN-XFP)
- BRAS 1-port POS192 XFP interface card (BT-1POS-OC192-XFP)
- BRAS 4-port gigabit Ethernet SFP interface card (BT-4GE-SFP)
- BRAS 1-port POS48 short-distance interface card (BT-1POS-OC48-SFF-SC)
- BRAS 1-port POS48 long-distance interface card (BT-1POS-OC48-SFF-LC)
- BRAS 1-port POS48 extra-long-distance interface card (BT-1POS-OC48-SFF–LH)
- BRAS 16-port fast Ethernet electric interface card (BT-16FE-RJ)
- BRAS 16-port fast Ethernet optical interface card (BT-16FE-SFP)
- BRAS 8-port ATM3 interface card (BT-8ATM-OC3-SFP)

With respect to software, a network operating system (ROS) platform is developed. ROS is property of ZTE Corporation and is used for ZXUAS 10800E Carrier Class BRAS. ZXUAS 10800E Carrier Class BRAS has powerful protocol support functions, supporting the following network protocols and standards:

- Link layer protocols: PPP, MPPP, 802.1Q
- Network layer protocols: IP, ICMP, ARP
- Transport layer protocols: TCP, UDP
- Routing protocols: RIPv1/v2, OSPFv2, IS-IS, BGP4
- Supporting MPLS/VPN
- Application layer protocols: Telnet, FTP, TFTP, H.323
- Network layer control and application: ACL
- Network management protocols: SNMPv1/v2/v3, RMONv1, NTP

Technical Features and Parameters

Technical features and parameters of ZXUAS 10800E are listed in Table 3.

TABLE 3 TECHNICAL FEATURES AND PARAMETERS

Item	Description
Size	608.21 × 442 × 482.6 (mm)
Weight	50kg
DC Power Supply	-36V~-72V
AC Power Supply	100V~240V
AC Power Frequency	100V~240V
Power consumption	<1200W
Reliability	MTBF: >200000 hours MTTR: <10 minutes
Temperature	Working temperature: 0℃~+45℃ Storage temperature: -10℃~+70℃
Relative Humidity	20%~90%
Backbone Bandwidth	640Gbps
Packet Forwarding Rate	200Mpps
Routing Table Capacity	1M

Chapter 3

Structure and Principles

Overview

Introduction This chapter describes structure and principles of ZXUAS 10800E Carrier Class BRAS.

Contents This chapter includes the following topics.

Hardware Structure

Introduction Hardware design of ZXUAS 10800E Carrier Class BRAS adopts modular design based on high-speed serial backplane. Its architecture adopts popular multi-processor, concurrent processing CROSSBAR space division switching structure. Main parts of system adopt 1+1 redundancy design, smooth upgrading capability and good maintainability of system has been taken into account during the design.

ZXUAS 10800E Carrier Class BRAS has eight BNPCs.

According to functions realized by hardware circuits, ZXUAS 10800E Carrier Class BRAS mainly comprises of the following parts:

- High-speed backplane unit
- Protocol processing and control function sub-unit

- High-speed switching network function sub-unit
- High-speed network processing function sub-unit
- High-speed interface function sub-unit
- Bridge monitoring alarm sub-system
- Power supply sub-system
- Mechanical structure sub-system

Sub-Unit Functions

High-speed backplane unit consists of a double-faced backplane. Backplane is connected with other functional units through the data bus, control bus, clock bus. Power supply sub-system, also through backplane, provides –48V DC power supply that is filtered once for respective functional units.

Protocol processing and control function sub-unit, and high-speed network processing function sub-unit adopt redundancy design, that is, ultra protocol processor control card and switch fabric card adopt 1+1 redundancy design. To facilitate maintenance and management, ZXUAS 10800E Carrier Class BRAS also connects the operation and maintenance background through 10/100BASE-TX or Console interface on protocol processor control card.

Power Supply

ZXUAS 10800E Carrier Class BRAS supports two kinds of power supplies: 220V AC power supply and –48 DC power supply. 220V AC power supply adopts three 800W power supply modules to make 2+1 redundancy design. Each module commutates 220V AC power supply into —48V DC power supply. In –48 DC power supply mode, the power supply is obtained by connecting external power supply or through commutation by power supply component. It supplies –48V DC voltage to other cards in system after filtered by primary power supply processing system of ZXUAS 10800E Carrier Class BRAS. Respective cards convert –48V power supply into the working voltages required by respective chips (5V, 3.3V, 2.5V, etc) through the DC/DC conversion.

Various interface network processor cards and switch fabric cards communicate with ultra protocol processor control card through 100M fast Ethernet. Primary power supply module communicates with ultra protocol processor control card through RS232 serial line. Also, Ethernet communication mode is adopted for communication between the ultra protocol processor control card, operation/ maintenance background and monitoring alarm system.

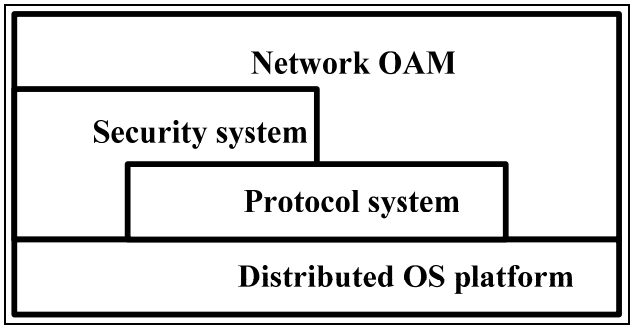
High-Speed Serial Line

High-speed serial line (2.64384GB/s) is used for data transmission between each interface network processor card and switch fabric card. To facilitate addition of switching arbitration scheduler, a piece of communication bus is added between each interface network processor card and each switch fabric card.

Software Structure

As soul of whole router system, ZXUAS 10800E Carrier Class BRAS software part is responsible for creation of routing table, security management, user interface management and so on. In terms of structure, software part consists of the following subsystems, as illustrated in Figure 2.

FIGURE 2 ZXUAS 10800E CARRIE CLASS BRAS SOFTWARE SYSTEM



Distributed OS Platform

Distributed operating system (OS) is a multi-processor, multi-task real time operating system. This is basis for upper layer software to run in router architecture. This is responsible for managing distributed hardware structure of whole router system in lower layer and providing a uniform operating platform to upper layer programs of each processor.

Protocol System

Protocol system is kernel of router software architecture. This system is responsible for route selection, forwarding, interaction, creation and maintenance of routing table. Protocol system can be divided into support protocol system and routing protocol system.

- Support Protocol System

  Support protocol system implements TCP, UDP, IP, and TELNET protocols. This is the basis for OSPF, BGP, and SNMP also knows as bottom layer bearer for network Operation, Administration and Maintenance (OAM) commands.

- Routing Protocol System

  Routing protocol system implements IP, ARP, ICMP, RIP, OSPF, IS-IS and BGP dynamic routing protocols, synchronization and maintenance of routing table, and routing interaction that are core functions.

Network OAM

Network OAM system is in top layer of whole router and is main approach for operator to operate and control the router. System implements SNMPv2 Agent function and provides command line operation window. User can perform network management tjrough serial terminal, Telnet and SNMP Manager, mainly including network configuration management, fault management, performance management, and security management.

Security system

Security system controls security of the UAS network and protocols. This is responsible for data encryption, decryption, key analysis, and protocol authentication.

Ultra Protocol Processor Control Card

Contents

Ultra Protocol Processor Control Card includes the following topics.

Ultra Protocol Processor Control Card Overview

BUPC3 Functions

BRAS Ultra Protocol processor control Card (BUPC3) is the main control node of ZXUAS 10800E Carrier Class BRAS, and has following major functions:

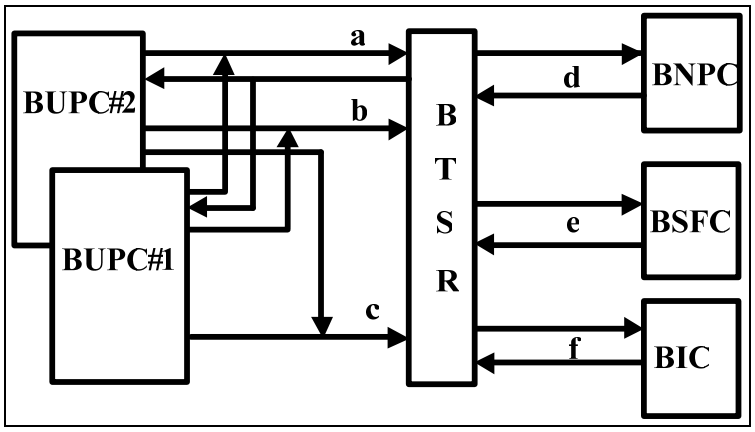
- Managing and maintaining the entire UAS, guaranteeing all line interface cards work normally and executing routing and forwarding IP data packets.
- Conducting routing protocol processing (including RIPv1/v2, OSPFv2, IS-IS, and BGP4/4+), maintaining global routing table and guaranteeing partial routing table of each line interface card is consistent with global routing table.
- Conducting SNMP processing and providing remote monitoring, management function of UAS.
- Providing interface of operation and management functions of UAS system; realizing the functions of maintaining, configuring, and managing the UAS.

To ensure high reliability of the system, active/standby mode is adopted for two BUPC3s of ZXUAS 10800E Carrier Class BRAS.

Structural Relationship

Position of BUPC3 in the system and brief interface connection relationship with other cards is shown in Figure 3.

FIGURE 3 STRUCTURAL RELATIONSHIP OF BUPC IN SYSTEM



a~f has following meanings respectively.

a: 16-channel Ethernet interface signals; realizing the active/standby mode on the BUPC3.

b: interface signals with other cards, for example, the signal for card being in position, card reset signal, and active/standby card interface signal; realizing the active/standby mode on the BUPC3.

c: background management interface signals; realizing the active/standby mode on the BUPC3.

d: interface Ethernet signals of the BNPC and BUP3, including the signal for card being in position and card reset signal.

e: Ethernet signal for signals of the BSFC3 and BUPC3, including the signal for card being in position and card reset signal, as well as the active/standby indication signal.

f: background management interface signal of BIC and BUPC3.

Working Principles

ZXUAS 10800E Carrier Class BRAS BUPC3 consists of the following modules and interfaces:

- Routing module
- Management module
- Control and monitoring module
- Background management interface
- Commissioning interface

Routing module and management module are two sets of processor systems, including CPU, North Bridge, and South Bridge.

Routing Module

Routing module is one of the dual-processor systems on BUPC3. It is specifically used to run large dynamic routing protocols such

as OSPFv2/v3, IS-IS and BGP4/4+, guaranteeing high performance and high reliability.

CPU of routing module (RPU) generates the PCI bus through bridge chip. It connects one port of internal communication module to receive and send data through 10/100M PCI network controller. Transmission bandwidth between routing module and internal communication module is 100Mb/s, thus, earning enough communication bandwidth between the routing module and each card.

Management Module

Management module is the other dual-processor system of BUPC3. It mainly realizes overall functions such as control, maintenance, configuration and management, facilitating flexible upgrading and perfection of versions.

CPU of management module (MPU) generates PCI bus through bridge chip and connects two 100M Ethernet controllers on PCI bus. Among them, one Ethernet controller connects one port of internal communication module, so as to communicate with RPU and other cards. Other Ethernet controller connects background maintenance network, so as to communicate with operation and maintenance terminal and to conduct the security filtering for packets sent from the background.

Control and Monitoring Module

Control and monitoring module is realized through the Field Programmable Gate Array (FPGA). Its major functions are:

- Providing equipment address allocation and logical code translation of ISA bus.
- Confirming active/standby working states of two BUPC3s, including the power-on initial state establishment and active/standby switching, command-able switching, manual switching, reset switching, fault switching (Watchdog overflow).
- Monitoring running status of other cards in system, and informing upper layer software of state change of other cards in interrupted mode.
- Monitoring running status of these two CPUs (MPU and RPU).

Internal Communication Module

In BUPC3 of ZXUAS 10800E Carrier Class BRAS, there is an internal communication module (Ethernet switching module). This switching module provides communication links for BUPC3, SNPC, BSFC3, and background management.

Internal communication module in ZXUAS 10800E Carrier Class BRAS provides 16 Ethernet interfaces. These 16 Ethernet interfaces are allocated as follows:

- MPU internal network adaptor: 1
- RPU network adaptor: 1
- Active/standby BUPC communication: 1
- Commissioning network port: 2
- BNPC: 8

- BSFC: 2
- Idle: 1

Front Panel

The front panel of BUPC3 is shown in Figure 4.

FIGURE 4 FRONT PANEL OF BUPC3

On the front panel of BUPC3, there are four LED indicators and two switches. The functions of these indicators and switches are described in Table 4.

TABLE 4 BUPC3 FRONT PANEL INDICATOR AND SWITCH FUNCTIONS

Item	Description
RUN Indicator (Green)	It flashes with a frequency of 1/second if the system runs normally
ALM Indicator (Red)	It is on if fault occurs to the system and is off in normal state.
MST Indicator (Green)	This is an active status indicator. It is on if the card is in the active state and meanwhile the standby status indicator is off.
OFF Indicator (Green)	This is a standby status indicator: It is on if the card is in the standby state and meanwhile the active status indicator is off.
RST Switch	This is a reset switch. It is used to reset the card.
EXCH Switch	This is a manual switching switch. It is used to manually switch between the active state and the standby state.

Switch Fabric Card

Contents Switch Fabric Card includes the following topics.

Switch Fabric Card Overview

BSFC3 Functions

Large capacity high-speed switching network sub-unit is the core of UAS. Function bearer is Switch Fabric Card3 (BSFC3), whose major function is to realize switching of IP packets. This can automatically conduct routing switching of variable-length IP packets without CPU control. Its major functions are:

- Realizing high-speed switching of IP packets through point-to-point connection on backplane of high-speed serial bit stream between CROSSBAR chip and BNPC, with switching function of CROSSBAR chip.
- Providing high-precision and high-stability system clock for system (complying with the ITU-TG.813 recommendations) by using internal clock module with digital phase-lock loop circuit through the external timing or line timing.
- Managing and controlling running status of BSFC3 and communicating with BUPC3.

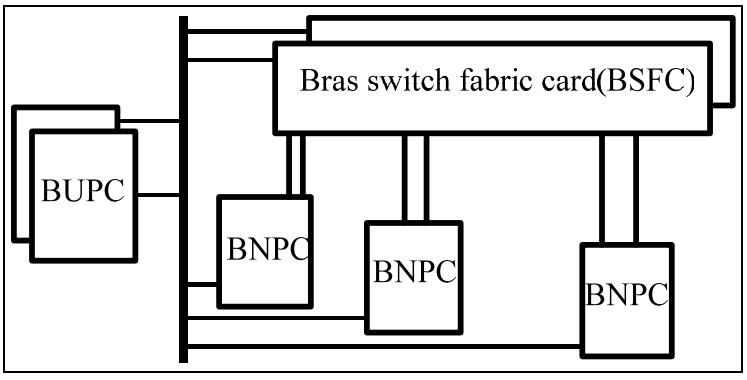
BSFC3 of ZXUAS 10800E Carrier Class BRAS adopts 64G high-speed CROSSBAR switching structure. It realizes serial point-to-point connection with 8 BNPCs through high-speed backplane BTSR, so as to conduct internal unblocked switching and transmission of multiple IP packets together with high-speed backplane chip on BNPC3.

As BSFC3 holds a very important position in the system, so the active/standby dual hot backup mode is adopted. Each BSFC3 can notify respective BNPCs of the active/standby working mode of this card through relevant signal lines, thus enabling IP packets to be transmitted on the high-speed link of the active card.

Structural Relationship

The structural relationship of BSFC3 in system is shown in Figure 5.

FIGURE 5 BSFC3 STRUCTURAL RELATIONSHIP

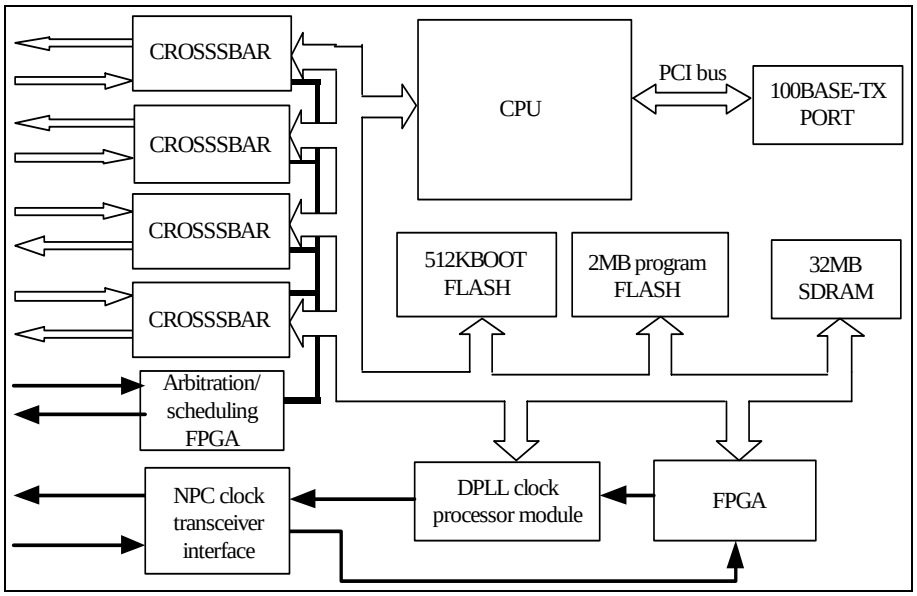


Serial high-speed signal line is used between BSFC3 and each BNPC. 100BASE-TX communication control signal line is used for connection with BUPC.

Working Principles

The working principle of BSFC3 is shown in Figure 6.

FIGURE 6 BSFC3 PRINCIPLES



ZXUAS 10800E Carrier Class BRAS, switching of IP packets is conducted by CROSSBAR chip on BSFC and high-speed serial backplane chip on BNPC. CROSSBAR chip has following functions and features:

- High-speed serial line with coding rate of 2.64384GB/s is used between CROSSBAR chip on BSFC3 and high-speed serial backplane chip on BNPC, conducting the point-to-point connection through backplane.
- CROSSBAR chip is a 16x16, fully synchronous space division switching chip.
- CROSSBAR chip has parallel CPU interfaces for controlling working mode inside chip and reading state information on switching.
- CROSSBAR chip uses primary clock of 62.5MHz, which is synchronization clock for all high-speed serial backplane chips to receive data through serial data channel. The synchronization is automatically realized.

Front Panel

The front panel of BSFC3 of ZXUAS 10800E is shown in Figure 7.

FIGURE 7 FRONT PANEL OF BSFC3

On the front panel of BSFC3, there are four LED indicators and two switches. The functions of these indicators and switches are described in Table 5.

TABLE 5 BSFC3 FRONT PANEL INDICATOR AND SWITCH FUNCTIONS

Item	Description
RUN Indicator (Green)	Run indicator: It flashes synchronously with that of BUPC3 if the system runs normally.
ALM Indicator (Red)	Alarm indicator: It is on if fault occurs to the system and is off in normal state.
MST Indicator (Green)	Active status indicator: It is on if the card is in the active state and meanwhile the standby status indicator is off.
OFF Indicator (Green)	Standby status indicator: It is on if the card is in the standby state and meanwhile the active status indicator is off.
RST Switch	Reset switch: It is used to reset the card.
EXCH Switch	Manual switching switch: It is used to manually switch between the active state and the standby state.

Network Processor Card

BNPC Functions

Major functions of BRAS Network Processor Card (BNPC) are:

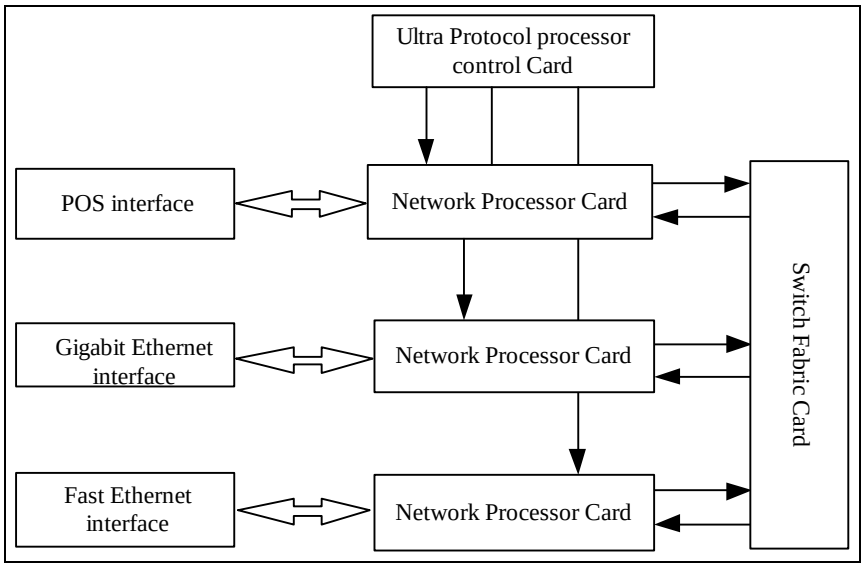
- In receiving direction, parsing IP packets from link layer frames; making TTL and Checksum checks for IP packet headers; conducting address filtering and routing for IP packet headers; cooperating with switching network to edit IP packet headers and to manage buffer and queue scheduling of packets.
- In sending direction, shucking off switching flag headers of IP packets sent from switching structure; encapsulating them as data link layer frames and then sending them out.

The types of interface connecting to BNPC can be Ethernet, POS and ATM.

Structural Relationship

The structural relationship of BNPC in the system is shown in Figure 8.

FIGURE 8 STRUCTURAL RELATIONSHIP OF BNPC



BNPC Types

BNPC has two types.

- BNPCH: BRAS Network Processor Card of H Type

  It connects with interfaces on high-speed line boards, such as 16-port fast Ethernet board, 4-port gigabit Ethernet board, ATM155 board and POS48 board.

- BNPCIX: BRAS Network Processor Card of IX Type

  It connects with interfaces on extra-high-speed line boards, such as 10 gigabit board and 10-port gigabit Ethernet board.

BNPC is used to address and forward IP packets from line cards and process BRAS services.

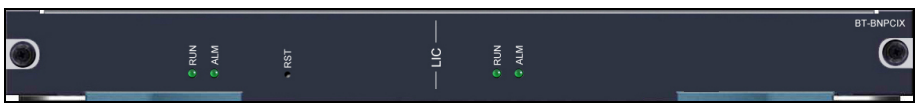
Front Panels

The front panel of BNPCH is shown in Figure 9.

FIGURE 9 FRONT PANEL OF BNPCH

The front panel of BNPCIX is shown in Figure 10.

FIGURE 10 FRONT PANEL OF BNPCIX



On the front panel of BNPCH and BNPCIX, there are four LED indicators and one switch. The functions of these indicators and switch are described in Table 6.

TABLE 6 BNPC FRONT PANEL INDICATOR AND SWITCH FUNCTIONS

Item	Description
RUN Indicator (Green)	Run indicator: It flashes synchronously with that of BSFC3 if the system runs normally.
ALM Indicator (Red)	Alarm indicator: It is on if fault occurs to the system and is off in normal state.
LIC RUN Indicator (Green)	Card state indicator: It is on if the card is in normal state and it is off if fault occurs.
LIC ALM Indicator (Green)	Card alarm indicator: It is on if fault occurs to the system and is off in normal state.
RST Switch	Reset switch: It is used to reset the card.

Bridge Interface and Alarm Monitor Card

Contents

Bridge Interface and Alarm monitor Card includes the following topics.

Bridge Interface and Alarm Monitor Card Overview

BIC Functions

Bridge Interface & Alarm Monitor Card (BIC) is monitoring and interface transit card of UAS. Its major functions are:

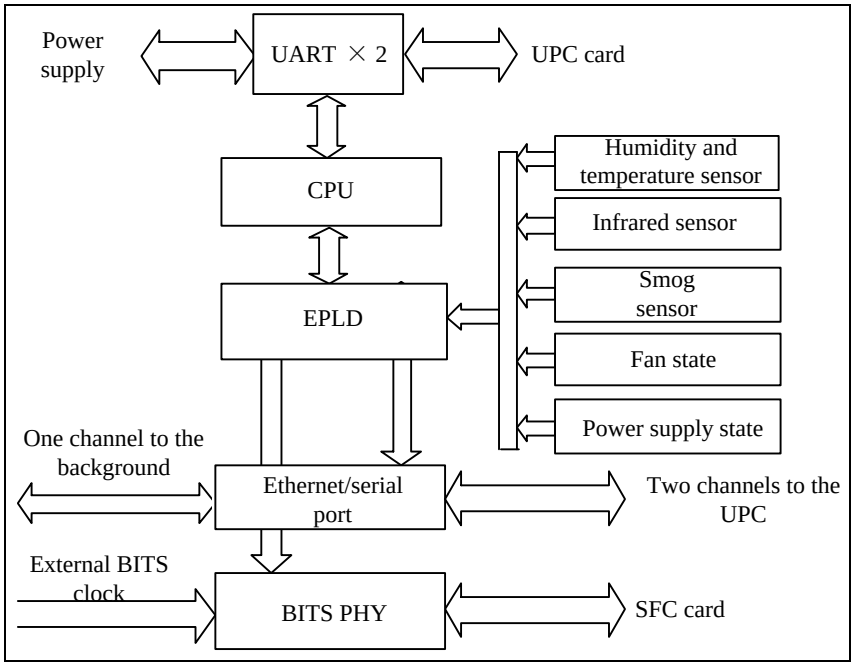
- Monitoring running environment of system
- Providing BITS clock interface, serial interface and Ethernet transit
- Providing auxiliary alarm information

Working Principles

On BIC, there is a set of CPU system. CPU periodically collects external environmental data through EPLD, reading and controlling states of infrared sensor, humidity and temperature sensor, cooling fans and primary power supply. Besides, it communicates with MPU of BUPC3 through the serial port.

Working principles of BIC is shown in Figure 11.

FIGURE 11 WORKING PRINCIPLES OF BIC



Smog Sensor Smog sensor on BIC generates current signals once it detects smog, and then card converts current signals into level signals, which is sent to EPLD.

Humidity and Temperature Sensor Temperature and humidity sensor modulates variation of temperature and humidity into square wave varying with frequency. Building a counter in EPLD can obtain temperature and humidity corresponding to environment.

Infrared Sensor After infrared sensor is started, this can detect ambient environment at any time and once this detects that someone is coming near, this signal will have level reversion.

Primary Power Supply Monitoring Interface Primary power supply monitoring module provides two kinds of interfaces. One of them is standard serial port and other is private interface which can be used to monitor states of over-voltage and under-voltage.

Fan Monitoring Interface Fan monitoring and control card sends states of fans to related registers of EPLD for query.

Front Panel

The front panel of BIC is shown in Figure 12.

FIGURE 12 FRONT PANEL OF BIC

There are nine interfaces on the front panel of BIC. Their functions are described in Table 7.

TABLE 7 INTERFACE FUNCTIONS OF BIC

Type	Description
10/100M Ethernet Interface	Connecting with background computer through RJ45 straight-through line
COM Interface	Connecting with background network management system through serial console line
FAN Interface	Monitor interface of fan group
PWR Interface	Monitor interface of power supply
SENSOR1 Interface	Monitor interface of sensor
SENSOR2 Interface	Monitor interface of sensor
SENSOR3 Interface	Monitor interface of sensor
2MHz Interface	BITS Clock Interface, connecting with BITS clock through 75Ω coaxial cable
2Mbits Interface	BITS Clock Interface, connecting with BITS clock through 75Ω coaxial cable

There are two indicators on the front panel of BIC. Their functions are described in Table 8.

TABLE 8 INDICATOR FUNCTIONS OF BIC

Item	Description
RUN indicator (Green)	Run indicator: When it is on, it indicates normal running.
ALM indicator (Red)	Environment alarm indicator: When it is on, it indicates there are environment alarms, and checks are needed.

Line Card Interface

Introduction Line interface card is external interface of wire speed UAS. It is used to access interface services of different rates and different types. Line interface card provides one or more high-speed network interfaces.

Contents Line Card Interface includes the following topics.

BT-16FE-RJ Card

BT-16FE-RJ card is a fast Ethernet interface card of G type for BRAS. It provides sixteen 100Base-TX interfaces. Their major functions are to receive, send and extract Ethernet frames (MAC frames)

BT-16FE-RJ card and BNPCH are connected through backplane.

The front panel of BT-16FE-RJ card is shown in Figure 13.

FIGURE 13 FRONT PANEL OF BT-16FE-RJ CARD

There are sixteen RJ-45 ports on the front panel of BT-16FE-RJ card. Each port has two LED indicators in green and yellow respectively. Their functions are described in Table 9.

TABLE 9 INDICATOR FUNCTIONS

Indicator	Description
Green Indicator	On: Ethernet is in 100M link state; Off: Ethernet is in 10M link state or physical link is not through.

Indicator	Description
Yellow Indicator	On: physical link with peer end is established; Flashing: there is data being transmitted on physical link; Off: physical link is not through.

BT-16FE-SFP Card

BT-16FE-SFP card is a fast Ethernet optical interface of G type card for BRAS. It provides sixteen 100BASE-FX Ethernet optical interfaces. Their major functions are to receive, send and extract Ethernet frames (MAC frames) and to schedule and control FIFO queues on the interfaces.

BT-16FE-SFP card and BNPCH are connected through backplane.

The front panel of BT-16FE-SFP card is shown in Figure 14.

FIGURE 14 FRONT PANEL OF BT-16FE-SFP CARD

There are sixteen SFP ports on the front panel of BT-16FE-SFP card. Each port has two LED indicators in green and yellow respectively. Their functions are described in Table 10.

