ZXR10 2920/2928/2952 Access Switch

User Manual(Volume I)

Version 1.0

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

LEGAL INFORMATION

Copyright © 2006 ZTE CORPORATION.

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

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

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

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

ZTE CORPORATION reserves the right to upgrade or make technical change to this product without further notice.

Users may visit ZTE technical support website http://ensupport. zte. com. cn to inquire related information.

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

Revision History

Date	Revision No.	Serial No.	Reason for Issue
7/11/2007	R1.0	sjzl20071746	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">ZXR10 2920/2928/2952(V1.00) Access Switch User Manual （Volume I）</td></tr>
<tr><td>Product Version</td><td>V1.0</td><td>Document Revision Number</td><td>R1.0</td></tr>
<tr><td>Serial No.</td><td>sjzl20071746</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

About This Manual

Purpose

This manual provides procedures and guidelines that support the ZXR10 2920/2928/2952.

Intended Audience

This manual is intended for engineers and technicians who perform operation on Layer 2 switches.

Prerequisite Skill and Knowledge

To use this document effectively, users should have a general understanding of Layer 2 Switches and protocols. This is Volume 1 and the Volume 2 is based on Commands. Familiarity with the following is helpful:

- Virtual Local Area Network
- Link Aggregation Control Protocol
- Spanning Tree Protocol
- Access Control List

What Is in This Manual

This manual contains the following chapters:

TABLE 1 CHAPTER SUMMARY

Chapter	Summary
Chapter 1, Safety Instruction	This chapter introduces the safety instructions and sign descriptions.
Chapter 2, System Overview	This chapter introduces the produce overview, functions and technical features.
Chapter 3, Structure	This chapter introduces the working

Chapter	Summary
and Principle	principle, technical and hardware structural information on each of the ZXR10 2920/2928/2952
Chapter 4, Installation and Debugging	This chapter provides an overview of installation and debugging processes of ZXR10 2920/2928/2952.
Chapter 5, Usage and Operation	This chapter provides an overview of configuration mode, command mode and command line use.
Chapter 6, System Management	This chapter introduces file system management FTP/TFTP configuration, file backup and restoration, software version upgrade.
Chapter 7, Service Configuration	This chapter provides and overview of configuration methods for various services of ZXR10 2920/2928/2952.
Chapter 8, Network Management	This chapter provides and overview of network management functions of the ZXR10 2920/2928/2952, such as Remote-Access, SSH, SNMP, RMON and cluster management.
Chapter 9, Maintenance	This chapter provides routine maintenance, common test methods and troubleshooting of ZXR10 2920/2928/2952.

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.

Mouse Operation Conventions

TABLE 3 MOUSE OPERATION CONVENTIONS

Typeface	Meaning
Click	Refers to clicking the primary mouse button (usually the left mouse button) once.
Double-click	Refers to quickly clicking the primary mouse button (usually the left mouse button) twice.
Right-click	Refers to clicking the secondary mouse button (usually the right mouse button) once.
Drag	Refers to pressing and holding a mouse button and moving the mouse.

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 Instruction

Overview

Introduction This chapter introduces the safety instructions and sign descriptions.

Contents This chapter includes the following topics.

TABLE 4 TOPICS IF CHAPTER 1

Safety Instructions

Equipment Installation This equipment can only be installed, operated and maintained by professional user.

Local Safety Please observe local safety specifications and relevant operating procedures in equipment installation, operation and maintenance. Otherwise, personal injury or equipment damage may occur. Safety precautions introduced in this manual are only supplementary to local safety codes.

ZTE shall not bear any liabilities incurred by violation of the universal safety operation requirements or violation of the safety standards for designing, manufacturing and using the equipment.

This page is intentionally blank.

Chapter 2

System Overview

Overview

Introduction This chapter introduces the product overview, functions and technical features.

Contents This chapter includes the following topics.

TABLE 5 TOPICS IN CHAPTER 2

Product Overview

background ZXR10 2920/2928/2952 series products are megabit L2+ Ethernet switch, providing gigabit upward Ethernet ports. They can provide different quantity of & interface-types of Ethernet port, mainly located at megabit access & converge to provide fast, efficient, and cost-effective access and convergence solutions.

Port & insert-card expanding instance that ZXR10 2920/2928/2952 switch series support are as follows:

- ZXR10 2920:support sixteen 100M & four 1000M ports
- ZXR10 2928: support twenty-four 100M & four 1000M ports
- ZXR10 2952: support forty-four 100M & four 1000M ports

Note:2920 & 2928 support insert-card expand.ZXR10 2920/2928/2952 switch series have the following characters.

Switching Capability

All the ports of ZXR10 2920/2928/2952 megabit switch series support the layer-2 switching at wire-speed. The filtration and stream sort transact based on port do not weaken the switching capability. Ports provide high throughput, packet discarding rate, time delay and dithering can satisfy the demand of the key application.

Reliability and characteristics

Features

ZXR10 2920/2928/2952 megabit switch series ensures the link redundancy backup through STP/RSTP/MSTP. RSTP switching that is based on IEEE-802.1w ensures the usability of the network. These switches support the LACP function of 802. 3ad function, and it supplies the load equalization backup and the link. Switches support Ethernet ring network mode through ZESR. High switching capability ensures that the operation do not be interrupted.

Particular function

The following are the kinds of operation characteristics and control:

- Use of different modes of VLAN sort. It can be classified by types of port, protocol, and strategy.
- Provide VPN on layer-2 through QinQ, in addition to SelectiveQinQ, and supply flexible control ability for optional outer layer label, which makes it convenient to operate and scheme.
- Supports the client-end VBAS function, and supplies efficient orientation technology support for client end.
- Milticast support technology, includes igmp-snooping and proxy function, fast-leaving characteristic and Multicast-Vlan Switching (MVS) function & IPTV support.

Security Controls

User Security Control

The following are user level security control:

- IEEE 802.1x implements dynamic and port-based security provides the user ID authentication function and MAC/IP/VLAN/PORT combines at random, and prevent illegal user to accessing the network.
- Segregating the ports is helpful to make sure that users can not monitor or access to other users on the same switch.
- DHCP monitoring prevents spiteful users deceiving the server and sending spurious address, so it can start protecting IP source and create a binding table for the IP address of the user, MAC address, ports and VLAN to prevent user deceiving or use IP address of other users.

Equipment Level Security

The following are the equipment level security control:

- CPU security control technology can resist DoS attack from CPU.
- SSH/SNMPv3 protocol supplies network management security.
- Multilevel security of console can prevent unauthenticated users changing the switch configuration.
- RADIUS authentication may carry on the common control to the switchboard.

Network Security

The following are the network security control:

- ACL based on port or Trunk makes it possible for users to apply security strategy to the ports of switches or Trunk.
- Binding MAC address and the filtration based on source or destination supply effective control over the flux based on address.
- Port MIRROR function is an effective tool for network management analyses.

QoS Guarantee

Applications of QoS are shown below:

- Standard 802.1p QoS and DSCP field sort label