TABLE 10 INDICATOR FUNCTIONS

Indicator	Description
Green Indicator	On: Ethernet is in 100M link state; Off: Ethernet is in 10M link state or physical link is not through.
Yellow Indicator	On: physical link with peer end is established; Flashing: there is data being transmitted on physical link; Off: physical link is not through.

BT-24GE-SFP Card

BT-24GE-SFP card is a gigabit Ethernet optical interface card for BRAS. It provides twenty-four gigabit Ethernet optical interfaces. Their major functions are to provide twenty-four accesses to Ethernet.

BT-24GE-SFP card and BNPCIX are connected through backplane.

The front panel of BT-24GE-SFP card is shown in Figure 15.

FIGURE 15 FRONT PANEL OF BT-24GE-SFP CARD

There are twenty-four SFP ports on the front panel of BT-24GE-SFP card. Each port has two LED indicators in green and yellow respectively. Their functions are described in Table 11.

TABLE 11 INDICATOR FUNCTIONS

Indicator	Description
Green Indicator	On: Ethernet is in link state; Off: physical link is not through.
Yellow Indicator	On: there is data being transmitted on physical link; Off: there is no data being transmitted on physical link.

BT-10x1GE-SFP Card

BT-10x1GE-SFP card provides ten gigabit SFP optical interfaces. It connects with BNPCIX and provides 10Gbps bandwidth for uplink and downlink.

The front panel of BT-10x1GE-SFP card is shown in Figure 16.

FIGURE 16 FRONT PANEL OF BT-10X1GE-SFP CARD

There are ten SFP ports on the front panel of BT-10x1GE-SFP card. Each port has two LED indicators in green and yellow respectively. Their functions are described in Table 12.

TABLE 12 INDICATOR FUNCTIONS

Indicator	Description
Green Indicator	On: Ethernet is in link state; Off: physical link is not through.
Yellow Indicator	On: there is data being transmitted on physical link; Off: there is no data being transmitted on physical link.

BT-4GE-SFP Card

BT-4GE-SFP card provides four gigabit SFP optical interfaces. It connects with BNPCH and provides 4Gbps bandwidth for uplink and downlink.

The front panel of BT-4GE-SFP card is shown in Figure 17.

FIGURE 17 FRONT PANEL OF BT-4GE-SFP CARD

There are four SFP ports on the front panel of BT-4GE-SFP card. Each port has two LED indicators in green and yellow respectively. Their functions are described in Table 13.

TABLE 13 INDICATOR FUNCTIONS

Indicator	Description
Green Indicator	On: Ethernet is in link state; Off: physical link is not through.
Yellow Indicator	On: there is data being transmitted on physical link; Off: there is no data being transmitted on physical link.

1-Port POS48 Interface Card

1-port POS48 interface card (OC-48c/ STM-16c POS interface card) provides one standard 2.5G optical interface for BRAS. Its major functions are:

- Realizing optical and electric conversion of one channel of 2.5GB/s signals.
- Mapping POS frames of OC-48c; conducting data width conversion; transmitting PPP packets together with BNPCH.
- Recovering clock and data of line.
- Extracting and operating related information of physical layer and data link layer, like information on running, maintenance and performance monitoring; reporting states of POS48 and line to BNPCT in interrupted mode.

1-port POS48 interface card has different types according to transmission distance and medium.

The front panel of BT-1POS-OC48-SFF-SC interface card is shown in Figure 18.

FIGURE 18 FRONT PANEL OF BT-1POS-OC48-SFF-SC CARD

The front panel of BT-1POS-OC48-SFF-LC interface card is shown in Figure 19.

FIGURE 19 FRONT PANEL OF BT-1POS-OC48-SFF-LC CARD

The front panel of BT-1POS-OC48-SFF–LH interface card is shown in Figure 20.

FIGURE 20 FRONT PANEL OF BT-1POS-OC48-SFF–LH CARD

Interface types and features are described in Table 14.

TABLE 14 INTERFACE TYPE AND FEATURE DESCRIPTIONS

Type	Description
SMF/2KM SC	LC connector, single-mode fiber, with wavelength of 1310nm and maximum transmission distance of 2km
SMF/15KM LC	LC connector, single-mode fiber, with wavelength of 1310nm and maximum transmission distance of 15km
SMF/80KM LH	LC connector, single-mode fiber, with wavelength of 1550nm and maximum transmission distance of 80km

There are four indicators on the front panel of 1-port POS48 interface card. Their functions are described in Table 15.

TABLE 15 INDICATOR FUNCTIONS

Indicator	Description
RUN (Green)	Indicating state of card, it is on when card works normally.
ALM (Red)	Indicating state of the card, it is on if fault occurs and is off in normal state.
SD (Green)	Indicating the status of the optical port, it is on if optical signals are available, and it is off if no

Indicator	Description
	optical signals are available.
PPP (Green)	Indicating the status of the link, it is on if the link is successfully set up and is off if the link fails to be set up.

BT-8ATM-OC3-SFP Card

BT-8ATM-OC3-SFP card provides eight standard OC-3c optical interfaces, realizing the standard 1+1 or 1:N protection function in SDH standard. The interface card support POS and ATM encapsulation. It connects with BNPCH through backplane, receiving and sending data packet according to OC-3c speed.

The front panel of BT-8ATM-OC3-SFP card is shown in Figure 21.

FIGURE 21 FRONT PANEL OF BT-8ATM-OC3-SFP CARD

There are ten indicators on the front panel of BT-8ATM-OC3-SFP card. Their functions are described in Table 16.

TABLE 16 INDICATOR FUNCTIONS

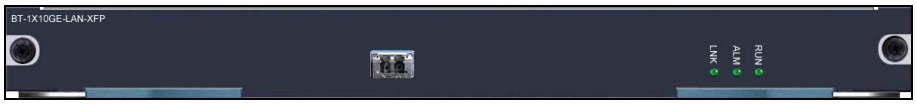
Indicator	Description
RUN (Green)	Indicating state of card, it is on when card works normally.
ALM (Red)	Indicating state of the card, it is on if fault occurs and is off in normal state.
P1 (Green)	Indicating the status of the No.1 optical port, it is on if optical signals are available, and it is off if no optical signals are available.
P2~P8 (Green)	Indicating the status of the No.2~8 optical port, it is on if optical signals are available, and it is off if no optical signals are available.

1-Port 10 Gigabit Ethernet Interface Card

1-Port 10 gigabit Ethernet interface card has two types, 10 gigabit LAN interface card and 10 gigabit WAN interface card. It connects with BNPCIX through SPI4.2 bus, with bandwidth of 10Gbps for uplink and downlink.

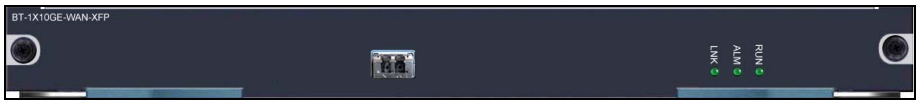
The front panel of BT-1x10GE-LAN-XFP card is shown in Figure 22.

FIGURE 22 FRONT PANEL OF BT-1X10GE-LAN-XFP CARD



The front panel of BT-1x10GE-WAN-XFP card is shown in Figure 23.

FIGURE 23 FRONT PANEL OF BT-1X10GE-WAN-XFP CARD



There are three indicators on the front panel of 1-Port 10 gigabit Ethernet interface card. Their functions are described in Table 17.

TABLE 17 INDICATOR FUNCTIONS

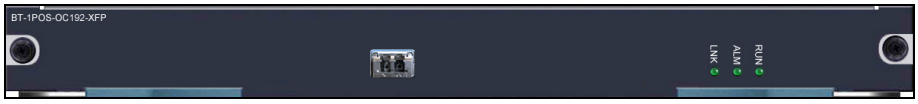
Indicator	Description
RUN (Green)	Indicating state of card, it is on when card works normally.
ALM (Red)	Indicating state of the card, it is on if fault occurs.
Link (Green)	It is on when there is optical signal received.

BT-1POS-OC192-XFP Card

BT-1POS-OC192-XFP card provides one LC 10 gigabit POS interface for BRAS. It connects with BNPCIX through SPI4.2 bus, with bandwidth of 10Gbps for uplink and downlink.

The front panel of BT-1POS-OC192-XFP card is shown in Figure 24.

FIGURE 24 FRONT PANEL OF BT-1POS-OC192-XFP CARD



There are three indicators on the front panel of BT-1POS-OC192-XFP card. Their functions are described in Table 18.

TABLE 18 INDICATOR FUNCTIONS

Indicator	Description
RUN (Green)	Indicating state of card, it is on when card works normally.
ALM (Red)	Indicating state of the card, it is on if fault occurs.
Link (Green)	It is on when there is optical signal received.

Chapter 4

Usage and Operation

Overview

Introduction This chapter describes configuration methods, command modes and use of command lines of ZXUAS 10800E Carrier Class BRAS.

Contents This chapter includes the following topics.

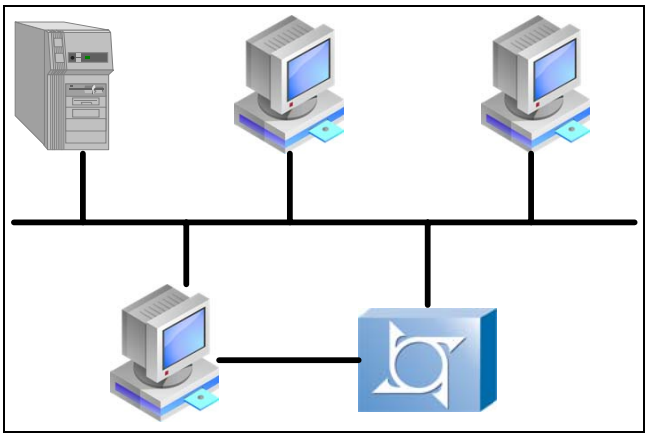
Configuration Methods

To provide users with maximum operation flexibility, ZXUAS 10800E Carrier Class BRAS provides multiple configuration methods. Users can select suitable configuration methods according to connected network, as shown in Figure 25. Configuration methods are described as follows:

- Configuration through COM port: This is main method to configure a UAS.

- Configuration through Telnet: In this method, UAS can be configured from any part of network
- Configuration through NM workstation: This method needs corresponding NM software supporting SNMP protocol.
- Downloading UAS configuration files through TFTP/FTP Server

FIGURE 25 ZXUAS 10800E CARRIER CLASS BRAS CONFIGURATION METHODS



Configuring Serial Port Connection

Purpose This topic describes how to configure serial port connection.

Steps To configure serial port connection, perform the following steps.

1. After connecting ZXUAS 10800E to a PC through serial port, select **Start > Programs > Accessories > Communications > HyperTerminal**.

   Result: A dialog box appears, as shown in Figure 26.

FIGURE 26 CONNECTION DESCRIPTION DIALOG BOX

2. Input a name and select an icon for ZXUAS 10800E, and then click **OK**.

   Result: A dialog box appears, as shown in Figure 27.

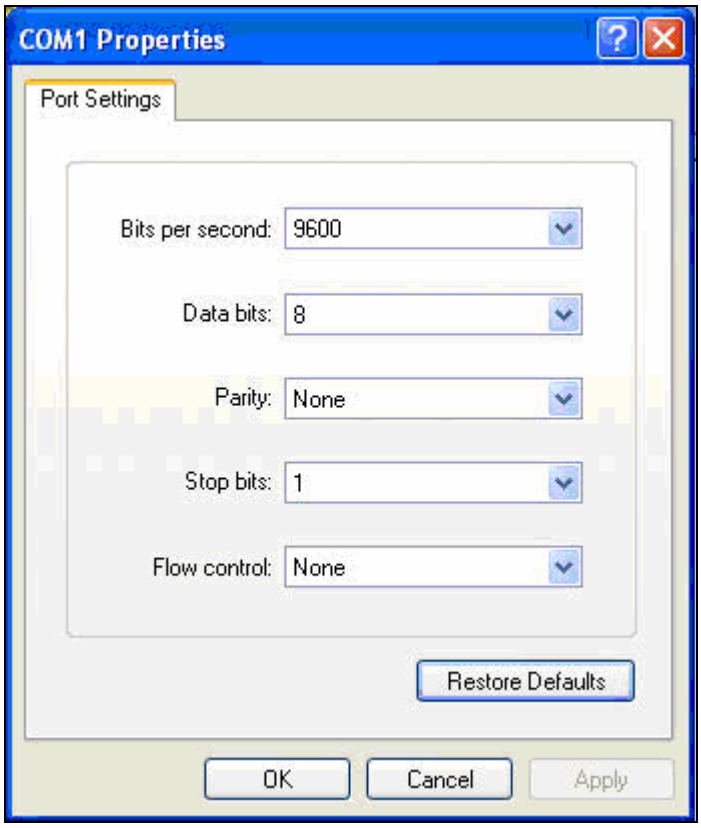
FIGURE 27 CONNECTION TO DIALOG BOX

3. Select a COM interface according to which interface is in use and then click **OK**.

   Note: Here take COM1 for example.

   Result: A dialog box appears, as shown in Figure 28.

FIGURE 28 COM1 PROPERTIES DIALOG BOX



4. Set COM port attribute. Parameter values are described in Table 19.

TABLE 19 PARAMETER VALUES

Parameters	Values
Bits per Second	9600
Data bit	8
Parity	None
Stop bit	1
Data flow control	None

END OF STEPS

Result Serial port connection has been configured.

Configuring Telnet Connection

Purpose This topic describes how to configure telnet connection.

Prerequisites To configure Telnet connection, meet the following requirements.

- Username and password have been set to prevent illegal users from accessing the equipment by Telnet.
- IP addresses of the equipment and the PC that a user is using should be in the same network segment.

Steps To configure telnet connection, perform the following steps.

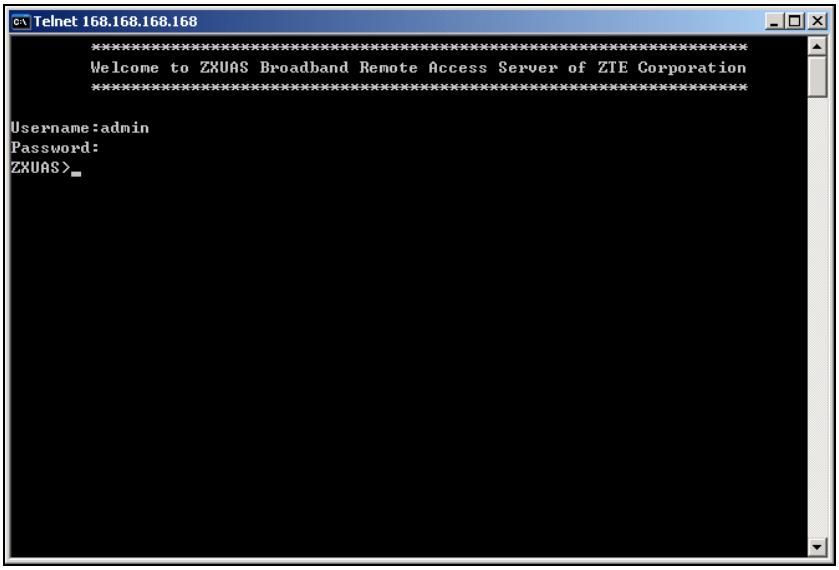
1. Select **Start > Run**, and input **telnet** <*ip-address*>.

   Note:

   - Parameter <*ip-address*> is the IP address of ZXUAS 10800E.
   - Instead of this step, users can input **telnet** <*ip-address*> in command line interface.

   Result: An interface appears, as shown in Figure 29.

FIGURE 29 TELNET LOGIN INTERFACE



2. Input user name and password to finish login.

END OF STEPS

Result Telnet connection has been configured.

Command Modes

Introduction To configure and manage UAS equipment conveniently, ZXUAS 10800E assigns commands to different modes according to different functions and rights. A command can only be carried out in a special mode. In any command mode, enter a question mark "?", and the commands that can be used in the mode are displayed. Command modes of ZXUAS 10800E are as follows:

- User mode

- Privileged mode
- Global configuration mode
- Interface configuration mode
- Route Configuration mode
- Diagnosis mode

Configuring User Mode

Purpose This topic describes how to configure user mode.

Steps To configure user mode, perform the following steps.

1. Use HyperTerminal to log in to system and system enters user mode automatically.

   Result: Prompt of user mode is a host name of UAS followed by a mark ">", as shown below (the default host name is ZXUAS):

   ```
   ZXUAS>
   ```

2. Use commands such as **ping** and **telnet** to view some system information.

END OF STEPS

Result User mode has been configured.

Configuring Privileged Mode

Purpose This topic describes how to configure privileged mode.

Steps To configure privileged mode, perform the following steps.

1. In user mode, input **enable** command and corresponding password to enter privileged mode, as shown below:

   ```
   ZXUAS>enable
   Password: (The password ate not displayed on the screen)
   ZXUAS#
   ```

   Note: In privileged mode, users can view more detailed configuration information and also can enter configuration mode to configure entire UAS. Therefore, a password must be used to prevent illegal use of unauthorized users.

2. To return from privileged mode to user mode, use **disable** command.

END OF STEPS

Result Privileged mode has been configured.

Configuring Global Configuration Mode

Purpose This topic describes how to configure global configuration mode.

Steps To configure global configuration mode, perform the following steps.

1. In privileged mode, input **config terminal** command to enter global configuration mode, as shown below:

```
ZXUAS#configure terminal
Enter configuration commands, one par line, End with Ctrl-Z
ZXUAS(config)#
```

Note: Commands in global configuration mode act on entire system, not merely on a protocol or interface.

2. To return from global configuration mode to privileged mode, use **exit** command or **end** command or press **<CTRL+Z>**.

END OF STEPS

Result Global configuration mode has been configured.

Configuring Interface Configuration Mode

Purpose This topic describes how to configure interface configuration mode.

Steps To configure interface configuration moce, perform the following steps.

1. In global configuration mode, use **interface** command to enter interface configuration mode, as shown below:

```
ZXUAS(config)#interface fei_2/1     (fei_2/1 is an interface
name, indicating first interface of Ethernet interface module in
slot 2)
ZXUAS(config-if)#
```

2. To return from interface configuration mode to global configuration mode, use **exit** command.
3. To return from interface configuration mode to privileged mode directly, use **end** command or press **<CTRL+Z>**.

END OF STEPS

Result Interface configuration mode has been configured.

Configuring Route Configuration Mode

Purpose This topic describes how to configure route configuration mode.

Steps

To configure route configuration mode, perform the following steps.

1. In global configuration mode, input **router** command to enter route configuration mode, as shown below:

```
ZXUAS(config)#router ospf 1
ZXUAS(config-router)#
```

Note: Routing protocols include RIP, OSPF, IS-IS and BGP. Here, routing protocol OSPF is configured.

2. To return from route configuration mode to global configuration mode, use **exit** command.
3. To return from route configuration mode to privileged mode directly, use **end** command or press **<CTRL+Z>**.

END OF STEPS

Result Route configuration mode has been configured.

Configuring Diagnosis Mode

Purpose This topic describes how to configure diagnosis mode.

Steps To configure diagnosis mode, perform the following steps.

1. In privileged mode, input **diagnose** command to enter diagnosis mode, as shown below:

```
ZXUAS#diagnose
Test commands:
ZXUAS(diag)#
```

Note: Diagnosis test commands are provided in diagnosis mode. These commands can be used to test cards used in a UAS, including bus and connectivity tests. In a diagnosis test, it is much better not to conduct UAS configuration.

2. To return from diagnosis mode to privileged mode, use **exit** command or **end** command or press **<CTRL+Z>**.

END OF STEPS

Result Diagnosis mode has been configured.

Using Online Help

Online Help In command mode, available commands list is displayed if question mark (?) is entered that follows the system prompt. Command key words list and parameters can be obtained through online help.

Purpose This topic describes how to use online help.

Steps To use online help, perform the following steps.

1. Input a question mark (?) in any command mode prompt toview all commands and brief command descriptions.

   Result: Command mode is viewed.

   Example: This example shows the use of question mark (?) in user mode.

```
ZXR10>?
Exec commands:
  enable   Turn on privileged commands
  exit     Exit from the EXEC
  login    Login as a particular user
  logout   Exit from the EXEC
  ping     Send echo messages
  quit     Quit from the EXEC
  show     Show running system information
  telnet   Open a telnet connection
  trace    Trace route to destination
  who      List users who is logining on
ZXR10>
```

2. Input a question mark (?) after a character or character string.

   Result: The list of commands or keywords beginning with that character or character string is displayed.

   Example: An example given below shows the character string.

```
ZXR10#co?
configure copy
ZXR10#co
```

   Note: There is no space between character (Character string) and the question mark (?).

3. Press **Tab** after the character. If the command or key word with the character string as the prefix is unique, align it and add a space after it.

   Result: A keyword beginning with that character string is displayed.

Example: An example is shown below.

```
ZXR10#con<Tab>
ZXR10#configure        (There is a space
between configure and cursor)
```

Note: There is no space between character string and **Tab**.

4. Input a question mark (?) after commands, key words and parameters.

   Result: It shows the keyword or parameter to be input next and its brief explanation.

   Example: An example is shown below.

```
ZXR10#configure ?
  terminal  Enter configuration mode
ZXR10#configure
```

   Note: A space should be input before the question mark (?).

END OF STEPS

Result Online command help has been configured

Notes

- If incorrect command, key words or parameters are entered, subscriber interface will provide error isolation with "^" after carriage return. "^" appears below the first character of the input incorrect command, key word or parameter. For example:

```
ZXR10#von ter
       ^
% Invalid input detected at '^' marker.
ZXR10#
```

- All commands in the command line operation are case-insensitive.

Command History

Input Command User interface provides a record of up to 10 previously entered commands. This feature is particularly useful to recall long or complex commands.

Re-invoke commands from the record buffer. Execute one of the following operations, as shown in Table 20.

TABLE 20 OPERATIONS FOR COMMAND HISTORY

Command	Function
Press **<Ctrl+P>** or < ↑ >	This recalls commands in the history buffer in a forward sequence

Command	Function
Press **<Ctrl+N>** or < ↓ >	This recalls commands in the history buffer in a backward sequence

In the privileged mode, use **show history** command to list the recently used commands.

This page is intentionally blank.

Chapter 5

System Management

Overview

Introduction This topic covers brief introduction about system management of ZXUAS 10800E Carrier Class BRAS.

Contents This chapter includes the following topics.

Introduction to File System

In ZXUAS 10800E Carrier Class BRAS, FLASH is used as major storage device for storing version files and configuration files. Operations such as version upgrading and configuration saving, must be conducted in flash.

There are three directories in Flash by default.

- IMG
- CFG
- DATA

IMG System mapping files (that is, image files) are stored under this directory. The extended name of the image files is .zar. The image files are dedicated compression files. Version upgrade

means to change the corresponding image files under the directory.

CFG This directory is for saving configuration files, whose name is startrun.dat. Information is saved in the Memory when using command to modify the switch configuration. To prevent the configuration information loss at the time of switch restart, use **write** command to write the information in the Memory into FLASH, and save the information in the startrun.dat file. When there is a need to clear the old configuration in the switch to reconfigure data, use **delete** command to delete startrun.dat file, then restart the switch.

DATA This directory is for saving log.dat file which records alarm information.

Operating File System Management

Background ZXUAS 10800E provides many commands for file operations. Command format is similar to DOS commands as present in Microsoft Windows Operating System.

Purpose This topic describes how to configure file system management.

Steps To configure file system management, perform the following steps.

1. To copy files between Flash and FTP/TFTP server, use the following command.

Format	Function
ZXR10#**copy** <*source-device*> <*source-file*> <*destination-device*> <*destination-file*>	This copies files between Flash and FTP/TFTP server

2. To view current directory path, use the following command.

Format	Function
ZXR10#**pwd**	This displays current directory path

3. To view files and subdirectories of a specified device or under a specified directory, use the following command.

Format	Function
ZXR10#**dir** [<*directory*>]	This displays files, subdirectory information under a designated directory

4. To delete a file under a designated directory of the current device, use the following command.

Format	Function
ZXR10#**delete** <*filename*>	This deletes the files under the a designated directory of the current device

Result: A Prompt appears, Are you sure to delete files with options [Yes/No].

5. To enter into specific directory, use the following command.

Format	Function
ZXR10#**cd** <*directory*>	This enables to enter specified directory or the current device

Result: This command sets the prompt into designated directory like flash: /(directory name).

6. To return to the superior directory, use the following command.

Format	Function
ZXR10#**cd..**	This returns to the superior directory

7. To make directory in flash, use the following command.

Format	Function
ZXR10#**mkdir** <*directory*>	This creates new directory in flash

8. To delete a directory in flash, use the following command.

Format	Function
ZXR10#**rmdir** <*directory-name*>	This deletes designated directory from flash

9. To modify the name of directory in flash, use the following command.

Format	Function
ZXR10#**rename** <*source-filename*> <*destination-filename*>	This modifies the name of the designated file or directory in a flash

END OF STEPS

Result File system management has been configured.

Example 1 This example shows how to view the current files in the Flash.

```
ZXUAS#dir
Directory of flash:/
       Attribute    size    date        time         name
   1   drwx         512    JUN-27-2002  15:28:56     CFG
   2   drwx         512    JUN-27-2002  15:28:56     DATA
   3   drwx         512    JUL-08-2002  07:51:56     IMG
65007616 bytes total (15863808 bytes free)
ZXUAS#cd img    (Enter the directory img)
ZXUAS#dir      (Show the current directory information)
Directory of flash:/img
       Attribute   size    date           time        name
   1   drwx        512     JUL-08-2002    07:51:56    .
   2   drwx        512     JUL-08-2002    07:51:56    ..
   3   -rwx      16364919  MAY-11-2005    11:37:06
ZXUAS.ZAR
65007616 bytes total (15863808 bytes free)
ZXUAS#
```

Example 2 This example shows how to create a directory ABC in the Flash and then delete it.

```
ZXUAS#mkdir ABC  (Add a subdirectory ABC under the current
directory)
ZXUAS#dir   (View the current directory information and
find that the directory ABC has been added successfully)
Directory of flash:/
       attribute    size   date           time        name
   1   drwx         512    JUN-27-2002    15:28:56    CFG
   2   drwx         512    JUN-27-2002    15:28:56    DATA
   3   drwx         512    JUL-08-2002    07:51:56    IMG
   4   drwx         512    AUG-06-2003    14:58:04    ABC
65007616 bytes total (15863808 bytes free)
ZXUAS#rmdir ABC         (Delete the subdirectory ABC)
ZXUAS#dir                 (View the current directory
information and find that the directory ABC has been
deleted successfully)
Directory of flash:/
       attribute    size   date           time        name
   1   drwx         512    JUN-27-2002    15:28:56    CFG
   2   drwx         512    JUN-27-2002    15:28:56    DATA
   3   drwx         512    JUL-08-2002    07:51:56    IMG
65007616 bytes total (15863808 bytes free)
ZXUAS#
```

Backing up Data

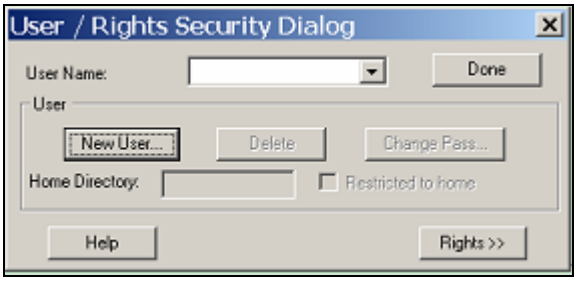
Purpose This topic describes how to back up data from FLASH to FTP/TFTP server, so that when configuration fault occurs, services can be recovered immediately.

Steps To back up data from FLASH to FTP/TFTP server, perform the following steps. Here take WFTPD software and FTP server as an example.

1. Start and set background FTP server.
   i. Start FTP server and select **Security > Users/Rights**.

   Result: A dialog box appears, as shown in Figure 30.

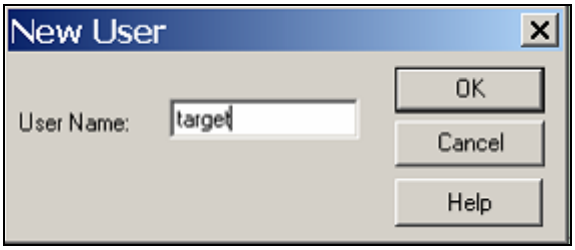
FIGURE 30 USER/RIGHT SECURITY DIALOG



   ii. Click **New User...** in Figure 30.

   Result: A dialog box appears, as shown in Figure 31.

FIGURE 31 NEW USER DIALOG BOX



   iii. Set user name and click **OK**.

   iv. Click **Change Pass...** button in Figure 30.

   Result: A dialog box appears, as shown in Figure 32.

FIGURE 32 CHANGE PASSWORD

v. Set password and click **OK**.

2. Input file path of version file or configuration file in **Home Directory** in Figure 30, and then click **Done**.
3. Use **copy** command to back up data from FLASH to FTP server.

   Example: This example shows how to use **copy** command to copy version information and configuration file to FTP server.

```
(back up version information)
ZXUAS#copy flash: /img/ZXUAS.zar ftp:
//10.61.98.88/ZXUAS.zar@admin: uas
(back up configuration file)
ZXUAS#copy      flash:      /cfg/startrun.dat      ftp:
//10.61.94.92/startrun.dat@admin: uas
```

4. Check whether the data in the file with specific path is the latest.

END OF STEPS

Result Data has been backed up.

Note Before starting FTP/TFTP server in background, check the following points:

- Serial/Ethernet interface of BIC board connects with that of background PC and operations can be implemented through HyperTerminal.
- IP addresses of background PC and ZXUAS 10800E Ethernet interface are in the same network segment. Make sure that the PC and ZXUAS 10800E can ping to each other successfully.
- Before copy startrun.dat to FTP server, use **write** command to save configuration information to startrun.dat. This makes the data latest.

Restoring Data

Purpose This topic describes how to restore data from FTP server to FLASH when configuration fault occurs.

Steps To restore data from FTP server to FLASH, perform the following steps.

1. Start and set background FTP server.

   Note: For detailed steps, refer to step 1 in Backing up Data.

2. Use **copy** command to restore data from FTP server to FLASH.

   Note: If the file of the same name has been existed in specific directory, delete or rename the primary file and then start to copy.

   Example: This example shows how to restore data from FTP server to FLASH.

```
ZXUAS#copy ftp://10.61.98.88/ZXUAS.zar@admin:uas flash:
/img/ZXUAS.zar
%Code 266: Error stating(special destination file
exists)

ZXUAS#delete /img/ZXUAS.zar          (delete ZXUAS.zar)
ZXUAS#copy ftp: //10.61.98.88/ZXUAS.zar@admin:uas
flash: /img/ZXUAS.zar   (restore version file)
ZXUAS#copy   ftp:   //10.61.94.92/startrun.dat@admin:uas
flash: /cfg/startrun.dat  (restore configuration file)
```

3. Check the data copied from FTP server.

END OF STEPS

Result Data has been restored.

Upgrading the Version at Normality

Purpose This topic describes how to upgrade the version for ZXUAS 10800E in normal case.

Prerequisites The following requirements are to be completed before software version upgrade.

- Connect the console interface of ZXUAS 10800E to the serial interface of background host. Connect management Ethernet interface of ZXUAS 10800E to network interface of background host.
- IP address of background host for upgrade and ZXUAS 10800E console interface are in the same network segment.

- Start the background FTP server.

Steps To upgrade the version at normality, perform the following steps.

1. View the information of the running version.
2. Use **delete** command to delete the old version file. It is possible to keep the old version file by renaming it in the case that FLASH space is sufficient.
3. Copy the new version file in background FTP server to IMG directory in FLASH. Version file name is ZXUAS.zar.
4. Check whether new version file is available in directory IMG in FLASH or not. If the new version file is unavailable, it indicates the copy failure, then execute step 3 to recopy the version.
5. Reboot ZXUAS 10800E, check the running version to confirm whether the upgrade is successful or not.

END OF STEPS

Result Version upgrade at normality has finished.

Upgrading the Version at Abnormality

Purpose This topic describes how to upgrade the version for ZXUAS 10800E in abnormal case.

Prerequisites The following requirements are to be completed before software version is upgraded.

- Connect the console interface of ZXUAS 10800E to the serial interface of background host. Connect management Ethernet interface of ZXUAS 10800E to network interface of background host.
- IP address of background host for upgrade and ZXUAS 10800E console interface are in the same network segment.
- Start the background FTP server.

Steps To upgrade the version for ZXUAS 10800E in abnormal case, perform the following steps.

1. Start ZXUAS 10800E with HyperTerminal and press any key to enter Boot status. The following content appears:

```
System Bootstrap, ZXUAS-10800E System Boot Version: 2.2
Creation date: Jan 19 2005, 17:17:02
Copyright (c) 2002 by ZTE Corporation

Boot Location [0:Net,1:Flash] : 0
Client IP [0:bootp]           : 168.168.168.228
Netmask                       : 255.255.255.0
Server IP [0:bootp]           : 168.168.168.1
Gateway IP                    : 0.0.0.0
FTP User                      : uas
FTP Password                  :
Boot Path                     : ZXUAS.zar
Enable Password               :

Serial Number                 : 10020

Press any key to stop for change parameters...
d1
[ZXUAS Boot]:
```

2. Input "c" in Boot status and press **Enter** to enter parameter modification status.

   i. Change the boot mode to boot from background FTP.

   ii. Change the FTP server address to the corresponding background host address.

   iii. Change the client terminal address and gateway address to ZXUAS 10800E management Ethernet interface address.

   iv. Set corresponding subnet mask and FTP username and password.

   Result: [ZXR10 Boot] prompt appears after above parameter modification is completed, as shown below.

```
[ZXUAS Boot]: c

'.' = clear field;  '-' = go to previous field;  ^D =
quit
Boot Location [0:Net,1:Flash]: 0    (0 means booting
from background FTP; 1 means booting from
FLASH)
Client IP [0:bootp]: 168.168.168.228   (Corresponds
to management Ethernet port address)
Netmask: 255.255.255.0
Server IP [0:bootp]: 168.168.168.1   (Corresponds to
background FTP server address)
Gateway IP: 0.0.0.0      (Use management Ethernet
port address as gateway)
FTP User: uas    (Corresponds to FTP username
uas)
FTP Password:          (Corresponds to target
user password)
FTP Password Conf:
Boot Path: ZXUAS.zar         (Use default)
Enable Password:             (Use default)
Enable Password Confirm:     (Use default)

[ZXUAS Boot]:
```

3. Input "@". System boots the version from background FTP server automatically after carriage return.

```
[ZXUAS Boot]: @
Attaching network interface
lo0... .............[  OK  ]
FTP getting file
ZXUAS.zar[33552369].............[  OK  ]
Attached TCP/IP interface to lBNPCi unit 1
Attaching interface lo0...done

Adding 17819 symbols for standalone.
             CPU: PC PENTIUM.  Processor #0.
EnableMPUL2
cache...............................[  OK  ]
Read NvRam..........................[  OK  ]
Configure flash card................[  OK  ]
Copy img files......................[  OK  ]
Reset All Cards.....................[  OK  ]
Initialize NvRam....................[  OK  ]
Board interrupts initialized.........[  OK  ]
Start version ftp server............[  OK  ]

Restricted Rights Legend
ZTE Corporation.
Pudong District, Shanghai, China


ZXUAS Operating System Software, ZTE Corporation
ZXUAS ROS  Version V4.8.01, (RELEASE VERSION)
ZXUAS 10800E  Software Version V2.8.01.A07, (RELEASE
VERSION)
Compiled May  10 2007, 08:50:49
Copyright (c) 2005-2010 by ZTE Corporation
ZXUAS 10800E Intel Pentium Processor with 512M bytes of
memory
8K bytes of non-volatile configuration memory
64M bytes of processor board System flash (Read/Write)

synchronizing ..................................OK!

****************************************************
Welcome to ZXUAS Broadband Remote Access Server of ZTE
Corporation
****************************************************

ZXUAS>
```

4. If system has been started normally, use **show version** command to check whether the new version is running in the memory or not. If it is the old running version, it indicates that booting from background server failed, in this case repeat the operations from step 1.
5. Delete the old version file zxr10.zar in the directory IMG in FLASH using command **delete,** Old version file is renamed for backup due to of space in FLASH is sufficient.
6. Copy the new version file in background FTP server to IMG directory in FLASH. Version file name is ZXUAS.zar.

```
ZXUAS#copy ftp: mng
//168.4.168.89/ZXUAS.zar@target:target flash:
/img/ZXUAS.zar
Starting copying file
..................................................
..................................................
file copying successful.
ZXUAS#
```

7. Check whether new version file is available in FLASH or not. If the new version file is unavailable, it indicates the file copy failure, execute step 6 to re-copy the version.
8. Restart ZXUAS 10800E and use the methods in step 4 to set boot mode as boot from FLASH. At this time, "Boot path" is changed into"/flash/img/ZXUAS.zar" automatically.

   Note: Boot mode is changed to boot from FLASH by using command **nvram imgfile-location local** in global configuration mode.
9. Input "@" in [ZXR10 Boot]: now system will boot a new version from FLASH after carriage return.
10. After a normal boot-up, check the running version to confirm the successful upgrade.

END OF STEPS

Result Version uograding at abnormality has finished.

Configuring System Parameters

Purpose This topic describes how to configure system parameters on ZXUAS 10800E.

Steps To configure system parameters, perform the following steps.

1. To set a hostname of system, use the following command.

Format	Function
ZXR10(config)#**hostname** *<network-name>*	This sets hostname of system

Note: Log on to router again after hostname modification and the prompt will include the new hostname.

2. To set welcome message upon system boot or when login on telnet, use the following command.

Format	Function
ZXR10(config)#**banner incoming**	This sets the greeting words for system startup

Example: This example shows how to set welcome message upon system.

```
ZXUAS(config)#banner incoming #
Enter TEXT message.  End with the character '#'.
**********************************
    Welcome to ZXUAS Router World
**********************************
#
ZXUAS(config)#
```

3. To prevent an unauthorized user from modifying the configuration, use the following command.

Format	Function
ZXR10(config)#**enable secret** {**0** *<password>*|5 *<password>*|*<password>*}	This sets password

4. To set Telnet username and password, use the following command.

Format	Function
ZXR10(config)#**username** **<***username***>** **password** *<password>*	This sets Telnet user and password

5. To set system time, use the following command.

Format	Function
ZXR10(config)#**clock set** *<current-time> <month> <day> <year>*	This sets system time

END OF STEPS

Result System parameters have been configured.

Viewing System Information

Purpose

This topic describes how to view system information.

Steps

To view system information, perform the following steps.

1. To view hardware and software versions of the system, use the following command.

Format	Function
ZXR10#**show version**	This displays the version information about the software and hardware of system

Example: The following information is displayed after carrying out **show version** command.

```
ZXUAS#show version
ZXUAS Router Operating System Software, ZTE Corporation
ZXUAS ROS Version V4.8.01
ZXUAS 10800E Software, Version V2.8.01.A07, RELEASE
SOFTWARE
Copyright (c) 2000-2005 by ZTE Corporation
Compiled May  10 2007, 08:50:49

System image files from net
<ftp://168.1.156.156/ZXUAS.zar>
System uptime is 5 days, 19 hours, 23 minutes

[RPU,panel 1,master]
Main processor: PENTIUM II with 512M bytes of memory
ROM: System Bootstrap, Version: ZXUAS 10800E BOOT
2.6.03,RELEASE SOFTWARE
[MPU,panel 1,master]
Main processor: PENTIUM II with 512M bytes of memory
8K bytes of non-volatile configuration memory
64M bytes of processor board System flash (Read/Write)
ROM: System Bootstrap, Version:ZXUAS 10800E BOOT
2.6.03,RELEASE SOFTWARE
System serial: 15002
[BSFC3,panel 2,master]
Main processor: PowerPC 8240 with 64M bytes of memory
ROM: System Bootstrap, Version: ,RELEASE SOFTWARE
[BNPCI,panel 3]
Main processor: ARM with 256M bytes of memory in slot 3
System with multiple processors (2 Network processors)
Every network processor with 256M bytes of memory
ROM(8M): System Bootstrap, Version:
, RELEASE SOFTWARE
FPGA Version(Switch) : V43
FPGA Version(Interface): V27
[BNPCH,panel 10]
Main processor: ARM with 256M bytes of memory in slot
10
System with multiple processors (2 Network processors)
Every network processor with 256M bytes of memory
ROM(8M): System Bootstrap, Version:
, RELEASE SOFTWARE
FPGA Version(Switch) : V43
FPGA Version(Interface): V23
```

2. To view running configuration, use the following command.

Format	Function
ZXR10#**show running-config**	This displays the running configuration

END OF STEPS

Result System information has been displayed.

Chapter 6

Interface Configuration

Overview

Introduction This chapter describes interface configuration on ZXUAS 10800E Carrier Class BRAS.

Contents This chapter includes the following topics.

Interfaces Types

There are tow types of interfaces on ZXUAS 10800E Carrier Class BRAS:

- Physical interfaces
- Logical interfaces

Physical interfaces are interfaces that exist actually, such as Ethernet interface, POS interfaces and ATM interfaces.

Logical interfaces are interfaces that exist due to configuration. They are also called virtual interfaces, such as VLAN sub-interfaces and Loopback interfaces.

Interface Naming Rules

Interfaces of ZXUAS 10800E are named in the following rule: <interface type>_<slot ID>/<port ID> <sub-interface or channel ID>.

- <interface type>: it is described in Table 21.

TABLE 21 <INTERFACE TYPE>

<interface type>	description
fei	Fast Ethernet interface
gei	Gigabit Ethernet interface
xgei	10 gigabit Ethernet interface
pos48	2.5G POS interface
pos192	10G POS interface
atm155	155M ATM interface
smartgroup	SmartGroup interface
loopback	Loopback interface

- <slot ID>: it refers to physical slots where line interface module is installed, ranging from 1 to 8.
- <port ID>: it refers to number allocated to line interface module connector. The value range and assignment of port IDs depend upon different types of line interface modules.

Ethernet Interface Configuration

Contents Ethernet interface configuration includes the following topics.

Ethernet Interface Overview

Ethernet interfaces of ZXUAS 10800E include fast Ethernet interface, gigabit Ethernet interface and 10 gigabit Ethernet interface.

Fast Ethernet Interface Fast Ethernet interface works at the speed of 10M or 100M, supporting half duplex and full duplex modes. It has auto-

negotiation function. By default, auto-negotiation function is enabled.

Gigabit Ethernet Interface

Gigabit Ethernet interface works at the speed of 1000M, supporting full duplex mode. By default, auto-negotiation function is enabled.

10 Gigabit Ethernet Interface

10 gigabit Ethernet interface works at the speed of 10G and in full duplex mode.

Configuring Ethernet Interface

Purpose

This topic describes how to configure Ethernet interface.

Steps

To configure Ethernet interface, perform the following steps.

1. To configure interface IP address, use the following command.

Format	Function
ZXUAS(config-if)#**ip address** <*ip-address*> <*net-mask*>	This configures interface IP address

2. To configure interface MTU, use the following command.

Format	Function
ZXUAS(config-if)#**ip mtu** <*bytes*>	This configures interface MTU

3. To configure interface speed, use the following command.

Format	Function
ZXUAS(config-if)#**speed** {**10|100|1000**}	This configures interface speed

4. To configure interface duplex mode, use the following command.

Format	Function
ZXUAS(config-if)#**duplex** {**half|full**}	This configures interface duplex mode

5. To enable auto-negotiation function, use the following command.

Format	Function
ZXUAS(config-if)#**negotiation auto**	This enables auto-negotiation function

END OF STEPS

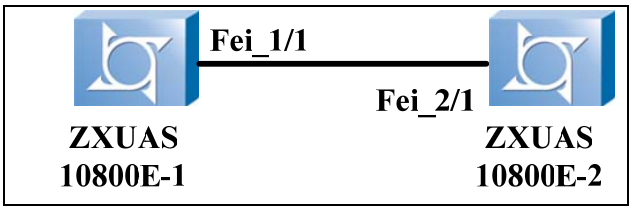
Result

Ethernet interface has been configured.

Example This example shows Ethernet interface configuration.

As shown in Figure 33, Ethernet interface of ZXUAS 10800E-1 is connected to Ethernet interface of ZXUAS 10800E-2.

FIGURE 33 ETHERNET INTERFACE CONFIGURATION



ZXUAS 10800E-1 configuration:

```
ZXUAS(config)#interface fei_1/1
ZXUAS(config-if)#ip address 10.1.1.2 255.255.255.252
ZXUAS(config-if)#duplex full
```

ZXUAS 10800E-2 configuration:

```
ZXUAS(config)#interface fei_2/1
ZXUAS(config-if)#ip address 10.1.1.1 255.255.255.252
ZXUAS(config-if)#duplex full
```

POS Interface Configuration

Contents POS interface configuration includes the following topics.

POS Interface Overview

SONET SONET (Synchronous Optical Network), a synchronous mechanism defined by ANSI, is a global standard transmission protocol. Its transmission speeds consist of a sequence, including STM (SDH Transport Module)-1 (155Mbit/s), STM-4c (622Mbit/s) and STM-16c/STM-16 (2.5Gbit/s). Speed of each higher level is four multiples of that of the lower level.

SDH SDH (Synchronous Digital Hierarchy), defined by CCITT (now called ITU-T), uses a sub aggregation of SONET. SDH can realize signal multiple access due to synchronous signals.

POS POS (Packet over SONET/SDH) is a group of SONET/SDH and is used in MAN and WAN. It supports grouping, such as IP grouping.

Basic protocol system of POS is listed below:

- Use SONET as physical layer protocol.
- Encapsulate grouping service in HDLC frames.
- Use PPP as link control protocol on data link layer.
- IP packet switching services run on network layer.

POS maps data packets with changeable length into SONET synchronous load, with SONET transmission standard on physical layer. It provides a high-speed, reliable and point to point data link.

There are two types of POS interfaces on ZXUAS 10800E: POS 10G and POS 2.5G. In POS interface configuration, default encapsulation type is PPP. The following topic takes POS 2.5G for example.

Configuring POS Interface

Purpose This topic describes how to configure POS interface.

Steps To configure POS interface, perform the following steps.

1. To configure IP address on POS interface, use the following command.

Format	Function
ZXUAS(config-if)#**ip address** *<ip-address> <net-mask>*	This configures IP address on POS interface

2. To configure mark on POS interface, use the following command.

Format	Function
ZXUAS(config-if)#**flag** {**c2** *<0-255>*|**j0** *<0-255>*|**s1s0** *<0-2>*}	This configures mark on POS interface

3. To configure frame format on POS interface, use the following command.

Format	Function
ZXUAS(config-if)#**framing** {**sonet**|**sdh**}	This configures frame format on POS interface

4. To configure interface loopback mode, use the following command.

Format	Function
ZXUAS(config-if)#**loopback** {**internal**|**line**}	This configures interface loopback mode

5. To configure interface MTU, use the following command.

Format	Function
ZXUAS(config-if)#**ip mtu** <*bytes*>	This configures interface MTU

6. To configure threshold of code error rate on POS interface, use the following command.

Format	Function
ZXUAS(config-if)#**threshold** {**sd-ber** <*4-9*>|**sf-ber** <*3-8*>}	This configures threshold of code error rate on POS interface

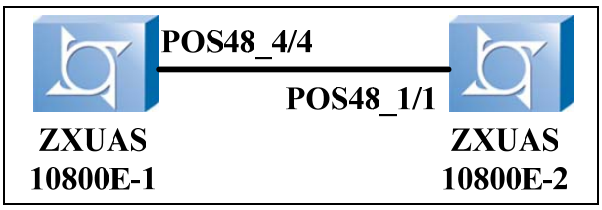
END OF STEPS

Result POS interface has been configured.

Example This example shows POS interface configuration.

As shown in Figure 34, POS interface of ZXUAS 10800E-1 is connected to POS interface of ZXUAS 10800E-2.

FIGURE 34 POS INTERFACE CONFIGURATION



ZXUAS 10800E-1 configuration:

```
ZXUAS(config)#interface pos48_4/4
ZXUAS(config-if)#ip address 192.168.1.1 255.255.255.252
```

ZXUAS 10800E-2 configuration:

```
ZXUAS(config)#interface pos48_3/1
ZXUAS(config-if)#framing sdh
ZXUAS(config-if)#ip mtu 1500
ZXUAS(config-if)#ip address 192.168.1.2 255.255.255.0
ZXUAS(config-if)#flag s1s0 2
ZXUAS(config-if)#flag c2 22
```

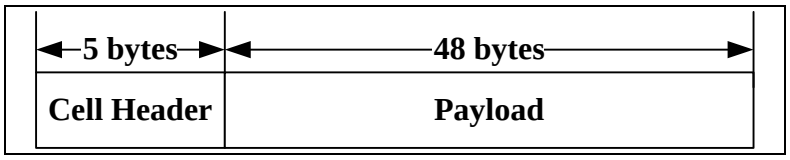
ATM Interface Configuration

Contents ATM interface configuration includes the following topics.

ATM Interface Overview

ATM Cell ATM uses cell as basic unit to transmit, forward and switch data. ATM cell format is shown in Figure 35. Each cell transmits data independently. Transmission delay is little due to the short length of cell.

FIGURE 35 ATM CELL FORMAT



Virtual Circuit ATM is a connection oriented switch technology based on virtual circuit. Each virtual circuit is identified VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier). Each VCI or VPI only has local meaning on the link between ATM nodes.

Basic Protocol Frame ATM basic protocol frame consists of three stages:

- User stage
- Control stage
- Management stage

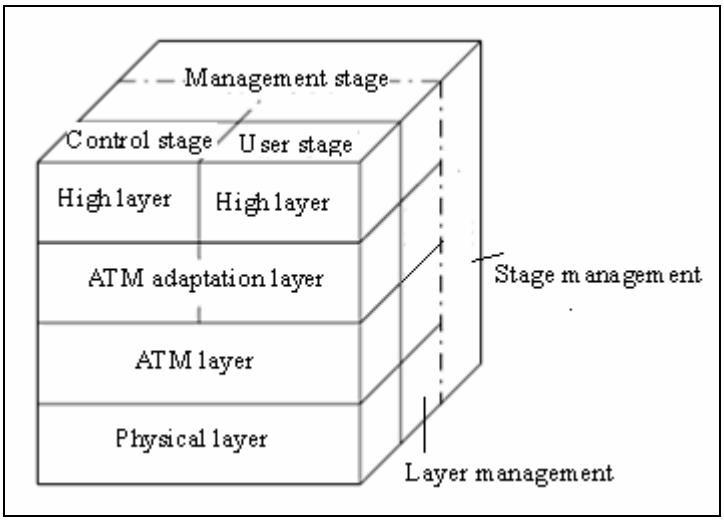
User stage and control stage have four layers: physical layer, ATM layer, adaption layer and high layer.

Management stage is classified into layer management and stage management. Layer management manages different layers of the stages. Stage management manages communications between the stages.

Control stage implements communications with signaling protocols.

The relationship of the layers and stages is shown in Figure 36.

FIGURE 36 RELATIONSHIP OF LAYERS AND STAGES



AAL (ATM Adaptation Layer) is the interface connecting high layer and ATM layer. It forwards information between high layer and ATM layer. There are four types of AALs: AAL1, AAL2, AAL3/4 and AAL5. Each type of AAL supports some different types of services in ATM network.

Configuring ATM Interface

Purpose This topic describes how to configure ATM interface.

Steps To configure ATM interface, perform the following steps.

1. To configure IP address on ATM interface, use the following command.

Format	Function
ZXUAS(config-if)#**ip address** *<ip-address> <net-mask>*	This configures IP address on ATM interface

2. To configure ATM interface frame format, use the following command.

Format	Function
ZXUAS(config-if)#**frame** {**sonet**|**sdh**}	This configures ATM interface frame format

3. To configure ATM interface MTU, use the following command.

Format	Function
ZXUAS(config-if)#**ip mtu** *<bytes>*	This configures ATM interface frame format

4. To create PVC, use the following command.

Format	Function
ZXUAS(config-if)#**atm pvc** <*vpi*> < *vci*>	This creates PVC

5. To configure packet switch function on ATM interface, use the following command.

Format	Function
ZXUAS(config-if)#**switch-leased-line**	This configures packet switch function on ATM interface

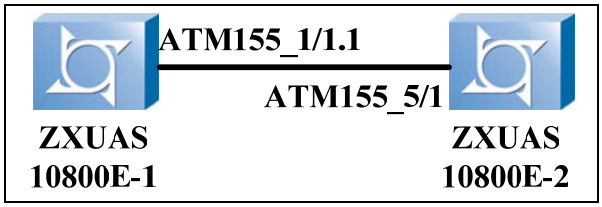
END OF STEPS

Result ATM interface has been configured.

Example This example shows ATM interface configuration.

As shown in Figure 37, ATM interface of ZXUAS 10800E-1 is connected to ATM interface of ZXUAS 10800E-2.

FIGURE 37 ATM INTERFACE CONFIGURATION



ZXUAS 10800E-1 configuration:

```
ZXUAS(config)#interface atm155_1/1.1
ZXUAS(config-if)#atm pvc 2 40
ZXUAS(config-if)#ip address 10.10.0.2 255.255.255.252
```

ZXUAS 10800E-2 configuration:

```
ZXUAS(config)#interface atm155_5/1
ZXUAS(config-if)#atm pvc 2 40
ZXUAS(config-if)#ip address 10.10.0.1 255.255.255.252
ZXUAS(config-if)#frame sdh
ZXUAS(config-if)#ip mtu 1500
```

Smartgroup Interface Configuration

Contents Smartgroup interface configuration includes the following topics.

Smartgroup Interface Overview

Smartgroup refers to aggregation of multiple physical interfaces into one logical interface, providing higher aggregated bandwidth and better reliability. One smartgroup interface can contain up to eight Ethernet interfaces in the same board slot. One Ethernet interface board can support up to 64 smartgroup interfaces.

Configuring Smartgroup Interface

Purpose This topic describes how to configure smartgroup interface.

Steps To configure smartgroup interface, perform the following steps.

1. To enter smartgroup interface configuration mode, use the following command.

Format	Function
ZXUAS(config)#**interface smartgroup** <*number*>	This enters smartgroup interface configuration mode

2. To configure IP address on smartgroup interface, use the following command.

Format	Function
ZXUAS(config-if)#**ip address** <*ip-address*> <*net-mask*>	This configures IP address on smartgroup interface

3. To configure load balance policy on smartgroup interface, use the following command.

Format	Function
ZXUAS(config-if)#**smartgroup load-balance** {**per-packet**| **per-destination**}	This configures load balance policy on smartgroup interface

4. To configure smartgroup interface MTU, use the following command.

Format	Function
ZXUAS(config-if)#**ip mtu** <*bytes*>	This configures smartgroup interface MTU

5. To add an Ethernet interface to smartgroup, enter Ethernet interface configuration mode, then use the following command.

Format	Function
ZXUAS(config-if)#**smartgroup** <*number*> **mode on**	This adds an Ethernet interface to smartgroup

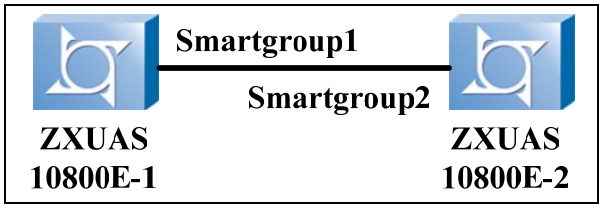
END OF STEPS

Result Smartgroup interface has been configured.

Example1 This example shows smartgroup interface configuration.

As shown in Figure 38, smartgroup interface of ZXUAS 10800E-1 is connected to smartgroup interface of ZXUAS 10800E-2.

FIGURE 38 SMARTGROUP INTERFACE CONFIGURATION



ZXUAS 10800E-1 configuration:

```
ZXUAS(config)#interface smartgroup 1
ZXUAS(config-if)#ip address 192.168.1.1 255.255.255.252
ZXUAS(config)#interface fei_8/1
ZXUAS(config-if)#smartgroup 1 mode on
ZXUAS(config)#interface fei_8/2
ZXUAS(config-if)#smartgroup 1 mode on
```

ZXUAS 10800E-2 configuration:

```
ZXUAS(config)#interface smartgroup 2
ZXUAS(config-if)#ip address 192.168.1.2 255.255.255.252
ZXUAS(config)#interface fei_8/1
ZXUAS(config-if)#smartgroup 2 mode on
ZXUAS(config)#interface fei_8/2
ZXUAS(config-if)#smartgroup 2 mode on
```

Example2 This example shows smartgroup interface used as user access.

Configuration of smartgroup interface connecting to network is shown below:

```
ZXUAS#configure terminal
ZXUAS(config)#interface smartgroup10
ZXUAS(config-if)#ip address 165.168.1.10 255.255.0.0
ZXUAS(config-if)#smartgroup load-balance per-packet
ZXUAS(config-if)#exit
ZXUAS(config)#interface fei_2/5
ZXUAS(config-if)#smartgroup 10 mode on
ZXUAS(config-if)#exit
ZXUAS(config)#int fei_2/6
ZXUAS(config-if)#smartgroup 10 mode on
ZXUAS(config-if)#
```

Configuration of smartgroup interface connecting to users is shown below:

```
ZXUAS#configure terminal
ZXUAS(config)#interface smartgroup20
ZXUAS(config-if)#ip address 168.168.1.10 255.255.0.0
ZXUAS(config-if)#smartgroup load-balance per-packet
ZXUAS(config-if)#exit
ZXUAS(config)#interface smartgroup20.1 bras
ZXUAS(config-subif)#encapsulation multi
ZXUAS(config-subif)#bind multi vbui vbui1 authentication
chap-pap
ZXUAS(config-subif)#subscriber location vbas
```

Chapter 7

BRAS Service

Overview

Introduction This chapter describes basic concepts and configuration of BRAS access features.

Contents This chapter includes the following topics.

BRAS Overview

BRAS Functions

BRAS is an application running on UAS. BRAS provides the following functions:

- Aggregates the output from digital subscriber line access multiplexers (DSLAM)
- Provides user Point-to-Point Protocol (PPP) sessions or IP-over-Asynchronous
- Enforces quality of service (QoS) policies
- Routes traffic into an Internet service provider (ISP) backbone network

Virtual Routing Field

Virtual Routing Field (VRF) is a private IP routing field, identified by VPN ID. In a VPN network, each VRF can be seen as a virtual router, as if it is a specific PE.

Virtual Router

A Virtual Router (VR) includes the following elements:

- An independent route table
- A set of interfaces belonging to this VRF
- A set of routing protocols only used in this VRF

Each PE can maintain one or more VRFs, as well as a public route table. VRFs are isolated from each other.

Domain

Domain is an aggregate of BRAS service management features, which has AAA system, legal user group and some services management policy.

ZXUAS 10800E manages user groups with domain. Each domain has its own resources and configurations, including:

- Alias: unique identification for users
- Maximum domain user number
- Authentication and Accounting mode
- Authentication and accounting servers group association
- Default user template
- Maximum synchronization users of domain
- Associated VRF

Virtual BRAS User Interface

VBUI is a logical interface for IP protocol, only used for BRAS services. IP address, related network mask, ARP protocol, the MTU, control list and other protocols should be configured on VBUI. VBUI supports more than one physical circuit.

User

User means that the one who can access the device and obtain services or management legally. Each legal user has respective attributes. Personal service information is contained in these attributes, including name, password, IP Address, IP Address policy, Qos parameters and ACL parameters.

Dynamic User Dynamic user is a concept which records the whole process and information for a user access to the device. The life of dynamic user begins when a user accesses to the device and ends when the user leaves from the device.

Interface Interface means a physical interface which has the maximum user number for every special service.

Circuit The circuit refers to a logical circuit, such as DOT1Q VLAN, ATM PVC and non-DOT1Q encapsulated Ethernet interface.

Binding Only when circuit and PPP link is bound with VBUI can users accessing to the service network obtain services. Binding is the core concept for BRAS access service.

There two types of bindings:

- Static binding

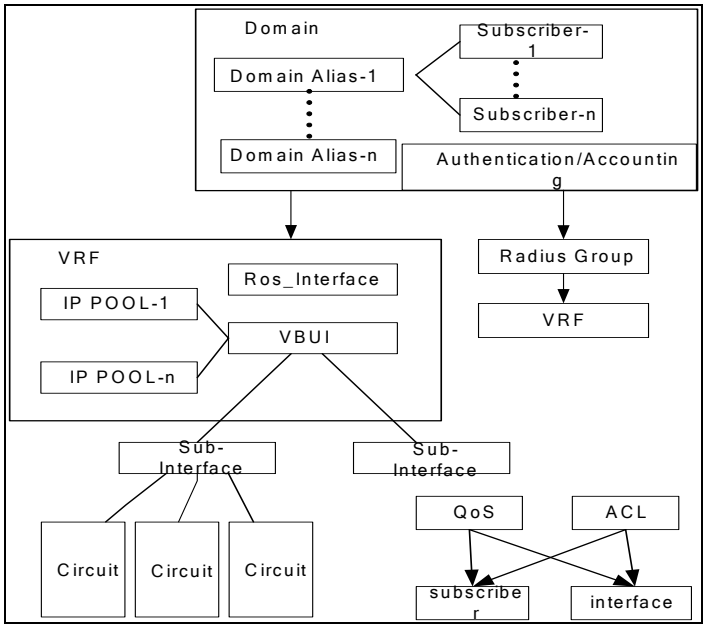
  Bind relationship can be designate directly.

- Dynamic binding

  According to IP address that user gets from the device (PPP protocol), the system finds the corresponding interface and gets the relationship between the user and the interface.

Object Relationships Object relationships are shown in Figure 39.

FIGURE 39 OBJECT RELATIONSHIPS



Configuring Physical Interface

Purpose This topic describes how to configure physical interfaces of ZXUAS 10800E.

Steps To configure physical interfaces, perform the following steps.

1. To enable interface, use the following command.

Format	Function
ZXUAS(config-if)#**no shutdown**	This enables interface

2. To configure IP address, use the following command.

Format	Function
ZXUAS(config-if)#**ip address** *<ip-address> <net-mask>*	This configures IP address

3. To configure interface speed, use the following command.

Format	Function
ZXUAS(config-if)#**speed** {**10|100|1000**}	This configures interface speed

4. To configure duplex mode, use the following command.

Format	Function
ZXUAS(config-if)#**duplex** {**half|full**}	This configures duplex mode

5. To associate an interface with VRF, use the following command.

Format	Function
ZXUAS(config-if)#**ip vrf forwarding** *<vrf-name>*	This associates an interface with VRF

6. To view interface information, use the following command.

Format	Function
ZXUAS(config)#**show ip interface** *<interface>*	This views interface information

END OF STEPS

Result Physical interface has been configured.

Example This example shows how to configure a physical interface and view configuration information.

```
ZXUAS#configure  terminal
ZXUAS(config)#interface fei_1/2
ZXUAS(config-if)#no shutdown
ZXUAS(config-if)#ip address 10.61.86.88 255.0.0.0
ZXUAS(config-if)#speed 100
ZXUAS(config-if)#duplex full
/*view interface information*/
ZXUAS(config)#show ip interface fei_1/2
fei_1/2  AdminStatus is up, PhyStatus is up, line protocol
is up
  Internet address is 10.61.86.88/8
  Broadcast address is 255.255.255.255
  MTU is 1500 bytes
  ICMP unreachables are always sent
  ICMP redirects replies are always sent
  Policy routing is disabled
  Inbound access list is not set
  Outgoing access list is not set
  0 unicast RPF ACL drop
  0 unicast RPF All drop
  ARP Timeout: 00:10:00
ZXUAS(config)#
```

Configuring User Circuit Interface

Background ZXUAS 10800E is a broadband access server based on router. It does not have its own user circuit. To identify with physical interface, user circuit interface is identified by **sub-interface + bras**.

Purpose This topic describes how to configure user circuit interface.

Steps To configure user circuit interface, perform the following steps.

1. To enter circuit interface configuration mode, use the following command.

Format	Function
ZXUAS(config)#**interface** *type slot/port.subinterface* **bras**	This enters circuit interface configuration mode

2. To configure access type, use the following command.

   ZXUAS(config-subif)#**access-type {async|sync|isdn-sync|isdn-async-v120|isdn-async-v110|virtual|piafs|hdlc-clear-channel|x25|x75|g3fax|sdsl|adsl-cap|adsl-**

dmt|idsl|ethernet|xdsl|cable|wireless|wirelessieee802-11}

3. To create PVC, use the following command.

Format	Function
ZXUAS(config-subif)#**atm pvc** <*vpi*> < *vci*>	This creates PVC

4. To bind PPP-encapsulated circuit with PPP-authenticated interface, use the following command.

Format	Function
ZXUAS(config-subif)#**bind authentication** {**chap|chap-pap|pap**} [**maximum** <*numbers*>]	This binds PPP-encapsulated circuit with PPP-authenticated interface

5. To bind multiple PPP-encapsulated circuits to interface, use the following command.

Format	Function
ZXUAS(config-subif)#**bind multi vbui** <*VBUI-interface*> **authentication** {**chap|chap-pap|pap**} [**maximum** <*numbers*>]	This binds multiple PPP-encapsulated circuits to interface

6. To bind circuit to VBUI statically, use the following command.

Format	Function
ZXUAS(config-subif)#**bind vbui** <*VBUI-interface*> **[maximum** <*numbers*>]	This binds circuit to VBUI statically

7. To add VLAN-ID for new-created Ethernet interface, use the following command.

Format	Function
ZXUAS(config-subif)#**dot1q** {<*vlan-id* >**|none|tunneling ethertype** <*type*>}	This adds VLAN-ID for new-created Ethernet interface

8. To configure VLAN-ID and MAC address for DSLAM of a VBUI, use the following command.

Format	Function
ZXUAS(config-subif)#**dslam** <*dslam-name*> <*vlan-id*> <*vlan-mac-address* >	This configures VLAN-ID and MAC address for DSLAM of a VBUI

9. To configure encapsulation type, use the following command.

Format	Function
ZXUAS(config-subif)#**encapsulation** <*type*>	This configures encapsulation type

10. To configure subscriber location, use the following command.

Format	Function
ZXUAS(config-subif)#**subscriber location** <*location*>	This configures subscriber location

11. To configure circuit interface description, use the following command.

Format	Function
ZXUAS(config-subif)#**description** <*string*>	This configures circuit interface description

12. To configure tpid of outer-layer label in QinQ encapsulation mode, use the following command.

Format	Function
ZXUAS(config-subif)#**tpid** <*0xHHHH*>	This configures tpid of outer-layer label in QinQ encapsulation mode

13. To configure user authentication mode in telnet login, use the following command.

Format	Function
ZXUAS(config)#**user-authentication-type** {**local**|**radius** <1-2000> [**chap**|**pap**]}	This configures user authentication mode in telnet login

END OF STEPS

Result User circuit interface has been configured.

Example This example shows how to configure user circuit interface and view interface information.

```
ZXUAS#configure  terminal
ZXUAS(config)#interface fei_1/1.1 bras
ZXUAS(config-subif)#encapsulation multi
ZXUAS(config-subif)#bind multi vbui vbui1 authentication
chap-pap
ZXUAS(config-subif)#subscriber location dhcp-option82
ZXUAS(config-subif)#description zte
ZXUAS(config-subif)#end
ZXUAS(config)#show interface fei_1/1.1
fei_1/1.1 is up,  line protocol is up
  Description is zte
  Keepalive set:0 sec
  MAC address is 00d0.d0c0.0c80
  The port is electric
  Duplex half
  access-type ethernet
  encapsulation multi
  bind multi vbui vbui1 authentication chap-pap maximum
8000
  ppp idle interval 5 traffic-limit 0
  ppp keepalive timer 1 count 10
  ARP Timeout:00:00:00
  Internet address is unassigned
  MTU 1500 bytes
  MRU 1500 bytes          BW 10000 Kbits
ZXUAS(config)#
```

User VBUI Configuration

Contents User VBUI configuration includes the following topics.

User VBUI Configuration Overview

User VBUI information includes IP address, user address pool, user DSN and so on.

DHCP Packets DHCP packets sent to ZXUAS 10800E from down link equipment contain option60 attribute. User name and password are

included in this attribute, which can be used to boot and authenticate. When ZXUAS 10800E users get online, system judges whether users are allowed to get on line or not according to the value of option60 attribute.

ZXUAS 10800E connects with equipment such as DSLAM, and then DSLAM connects with users. To obtain user location information, ZXUAS 10800E and DSLAM run VBAS or option82.

Configuring User VBUI

Purpose This topic describes how to configure user VBUI.

Steps To configure user VBUI, perform the following steps.

1. To configure VBUI interface address, use the following command.

Format	Function
ZXUAS(config-if)#**ip address** <*ip-address*> <*net-mask*>	This configures VBUI interface address

2. To configure aging time of ARP table, use the following command.

Format	Function
ZXUAS(config-if)#**arp timeout** <*seconds*>	This configures aging time of ARP table

3. To identify option60 on user VBUI, use the following command.

Format	Function
ZXUAS(config-if)#**dhcp option60**	This identifies option60 on user VBUI

4. To configure trust option82, use the following command.

Format	Function
ZXUAS(config-if)#**dhcp trust-option82**	This configures trust option82

5. To configure idle period of user, use the following command.

Format	Function
ZXUAS(config-if)#**dhcp idle period** <*seconds*> **traffic** <*kbytes*>	This configures idle period of user

6. To configure IP address pool, use the following command.

Format	Function
ZXUAS(config-if)#**ip pool** [<*pool-number*>] <*poolname*> <*start-ip*> <*end-ip*> [**dhcp-slot <***slot***>**|**domain** <*domain-number*>]	This configures IP address pool

7. To configure primary DSN, use the following command.

Format	Function
ZXUAS(config-if)#**dns primary** <*ip-address*>	This configures primary DSN

8. To configure authentication switch when users are obtaining addresses, use the following command.

Format	Function
ZXUAS(config-if)#**ip dhcp auth-on-up** {**disable|enable**}	This configures authentication switch when users are obtaining addresses

9. To configure detection for abnormal off-line of DHCP access, use the following command.

Format	Function
ZXUAS(config-if)#**dhcp user-detect timer** <*user-detect-interval*><*user-detect-times*>	This configures detection for abnormal off-line of DHCP access

10. To configure web authentication, use the following command.

Format	Function
ZXUAS(config-if)#**web authentication subscriber {none|web [force]}**	This configures web authentication

11. To designate web server, use the following command.

Format	Function
ZXUAS(config-if)#**web server** <*ip-addr*> [**port** <*udp-port*>]	This designates web server

END OF STEPS

Result User VBUI has been configured.

Example This example shows how to configure user VBUI.

```
ZXUAS#configure terminal
ZXUAS(config)#interface vbui100
ZXUAS(config-if)#arp timeout 5000
ZXUAS(config-if)#dhcp option60
ZXUAS(config-if)#dhcp trust-option82
ZXUAS(config-if)#ip address 100.100.128.100 255.0.0.0
ZXUAS(config-if)#ip pool abc 100.100.128.1 100.100.128.254
ZXUAS(config-if)#dhcp idle period 180 traffic 50
ZXUAS(config-if)#dns primary 200.101.1.10
ZXUAS(config-if)#web authentication subscriber web force
ZXUAS(config-if)#web server 10.61.96.90
ZXUAS(config-if)#ip dhcp auth-on-up enable
ZXUAS(config-if)#dhcp user-detect
```

Configuring SAL

Background When Service Access List (SAL) is applied on circuit, system will permit or refuse some PPP supported domains and IP address to access the server.

Purpose This topic describes how to configure service access list.

Steps To configure service access list, perform the following steps.

1. To enter bras configuration mode, use the following command.

Format	Function
ZXUAS(config)#**bras**	This enters bras configuration mode

2. To enter SAL configuration mode, use the following command.

Format	Function
ZXUAS(config-bras)#**sal** <*sal-number*>	This enters SAL configuration mode

3. To configure SAL alias, use the following command.

Format	Function
ZXUAS(config-sal-1)#**alias** <*name*> [**advertise**]	This configures SAL alias

4. To configure default domain of user access, use the following command.

Format	Function
ZXUAS(config-sal-1)#**default domain** <*domain-name*>	This configures default domain of user access

5. To deny domain access, use the following command.

Format	Function
ZXUAS(config-sal-1)#**deny** {**domain** <*domain-name*>|**any**}	This denies domain access

6. To permit domain access, use the following command.

Format	Function
ZXUAS(config-sal-1)#**permit** {**domain** <*domain-name*>|**any**}	This permits domain access

7. To translate user domain name, use the following command.

Format	Function
ZXUAS(config-sal-1)#**translate** {**src-domain** <*src-domain*>|**any**} **des-domain** <*dest-domain*>	This translates user domain name

8. To apply SAL to interface, use the following command.

Format	Function
ZXUAS(config-subif)#**sal** <*sal-number*>	This applies SAL to interface

END OF STEPS

Result SAL has been configured.

Example This example shows how to configure SAL.

```
ZXUAS(config)#bras
ZXUAS(config-bras)#sal 1
ZXUAS(config-sal-1)#alias special-sal
ZXUAS(config-sal-1)#default domain zte.com.cn
ZXUAS(config-sal-1)#deny domain 8
ZXUAS(config-sal-1)#permit domain another.com.cn
ZXUAS(config-sal-1)#translate src-domain zte.com.cn des-
domain another.com.cn
ZXUAS(config-sal-1)#exit
ZXUAS(config-bras)#exit
ZXUAS(config)#int fei_1/1.1 bras
ZXUAS(config-subif)#sal 1
```

Configuring Delimiter

Purpose This topic describes how to configure delimiter.

Step To configure delimiter, use the following command.

Format	Function
ZXUAS(config-bras)#**domain-delimiter** <*delimiter*>	This configures delimiter

END OF STEP

Result Delimiter has been configured.

Example This example shows how to configure delimiter.

```
ZXUAS(config)#bras
ZXUAS(config-bras)# domain-delimiter @
```

Configuring Domain

Purpose This topic describes how to configure domain.

Steps To configure domain, perform the following steps.

1. To enter domain configuration mode, use the following command.

Format	Function
ZXUAS(config-bras)#**domain** < *domain-number*>	This enters domain configuration mode

2. To configure domain alias, use the following command.

Format	Function
ZXUAS(config-domain-2)#**alias** <*name*> [**advertise**]	This configures domain alias

3. To configure accounting server group associated with domain, use the following command.

Format	Function
ZXUAS(config-domain-2)#**accounting-group** <*group-number*> **[second]**	This configures accounting server group associated with domain

4. To configure accounting type of users in domain, use the following command.

Format	Function
ZXUAS(config-domain-2)#**accounting-type** {**none**|**radius**}	This configures accounting type of users in domain

5. To configure authentication server group associated with domain, use the following command.

Format	Function
ZXUAS(config-domain-2)#**authentication-group** <*group-number*>	This configures authentication server group associated with domain

6. To configure authentication type of users in domain, use the following command.

Format	Function
ZXUAS(config-domain-2)#**authentication-type** {**none**|**local**|**radius**|**local-radius**|**radius-local**|**radius-none**}	This configures authentication type of users in domain

7. To force to display a web to users, use the following command.

Format	Function
ZXUAS(config-domain-2)#**ppp web-force timer** <*time*> **count** <*times*>	This forces to display a web to users

8. To configure L2TP accounting mode, use the following command.

Format	Function
ZXUAS(config-domain-2)#**l2tp-accounting** {**class1**|**class2**|**none**}	This configures L2TP accounting mode

9. To configure circuit authentication, use the following command.

Format	Function
ZXUAS(config-domain-2)#**circuit-authentication** {**enable**|**disable**}	This configures circuit authentication

10. To associate domain with VRF, use the following command.

Format	Function
ZXUAS(config-domain-2)#**ip vrf** <*vrf-name*>	This associates domain with VRF

11. To configure maximum subscriber number in a domain, use the following command.

Format	Function
ZXUAS(config-domain-2)#**max-subscriber** <*number*>	This configures maximum subscriber number in a domain

12. To configure quick-redial, use the following command.

Format	Function
ZXUAS(config-domain-2)#**quick-redial** {**enable**|**disable**}	This configures quick-redial

13. To configure accounting update mode, use the following command.

Format	Function
ZXUAS(config-domain-2)#**accounting-update** {**<***accounting-period***>**|**ipcp-up**}	This configures accounting update mode

14. To configure domain name description, use the following command.

Format	Function
ZXUAS(config-domain-2)#**pppoe motm** <*str*>	This configures domain name description

15. To configure accounting share in domain, use the following command.

Format	Function
ZXUAS(config-domain-2)#**account-share** {**enable**|**disable**}	This configures accounting share in domain

16. To configure mix authorization in domain, use the following command.

Format	Function
ZXUAS(config-domain-2)#**mix-authorization** {**enable**|**disable**}	This configures mix authorization in domain

17. To configure time container in domain, use the following command.

Format	Function
ZXUAS(config-domain-2)#**timer-container-apply** <*30000-30127*> {**enable**|**disable**}	This configures time container in domain

END OF STEPS

Result Domain has been configured.

Example This example shows how to configure domain.

```
ZXUAS#configure terminal
ZXUAS(config)#bras
ZXUAS(config-bras)#
ZXUAS(config-bras)#domain 2
ZXUAS(config-domain-2)#alias zte.com
ZXUAS(config-domain-2)#accounting-group 8
ZXUAS(config-domain-2)#accounting-type radius
ZXUAS(config-domain-2)#authentication-group 10
ZXUAS(config-domain-2)#authentication-type radius
ZXUAS(config-domain-2)#l2tp-accounting class1
ZXUAS(config-domain-2)#ppp web-force timer 5 count 2
ZXUAS(config-domain-2)#circuit-authentication enable
ZXUAS(config-domain-2)#max-subscriber 1000
```

Configuring Domain User Template

Purpose This topic describes how to configure domain user template.

Steps To configure domain user template, perform the following steps.

1. To enter user template configuration mode, use the following command.

Format	Function
ZXUAS(config-domain-10)#**subscriber-template**	This enters user template configuration mode

2. To configure ACL associated with user template, use the following command.

Format	Function
ZXUAS(config-domain-subtmp)#**access-list** {<*acl-name*>|<*acl-number*>}	This configures ACL associated with user template

3. To configure downlink ACL associated with user template, use the following command.

Format	Function
ZXUAS(config-domain-subtmp)#**access-list-outside** {**acl-number**|**acl-name**}	This configures downlink ACL associated with user template

4. To configure IP address obtainment type of users, use the following command.

Format	Function
ZXUAS(config-domain-subtmp)#**ip address** {**pool** <*pool-name*>|**interface** <*interface-name*>|**vrf**}	This configures IP address obtainment type of users

5. To get a designated URL automatically after PPPoE users establish sessions, use the following command.

Format	Function
ZXUAS(config-domain-subtmp)#**ppp url** <*url*>	This gets a designated URL automatically after PPPoE users establish sessions

6. To configure absolute timeout time, use the following command.

Format	Function
ZXUAS(config-domain-subtmp)#**timeout absolute** <*seconds*>	This configures absolute timeout time

END OF STEPS

Result Domain user template has been configured.

Example This example shows how to configure domain user template.

```
ZXUAS#config terminal
ZXUAS(config)#bras
ZXUAS(config-bras)#domain 10
ZXUAS(config-domain-10)#subscriber-template
ZXUAS(config-domain-subtmp)#ip address pool my-pool
ZXUAS(config-domain-subtmp)#ppp url http://www.zte.com.cn/
ZXUAS(config-domain-subtmp)#timeout absolute 200
```

Configuring User

Purpose This topic describes how to configure users.

Steps To configure users, perform the following steps.

1. To enter subscriber configuration mode, use the following command.

Format	Function
ZXUAS(config-bras)#**subscriber** <*name*> <*domain*>	This enters subscriber configuration mode

2. To configure IP address obtainment mode, use the following command.

Format	Function
ZXUAS(config-sub-loyalty)#**ip address** {<*ip-address*>|**pool** <*pool-name*>|**interface** <*interface-name*>|**vrf**}	This configures IP address obtainment mode

3. To configure password, use the following command.

Format	Function
ZXUAS(config-sub-loyalty)#**password** <*str*>	This configures password

4. To configure the circuit through which user accesses to device, use the following command.

Format	Function
ZXUAS(config-sub-loyalty)#**cir-bind** {**bras** <*slot*> <*port*> [**vlan** <*vlan*>|**pvc** <*vpi*> <*vci*>]|**dslam** <*slot*> <*port*> [**vlan** <*vlan*>]}	This configures the circuit through which user accesses to device

5. To configure MAC address of network card use used to access, use the following command.

Format	Function
ZXUAS(config-sub-loyalty)#**mac-bind** <*mac*>	This configures MAC address of network card use used to access

6. To configure TCP connection number, use the following command.

Format	Function
ZXUAS(config-sub-loyalty)#**tcp-limit num** <*tcp-limit-number*>	This configures TCP connection number

END OF STEPS

Result User has been configured.

Example This example shows how to configure user.

```
ZXUAS#configure  terminal
ZXUAS(config)#bras
ZXUAS(config-bras)#subscriber loyalty domain-name
zte.com.cn
ZXUAS(config-sub-loyalty)#ip address pool tele-pool
ZXUAS(config-sub-loyalty)#tcp-limit mode  mon-sum-rate
ZXUAS(config-sub-loyalty)#tcp-limit rate 800
ZXUAS(config-sub-loyalty)#tcp-limit num 10
ZXUAS(config-sub-loyalty)#cir-bind bras 1 10 vlan 10
ZXUAS(config-sub-loyalty)#password loyal
ZXUAS(config-sub-loyalty)#pppoe url http://www.zte.com.cn/
```

Configuring PPP Quick-Redial

Purpose This topic describes how to configure PPP quick-redial.

Steps To configure PPP quick-redial, perform the following steps.

1. To enter domain configuration mode, use the following command.

Format	Function
ZXUAS(config-bras)#**domain** <*domain-number*>	This entes domain configuration mode

2. To enable or disable PPP quick-redial function, use the following command.

Format	Function
ZXUAS(config-domain-10)#**quick-redial {enable|disable}**	This enables or disables PPP quick-redial function

END OF STEPS

Result PPP quick-redial has been configured.

Example This example shows how to configure PPP quick-redial.

```
ZXUAS#configure terminal
ZXUAS(config)#bras
ZXUAS(config-bras)#domain 1
ZXUAS(config-domain-1)#quick-redial
```

Configuring Flow-Break Detection

Purpose This topic describes how to configure flow-break detection.

Steps To configure flow-break detection, perform the following steps.

1. To enter circuit interface configuration mode, use the following command.

Format	Function
ZXUAS(config)#**interface** *type slot/port.subinterface* **bras**	This enters circuit interface configuration mode

2. To configure flow-break detection function, use the following command.

Format	Function
ZXUAS(config-subif)#**ppp idle interval-period** <*seconds*> **traffic-limit** <*kbytes*>	This configures flow-break detection function

END OF STEPS

Result Flow-break detection has been configured.

Example This example shows how to configure flow-break detection.

```
ZXUAS#config terminal
Enter configuration commands, one per line.  End with
CTRL/Z.
ZXUAS(config)#int fei_1/1.1 bras
ZXUAS(config-subif)#ppp idle interval-period 60 traffic-
limit 50
```

Configuring Flow Statistics

Background Flow statistics is implemented according to IP packets. Flow statistics about circuits is implemented according to MAC packets.

Purpose This topic describes how to configure flow statistics.

Steps To configure flow statistics, perform the following steps.

1. To enter bras configuration mode, use the following command.

Format	Function
ZXUAS(config)#**bras**	This enters bras configuration mode

2. To enable or disable flow statistics function, use the following command.

Format	Function
ZXUAS(config-bras)#**flow-statistics {disable|enable}**	This enables or disables flow statistics function

END OF STEPS

Result Flow statistics has been configured.

Example This example shows how to configure flow statistics.

```
ZXUAS#configure terminal
Enter configuration commands, one per line.  End with
CTRL/Z.
ZXUAS(config)#bras
ZXUAS(config-bras)#flow-statistics enable
ZXUAS(config-bras)#
```

Configuring Circuit Access Type

Purpose This topic describes how to configure circuit access type.

Steps To configure circuit access type, perform the following steps.

1. To enter circuit configuration mode, use the following command.

Format	Function
ZXUAS(config)#**interface** *type slot/port.subinterface* **bras**	This enters circuit configuration mode

2. To configure circuit access type, use the following command.

   ZXUAS(config-subif)#**access-type** {**async|sync|isdn-sync|isdn-async-v120|isdn-async-v110|virtual|piafs|hdlc-clear-channel|x25|x75|g3fax|sdsl|adsl-cap|adsl-dmt|idsl|ethernet|xdsl|cable|wireless|wireless ieee802-11**}

END OF STEPS

Result Circuit access type has been configured.

Example This example shows how to configure circuit access type.

```
ZXUAS#config terminal
Enter configuration commands, one per line.  End with
CTRL/Z.
ZXUAS(config)#int fei_1/1.1 bras
ZXUAS(config-subif)#access-type adsl
```

Configuring Timer-Container

Purpose This topic describes how to configure timer-container.

Steps To configure timer-container, perform the following steps.

1. To enter bras configuration mode, use the following command.

Format	Function
ZXUAS(config)#**bras**	This enters bras configuration mode

2. To define a timer-container, use the following command.

Format	Function
ZXUAS(config-bras)#**timer-containers** <*timer-containers-id*>	This defines a timer-container

3. To configure timer rule, use the following command.

   ZXUAS(config-timer-30000)#**timer-rule** <*id*> {**include|exclude**} {[**start-date** <*start-date*>] [**end-date** <*end-date*>] [**start-time** <*start-time*>] [**end-time** <*end-time*>] [**week** <*week*>]}

4. To apply timer rule, use the following command.

Format	Function
ZXUAS(config-timer-30000)#**rule-apply** <*id*> {[**acl** <*acl-name*>] [**qos-down** <*qos-down*>] [**qos-up** <*qos-up*>]}	This applies timer rule

5. To configure associate timer-container with domain, use the following command.

Format	Function
ZXUAS(config-domain-10)#**timer-container-apply** <30000-30127> **{enable|disable}**	This configures associate timer-container with domain

END OF STEPS

Result Timer-container has been configured.

Example This example shows how to configure timer-container.

```
ZXUAS#configure terminal
ZXUAS(config)#bras
ZXUAS(config-bras)#
ZXUAS(config-bras)#timer-containers 30000
ZXUAS(config-timer-30000)#timer-rule 10 include start-time
8:30 end-time 17:30
ZXUAS(config-timer-30000)#timer-rule 10 exclude start-time
11:30 end-time 13:30
ZXUAS(config-timer-30000)#rule-apply 10 acl 100
ZXUAS(config-timer-30000)#exit
ZXUAS(config-bras)#domain 100
ZXUAS(config-domain-100)#timer-container-apply       30000
enable
```

Configuring Security Log

Background Security log records all user information in the network, including user source port, destination port, source IP, destination IP and protocol number.

Purpose This topic describes how to configure security log.

Steps To configure security log, perform the following steps.

1. To enter bras configuration mode, use the following command.

Format	Function
ZXUAS(config)#**bras**	This enters bras configuration mode

2. To configure security log, use the following command.

Format	Function
ZXUAS(config-bras)#**internet-log**	This configures security log

3. To define rule, use the following command.

Format	Function
ZXUAS(config-net-log)#**rule** *<ruleNo> <ip-addr>* {[**vrf_name**]|**username** *<name>*| **slot***<1-8> <1-32000>*}	This defines rule

END OF STEPS

Result Security log has been configured.

Example This example shows how to configure security log.

```
ZXUAS#configure terminal
Enter configuration commands, one per line.  End with
CTRL/Z.
ZXUAS(config)#bras
ZXUAS(config-bras)#internet-log
ZXUAS(config-net-log)#rule 10 username abc@10
```

Configuring IP Address Snooping

Background Unicast Reversed Path Forwarding (URPF) is a technology for preventing source IP address deceit. When circuit that connects to network receives data packets, system will implement URPF inspection to prevent IP address deceit before forwarding packets.

Purpose This topic describes how to configuring IP address snooping.

Step To configure IP address snooping, use the following command.

Format	Function
ZXUAS(config-if)#**ip verify strict**	This configures IP address snooping

END OF STEP

Result IP address snooping has been configured.

Example This example shows how to configure IP address snooping.

```
ZXUAS#configure terminal
Enter configuration commands, one per line.  End with
CTRL/Z.
ZXUAS(config)#interface fei_2/2
ZXUAS(config-if)#ip verify strict
```

Configuring Port Mirroring

Background Port mirroring function copies the data of one or more ports (mirrored ports) in the switch to a designated port (monitoring port). It can retrieve the data of mirrored port in the monitoring port by mirroring. Through which it can perform network flow analysis, and error diagnosis.

ZXUAS 10800E only supports port mirroring on the same interface card, that is, the mirroring port and monitoring port should be on the same interface card. One port can not be mirrored to multiple ports, while multiple ports can be mirrored to one port. When a port is used as mirrored port, it can not be a monitoring port at the same time.

Purpose This topic describes how to configure port mirroring.

Step To configure port mirroring, use the following command.

Format	Function
ZXUAS(config)# **mirror** {**slot** <*slot-number*> **destination-port** <*port-number*> **source-port** <*port-number*> **direction** <*both*|*rx*|*tx*>}	This configures port mirroring

END OF STEP

Result Port mirroring has been configured.

Example This example shows how to configure port mirroring.

```
ZXUAS#configure terminal
ZXUAS(config)#mirror slot 8 destination-port 8 source-port
2 direction both
```

Introduction to VLAN

Definition of VLAN Virtual Local Area Network (VLAN) is a technology that divides a physical network into multiple logical (virtual) LAN. Every VLAN has a VLAN identifier (VID).

Advantage of VLAN technology is that network administrators can divide the users in the same physical LAN into different broadcast domains (one broadcast domain is one VLAN). This ensures that the users with the same demands belong to same broadcast domain and users with different demands belong to different broadcast domain.

Every VLAN is like an independent logical LAN, having the same attributes with physical LAN. All broadcast and uni-cast traffic in the same VLAN are restricted to the VLAN instead of being forwarded to other VLAN. Communication between devices belonging to different VLAN is forwarded by the layer3 routers.

VLAN Features VLAN has the following features:

- Reduce broadcast traffic in the network
- Enhance network security
- Simplify network management and control

Configuring VLAN

Purpose This topic describes how to configure VLAN.

Steps To configure VLAN, perform the following steps.

1. To configure user VLAN, perform the following steps.

i. To enter circuit interface configuration mode, use the following command.

Format	Function
ZXUAS(config)#**interface** *type slot/port.subinterface* **bras**	This enters circuit interface configuration mode

ii. To encapsulate a circuit, use the following command.

Format	Function
ZXUAS(config-subif)#**encapsulation** <*type*>	This encapsulates a circuit

iii. To create a VLAN, use the following command.

Format	Function
ZXUAS(config-subif)#**dot1q** {<*vlan-id*>**|none|tunneling ethertype** <*type*>}	This creates a VLAN

iv. To bind VBUI to VLAN, use the following command.

Format	Function
ZXUAS(config-subif)#**bind vbui** <*VBUI-interface*> **[maximum** <*numbers*>]	This bind VBUI to VLAN

2. To configure network VLAN, perform the following steps.

i. To enter sub-interface configuration mode, use the following command.

Format	Function
ZXUAS(config)#**interface** *type slot/port.subinterface*	This enters sub-interface configuration mode

ii. To configure VLAN, use the following command.

Format	Function
ZXUAS(config-subif)#**encapsulation dot1Q** <*vlan-id*>	This configures VLAN

END OF STEPS

Result VLAN has been configured.

Example This example shows how to configure VLAN.

```
ZXUAS#configure terminal
ZXUAS(config)#interface fei_1/1.10 bras
ZXUAS(config-subif)#encapsulation dot1q ip-over-ethernet
ZXUAS(config-subif)#dot1q 10
ZXUAS(config-subif)#bind vbui vbui1

ZXUAS#configure terminal
ZXUAS(config)#interface fei_2/1.11
ZXUAS(config-subif)#encapsulation dot1q 10
```

Configuring QinQ

Background QinQ technology is to add a new VLAN tag after MAC address field in a tagged Ethernet frame. The new VLAN tag is called outer tag or public network tag. Before the frame is forwarded to other device, outer tag is removed.

Purpose This topic describes how to configure QinQ.

Steps To configure QinQ, perform the following steps.

1. To configure user QinQ, perform the following steps.

   i. To enter circuit interface configuration mode, use the following command.

Format	Function
ZXUAS(config)#**interface** *type slot/port.subinterface* **bras**	This entes circuit interface configuration mode

   ii. To encapsulate a circuit, use the following command.

Format	Function
ZXUAS(config-subif)#**encapsulation** <*type*>	This encapsulates a circuit

   iii. To configure VLAN, use the following command.

Format	Function
ZXUAS(config-subif)#**dot1q** {<*vlan-id*>**|none|tunneling ethertype** <*type*>}	This configures VLAN

   iv. To configure QinQ, use the following command.

Format	Function
ZXUAS(config-subif)#**qinq** <*vlan-id*> **second-dot1q** <*vlan-id*>	This configure QinQ

   v. To bind VBUI to VLAN, use the following command.

Format	Function
ZXUAS(config-subif)#**bind vbui** <*VBUI-interface*> [**maximum** <*numbers*>]	This binds VBUI to VLAN

2. To configure network QinQ, use the following command.

   i. To enter sub-interface configuration mode, use the following command.

Format	Function
ZXUAS(config)#**interface** *type slot/port.subinterface*	This enters sub-interface configuration mode

   ii. To configure network QinQ, use the following command.

Format	Function
ZXUAS(config-subif)#**qinq internal-vlan** <*1-4094*> **external-vlan** <*1-4094*>	This configures network QinQ

END OF STEPS

Result QinQ has been configured.

Example This example shows how to configure QinQ.

```
ZXUAS#configure terminal
ZXUAS(config)#interface fei_1/1.12 bras
ZXUAS(config-subif)#encapsulation dot1q ip-over-ethernet
ZXUAS(config-subif)#dot1q 12
ZXUAS(config-subif)#qinq 12 second-dot1q 20
ZXUAS(config-subif)#bind vbui vbui1

ZXUAS#configure terminal
ZXUAS(config)#interface fei_2/1.12
ZXUAS(config-subif)#qinq internal-vlan 12 external-vlan 20
```

Chapter 8

PPPoX Configuration

Overview

Introduction This chapter describes PPPoX and configuration on ZXUAS 10800E.

Contents This chapter includes the following topics.

PPP Overview

Point-to-Point Protocol (PPP) is a link protocol that bears packets of network layer on point-to point link. As PPP provides user authentication and is easy to extend. It supports both synchronous and asynchronous communication.

PPP System PPP provides a complete set of protocols, including the following parts:

- Link Control Protocol (LCP)
- Network Control Protocol (NCP)

- Authentication protocols

LCP LCP is responsible for creating, maintaining and terminating a physical connection.

NCP NCP is a protocol suite responsible for running network protocols on the physical connection and clearing faults that occur to upper-level network protocols.

Authentication Protocols Authentication protocols are used to implement authentication for users. There are two authentication protocols: Password Authentication Protocol (PAP) and Challenge-Handshake Authentication Protocol (CHAP).

PAP PAP uses two-way handshake authentication, and the user name and password are transmitted on links in simple text. PAP authentication process is as follows:

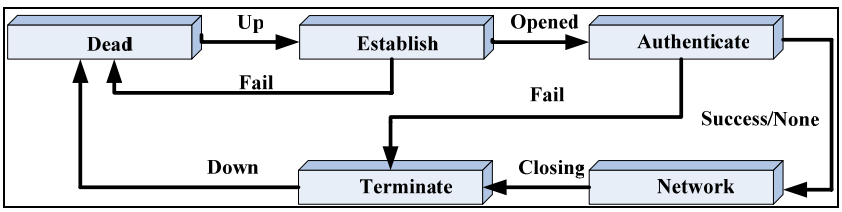
1. Authenticated party sends user name and password to the authenticating party.
2. Authenticating party checks whether this user is available and whether the password is correct according to user configuration, and returns different responses.

CHAP CHAP is more secure than PAP. CHAP uses three-way handshake authentication. CHAP authentication process is as follows:

1. Authenticating party sends some random messages to authenticated party.
2. The party to be authenticated uses its own password and MD5 algorithm to encrypt the random messages, and sends back the encrypted text to the authenticating party.
3. Authenticating party uses the stored password and MD5 algorithm to encrypt the original random messages, compares the two encrypted texts, and then gives different response according to the comparison result.

PPP Flow PPP flow is shown in Figure 40.

FIGURE 40 PPP FLOW



PPPoX Service

PPPoX service means users access ZXUAS 10800E and pass authentication by PPP dialing.

Basic Flow Basic flow of PPPoX service is as follows:

1. When data packets leave PPP dialing program, they are encapsulated with PPP frame and become PPP messages.
2. During transmission course, PPP messages are encapsulated by Ethernet, VLAN or ATM, and then they reach ZXUAS 10800E.
3. ZXUAS 10800E removes frames encapsulated by Ethernet, VLAN or ATM to get PPP messages, then gives PPP messages to PPP module.
4. PPP module removes PPP encapsulation to get data packets.

PPPoX Types

According to different networks, there are different PPPoX service types. They are described in Table 22.

TABLE 22 PPPOX TYPES

Type	Description
PPPoE	During transmission course, PPP messages are encapsulated by Ethernet, and then they reach ZXUAS 10800E.
PPPoEoV	During transmission course, PPP messages are encapsulated by Ethernet and VLAN, and then they reach ZXUAS 10800E.
PPPoEoA	During transmission course, PPP messages are encapsulated by Ethernet and AAL5, and then they reach ZXUAS 10800E.
PPPoA	During transmission course, PPP messages are encapsulated by AAL5, and then they reach ZXUAS 10800E.

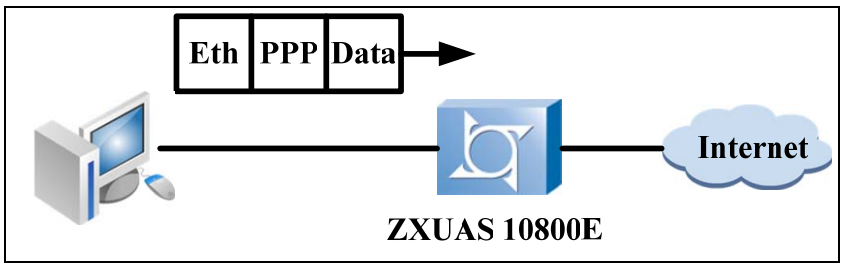
PPPoE Overview

Introduction

For PPPoE service, after PPP messages are encapsulated by Ethernet, they are not encapsulated or changed by other devices during transmission course.

Basic network of PPPoE service is shown in Figure 41. Maybe PPP messages pass by L2 devices, such as HUB and LAN switch, but these devices do not encapsulate or change format of PPPoE messages.

FIGURE 41 BASIC NETWORK OF PPPOE SERVICE



PPPoE Configuration

Contents PPPoE configuration includes the following topic.

Configure Network Interface

Purpose This topic describes how to configure interface connecting to Ethernet.

Steps To configure interface connecting to Ethernet, perform the following steps.

1. To enter interface configuration mode, use the following command.

Format	Function
ZXUAS(config)#**interface** *type slot/port*	This enters interface configuration mode

2. To configure IP address, use the following command.

Format	Function
ZXUAS(config-if)#**ip address** *<ip-address> <net-mask>*	This configures IP address

END OF STEPS

Result Interface connecting to Ethernet has been configured.

Example This example shows how to configure interface connecting to Ethernet.

```
ZXUAS(config)#interface fei_7/1
ZXUAS(config-if)#ip address 200.0.0.100 255.255.0.0
```

Configuring VBUI

Purpose This topic describes how to configure VBUI.

Steps To configure VBUI, perform the following steps.

1. To enter interface configuration mode, use the following command.

Format	Function
ZXUAS(config)# **interface vbui**< *VBUI-interface* >	This enters interface configuration mode

2. To configure VBUI IP address, use the following command.

Format	Function
ZXUAS(config-if)#**ip address** <*ip-address*> <*net-mask*>	This configures VBUI IP address

3. To configure IP address pool, use the following command.

Format	Function
ZXUAS(config-if)#**ip pool** [<*pool-number*>] <*poolname*> <*start-ip*> <*end-ip*> [**dhcp-slot <***slot***>**|**domain** <*domain-number*>]	This configures IP address pool

4. To configure primary DNS, use the following command.

Format	Function
ZXUAS(config-if)#**dns primary** <*ip-address*>	This configures primary DNS

5. To configure secondary DNS, use the following command.

Format	Function
ZXUAS(config-if)#**dns secondary** <*ip-address*>	This configures secondary DNS

6. To configure ARP aging time, use the following command.

Format	Function
ZXUAS(config-if)#**arp timeout** <*seconds*>	This confiugres ARP aging time

7. To identify option60 on VBUI, use the following command.

Format	Function
ZXUAS(config-if)#**dhcp option60**	This identifies option60 on VBUI

END OF STEPS

Result VBUI has been configured.

Example This example shows how to configure VBUI.

```
ZXUAS(config)#int vbui1
ZXUAS(config-if)#ip address 12.1.1.3 255.255.0.0
ZXUAS(config-if)#ip pool my-pool 12.1.1.1 12.1.1.200
ZXUAS(config-if)#dns primary 202.0.0.1
ZXUAS(config-if)#dns secondary 202.0.0.2
ZXUAS(config-if)#arp timeout 5000
ZXUAS(config-if)#dhcp option60
```

Configuring Domain

Purpose This topic describes how to configure domain.

Steps To configure domain, perform the following steps.

1. To enter bras configuration mode, use the following command.

Format	Function
ZXUAS(config)#**bras**	This enters bras configuration mode

2. To create a domain, use the following command.

Format	Function
ZXUAS(config-bras)#**domain** <*domain-number*>	This creates a domain

3. To configure domain alias, use the following command.

Format	Function
ZXUAS(config-domain-2)#**alias** <*name*> [**advertise**]	This configures domain alias

4. To configure user authentication mode, use the following command.

Format	Function
ZXUAS(config-domain-2)#**authentication-type** {**none|local|radius|local-radius|radius-local|radius-none**}	This configures user authentication mode

5. To configure user accounting mode, use the following command.

Format	Function
ZXUAS(config-domain-2)#**accounting-type** {**none|radius**}	This configures user accounting mode

6. To configure maximum user number, use the following command.

Format	Function
ZXUAS(config-domain-2)#**max-subscriber** <*number*>	This configures maximum user number

END OF STEPS

Result Domain has been configured.

Example This example shows how to configure domain.

```
ZXUAS(config)#bras
ZXUAS(config-bras)#domain 2
ZXUAS(config-domain-2)#alias zte.com advertise
ZXUAS(config-domain-2)#authentication-type local
ZXUAS(config-domain-2)#accounting-type none
ZXUAS(config-domain-2)#max-subscriber 1000
```

Configuring User

Purpose This topic describes how to configure a user.

Steps To configure a user, perform the following steps.

1. To enter bras configuration mode, use the following command.

Format	Function
ZXUAS(config)#**bras**	This enters bras configuration mode

2. To enter subscriber configuration mode, use the following command.

Format	Function
ZXUAS(config-bras)#**subscriber** <*name*> <*domain*>	This enters subscriber configuration mode

3. To configure user password, use the following command.

Format	Function
ZXUAS(config-sub-test)#**password** <*str*>	This configures user password

4. To configure IP address obtainment mode, use the following command.

Format	Function
ZXUAS(config-sub-test)#**ip address** {<*ip-address*>|**pool** <*pool-name*>|**interface** <*interface-name*>|**vrf**}	This configures IP address obtainment mode

5. To configure user TCP rate, use the following command.

Format	Function
ZXUAS(config-sub-test)#**tcp-limit rate** <*tcp- limit- rate*>	This configures user TCP rate

6. To configure TCP connection number, use the following command.

Format	Function
ZXUAS(config-sub-test)#**tcp-limit num** <*tcp-limit-number*>	This configures TCP connection number

7. To configure the circuit through which user accesses to device, use the following command.

Format	Function
ZXUAS(config-sub-test)#**cir-bind** {**bras** <*slot*> <*port*> [**vlan** <*vlan*>|**pvc** <*vpi*> <*vci*>]|**dslam** <*slot*> <*port*> [**vlan** <*vlan*>]}	This configures the circuit through which user accesses to device

END OF STEPS

Result User has been configured.

Example This example shows how to configure a user.

```
ZXUAS(config)#bras
ZXUAS(config-bras)#subscriber test domain-name zte.com
ZXUAS(config-sub-test)#password test
ZXUAS(config-sub-test)#ip address pool my-pool
ZXUAS(config-sub-test)#tcp-limit rate 800
ZXUAS(config-sub-test)#tcp-limit num 10
ZXUAS(config-sub-test)#cir-bind bras 1 10 vlan 10
ZXUAS(config-sub-test)#exit
```

Configuring User Circuit

Purpose This topic describes how to configure a circuit connecting to users.

Steps To configure a circuit connecting to users, perform the following steps.

1. To enter circuit interface configuration mode, use the following command.

Format	Function
ZXUAS(config)#**interface** *type slot/port.subinterface* **bras**	This enters circuit interface configuration mode

2. To create PVC, use the following command.

Format	Function
ZXUAS(config-subif)#**atm pvc** <*vpi*> <*vci*>	This creates PVC

3. To configure encapsulation type, use the following command.

Format	Function
ZXUAS(config-subif)#**encapsulation** <*type*>	This configures encapsulation type

4. To bind authentication mode, use the following command.

Format	Function
ZXUAS(config-subif)#**bind authentication** {**chap**|**chap-pap**|**pap**} [**maximum** <*numbers*>]	This binds authentication mode

5. To configure not to use DOT1q encapsulation, use the following command.

Format	Function
ZXUAS(config-subif)#**dot1q none**	This configures not to use DOT1q encapsulation

END OF STEPS

Result Circuit connecting to users has been configured.

Example This example shows how to configure a circuit connecting to users.

```
ZXUAS(config)#interface atm155_1/1.1 bras
ZXUAS(config-subif)#atm pvc 8 81
ZXUAS(config-subif)#encapsulation ppp-over-ethernet
ZXUAS(config-subif)#bind authentication pap
ZXUAS(config-subif)#dot1q none
```

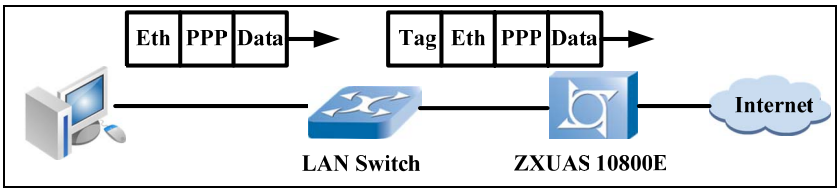
PPPoEoV Overview

For PPPoEoV service, PPP messages are encapsulated by Ethernet when they pass by Ethernet interfaces, then they become PPPoE messages. When PPPoE messages pass by LAN switch, VLAN tags are added to PPPoE messages, and they

become PPPoEoV messages. At last, PPPoEoV messages reach ZXUAS 10800E.

Basic network of PPPoEoV service is shown in Figure 42.

FIGURE 42 BASIC NETWORK OF PPPOEOV SERVICE



PPPoEoV Configuration

Contents PPPoEoV configuration includes the following topics.

Configure Network Interface

Purpose This topic describes how to configure interface connecting to Ethernet.

Steps To configure interface connecting to Ethernet, perform the following steps.

1. To enter interface configuration mode, use the following command.

Format	Function
ZXUAS(config)#**interface** *type slot/port*	This enters interface configuration mode

2. To configure IP address, use the following command.

Format	Function
ZXUAS(config-if)#**ip address** *<ip-address> <net-mask>*	This configures IP address

END OF STEPS

Result Interface connecting to Ethernet has been configured.

Example This example shows how to configure interface connecting to Ethernet.

```
ZXUAS(config)#interface fei_7/1
ZXUAS(config-if)#ip address 200.0.0.100 255.255.0.0
```

Configuring VBUI

Purpose This topic describes how to configure VBUI.

Steps To configure VBUI, perform the following steps.

1. To enter interface configuration mode, use the following command.

Format	Function
ZXUAS(config)# **interface vbui**< *VBUI-interface* >	This enters interface configuration mode

2. To configure VBUI IP address, use the following command.

Format	Function
ZXUAS(config-if)#**ip address** <*ip-address*> <*net-mask*>	This configures VBUI IP address

3. To configure IP address pool, use the following command.

Format	Function
ZXUAS(config-if)#**ip pool** [<*pool-number*>] <*poolname*> <*start-ip*> <*end-ip*> [**dhcp-slot <***slot***>**|**domain** <*domain-number*>]	This configures IP address pool

4. To configure primary DNS, use the following command.

Format	Function
ZXUAS(config-if)#**dns primary** <*ip-address*>	This configures primary DNS

5. To configure secondary DNS, use the following command.

Format	Function
ZXUAS(config-if)#**dns secondary** <*ip-address*>	This configures secondary DNS

6. To configure ARP aging time, use the following command.

Format	Function
ZXUAS(config-if)#**arp timeout** <*seconds*>	This confiugres ARP aging time

7. To identify option60 on VBUI, use the following command.

Format	Function
ZXUAS(config-if)#**dhcp option60**	This identifies option60 on VBUI

END OF STEPS

Result VBUI has been configured.

Example This example shows how to configure VBUI.

```
ZXUAS(config)#int vbui1
ZXUAS(config-if)#ip address 12.1.1.3 255.255.0.0
ZXUAS(config-if)#ip pool my-pool 12.1.1.1 12.1.1.200
ZXUAS(config-if)#dns primary 202.0.0.1
ZXUAS(config-if)#dns secondary 202.0.0.2
ZXUAS(config-if)#arp timeout 5000
ZXUAS(config-if)#dhcp option60
```

Configuring Domain

Purpose This topic describes how to configure domain.

Steps To configure domain, perform the following steps.

1. To enter bras configuration mode, use the following command.

Format	Function
ZXUAS(config)#**bras**	This enters bras configuration mode

2. To create a domain, use the following command.

Format	Function
ZXUAS(config-bras)#**domain** <*domain-number*>	This creates a domain

3. To configure domain alias, use the following command.

Format	Function
ZXUAS(config-domain-2)#**alias** <*name*> [**advertise**]	This configures domain alias

4. To configure user authentication mode, use the following command.

Format	Function
ZXUAS(config-domain-2)#**authentication-type** {**none|local|radius|local-radius|radius-local|radius-none**}	This configures user authentication mode

5. To configure user accounting mode, use the following command.

Format	Function
ZXUAS(config-domain-2)#**accounting-type** {**none|radius**}	This configures user accounting mode

END OF STEPS

Result Domain has been configured.

Example This example shows how to configure domain.

```
ZXUAS(config)#bras
ZXUAS(config-bras)#domain 2
ZXUAS(config-domain-2)#alias zte.com advertise
ZXUAS(config-domain-2)#authentication-type local
ZXUAS(config-domain-2)#accounting-type none
```

Configuring User

Purpose This topic describes how to configure a user.

Steps To configure a user, perform the following steps.

1. To enter bras configuration mode, use the following command.

Format	Function
ZXUAS(config)#**bras**	This enters bras configuration mode

2. To enter subscriber configuration mode, use the following command.

Format	Function
ZXUAS(config-bras)#**subscriber** <*name*> <*domain*>	This enters subscriber configuration mode

3. To configure user password, use the following command.

Format	Function
ZXUAS(config-sub-test)#**password** <*str*>	This configures user password

4. To configure IP address obtainment mode, use the following command.

Format	Function
ZXUAS(config-sub-test)#**ip address** {<*ip-address*>|**pool** <*pool-name*>|**interface** <*interface-name*>|**vrf**}	This configures IP address obtainment mode

5. To configure user TCP rate, use the following command.

Format	Function
ZXUAS(config-sub-test)#**tcp-limit rate** <*tcp- limit- rate*>	This configures user TCP rate

6. To configure TCP connection number, use the following command.

Format	Function
ZXUAS(config-sub-test)#**tcp-limit num** <*tcp-limit-number*>	This configures TCP connection number

7. To configure the circuit through which user accesses to device, use the following command.

Format	Function
ZXUAS(config-sub-test)#**cir-bind** {**bras** <*slot*> <*port*> [**vlan** <*vlan*>|**pvc** <*vpi*> <*vci*>]|**dslam** <*slot*> <*port*> [**vlan** <*vlan*>]}	This configures the circuit through which user accesses to device

END OF STEPS

Result User has been configured.

Example This example shows how to configure a user.

```
ZXUAS(config)#bras
ZXUAS(config-bras)#subscriber test domain-name zte.com
ZXUAS(config-sub-test)#password test
ZXUAS(config-sub-test)#ip address pool my-pool
ZXUAS(config-sub-test)#tcp-limit rate 800
ZXUAS(config-sub-test)#tcp-limit num 10
ZXUAS(config-sub-test)#cir-bind bras 1 10 vlan 10
ZXUAS(config-sub-test)#exit
```

Configuring User Circuit

Purpose This topic describes how to configure a circuit connecting to users.

Steps To configure a circuit connecting to users, perform the following steps.

1. To enter circuit interface configuration mode, use the following command.

Format	Function
ZXUAS(config)#**interface** *type slot/port.subinterface* **bras**	This enters circuit interface configuration mode

2. To create PVC, use the following command.

Format	Function
ZXUAS(config-subif)#**atm pvc** <*vpi*> <*vci*>	This creates PVC

3. To configure encapsulation type, use the following command.

Format	Function
ZXUAS(config-subif)#**encapsulation** <*type*>	This configures encapsulation type

4. To bind authentication mode, use the following command.

Format	Function
ZXUAS(config-subif)#**bind authentication** {**chap**|**chap-pap**|**pap**} [**maximum** <*numbers*>]	This binds authentication mode

5. To forward PPPoE packets with VLAN-ID tag, use the following command.

Format	Function
ZXUAS(config-subif)#**dot1q** {<*vlan-id* >|**none**|**tunneling ethertype** <*type*>}	This forwards PPPoE packets with VLAN-ID tag

END OF STEPS

Result Circuit connecting to users has been configured.

Example This example shows how to configure a circuit connecting to users.

```
ZXUAS(config)#interface fei_7/14.1 bras
ZXUAS(config-subif)#encapsulation ppp-over-ethernet
ZXUAS(config-subif)#bind authentication pap
ZXUAS(config-subif)#dot1q 10,20,30,40
```

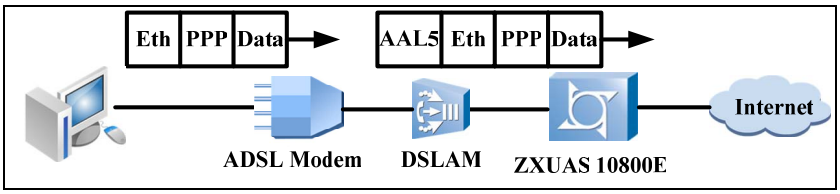
PPPoEoA Overview

For PPPoEoA service, PPP messages are encapsulated by Ethernet when they pass by Ethernet interfaces, then they become PPPoE messages. When PPPoE messages pass by ADSL Modem, they are encapsulated by AAL5, and they become

PPPoEoA messages. At last, they are forwarded by DSLAM and reach ZXUAS 10800E.

Basic network of PPPoEoA service is shown in Figure 43.

FIGURE 43 BASIC NETWORK OF PPPOEOA SERVICE



PPPoEoA Configuration

Contents PPPoEoA configuration includes the following topics.

Configuring Network Interface

Purpose This topic describes how to configure interface connecting to Ethernet.

Steps To configure interface connecting to Ethernet, perform the following steps.

1. To enter interface configuration mode, use the following command.

Format	Function
ZXUAS(config)#**interface** *type slot/port*	This enters interface configuration mode

2. To configure IP address, use the following command.

Format	Function
ZXUAS(config-if)#**ip address** *<ip-address> <net-mask>*	This configures IP address

END OF STEPS

Result Interface connecting to Ethernet has been configured.

Example This example shows how to configure interface connecting to Ethernet.

```
ZXUAS(config)#interface fei_7/1
ZXUAS(config-if)#ip address 200.0.0.100 255.255.0.0
ZXUAS(config-if)#exit
```

Configuring VBUI

Purpose This topic describes how to configure VBUI.

Steps To configure VBUI, perform the following steps.

1. To enter interface configuration mode, use the following command.

Format	Function
ZXUAS(config)# **interface vbui**< *VBUI-interface* >	This enters interface configuration mode

2. To configure VBUI IP address, use the following command.

Format	Function
ZXUAS(config-if)#**ip address** <*ip-address*> <*net-mask*>	This configures VBUI IP address

3. To configure IP address pool, use the following command.

Format	Function
ZXUAS(config-if)#**ip pool** [<*pool-number*>] <*poolname*> <*start-ip*> <*end-ip*> [**dhcp-slot <***slot***>**|**domain** <*domain-number*>]	This configures IP address pool

4. To configure primary DNS, use the following command.

Format	Function
ZXUAS(config-if)#**dns primary** <*ip-address*>	This configures primary DNS

5. To configure secondary DNS, use the following command.

Format	Function
ZXUAS(config-if)#**dns secondary** <*ip-address*>	This configures secondary DNS

6. To configure ARP aging time, use the following command.

Format	Function
ZXUAS(config-if)#**arp timeout** <*seconds*>	This confiugres ARP aging time

7. To identify option60 on VBUI, use the following command.

Format	Function
ZXUAS(config-if)#**dhcp option60**	This identifies option60 on VBUI

END OF STEPS

Result VBUI has been configured.

Example This example shows how to configure VBUI.

```
ZXUAS(config)#int vbui1
ZXUAS(config-if)#ip add 12.1.1.3 255.255.0.0
ZXUAS(config-if)#ip pool my-pool 12.1.1.1 12.1.1.200
ZXUAS(config-if)#dns primary 202.0.0.1
ZXUAS(config-if)#dns secondary 202.0.0.2
ZXUAS(config-if)#arp timeout 5000
ZXUAS(config-if)#dhcp option60
```

Configuring Domain

Purpose This topic describes how to configure domain.

Steps To configure domain, perform the following steps.

1. To enter bras configuration mode, use the following command.

Format	Function
ZXUAS(config)#**bras**	This enters bras configuration mode

2. To create a domain, use the following command.

Format	Function
ZXUAS(config-bras)#**domain** <*domain-number*>	This creates a domain

3. To configure domain alias, use the following command.

Format	Function
ZXUAS(config-domain-2)#**alias** <*name*> [**advertise**]	This configures domain alias

4. To configure user authentication mode, use the following command.

Format	Function
ZXUAS(config-domain-2)#**authentication-type** {**none**|**local**|**radius**|**local-radius**|**radius-local**|**radius-none**}	This configures user authentication mode

5. To configure user accounting mode, use the following command.

Format	Function
ZXUAS(config-domain-2)#**accounting-type** {**none|radius**}	This configures user accounting mode

END OF STEPS

Result Domain has been configured.

Example This example shows how to configure domain.

```
ZXUAS(config)#bras
ZXUAS(config-bras)#domain 2
ZXUAS(config-domain-2)#alias zte.com advertise
ZXUAS(config-domain-2)#authentication-type local
ZXUAS(config-domain-2)#accounting-type none
```

Configuring User

Purpose This topic describes how to configure a user.

Steps To configure a user, perform the following steps.

1. To enter bras configuration mode, use the following command.

Format	Function
ZXUAS(config)#**bras**	This enters bras configuration mode

2. To enter subscriber configuration mode, use the following command.

Format	Function
ZXUAS(config-bras)#**subscriber** <*name*> <*domain*>	This enters subscriber configuration mode

3. To configure user password, use the following command.

Format	Function
ZXUAS(config-sub-test)#**password** <*str*>	This configures user password

4. To configure IP address obtainment mode, use the following command.

Format	Function
ZXUAS(config-sub-test)#**ip address** {<*ip-address*>|**pool** <*pool-name*>|**interface** <*interface-name*>|**vrf**}	This configures IP address obtainment mode

5. To configure user TCP rate, use the following command.

Format	Function
ZXUAS(config-sub-test)#**tcp-limit rate** <*tcp- limit- rate*>	This configures user TCP rate

6. To configure TCP connection number, use the following command.

Format	Function
ZXUAS(config-sub-test)#**tcp-limit num** <*tcp-limit-number*>	This configures TCP connection number

7. To configure the circuit through which user accesses to device, use the following command.

Format	Function
ZXUAS(config-sub-test)#**cir-bind** {**bras** <*slot*> <*port*> [**vlan** <*vlan*>|**pvc** <*vpi*> <*vci*>]|**dslam** <*slot*> <*port*> [**vlan** <*vlan*>]}	This configures the circuit through which user accesses to device

END OF STEPS

Result User has been configured.

Example This example shows how to configure a user.

```
ZXUAS(config)#bras
ZXUAS(config-bras)#subscriber test domain-name zte.com
ZXUAS(config-sub-test)#password test
ZXUAS(config-sub-test)#ip address pool my-pool
ZXUAS(config-sub-test)#tcp-limit rate 800
ZXUAS(config-sub-test)#tcp-limit num 10
ZXUAS(config-sub-test)#cir-bind bras 1 10 vlan 10
```

Configuring User Circuit

Purpose This topic describes how to configure a circuit connecting to users.

Steps To configure a circuit connecting to users, perform the following steps.

1. To enter circuit interface configuration mode, use the following command.

Format	Function
ZXUAS(config)#**interface** *type slot/port.subinterface* **bras**	This enters circuit interface configuration mode

2. To create PVC, use the following command.

Format	Function
ZXUAS(config-subif)#**atm pvc** <*vpi*> <*vci*>	This creates PVC

3. To configure encapsulation type, use the following command.

Format	Function
ZXUAS(config-subif)#**encapsulation** <*type*>	This configures encapsulation type

4. To bind authentication mode, use the following command.

Format	Function
ZXUAS(config-subif)#**bind authentication** {**chap**|**chap-pap**|**pap**} [**maximum** <*numbers*>]	This binds authentication mode

5. To configure not to use DOT1q encapsulation, use the following command.

Format	Function
ZXUAS(config-subif)#**dot1q none**	This configures not to use DOT1q encapsulation

END OF STEPS

Result Circuit connecting to users has been configured.

Example This example shows how to configure a circuit connecting to users.

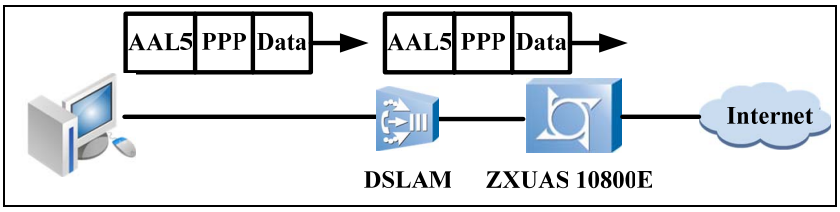
```
ZXUAS(config)#interface atm155_1/1.1 bras
ZXUAS(config-subif)#atm pvc 8 81
ZXUAS(config-subif)#encapsulation ppp-over-ethernet
ZXUAS(config-subif)#bind authentication pap
ZXUAS(config-subif)#dot1q none
```

PPPoA Overview

For PPPoA service, PPP messages are encapsulated by AAL5, and then they reach ZXUAS 10800E.

Basic network of PPPoA service is shown in Figure 44.

FIGURE 44 BASIC NETWORK OF PPPOA SERVICE



PPPoA Configuration

Contents PPPoA configuration includes the following topics.

Configuring Network Interface

Purpose This topic describes how to configure interface connecting to Ethernet.

Steps To configure interface connecting to Ethernet, perform the following steps.

1. To enter interface configuration mode, use the following command.

Format	Function
ZXUAS(config)#**interface** *type slot/port*	This enters interface configuration mode

2. To configure IP address, use the following command.

Format	Function
ZXUAS(config-if)#**ip address** *<ip-address> <net-mask>*	This configures IP address

END OF STEPS

Result Interface connecting to Ethernet has been configured.

Example This example shows how to configure interface connecting to Ethernet.

```
ZXUAS(config)#interface fei_7/1
ZXUAS(config-if)#ip address 200.0.0.100 255.255.0.0
ZXUAS(config-if)#exit
```

Configuring VBUI

Purpose This topic describes how to configure VBUI.

Steps To configure VBUI, perform the following steps.

1. To enter interface configuration mode, use the following command.

Format	Function
ZXUAS(config)# **interface vbui**< *VBUI-interface* >	This enters interface configuration mode

2. To configure VBUI IP address, use the following command.

Format	Function
ZXUAS(config-if)#**ip address** <*ip-address*> <*net-mask*>	This configures VBUI IP address

3. To configure IP address pool, use the following command.

Format	Function
ZXUAS(config-if)#**ip pool** [<*pool-number*>] <*poolname*> <*start-ip*> <*end-ip*> [**dhcp-slot <***slot***>**|**domain** <*domain-number*>]	This configures IP address pool

4. To configure primary DNS, use the following command.

Format	Function
ZXUAS(config-if)#**dns primary** <*ip-address*>	This configures primary DNS

5. To configure secondary DNS, use the following command.

Format	Function
ZXUAS(config-if)#**dns secondary** <*ip-address*>	This configures secondary DNS

6. To configure ARP aging time, use the following command.

Format	Function
ZXUAS(config-if)#**arp timeout** <*seconds*>	This confiugres ARP aging time

7. To identify option60 on VBUI, use the following command.

Format	Function
ZXUAS(config-if)#**dhcp option60**	This identifies option60 on VBUI

END OF STEPS

Result VBUI has been configured.

Example This example shows how to configure VBUI.

```
ZXUAS(config)#interface vbui1
ZXUAS(config-if)#ip add 12.1.1.3 255.255.0.0
ZXUAS(config-if)#ip pool my-pool 12.1.1.1 12.1.1.200
ZXUAS(config-if)#dns primary 202.0.0.1
ZXUAS(config-if)#dns secondary 202.0.0.2
ZXUAS(config-if)#arp timeout 5000
ZXUAS(config-if)#dhcp option60
```

Configuring Domain

Purpose This topic describes how to configure domain.

Steps To configure domain, perform the following steps.

1. To enter bras configuration mode, use the following command.

Format	Function
ZXUAS(config)#**bras**	This enters bras configuration mode

2. To create a domain, use the following command.

Format	Function
ZXUAS(config-bras)#**domain** <*domain-number*>	This creates a domain

3. To configure domain alias, use the following command.

Format	Function
ZXUAS(config-domain-2)#**alias** <*name*> [**advertise**]	This configures domain alias

4. To configure user authentication mode, use the following command.

Format	Function
ZXUAS(config-domain-2)#**authentication-type** {**none**|**local**|**radius**|**local-radius**|**radius-local**|**radius-none**}	This configures user authentication mode

5. To configure user accounting mode, use the following command.

Format	Function
ZXUAS(config-domain-2)#**accounting-type** {**none|radius**}	This configures user accounting mode

END OF STEPS

Result Domain has been configured.

Example This example shows how to configure domain.

```
ZXUAS(config)#bras
ZXUAS(config-bras)#domain 2
ZXUAS(config-domain-2)#alias zte.com advertise
ZXUAS(config-domain-2)#authentication-type local
ZXUAS(config-domain-2)#accounting-type none
```

Configuring User

Purpose This topic describes how to configure a user.

Steps To configure a user, perform the following steps.

1. To enter bras configuration mode, use the following command.

Format	Function
ZXUAS(config)#**bras**	This enters bras configuration mode

2. To enter subscriber configuration mode, use the following command.

Format	Function
ZXUAS(config-bras)#**subscriber** <*name*> <*domain*>	This enters subscriber configuration mode

3. To configure user password, use the following command.

Format	Function
ZXUAS(config-sub-test)#**password** <*str*>	This configures user password

4. To configure IP address obtainment mode, use the following command.

Format	Function
ZXUAS(config-sub-test)#**ip address** {<*ip-address*>|**pool** <*pool-name*>|**interface** <*interface-name*>|**vrf**}	This configures IP address obtainment mode

5. To configure user TCP rate, use the following command.

Format	Function
ZXUAS(config-sub-test)#**tcp-limit rate** <*tcp- limit- rate*>	This configures user TCP rate

6. To configure TCP connection number, use the following command.

Format	Function
ZXUAS(config-sub-test)#**tcp-limit num** <*tcp-limit-number*>	This configures TCP connection number

7. To configure the circuit through which user accesses to device, use the following command.

Format	Function
ZXUAS(config-sub-test)#**cir-bind** {**bras** <*slot*> <*port*> [**vlan** <*vlan*>|**pvc** <*vpi*> <*vci*>]|**dslam** <*slot*> <*port*> [**vlan** <*vlan*>]}	This configures the circuit through which user accesses to device

END OF STEPS

Result User has been configured.

Example This example shows how to configure a user.

```
ZXUAS(config)#bras
ZXUAS(config-bras)#subscriber test domain-name zte.com
ZXUAS(config-sub-test)#password test
ZXUAS(config-sub-test)#ip address pool my-pool
ZXUAS(config-sub-test)#tcp-limit rate 800
ZXUAS(config-sub-test)#tcp-limit num 10
ZXUAS(config-sub-test)#cir-bind bras 1 10 vlan 10
```

Configuring User Circuit

Purpose This topic describes how to configure a circuit connecting to users.

Steps To configure a circuit connecting to users, perform the following steps.

1. To enter circuit interface configuration mode, use the following command.

Format	Function
ZXUAS(config)#**interface** *type slot/port.subinterface* **bras**	This enters circuit interface configuration mode

2. To create PVC, use the following command.

Format	Function
ZXUAS(config-subif)#**atm pvc** <*vpi*> <*vci*>	This creates PVC

3. To configure encapsulation type, use the following command.

Format	Function
ZXUAS(config-subif)#**encapsulation** <*type*>	This configures encapsulation type

4. To bind authentication mode, use the following command.

Format	Function
ZXUAS(config-subif)#**bind authentication** {**chap**|**chap-pap**|**pap**} [**maximum** <*numbers*>]	This binds authentication mode

5. To configure not to use DOT1q encapsulation, use the following command.

Format	Function
ZXUAS(config-subif)#**dot1q none**	This configures not to use DOT1q encapsulation

END OF STEPS

Result Circuit connecting to users has been configured.

Example This example shows how to configure a circuit connecting to users.

```
ZXUAS(config)#interface atm155_1/1.1 bras
ZXUAS(config-subif)#atm pvc 8 81
ZXUAS(config-subif)#encapsulation bridge1483
ZXUAS(config-subif)#bind authentication pap
ZXUAS(config-subif)#dot1q none
```

This page is intentionally blank.

Chapter 9

IPoX Configuration

Overview

Introduction This chapter describes IPoX and configuration on ZXUAS 10800E.

Contents This chapter includes the following topics.

IPoX Service Overview

IPoX is a set of services for access authentication. In IPoX services, users access network through Ethernet or Asymmetrical Digital Subscriber Line (ADSL). Users obtain fixed IP addresses or obtain IP addresses through DHCP. Users should pass WEB authentication, fast authentication or binding authentication before access network.

IPoX Service Types IPox service types are described in Table 23.

TABLE 23 IPOX SERVICE TYPES

Type	Description
IPoE	During transmission course, IP messages are encapsulated by Ethernet, and then they reach ZXUAS 10800E.

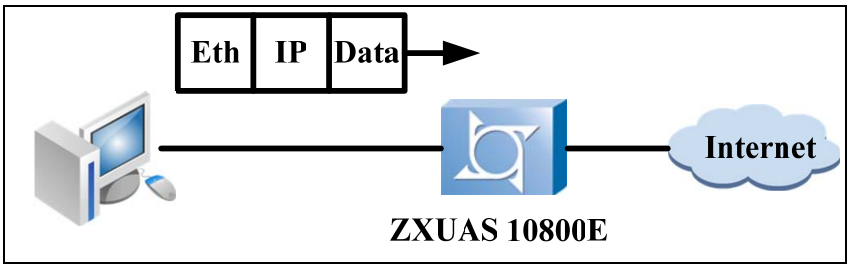
Type	Description
IPoEoV	During transmission course, IP messages are encapsulated by Ethernet and VLAN, and then they reach ZXUAS 10800E.
IPoEoA	During transmission course, IP messages are encapsulated by Ethernet and AAL5, and then they reach ZXUAS 10800E.
Static User	User configures a fixed IP address on his own PC, and administrator sets the user as a legal user on ZXUAS 10800E.

IPoE Overview

For IPoE service, after IP messages are encapsulated by Ethernet, they are not encapsulated or changed by other equipment during transmission course.

Basic network of IPoE service is shown in Figure 45. IP messages may pass by L2 devices, such as HUB and LAN switch, but these devices do not encapsulate or change format of IPoE messages.

FIGURE 45 BASIC NETWORK OF IPOE SERVICE



IPoE Configuration

Contents IPoE configuration includes the following topics.

Configuring Network Interface

Purpose This topic describes how to configure interface connecting to Ethernet.

Steps To configure interface connecting to Ethernet, perform the following steps.

1. To enter interface configuration mode, use the following command.

Format	Function
ZXUAS(config)#**interface** *type slot/port*	This enters interface configuration mode

2. To configure IP address, use the following command.

Format	Function
ZXUAS(config-if)#**ip address** <*ip-address*> <*net-mask*>	This configures IP address

END OF STEPS

Result Interface connecting to Ethernet has been configured.

Example This example shows how to configure interface connecting to Ethernet.

```
ZXUAS(config)#interface fei_7/1
ZXUAS(config-subif)#ip address 200.0.0.100 255.255.0.0
ZXUAS(config-subif)#exit
```

Configuring VBUI

Purpose This topic describes how to configure VBUI.

Steps To configure VBUI, perform the following steps.

1. To enter interface configuration mode, use the following command.

Format	Function
ZXUAS(config)# **interface vbui**< *VBUI-interface* >	This enters interface configuration mode

2. To configure VBUI IP address, use the following command.

Format	Function
ZXUAS(config-if)#**ip address** <*ip-address*> <*net-mask*>	This configures VBUI IP address

3. To configure IP host, use the following command.

ZXUAS(config-if)#**ip host** <*start-ip-address*> [**through** <*end-ip-address*>|<*mac_address*>] **slot** <*slot*> **port** <*port*> [**pvc** <*vpi*> <*vci*>|**vlan** <*vlanid*> [**second-vlan** <*vlanid*>]] **[up-rate** <*value*>**] [down-rate** <*value*>] [**username** <*username*> **password** <*password*>]

END OF STEPS

Result VBUI has been configured.

Example This example shows how to configure VBUI.

```
ZXUAS(config)#interface vbui1
ZXUAS(config-if)#ip address 12.1.1.3 255.255.0.0
ZXUAS(config-if)#ip host 12.1.1.4 slot 7 port 14
ZXUAS(config-if)#exit
```

Configuring User Circuit

Purpose This topic describes how to configure a circuit connecting to users.

Steps To configure a circuit connecting to users, perform the following steps.

1. To enter circuit interface configuration mode, use the following command.

Format	Function
ZXUAS(config)#**interface** *type slot/port.subinterface* **bras**	This enters circuit interface configuration mode

2. To configure encapsulation type, use the following command.

Format	Function
ZXUAS(config-subif)#**encapsulation** <*type*>	This configures encapsulation type

3. To configure static binding, use the following command.

Format	Function
ZXUAS(config-subif)#**bind vbui** <*VBUI-interface*>	This configures static binding

4. To configure not to use DOT1q encapsulation, use the following command.

Format	Function
ZXUAS(config-subif)#**dot1q none**	This configures not to use DOT1q encapsulation

END OF STEPS

Result Circuit connecting to users has been configured.

Example This example shows how to configure a circuit connecting to users.

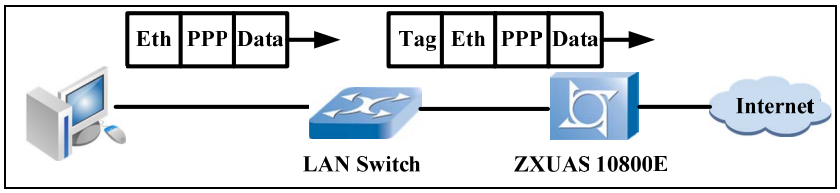
```
ZXUAS(config)#interface fei_7/14.1 bras
ZXUAS(config-subif)#enc ip-over-ethernet
ZXUAS(config-subif)#bind vbui vbui1
ZXUAS(config-subif)#dot1q no
ZXUAS(config-subif)#end
```

IPoEoV Overview

For IPoEoV service, IP messages are encapsulated by Ethernet when they pass by Ethernet interfaces, then they become IPoE messages. When IPoE messages pass by LAN switch, VLAN tags are added to IPoE messages, and they become IPoEoV messages. At last, IPoEoV messages reach ZXUAS 10800E.

Basic network of IPoEoV service is shown in Figure 46.

FIGURE 46 BASIC NETWORK OF IPOEOV SERVICE



IPoEoV Configuration

Contents IPoEoV configuration includes the following topics.

Configuring Network Interface

Purpose This topic describes how to configure interface connecting to Ethernet.

Steps To configure interface connecting to Ethernet, perform the following steps.

1. To enter interface configuration mode, use the following command.

Format	Function
ZXUAS(config)#**interface** *type slot/port*	This enters interface configuration mode

2. To configure IP address, use the following command.

Format	Function
ZXUAS(config-if)#**ip address** <*ip-address*> <*net-mask*>	This configures IP address

END OF STEPS

Result Interface connecting to Ethernet has been configured.

Example This example shows how to configure interface connecting to Ethernet.

```
ZXUAS(config)#interface fei_7/1
ZXUAS(config-subif)#ip address 200.0.0.100 255.255.0.0
ZXUAS(config-subif)#exit
```

Configuring VBUI

Purpose This topic describes how to configure VBUI.

Steps To configure VBUI, perform the following steps.

1. To enter interface configuration mode, use the following command.

Format	Function
ZXUAS(config)# **interface vbui**< *VBUI-interface* >	This enters interface configuration mode

2. To configure VBUI IP address, use the following command.

Format	Function
ZXUAS(config-if)#**ip address** <*ip-address*> <*net-mask*>	This configures VBUI IP address

3. To configure IP host, use the following command.

   ZXUAS(config-if)#**ip host** <*start-ip-address*> [**through** <*end-ip-address*>|<*mac_address*>] **slot** <*slot*> **port** <*port*> [**pvc** <*vpi*> <*vci*>|**vlan** <*vlanid*> [**second-vlan** <*vlanid*>]] **[up-rate** <*value*>**] [down-rate** <*value*>] [**username** <*username*> **password** <*password*>]

END OF STEPS

Result VBUI has been configured.

Example This example shows how to configure VBUI.

```
ZXUAS(config)#interface vbui1
ZXUAS(config-if)#ip address 12.1.1.3 255.255.0.0
ZXUAS(config-if)#ip host 12.1.1.4 slot 7 port 14 vlan 10
ZXUAS(config-if)#exit
```

Configuring User Circuit

Purpose This topic describes how to configure a circuit connecting to users.

Steps To configure a circuit connecting to users, perform the following steps.

1. To enter circuit interface configuration mode, use the following command.

Format	Function
ZXUAS(config)#**interface** *type slot/port.subinterface* **bras**	This enters circuit interface configuration mode

2. To configure encapsulation type, use the following command.

Format	Function
ZXUAS(config-subif)#**encapsulation** <*type*>	This configures encapsulation type

3. To configure static binding, use the following command.

Format	Function
ZXUAS(config-subif)#**bind vbui** <*VBUI-interface*>	This configures static binding

4. To forward IPoE packets with VLAN-ID tag, use the following command.

Format	Function
ZXUAS(config-subif)#**dot1q** {<*vlan-id* >**|none|tunneling ethertype** <*type*>}	This forwards IPoE packets with VLAN-ID tag

END OF STEPS

Result Circuit connecting to users has been configured.

Example This example shows how to configure a circuit connecting to users.

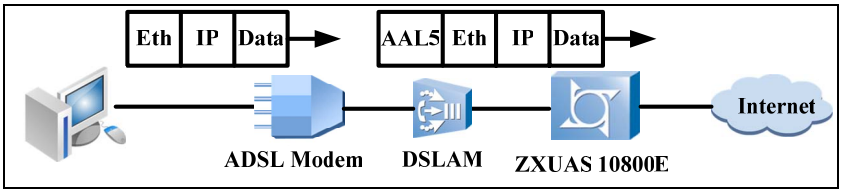
```
ZXUAS(config)#interface fei_7/14.1 bras
ZXUAS(config-subif)#encapsulation ip-over-ethernet
ZXUAS(config-subif)#bind vbui vbui1
ZXUAS(config-subif)#dot1q 10
ZXUAS(config-subif)#end
```

IPoEoA Overview

For IPoEoA service, IP messages are encapsulated by Ethernet when they pass by Ethernet interfaces, then they become IPoE messages. When IPoE messages pass by ADSL Modem, they are encapsulated by AAL5, and they become IPoEoA messages. At last, they are forwarded by DSLAM to ZXUAS 10800E.

Basic network of IPoEoA service is shown in Figure 47.

FIGURE 47 BASIC NETWORK OF IPOEOA SERVICE



IPoEoA Configuration

Contents IPoEoA configuration includes the following topics.

Configuring Network Interface

Purpose This topic describes how to configure interface connecting to Ethernet.

Steps To configure interface connecting to Ethernet, perform the following steps.

1. To enter interface configuration mode, use the following command.

Format	Function
ZXUAS(config)#**interface** *type slot/port*	This enters interface configuration mode

2. To configure IP address, use the following command.

Format	Function
ZXUAS(config-if)#**ip address** *<ip-address> <net-mask>*	This configures IP address

END OF STEPS

Result Interface connecting to Ethernet has been configured.

Example This example shows how to configure interface connecting to Ethernet.

```
ZXUAS(config)#interface fei_7/1
ZXUAS(config-subif)#ip address 200.0.0.100 255.255.0.0
ZXUAS(config-subif)#exit
```

Configuring VBUI

Purpose This topic describes how to configure VBUI.

Steps To configure VBUI, perform the following steps.

1. To enter interface configuration mode, use the following command.

Format	Function
ZXUAS(config)# **interface vbui**< *VBUI-interface* >	This enters interface configuration mode

2. To configure VBUI IP address, use the following command.

Format	Function
ZXUAS(config-if)#**ip address** <*ip-address*> <*net-mask*>	This configures VBUI IP address

3. To configure IP host, use the following command.

   ZXUAS(config-if)#**ip host** <*start-ip-address*> [**through** <*end-ip-address*>|<*mac_address*>] **slot** <*slot*> **port** <*port*> [**pvc** <*vpi*> <*vci*>|**vlan** <*vlanid*> [**second-vlan** <*vlanid*>]] **[up-rate** <*value*>**]** **[down-rate** <*value*>] [**username** <*username*> **password** <*password*>]

END OF STEPS

Result VBUI has been configured.

Example This example shows how to configure VBUI.

```
ZXUAS(config)#interface vbui1
ZXUAS(config-if)#ip address 12.1.1.3 255.255.0.0
ZXUAS(config-if)#ip host 12.1.1.4 slot 7 port 14
ZXUAS(config-if)#exit
```

Configuring User Circuit

Purpose This topic describes how to configure a circuit connecting to users.

Steps To configure a circuit connecting to users, perform the following steps.

1. To enter circuit interface configuration mode, use the following command.

Format	Function
ZXUAS(config)#**interface** *type slot/port.subinterface* **bras**	This enters circuit interface configuration mode

2. To create PVC, use the following command.

Format	Function
ZXUAS(config-subif)#**atm pvc** <*vpi*> <*vci*>	This creates PVC

3. To configure encapsulation type, use the following command.

Format	Function
ZXUAS(config-subif)#**encapsulation** <*type*>	This configures encapsulation type

4. To configure static binding, use the following command.

Format	Function
ZXUAS(config-subif)#**bind vbui** <*VBUI-interface*>	This configures static binding

5. To configure not to use DOT1q encapsulation, use the following command.

Format	Function
ZXUAS(config-subif)#**dot1q none**	This configures not to use DOT1q encapsulation

END OF STEPS

Result Circuit connecting to users has been configured.

Example This example shows how to configure a circuit connecting to users.

```
ZXUAS(config)#interface fei_7/14.1 bras
ZXUAS(config-subif)#enc ip-over-ethernet
ZXUAS(config-subif)#bind vbui vbui1
ZXUAS(config-subif)#dot1q none
ZXUAS(config-subif)#end
```

Chapter 10

DHCP Configuration

Overview

Introduction This chapter describes DHCP and configuration on ZXUAS 10800E.

Contents This chapter includes the following topics.

DHCP Overview

With extension of network scale and enhancement of network complexity, there are situations when PC position changes or IP addresses are not enough to allocate. Dynamic Host Configuration Protocol (DHCP) allows a host to obtain an IP address from a DHCP server for normal communications in such situations.

IP Address Allocation Types DHCP supports three types of IP address allocations:

- Automatic allocation

  DHCP assigns a permanent IP address to a client.

- Dynamic allocation

  DHCP assigns an IP address to a client for a limited period of time. The valid time segment of using the address is called

lease period. Once the lease period expires, the host must request the server for continuous lease. The host cannot continue to lease until the server accepts the request, otherwise it must give up unconditionally.

- Manual allocation

  Network administrator assigns an IP address to a client and DHCP is used simply to convey the assigned address to the client.

Priorities of Allocated Addresses

Priorities of IP addresses allocated by DHCP servers are described below, in the order of from high to low.

- IP addresses in DHCP server database that are bound statically with MAC addresses of clients
- IP addresses used by clients before
- Available IP addresses that are first found in address pool
- Over-lease IP addresses or conflicted IP addresses

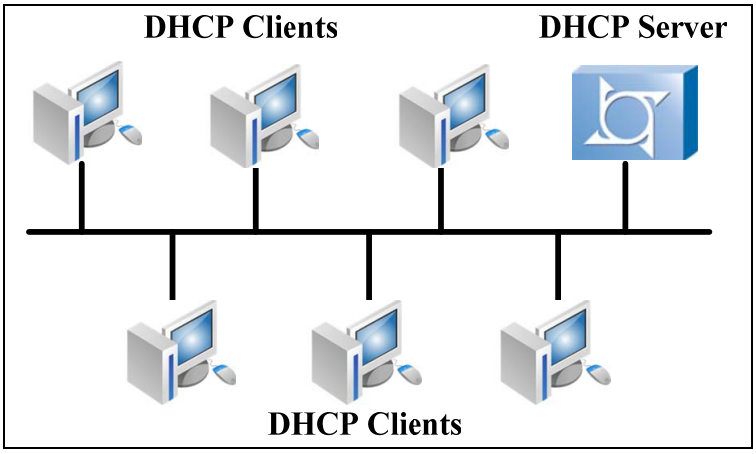
DHCP Server

DHCP server is used in the following situations:

- In a vast network, manual configuration costs too much time and it is hard to manage the whole network.
- There are much more hosts than available IP addresses in a network. It fails to allocate a fixed IP address for each host.
- There are few hosts using fixed IP addresses and most of hosts using un-fixed IP addresses.

Network of DHCP server is shown in Figure 48.

FIGURE 48 NETWORK OF DHCP SERVER



Working Procedure

When a client logs in the network for the first time, a DHCP server works in the following steps:

1. A host sends a DHCP Discover broadcast message requesting an IP address and other configuration parameters.
2. A DHCP server returns a DHCP Offer message containing a valid IP address.
3. Host selects the server from which it receives DHCP Offer message in the first time, and sends a DHCP Request broadcast message, which contains information about the server it chooses.
4. Selected DHCP server returns a DHCP Ack message for acknowledgement.

By now the host can use the IP address and relevant configuration obtained from the DHCP server for communication.

When a client re-logs in the network, a DHCP server works in the following steps:

1. Client broadcasts DHCP Request message that contains IP address the server allocated last time.
2. If the IP address the server allocated to client last time is available, the server returns DHCP Ack message to inform client to use the IP address it used last time.
3. If the IP address the server allocated to client last time is used by other client now, the server returns DHCP Nak message. When client receives DHCP Nak message, it sends DHCP Discover message to request a new IP address.

IP Lease IP address allocated to client in dynamic allocation method has a period of validity. When the IP expires, server will get it back. If the client wants to use this IP, it is required to update lease.

Lease Update In practice, when IP lease period is left half, client sends a DHCP Request message automatically to the server to update the lease. If this IP is valid, the server returns a DHCP Ack message to inform the client that lease is updated.

DHCP Relay

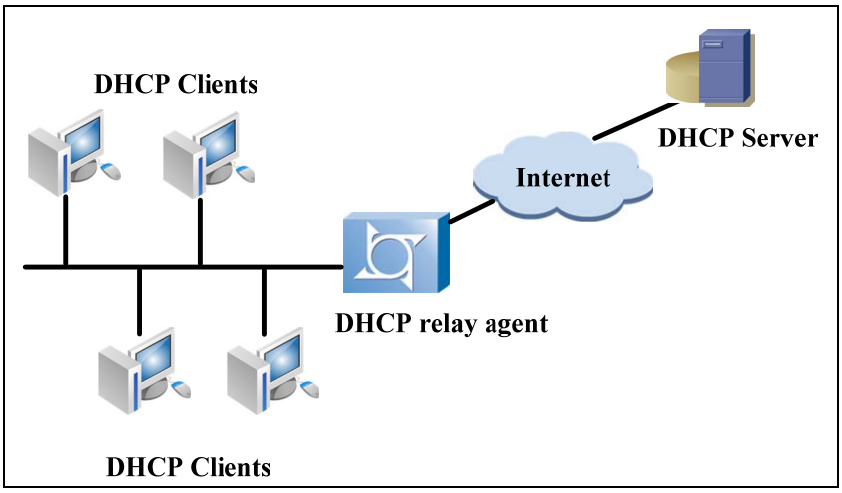
Background The early DHCP is only suitable when DHCP clients and server are in the same network segment. To implement dynamic host configuration, it is required to set a DHCP server in each network segment.

DHCP relay solves this problem. Clients in a LAN can communicate with DHCP servers in other sub-networks through DHCP relay.

Either a host or a router can be a DHCP relay.

Network of DHCP relay is shown in Figure 49.

FIGURE 49 NETWORK OF DHCP RELAY



Working Procedure

1. When DHCP client starts to initialize DHCP, it broadcasts DHCP Request message in local network.
2. If there is a DHCP server in local network, DHCP configuration can be implemented without DHCP relay.
3. If there is no DHCP server in local network, when devices that are with DHCP relay function and connects with local network receive DHCP Request message, they forward the message to DHCP relay in other network.
4. DHCP server implements configuration according to information provided by client, and sends configuration information to client through DHCP relay.

It can be considered that DHCP provides transparent transmission function for DHCP broadcast messages. It forwards broadcast messages from DHCP client (or from server) to DHCP server (or to client) in other network segment transparently.

DHCP Server Configuration

Introduction

In DHCP server configuration, ZXUAS 10800E manages address pool by itself, and responds to DHCP requests from clients to complete address allocation.

Contents

DHCP server configuration includes the following topics.

Configuring Network Interface

Purpose This topic describes how to configure interface connecting to Ethernet.

Steps To configure interface connecting to Ethernet, perform the following steps.

1. To enter interface configuration mode, use the following command.

Format	Function
ZXUAS(config)#**interface** *type slot/port*	This enters interface configuration mode

2. To configure IP address, use the following command.

Format	Function
ZXUAS(config-if)#**ip address** <*ip-address*> <*net-mask*>	This configures IP address

END OF STEPS

Result Network interface has been configured.

Configuring VBUI

Purpose This topic describes how to configure VBUI.

Steps To configure VBUI, perform the following steps.

1. To enter interface configuration mode, use the following command.

Format	Function
ZXUAS(config)# **interface vbui**< *VBUI-interface* >	This enters interface configuration mode

2. To configure VBUI IP address, use the following command.

Format	Function
ZXUAS(config-if)#**ip address** <*ip-address*> <*net-mask*>	This configures VBUI IP address

3. To configure IP address pool, use the following command.

Format	Function
ZXUAS(config-if)# **ip pool** [<*pool-number*>] <*poolname*> <*start-ip*> <*end-ip*> [**dhcp-slot** <*slot*>|**domain** <*domain-number*>]	This configures IP address pool

4. To configure DHCP mode, use the following command.

Format	Function
ZXUAS(config-if)#**ip dhcp mode** {**relay**|**server**}	This configures DHCP mode

5. To configure DCHP server gateway, use the following command.

Format	Function
ZXUAS(config-if)#**ip dhcp server gateway** <*gateway-ip-address*>	This configures DCHP server gateway

END OF STEPS

Result VBUI has been configured.

Configuring DHCP Function

Purpose This topic describes how to configure DHCP function.

Step To configure DHCP function, use the following command.

Format	Function
ZXUAS(config)#**ip dhcp enable**	This enables DHCP function

END OF STEP

Result DHCP function has been configured.

Configuring DNS

Purpose This topic describes how to configure DNS.

Step To configure DNS, use the following command.

Format	Function
ZXUAS(config)#**ip dhcp server dns** <*mdns-address*> [<*sdns-address*>]	This configures primary DNS and secondary DNS

END OF STEP

Result DNS has been configured.

Configuring User Circuit

Purpose This topic describes how to configure a circuit connecting to users.

Steps To configure a circuit connecting to users, perform the following steps.

1. To enter circuit interface configuration mode, use the following command.

Format	Function
ZXUAS(config)#**interface** *type slot/port.subinterface* **bras**	This enters circuit interface configuration mode

2. To configure encapsulation type, use the following command.

Format	Function
ZXUAS(config-subif)#**encapsulation** <*type*>	This configures encapsulation type

3. To configure static binding, use the following command.

Format	Function
ZXUAS(config-subif)#**bind vbui** <*VBUI-interface*>	This configures static binding

4. To configure not to use DOT1q encapsulation, use the following command.

Format	Function
ZXUAS(config-subif)#**dot1q none**	This configures not to use DOT1q encapsulation

END OF STEPS

Result User circuit has been configured.

DHCP Relay Configuration

Introduction In DHCP relay configuration, ZXUAS works as a DHCP relay agent and forwards DHCP requests from clients to specific servers.

Contents DHCP relay configuration includes the following topics.

Configuring Network Interface

Purpose This topic describes how to configure interface connecting to Ethernet.

Steps To configure interface connecting to Ethernet, perform the following steps.

1. To enter interface configuration mode, use the following command.

Format	Function
ZXUAS(config)#**interface** *type slot/port*	This enters interface configuration mode

2. To configure IP address, use the following command.

Format	Function
ZXUAS(config-if)#**ip address** <*ip-address*> <*net-mask*>	This configures IP address

END OF STEPS

Result Network interface has been configured.

Configuring VBUI

Purpose This topic describes how to configure VBUI.

Steps To configure VBUI, perform the following steps.

1. To enter interface configuration mode, use the following command.

Format	Function
ZXUAS(config)# **interface vbui**< *VBUI-interface* >	This enters interface configuration mode

2. To configure VBUI IP address, use the following command.

Format	Function
ZXUAS(config-if)#**ip address** <*ip-address*> <*net-mask*>	This configures VBUI IP address

3. To configure DHCP mode, use the following command.

Format	Function
ZXUAS(config-if)#**ip dhcp mode** {**relay**|**server**}	This configures DHCP mode

4. To configure DHCP relay agent, use the following command.

Format	Function
ZXUAS(config-if)#**ip dhcp relay agent** <*agent-ip-address*>	This configures DHCP relay agent

5. To configure address of DHCP relay server, use the following command.

Format	Function
ZXUAS(config-if)#**ip dhcp relay server** <*server-ip-address*>}	This configures address of DHCP relay server

6. To configure authentication switch when users are obtaining addresses, use the following command.

Format	Function
ZXUAS(config-if)#**ip dhcp auth-on-up** {**disable|enable**}	This configures authentication switch when users are obtaining addresses

7. To configure idle period of DHCP user, use the following command.

Format	Function
ZXUAS(config-if)#**dhcp idle period** <*seconds*> **traffic** <*kbytes*>	This configures idle period of DHCP user

8. To identify option60, use the following command.

Format	Function
ZXUAS(config-if)#**dhcp option60**	This identifies option60

END OF STEPS

Result VBUI has been configured.

Configuring DHCP Function

Purpose This topic describes how to configure DHCP function.

Steps To configure DHCP function, perform the following steps.

1. To enable DHCP function, use the following command.

Format	Function
ZXUAS(config)#**ip dhcp enable**	This enables DHCP function

2. To release source when DHCP clients are off-line, use the following command.

Format	Function
ZXUAS(config)#**ip dhcp relay send-release**	This releases source when DHCP clients are off-line

END OF STEPS

Result DHCP function has been configured.

Configuring User Circuit

Purpose This topic describes how to configure a circuit connecting to users.

Steps To configure a circuit connecting to users, perform the following steps.

1. To enter circuit interface configuration mode, use the following command.

Format	Function
ZXUAS(config)#**interface** *type slot/port.subinterface* **bras**	This enters circuit interface configuration mode

2. To configure encapsulation type, use the following command.

Format	Function
ZXUAS(config-subif)#**encapsulation** <*type*>	This configures encapsulation type

3. To configure static binding, use the following command.

Format	Function
ZXUAS(config-subif)#**bind vbui** <*VBUI-interface*>	This configures static binding

4. To configure not to use DOT1q encapsulation, use the following command.

Format	Function
ZXUAS(config-subif)#**dot1q none**	This configures not to use DOT1q encapsulation

END OF STEPS

Result User circuit has been configured.

DHCP Web Access Control Overview

For dynamic IP access, a user should send address application to BRAS through DHCP client. When BRAS gets the application, it allocates an address to the user and generates data forwarding path for the user.

If web authentication is enabled, a user should fill in user information on specific web server to start authentication. Web server gives user information to ZXUAS 10800E and ZXUAS 10800E implements authentication. If the user passes authentication, then he can get on-line.

DHCP Web Access Control Configuration

Contents DHCP Web Access Control configuration includes the following topics.

Configuring Network Interface

Purpose This topic describes how to configure interface connecting to Ethernet.

Steps To configure interface connecting to Ethernet, perform the following steps.

1. To enter interface configuration mode, use the following command.

Format	Function
ZXUAS(config)#**interface** *type slot/port*	This enters interface configuration mode

2. To configure IP address, use the following command.

Format	Function
ZXUAS(config-if)#**ip address** *<ip-address> <net-mask>*	This configures IP address

END OF STEPS

Result Nerwork interface has been configured.

Configuring VBUI

Purpose This topic describes how to configure VBUI.

Steps To configure VBUI, perform the following steps.

1. To enter interface configuration mode, use the following command.

Format	Function
ZXUAS(config)# **interface vbui**< *VBUI-interface* >	This enters interface configuration mode

2. To configure VBUI IP address, use the following command.

Format	Function
ZXUAS(config-if)#**ip address** <*ip-address*> <*net-mask*>	This configures VBUI IP address

3. To configure IP address pool, use the following command.

Format	Function
ZXUAS(config-if)# **ip pool** [<*pool-number*>] <*poolname*> <*start-ip*> <*end-ip*> [**dhcp-slot <***slot***>**|**domain** <*domain-number*>]	This configures IP address pool

4. To configure DHCP mode, use the following command.

Format	Function
ZXUAS(config-if)#**ip dhcp mode** {**relay**|**server**}	This configures DHCP mode

5. To configure DCHP server gateway, use the following command.

Format	Function
ZXUAS(config-if)#**ip dhcp server gateway** <*gateway-ip-address*>	This configures DCHP server gateway

6. To configure web authentication mode, use the following command.

Format	Function
ZXUAS(config-if)#**web authentication subscriber {none|web [force]}**	This configures web authentication mode

7. To configure web authentication server, use the following command.

Format	Function
ZXUAS(config-if)#**web server** <*ip-addr*> [**port** <*udp-port*>]	This configures web authentication server

8. To configure user parameters, use the following command.

Format	Function
ZXUAS(config-if-websvr)# **http-param {uas** *name value* |**user** *name***}**	This configures user parameters

END OF STEPS

Result VBUI has been configured.

Configuring Domain

Purpose This topic describes how to configure domain.

Steps To configure domain, perform the following steps.

1. To enter bras configuration mode, use the following command.

Format	Function
ZXUAS(config)#**bras**	This enters bras configuration mode

2. To create a domain, use the following command.

Format	Function
ZXUAS(config-bras)#**domain** <*domain-number*>	This creates a domain

3. To configure domain alias, use the following command.

Format	Function
ZXUAS(config-domain-2)#**alias** <*name*> [**advertise**]	This configures domain alias

4. To configure user authentication mode, use the following command.

Format	Function
ZXUAS(config-domain-2)#**authentication-type** {**none|local|radius|local-radius|radius-local|radius-none**}	This configures user authentication mode

5. To configure user accounting mode, use the following command.

Format	Function
ZXUAS(config-domain-2)#**accounting-type** {**none|radius**}	This configures user accounting mode

6. To configure authentication server group, use the following command.

Format	Function
ZXUAS(config-domain-2)#**authentication-group** <*group-number*>	This configures authentication server group

7. To configure accounting server group, use the following command.

Format	Function
ZXUAS(config-domain-2)#**accounting-group** < *group-number* > **[second]**	This configures accounting server group

END OF STEPS

Result Domain has been configured.

Configuring User

Purpose This topic describes how to configure a user.

Steps To configure a user, perform the following steps.

1. To enter bras configuration mode, use the following command.

Format	Function
ZXUAS(config)#**bras**	This enters bras configuration mode

2. To enter subscriber configuration mode, use the following command.

Format	Function
ZXUAS(config-bras)#**subscriber** <*name*> <*domain*>	This enters subscriber configuration mode

3. To configure user, use the following command.

Format	Function
ZXUAS(config-sub-test)#**no ip address**	This configures user

END OF STEPS

Result User has been configured.

Configuring DHCP Function

Purpose This topic describes how to configure DHCP function.

Steps To configure DHCP function, perform the following steps.

1. To enable DHCP function, use the following command.

Format	Function
ZXUAS(config)#**ip dhcp enable**	This enables DHCP function

2. To release source when DHCP clients are off-line, use the following command.

Format	Function
ZXUAS(config)#**ip dhcp relay send-release**	This releases source when DHCP clients are off-line

END OF STEPS

Result DHCP function has been configured.

Configuring DNS

Purpose This topic describes how to configure DNS.

Step To configure DNS, use the following command.

Format	Function
ZXUAS(config)#**ip dhcp server dns** <*mdns-address*> [<*sdns-address*>]	This configures primary DNS and secondary DNS

END OF STEP

Result DNS has been configured.

Configuring User Circuit

Purpose This topic describes how to configure a circuit connecting to users.

Steps To configure a circuit connecting to users, perform the following steps.

1. To enter circuit interface configuration mode, use the following command.

Format	Function
ZXUAS(config)#**interface** *type slot/port.subinterface* **bras**	This enters circuit interface configuration mode

2. To configure encapsulation type, use the following command.

Format	Function
ZXUAS(config-subif)#**encapsulation** <*type*>	This configures encapsulation type

3. To configure static binding, use the following command.

Format	Function
ZXUAS(config-subif)#**bind vbui** <*VBUI-interface*>	This configures static binding

4. To configure not to use DOT1q encapsulation, use the following command.

Format	Function
ZXUAS(config-subif)#**dot1q none**	This configures not to use DOT1q encapsulation

END OF STEPS

Result User circuit has been configured.

Chapter 11

RADIUS Configuration

Overview

Introduction This chapter describes RADIUS protocol and configuration on ZXUAS 10800E.

Contents This chapter includes the following topics.

AAA Overview

Definition ZXUAS 10800E supports user authentication, authorization and accounting (AAA). The description of AAA is as follows:

- Authentication: It verifies user identities and decides whether to allow users to access network or not.
- Authorization: Network administrator can limit available network services for each user, which protects internal network sources.
- Accounting: Network administrator can charge the users for using network sources. Different accounting policies ban be implemented according to different demands.

Introduction to RADIUS

Introduction

Remote Authentication Dial-In User Service (RADIUS) is a distributed, client/server protocol. Radius manages dispersive dial-in service users.

Radius manages authentication, authorization, and accounting of users by a simple user database. It can modify service for users according to service type. Users submit authentication and accounting request to Radius server through BRAS.

When users want to establish connection to BRAS and obtain the right to visit some other networks, BRAS are responsible to send users' authentication and accounting information to RADIUS server. RADIUS protocol stipulates how to transmit this information between BRAS and RADIUS server. RADIUS server is responsible to receive users' requests from BRAS, authenticate name and password, and then sends configuration information needed by users to BRAS.

Authentication information is transmitted by using a secret key between BRAS and RADIUS server. In addition, any user passwords are sent encrypted between client and RADIUS server, to eliminate the possibility that someone snooping on an unsecured network could determine a user's password.

RADIUS configuration only defines some parameters between BRAS and RADIUS Serve. To make these parameters effective, it is required to appoint to use RADIUS method in domain mode, and to set authentication and accounting type as RADIUS.

Configuring RADIUS Authentication

Purpose

This topic describes how to configure RADIUS authentication.

Steps

To configure RADIUS authentication, perform the following steps.

1. To create an authentication server group, use the following command.

Format	Function
ZXUAS(config)#**radius authentication-group** *<group-number>*	This creates an authentication server group

2. To configure choice algorithm of RADIUS authentication server, use the following command.

Format	Function
ZXUAS(config-auth-group-10)#**algorithm** {**first**|**round-robin**}	This configures choice algorithm of RADIUS authentication server

3. To configure alias of RADIUS authentication server group, use the following command.

Format	Function
ZXUAS(config-auth-group-10)#**alias** <*name*>	This configures alias of RADIUS authentication server group

4. To configure NAS-IP of RADIUS authentication server group, use the following command.

Format	Function
ZXUAS(config-auth-group-10)#**nas-ip-address** <*ip-address*>	This configures NAS-IP of RADIUS authentication server group

5. To configure RADIUS authentication server and its parameters, use the following command.

Format	Function
ZXUAS(config-auth-group-10)#**server** <*server-num*> <*ipaddress*> **key** <*keystr*> [**port** <*portnum*>]	This configures RADIUS authentication server and its parameters

6. To configure user name format, use the following command.

Format	Function
ZXUAS(config-auth-group-10)#**user-name-format** {**include-domain**|**strip-domain**}	This configures user name format

7. To configure call station format, use the following command.

Format	Function
ZXUAS(config-auth-group-10)#**calling-station-format** <*number*>	This configures call station format

8. To configure deadline of RADIUS authentication server, use the following command.

Format	Function
ZXUAS(config-auth-group-10)#**deadtime** <*time*>	This configures deadline of RADIUS authentication server

9. To configure VRF related to RADIUS authentication server, use the following command.

Format	Function
ZXUAS(config-auth-group-10)#**ip vrf** <*vrf-name*>	This configures VRF related to RADIUS authentication server

10. To configure maximum retry times, use the following command.

Format	Function
ZXUAS(config-auth-group-10)#**max-retries** <*times*>	This configures maximum retry times

11. To configure NAS-PORT-ID format, use the following command.

Format	Function
ZXUAS(config-auth-group-10)#**nas-port-id-format** {**china-tel|class1|class2|class3**}	This configures NAS-PORT-ID format

12. To configure overtime of RADIUS authentication server, use the following command.

Format	Function
ZXUAS(config-auth-group-10)#**timeout** <*time*>	This configures overtime of RADIUS authentication server

13. To enable or disable private attributes, use the following command.

Format	Function
ZXUAS(config-auth-group-10)#**vendor {enable|disable}**	This enables or disables private attributes

14. To configure RADIUS auto change switch, use the following command.

Format	Function
ZXUAS(config)# **radius auto-change** {**on**|**off**}	This configures RADIUS auto change switch

END OF STEPS

Result RADIUS authentication has been configured.

Configuring RADIUS Accounting

Purpose This topic describes how to configure RADIUS accounting.

Steps To configure RADIUS accounting, perform the following steps.

1. To create an accounting server group, use the following command.

Format	Function
ZXUAS(config)#**radius accounting-group** <*group-number*>	This creates an accounting server group

2. To configure choice algorithm of RADIUS accounting server, use the following command.

Format	Function
ZXUAS(config-acct-group-8)#**algorithm** {**first**|**round-robin**}	This configures choice algorithm of RADIUS accounting server

3. To configure alias of RADIUS accounting server group, use the following command.

Format	Function
ZXUAS(config-acct-group-8)#**alias** <*name*>	This configures alias of RADIUS accounting server group

4. To configure NAS-IP of RADIUS accounting server, use the following command.

Format	Function
ZXUAS(config-auth-group-10)#**nas-ip-address** <*ip-address*>	This configures NAS-IP of RADIUS accounting server

5. To configure local buffer, use the following command.

Format	Function
ZXUAS(config-acct-group-8)#**local-buffer {enable|disable}**	This configures local buffer

6. To configure RADIUS accounting server and its parameters, use the following command.

Format	Function
ZXUAS(config-acct-group-8)#**server <***server-num***> <***ipaddress***> key <***keystr***>** [**port** <*portnum*>]	This configures RADIUS accounting server and its parameters

7. To configure user name format, use the following command.

Format	Function
ZXUAS(config-acct-group-8)#**user-name-format** {**include-domain|strip-domain**}	This configures user name format

8. To configure call station format, use the following command.

Format	Function
ZXUAS(config-acct-group-8)#**calling-station-format** <*number*>	This configures call station format

9. To configure deadline of RADIUS accounting server, use the following command.

Format	Function
ZXUAS(config-acct-group-8)#**deadtime** <*time*>	This configures deadline of RADIUS accounting server

10. To configure VRF related to RADIUS accounting server, use the following command.

Format	Function
ZXUAS(config-acct-group-8)#**ip vrf <***vrf-name***>**	This configures VRF related to RADIUS accounting server

11. To configure maximum retry times of RADIUS accounting server, use the following command.

Format	Function
ZXUAS(config-acct-group-8)#**max-retries** <*times*>	This configures maximum retry times of RADIUS accounting server

12. To configure NAS-PORT-ID format, use the following command.

Format	Function
ZXUAS(config-acct-group-8)#**nas-port-id-format** {**china-tel|class1|class2|class3**}	This configures NAS-PORT-ID format

13. To configure overtime of RADIUS accounting server, use the following command.

Format	Function
ZXUAS(config-acct-group-8)#**timeout** <*time*>	This configures overtime of RADIUS accounting server

14. To enable or disable private attributes, use the following command.

Format	Function
ZXUAS(config-acct-group-8)#**vendor {enable|disable}**	This enables or disables private attributes

15. To configure life time of accounting packet, use the following command.

Format	Function
ZXUAS(config-acct-group-8)#**life-time <***life-time***>**	This configures life time of accounting packet

END OF STEPS

Result RADIUS accounting has been configured.

Configuring RADIUS Server Reachability Detection

Background RADIUS server reachability detection is to detect current RADIUS server and judge whether the server is available and reachable.

Purpose This topic describes how to configure RADIUS server reachability detection.

Steps To configure RADIUS server reachability detection, perform the following steps.

1. To detect whether RADIUS authentication server is reachable or not, use the following command.

Format	Function
ZXUAS#**radius-ping authentication-group** <*group number* **>**	This detects whether RADIUS authentication server is reachable or not

2. To detect whether RADIUS accounting server is reachable or not, use the following command.

Format	Function
ZXUAS#**radius-ping accounting-group <***group number* **>**	This detects whether RADIUS accounting server is reachable or not

END OF STEPS

Result RADIUS server reachability detection has been configured.

Configuring RADIUS and Local Authorization

Background Before RADIUS authentication, users should pass local authentication, during which physical binding and session number are checked. RADIUS authentication is implemented. User authorization attributes that are not returned by RADIUS are supplied in local authorization configuration.

Purpose This topic describes how to configure RADIUS and local authorization.

Steps To configure RADIUS and local authorization, perform the following steps.

1. To enter bras configuration mode, use the following command.

Format	Function
ZXUAS(config)#**bras**	This enters bras configuration mode

2. To create a domain, use the following command.

Format	Function
ZXUAS(config-bras)#**domain** <*domain-number*>	This creates a domain

3. To enable or disable mix authorization, use the following command.

Format	Function
ZXUAS(config-domain-20)#**mix-authorization {enable|disable}**	This enables or disables mix authorization

4. To configure domain alias, use the following command.

Format	Function
ZXUAS(config-domain-20)#**alias** <*name*> [**advertise**]	This configures domain alias

5. To configure accounting server group, use the following command.

Format	Function
ZXUAS(config-domain-20)#**accounting-group** <*group-number*> [**second**]	This configures accounting server group

6. To configure accounting type, use the following command.

Format	Function
ZXUAS(config-domain-20)#**accounting-type** {**none|radius**}	This configures accounting type

7. To configure authentication server group, use the following command.

Format	Function
ZXUAS(config-domain-20)#**authentication-group** <*group-number*>	This configures authentication server group

8. To configure authentication type, use the following command.

Format	Function
ZXUAS(config-domain-20)#**authentication-type** {**none|local|radius|local-radius|radius-local|radius-none**}	This configures authentication type

9. To associate a user with a domain, use the following command.

Format	Function
ZXUAS(config-bras)#**subscriber** <*name*> <*domain*>	This associates a user with a domain

END OF STEPS

Result RADIUS and local authorization has been configured.

This page is intentionally blank.

Chapter 12

BRAS Security Configuration

Overview

Introduction This chapter describes BRAS security and configuration on ZXUAS 10800E.

Contents This chapter includes the following topics.

BRAS Security Overview

BRAS security configuration includes ARP packet filtration, data packet limit, circuit access control, MAC address access control and PPP authentication failure management.

Configuring BRAS Security

Purpose This topic describes how to configure BRAS security.

Steps To configure BRAS security, perform the following steps.

1. To enter bras configuration mode, use the following command.

Format	Function
ZXUAS(config)#**bras**	This enters bras configuration mode

2. To enter security configuration mode, use the following command.

Format	Function
ZXUAS(config-bras)#**security**	This enters security configuration mode

3. To limit rate of data to NPC, use the following command.

   ZXUAS(config-security)#**packet-limit** {**icmp** <*number*>|**igmp** <*number*>|**ip-fragment** <*number*>|**isis** <*number*>|**l2tp-control** <*number*>|**ldp-hello** <*number*>|**muldata** <*number*>|**nni-arp-reply** <*number*>|**nni-arp-request** <*number*>|**nni-bgp** <*number*>|**nni-ospf** <*number*>|**nni-radius** <*number*>|**nni-rip** <*number*>|**nni-snmp** <*number*>|**others** <*number*>|**pim** <number>|**resolve-next-hop-mac** <*number*>|**sechttp** <*number*>|**secposcont** <*number*>|**securpf** <*number*>|**telnet** <*number*>|**uni-arp-reply** <*number*>|**uni-arp-request**<*number*>|**uni-dhcp-control** <*number*> **uni-dhcp-discover** <number>|**uni-muldata** <*number*> <number>|**uni-ppp-control** <*number*>|**uni-ppp-data** <*number*> **uni-ppp-lcp-echo** <*number*>|**uni-ppp-padi** <*number*>|**vpls-learn-mac** <*number*>}

4. To configure MAC address access control, use the following command.

Format	Function
ZXUAS(config-security)#**permit mac <***mac_address***> ctrl-rate <***rate***>**	This configures MAC address access control

5. To configure PPP authentication failure management, use the following command.

   ZXUAS(config-security)#**ppp auth-fail** {**auto|record|none**} [**cap-time <***time***>**] [**fail-limit <***limit***>**] [**cap-limit <***limit***>**] [**cap-item <***size***>**] [**rec-item <***size***>**] [**rate-limit <***limit***>**]

END OF STEPS

Result BRAS security has been configured.

Chapter 13

Network Management Configuration

Overview

Introduction

This chapter describes NTP, SNMP RMON and system log, and related configuration on ZXUAS 10800E.

Contents

This chapter includes the following topics.

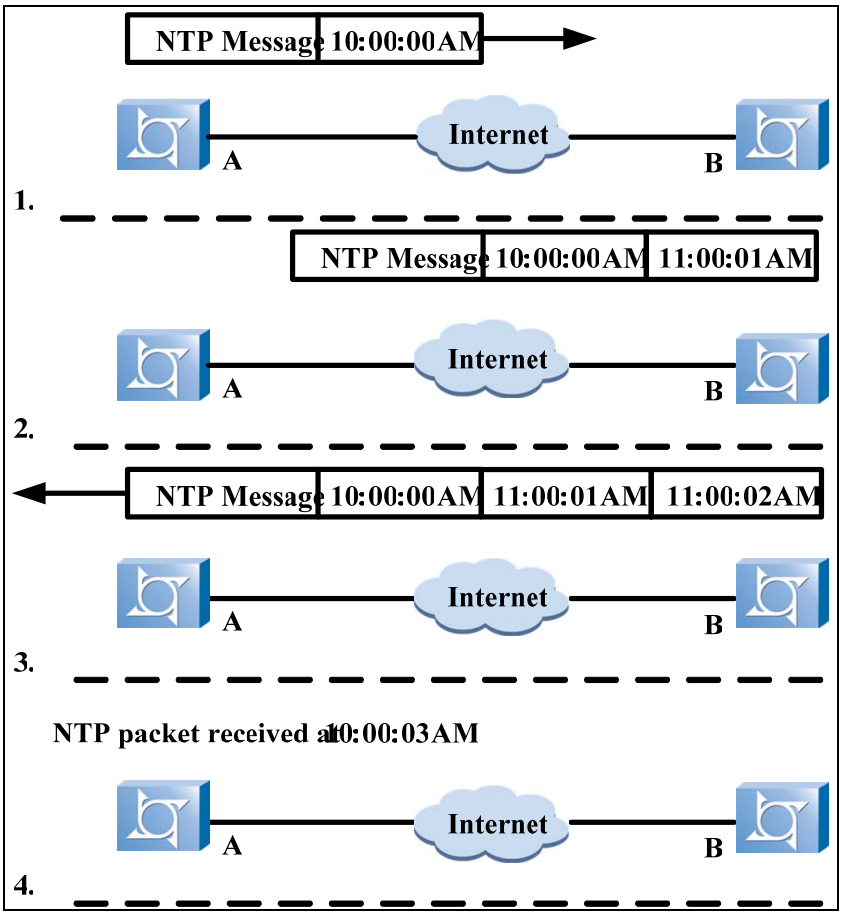
NTP Overview

Network Time Protocol (NTP) is an application layer protocol that releases accurate time in the whole network. Its transmission on network layer is based on UDP.

NTP Working Principle

NTP working principle is shown in Figure 50.

FIGURE 50 NTP WORKING PRINCIPLE



In Figure 50, devices A and B are connected through serial interface. Both devices have their own system clock independently. It is to synchronize the two system clicks now. Suppose:

- Before synchronization, time on system A clock is 10:00:00AM, and on system B clock is 11:00:00AM.
- Device B works as NTP server. That is, it is to synchronize system A clock to system B clock.
- It costs 1 second to transmit packets between device A and device B in unidirectional direction.

Procedure of clock synchronization is as follows:

1. A sends an NTP message to B, containing time stamp when the message leaves. It is 10:00:00AM (T_1).
2. When the message arrives at B, B adds time stamp to the message. It is 11:00:01AM (T_2).
3. When the message leaves B, B adds a new time stamp to the message. It is 11:00:02AM (T_3).
4. When A receives response message, A adds a new time stamp to the message. It is 10:00:03AM (T_4).

Therefore, A gets enough information to calculate two important parameters:

- Delay time of NTP message for a round: Delay=(T_4-T_1)-(T_3-T_2)
- Time offset: Offset=((T_2-T_1)+(T_3-T_4))/2

According to the information, device A synchronizes system clock with device B.

For detailed description of NTP working principle, refer to RFC1305.

Configuring NTP

Purpose This topic describes how to configure NTP.

Steps To configure NTP, perform the following steps.

1. To enable NTP function, use the following command.

Format	Function
ZXUAS(config)#**ntp enable**	This enables NTP function

2. To configure IP address of NTP server, use the following command.

Format	Function
ZXUAS(config)#**ntp server** <*ip-address*> [**version** <*number*>]	This configures IP address of NTP server

3. To configure source address of NTP protocol message, use the following command.

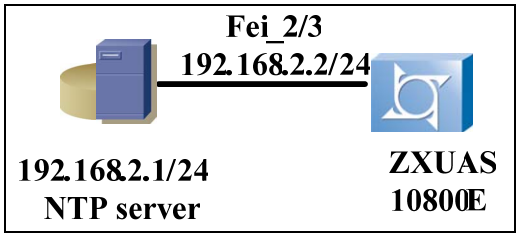
Format	Function
ZXUAS(config)#**ntp source** <*ip-address*>	This configures source address of NTP protocol message

END OF STEPS

Result NTP has been configured.

Example ZXUAS 10800E is an NTP client, as shown in Figure 51. Suppose NTP version is 2.

FIGURE 51 NTP CONFIGURATION



ZXUAS 10800E configuration:

```
ZXUAS(config)#interface fei_2/3
ZXUAS(config-if)#ip address 192.168.2.2 255.255.255.0
ZXUAS(config-if)#exit
ZXUAS(config)#ntp enable
ZXUAS(config)#ntp server 192.168.2.1 version 2
```

SNMP Overview

Simple Network Management Protocol (SNMP) is an application layer protocol, managing information transmission between Network Management System (NMS) and Agent.

SNMP Features

SNMP has the following features:

- Network administrators can view and modify information of any node in the network to find out trouble spot, solve problem and generate report.
- SNMP uses UDP as transmission protocol; therefore, it is supported by many products.
- SNMP uses polling mechanism and provides basic function set.

SNMP Structure

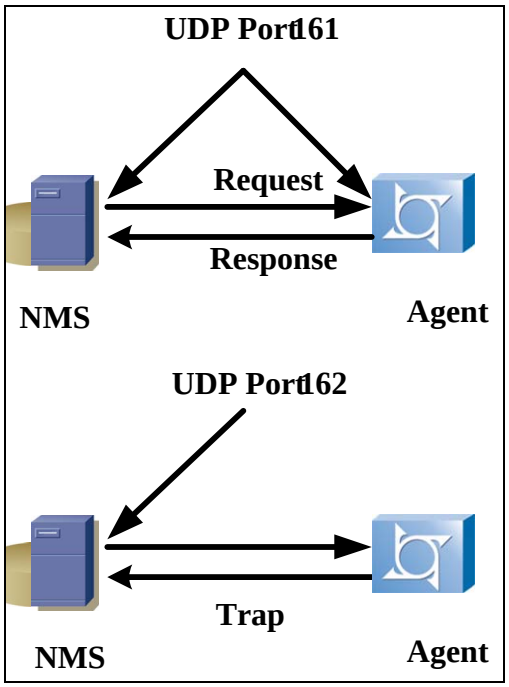
SNMP has two parts: NMS and Agent.

NMS sends different polling messages to devices in the network, receives response messages and Trap messages from managed devices, and display results.

Agent is a process on managed devices. It receives and deals with request messages from NMS, implements read or writing operation on management variables according to message types and then returns them to NMS. In abnormal cases during device startup, Agent sends Trap messages to report to NMS.

SNMP structure is shown in Figure 52.

FIGURE 52 SNMP STRUCTURE



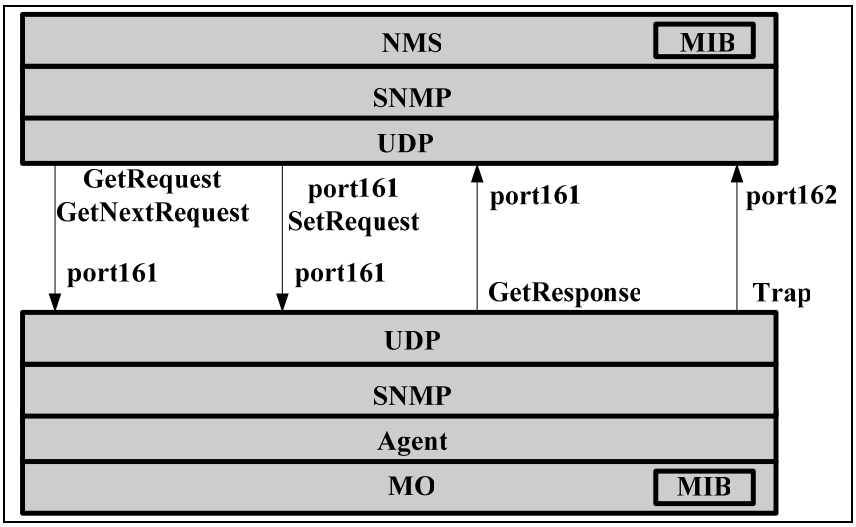
SNMP Working Procedure

Working procedure of SNMP is described as follows:

1. NMS sends request messages to managed devices. Each SNMP message is encapsulated as a UDP message.
2. Agent receives request messages on 161 port of UDP. After decoding and community name authentication, Agent gets the corresponding nodes of management variables in MIB and gets the values of variables. Then Agent generates response messages, codes them and sends them back to NMS.
3. NMS receives response (Trap) messages on 161 (162) port of UDP. After the same processing, NMS displays results.

Working procedure of SNMP is shown in Figure 53.

FIGURE 53 WORKING PROCEDURE OF SNMP



Configuring SNMP

Purpose This topic describes how to configure SNMP.

Steps To configure SNMP, perform the following steps.

1. To define SNMPv2 view, use the following command.

Format	Function
ZXUAS(config)#**snmp-server view** <*view-name*> <*subtree-id*> {**included|excluded**}	This defines SNMPv2 view

2. To configure SNMP message community, use the following command.

Format	Function
ZXUAS(config)#**snmp-server community** <*community-name*> [**view** <*view-name*>] [**ro|rw**]	This configures SNMP message community

3. To configure system contact method of MIB object, use the following command.

Format	Function
ZXUAS(config)#**snmp-server contact** <*mib-syscontact-text*>	This configures system contact method of MIB object

4. To configure system location of MIB object, use the following command.

Format	Function
ZXUAS(config)#**snmp-server location** <*mib-syslocation-text*>	This configures system location of MIB object

5. To enable sending Trap message, use the following command.

Format	Function
ZXUAS(config)#**snmp-server enable trap** [<*notification-type*>]	This enables sending Trap message

6. To enable sending Inform message, use the following command.

Format	Function
ZXUAS(config)#**snmp-server enable inform** [<*notification-type*>]	This enables sending Inform message

7. To configure SNMP server parameters, use the following command.

   ZXUAS(config)#**snmp-server host** [**mng**|**vrf** <*vrf-name*>] <*ip-address*> [**trap**|**inform**] **version** {**1**|**2c**|**3** {**auth**|**noauth**|**priv**}} <*community-name*> [**udp-port** <*udp-port*>] [<*trap-type*>]

END OF STEPS

Result SNMP has been configured.

Example This example shows how to configure SNMP.

```
ZXUAS(config)#snmp-server enable trap      /*enable SNMP*/
ZXUAS(config)#snmp-server community public view AllView rw
/*create a community, with purview of read and writing.
AllView is a community created by system beforehand,
including all internet nodes.*/
ZXUAS(config)#snmp host 10.61.86.123 trap version 1 public
udp-port 162   /*configure IP address of SNMP server and
set UDP port to 162*/
ZXUAS#show snmp config
snmp-server location No.889 bibo Rd. pudong District,
Shanghai, China
snmp-server contact +86-21-68895000-189572
snmp-server packetSize 1400
snmp-server engine-id 8309000203000102 89d64401
snmp-server community public view AllView rw
snmp-server view AllView internet included
snmp-server view DefaultView system included
snmp-server host 10.61.86.123 trap version 1 public udp-
port 162
snmp-server enable inform SNMP
snmp-server enable inform VPN
snmp-server enable inform BGP
snmp-server enable inform OSPF
snmp-server enable inform RMON
snmp-server enable inform STALARM
snmp-server enable trap SNMP
snmp-server enable trap VPN
snmp-server enable trap BGP
snmp-server enable trap OSPF
snmp-server enable trap RMON
snmp-server enable trap STALARM
ZXUAS#
```

RMON Overview

Remote Monitoring (RMON) is implemented based on SNMP system structure. RMON is compatible with current SNMP frame, therefore it needs no modification. RMON helps SNMP to monitor remote devices more effectively.

RMON decreases communication traffic between Network NMS, which is helpful to manage vast network.

RMON Structure

RMON includes two parts: NMS and Agent.

RMON NMS manages Agents in its management range.

RMON Agent works on network monitors or probes, tracing different traffic information.

Data Collecting Methods

RMON supports multiple monitors. It has two methods to collecting data.

One is to use RMON probe to collect data. NMS obtains managements information from RMON probe directly and control network sources. In this way, NMS gets all information about RMON MIB.

The other is to embed RMON Agent into network devices (such as router, switch, hub and so on) directly to make these devices have RMON probe function. RMON NMS uses SNMP basic commands to switch data information with SNMP Agent, and then collects network management information. In this way, RMON NMS can not get all information about RMON MIB due to device source limitation. RMON NMS only gets four groups of information: event information, alarm information, history information and statistical information.

Event Information

Event information defines event index number and processing methods. Events in event group are used in alarm configuration items and extended alarm configuration items. Events are processed in the following ways:

- Recorded in logs
- Contained in Trap messages that are sent to NMS
- Recorded in logs and contained in Trap messages that are sent to NMS

Alarm Information

RMON alarm management monitors designated alarm variables. When monitored variable value overflows threshold value, alarm occurs. Then system deals with alarm according to event definition.

After users define alarm table, system processes alarm table in the following way:

1. System samplings value of defined variable in defined interval.
2. System compares the obtained value with threshold value and triggers corresponding event.

Extended Alarm Information

Extended alarm items calculate values obtained by sampling, and then compare the values with threshold values.

After users define extended alarm table, system processes extended alarm table in the following way:

1. System samplings value of defined variable in defined interval.
2. System calculates a value according to defined formula.
3. System compares the result with threshold value and triggers corresponding event.

History Information

History data management function can be used to set device tasks, including collecting history data, collecting and saving data on specific ports. System samplings bandwidth utilization rate, number of error packets, total number of packets and so on.

The values collected in history group are statistical values in sampling interval.

Statistical Information

RMON statistical function can be used to monitor ports and errors on ports. Statistical information includes network collision number, number of CRC check error packets, extreme small (or large) packet number, broadcast packet number, multi-cast packet number, received byte number and received packet number.

Statistical information is accumulative information when a defined event starts.

Configuring RMON

Purpose

This topic describes how to configure RMON.

Steps

To configure RMON, perform the following steps.

1. To configure alarm and MIB object, use the following command.

   ZXUAS(config)#**rmon alarm** <*index*> <*variable*> <*interval*> {**delta**|**absolute**} **rising-threshold** <*value*> [<*event-index*>] **falling-threshold** <*value*> [<*event-index*>] [**owner** <*string*>]

2. To configure an event, use the following command.

Format	Function
ZXUAS(config)#**rmon event** <*index*> [**log**] [**trap** <*community*>] [**description** <*string*>] [**owner** <*string*>]	This configures an event

3. To enable history information collection function on an interface, use the following command.

   ZXUAS(config-if)#**rmon collection history** <*index*> [**owner** <*string*>] [**bucket** <*bucket-number*>] [**interval** <*seconds*>]

4. To enable statistical information collection function on an interface, use the following command.

Format	Function
ZXUAS(config-if)#**rmon collection statistics** <*index*> [**owner** <*string*>]	This enables statistical information collection function on an interface

END OF STEPS

Result RMON has been configured.

Example This example shows how to configure RMON and view RMON information.

Enable RMON event function and view event information.

```
ZXUAS(config)#rmon event 1 log trap rmontrap description
test owner rmontest
ZXUAS(config)#exit
ZXUAS#show rmon event
Event 1 is active, owned by rmontest
Description is test
Event firing causes log and trap to community rmontrap,
last fired 05:40:20
Current log entries:
        index       time   description
         1        05:40:14   test
ZXUAS#
```

Enable RMON alarm function and view alarm information.

```
ZXUAS(config)#rmon alarm 1 system.3.0 10 absolute rising-
threshold 1000 1 Falling-threshold 10 0 owner rmontest
ZXUAS(config)#exit
ZXUAS#show rmon alarm
Alarm 1 is active, owned by rmontest
Monitors system.3.0 every 10 seconds
Taking absolute samples, last value was 54000
Rising threshold is 1000, assigned to event 1
Falling threshold is 10, assigned to event 0
On startup enable rising or falling alarm
ZXUAS#
```

Enable RMON history function and view history information.

```
ZXUAS(config)#interface fei_1/1
ZXUAS(config-if)#rmon collection history 1 bucket 10
interval 10 owner rmontest
ZXUAS(config-if)#exit
ZXUAS(config)#exit
ZXUAS#show rmon history
Entry 1 is active, and owned by rmontest
Monitors ifEntry.1.1 every 10 seconds
Requested # of time intervals, ie buckets, is 10
Granted # of time intervals, ie buckets, is 10
Sample # 1 began measuring at 00:11:00
Received 38346 octets, 216 packets,
0 broadcast and 80 multicast packets,
0 undersized and 0 oversized packets,
0 fragments and 0 jabbers,
0 CRC alignment errors and 0 collisions.
# of dropped packet events is 0
Network utilization is estimated at 1
```

Enable statistical function and view statistical information.

```
ZXUAS(config)#interface fei_1/1
ZXUAS(config-if)#rmon collection statistics 1 owner
rmontest
ZXUAS(config-if)#exit
ZXUAS(config)#exit
ZXUAS#show rmon statistics
EtherStatsEntry 1 is active, and owned by rmontest
Monitors ifEntry.1.1 which has
Received 60739740 octets, 201157 packets,
1721 broadcast and 9185 multicast packets,
0 undersized and 0 oversized packets,
0 fragments and 0 jabbers,
0 CRC alignment errors and 32 collisions.
# of dropped packet events (due to lack of resources): 511
# of packets received of length (in octets):
64: 92955, 65-127: 14204, 128-255: 1116,
256-511: 4479, 512-1023: 85856, 1024-1518:2547
ZXUAS#
```

System Log Overview

ZXUAS 10800E allows users to set and query log information. Log information makes it easier to implement routine

maintenance. It shows alarms and interface state changes on devices.

Log information can be displayed on configuration terminal in real time, or can be stored as a file on devices or background log server. Syslog protocol can be configured on ZXUAS 10800E, and then the device transmits logs to background log server.

Configuring Syslog

Purpose This topic describes how to configure Syslog.

Steps To configure Syslog, perform the following steps.

1. To enable local log function, use the following command.

Format	Function
ZXUAS(config)#**logging on**	This enables local log function

2. To configure the size of log buffer, use the following command.

Format	Function
ZXUAS(config)#**logging buffer** <*buffer-size*>	This configures the size of log buffer

3. To configure the mode to clear log buffer, use the following command.

Format	Function
ZXUAS(config)#**logging mode** <*mode*> [<*interval*>]	This configures the mode to clear log buffer

4. To configure the lowest level of recorded log, use the following command.

Format	Function
ZXUAS(config)#**logging level** <*level*>	This configures the lowest level of recorded log

5. To configure the log level to be sent to Console, use the following command.

Format	Function
ZXUAS(config)#**logging console** <*level*>	This configures the log level to be sent to Console

6. To configure the log level to be sent as Trap information, use the following command.

Format	Function
ZXUAS(config)#**logging trap-enable** <*level*>	This configures the log level to be sent as Trap information

7. To send log to FTP server in real time, use the following command.

Format	Function
ZXUAS(config)#**logging trap** *<level>* *<community>* [**vrf** *<vrf-name>*|**mng**] *<host-address>*	This sends log to FTP server in real time

8. To configure the interval to send log to FTP server, use the following command.

   ZXUAS(config)#**logging filesavetime** {**interval** *<time>*\|**everyday** *<time>*\|**week** *<weekday>* *<time>*\|**month** *<mothday>* *<time>*} [**vrf** *<vrf-name>*\|**mng**] *<ftp-server>* *<username>* *<password>* [*<filename>*]

9. To record operation commands to FTP server, use the following command.

   ZXUAS(config)#**logging cmd ftp [vrf <vrfname> | mng] <ftp-server>** *<username>* *<password>* *<filename>* *<hh:mm:ss>* *<period>*

10. To configure the interval to record operation commands to FLASH, use the following command.

Format	Function
ZXUAS(config)#**logging cmdlog-interval** *<10-65535>*	This configures the interval to record operation commands to FLASH

11. To record log to Syslog server, use the following command.

    ZXUAS(config)#**syslog-server host** [**vrf** *<vrf-name>*\|**mng**] *<ip-address>* [**fport** *<fport>*] [**lport** *<lport>*] [alarmlog level *<level>*] [cmdlog] [debugmsg] [natlog]

END OF STEPS

Result Syslog has been configured.

Example This example shows how to configure Syslog.

```
ZXUAS#configure terminal
ZXUAS(config)#logging on
ZXUAS(config)#logging buffer 500
ZXUAS(config)#logging mode FULLEND
ZXUAS(config)#show logging alarm
 An alarm 19712 level 6 occurred at 06:57:15 10/19/2005
UTC sent by NPC 1 %ARP%The hardware address of IP
address 10.32.23.254 is changed from 000a.8a8b.5600 to
00d0.d0e0.92c0
 An alarm 19712 level 6 occurred at 06:57:15 10/19/2005
UTC sent by NPC 1 %ARP%The hardware address of IP
address 10.32.23.254 is changed from 00d0.d0e0.92c0 to
000a.8a8b.5600
An alarm 16643 level 5 occurred at 06:57:16 10/19/2005
UTC sent by UPC(MPU) 2 %DATABASE% the alarm buffer is
full,and will be cleared now!
 An alarm 19712 level 6 occurred at 06:57:45 10/19/2005
UTC sent by NPC 1 %ARP%The hardware address of IP
address 10.32.145.254 is changed from 000a.8a8b.5600 to
00d0.d0e0.92c0
 An alarm 19712 level 6 occurred at 06:57:45 10/19/2005
UTC sent by NPC 1 %ARP%The hardware address of IP
address 10.32.145.254 is changed from 00d0.d0e0.92c0 to
000a.8a8b.5600
 An alarm 19712 level 6 occurred at 06:57:51 10/19/2005
UTC sent by NPC 1 %ARP%The hardware address of IP
address 10.32.19.251 is changed from 000a.8a8b.5600 to
00d0.d0e0.92c0
 An alarm 19712 level 6 occurred at 06:57:52 10/19/2005
UTC sent by NPC 1 %ARP%The hardware address of IP
address 10.32.19.251 is changed from 00d0.d0e0.92c0 to
000a.8a8b.5600
 An alarm 19712 level 6 occurred at 06:58:04 10/19/2005
UTC sent by NPC 1 %ARP%The hardware address of IP
address 172.168.255.255 is changed from 00d0.d0e0.92c0
to 00d0.d0e2.31c0
 An alarm 19712 level 6 occurred at 06:58:04 10/19/2005
UTC sent by NPC 1 %ARP%The hardware address of IP
address 172.168.255.255 is changed from 00d0.d0e2.31c0
to 00d0.d0e1.5200
 An alarm 19712 level 6 occurred at 06:58:03 10/19/2005
UTC sent by NPC 1 %ARP%The hardware address of IP
address 172.168.255.255 is changed from 00d0.d0e1.5200
to 00d0.d0e0.92c0
```

```
An alarm 19712 level 6 occurred at 06:58:24 10/19/2005
UTC sent by NPC 1 %ARP%The hardware address of IP
address 10.67.1.1 is changed from 000a.8a8b.5600 to
00d0.d0e0.92c0
 An alarm 19712 level 6 occurred at 06:58:24 10/19/2005
UTC sent by NPC 1 %ARP%The hardware address of IP
address 10.67.1.1 is changed from 00d0.d0e0.92c0 to
000a.8a8b.5600
 An alarm 19712 level 6 occurred at 06:58:28 10/19/2005
UTC sent by NPC 1 %ARP%The hardware address of IP
address 10.32.66.252 is changed from 000a.8a8b.5600 to
00d0.d0e0.92c0
 An alarm 19712 level 6 occurred at 06:58:28 10/19/2005
UTC sent by NPC 1 %ARP%The hardware address of IP
address 10.32.66.252 is changed from 00d0.d0e0.92c0 to
000a.8a8b.5600
 An alarm 19712 level 6 occurred at 06:58:45 10/19/2005
UTC sent by NPC 1 %ARP%The hardware address of IP
address 192.168.1.255 is changed from 000a.8a8b.5600to
00d0.d0e0.92c0
 An alarm 19712 level 6 occurred at 06:58:45 10/19/2005
UTC sent by NPC 1 %ARP%The hardware address of IP
address 192.168.1.255 is changed from 00d0.d0e0.92c0 to
000a.8a8b.5600
 An alarm 19712 level 6 occurred at 06:58:48 10/19/2005
UTC sent by NPC 1 %ARP%The hardware address of IP
address 10.32.132.251 is changed from 000a.8a8b.5600 to
00d0.d0e0.92c0
ZXUAS(config)#logging level ERRORS
ZXUAS(config)#logging console ERRORS
ZXUAS(config)#logging trap-enable ERRORS
ZXUAS(config)#logging  ftp NOTIFICATIONS 200.1.1.2 uas
uas a.log
ZXUAS(config)#logging filesavetime interval 1:00:00
200.1.1.2 uas uas log
ZXUAS(config)#logging cmd ftp 200.1.1.2 uas uas cmd
16:00:00 1
ZXUAS(config)#logging cmdlog-interval 10
ZXUAS(config)# syslog-server host 200.1.1.2 alarmlog
level NOTIFICATIONS
ZXUAS(config)#show logging configure
logging on
logging buffer 200
logging mode fullcycle
logging console notifications
logging level notifications
```

```
logging ftp notifications 200.1.1.2 uas uas l.log
logging trap-enable notifications
logging filesavetime interval 01:00:00 200.1.1.2 uas uas
ZXUASAlarmLog
alarm cpuload-on
alarm cpuload-interval  30
alarm cpuload-threshold high-grade 95 middle-grade 85 low-
grade 75
logging cmd ftp 200.1.1.2 uas uas cmd 14:50:00 1
logging cmdlog-interval 10
syslog-server host 200.1.1.2 fport 514 lport 514 alarmlog
level notifications cmdlog natlog debugmsg
ZXUAS(config)#
```

This page is intentionally blank.

Glossary

Acronyms and Abbreviations

Abbreviation	Full Name
AAA	Authentication, Authorization and Accounting
ABR	Area Border Router
ACL	Access Control List
AD	Administrative Distance
ADSL	Asymmetrical Digital Subscriber Line
ARP	Address Resolution Protocol
AS	Autonomous System
ASBR	Autonomous System Border Router
ATM	Asynchronous Transfer Mode
BAS	Broadband Access Server
BGP	Border Gateway Protocol
BOOTP	BOOTstrap Protocol
BDR	Backup Designate Router
CHAP	Challenge Handshake Authentication Protocol
CIDR	Classless Inter-Domain Routing
CLNP	ConnectionLess Network Protocol
CLNS	ConnectionLess Network Sevice
CoS	Class of Service
CRC	Cyclic Redundancy Check
CRLDP	Constraint based Routing Label Distribution Protocol
CSN	Cryptographic Sequence Number
DHCP	Dynamic Host Configuration Protocol
DIS	Designate IS
DNS	Domain Name System
DR	Designate Router
EBGP	External Border Gateway Protocol
EGP	External Gateway Protocol

Abbreviation	Full Name
ES	End System
FEC	Forwarding Equivalence Class
FIFO	First In and First Out
FPGA	Field Programmable Gate Array
FSM	Finite State Machine
FTP	File Transfer Protocol
GBIC	Gigabit Interface Converter
GRE	General Routing Encapsulation
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol
IP	Internet Protocol
ISO	International Organization for Standardization
ISP	Internet Service Provider
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
LAPB	Link Access Procedure Balanced
LCP	Link Control Protocol
LDP	Label Distribution Protocol
LSA	Link State Advertisement
LSP	Link State PDU
LSR	Label Switch Router
MAC	Media Access Control
MD5	Message Digest 5
MED	MULTI_EXIT_DISC
MIB	Management Information Base
MPLS	Multi-Protocol Label Switching
MSTP	Multiple Spanning Tree Protocol
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NBMA	Non-Broadcast Multiple Access
NCP	Network Control Protocol
NIC	Network Information Center
NLRI	Network Layer Reachable Information
NMS	Network Management System

Abbreviation	Full Name
NSAP	Network Service Access Point
NSP	Network Service Provider
NTP	Network Time Protocol
NVT	Network Virtual Terminal
OAM	Operation And Management
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PAP	Password Authentication Protocol
PAT	Port Address Translation
PCM	Pulse Code Modulation
PDU	Protocol Data Unit
POS	Packet over SDH
PPP	Point-to-Point Protocol
PSNP	Partial Sequence Num PDU
QoS	Quality of Service
RARP	Reverse Address Resolution Protocol
RADIUS	Remote Authentication Dial In User Service
RFC	Request For Comments
RIP	Routing Information Protocol
RLE	Route lookup engine
RMON	Remote Monitoring
ROS	Router Operation System
RSTP	Rapid Spanning Tree Protocol
RSVP	Resource Reservation Protocol
SDH	Synchronous Digital Hierarchy
SDLC	Synchronous Data Link Control
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SNP	Sequence Num PDU
SPF	Shortest Path First
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
ToS	Type Of Service
TELNET	Telecommunication Network Protocol
TTL	Time To Live

Abbreviation	Full Name
UDP	User Datagram Protocol
VLSM	Variable Length Subnet Mask
VPN	Virtual Private Network
VRF	Virtual Routing Forwarding
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
WWW	World Wide Web

Figures

Tables

This page is intentionally blank.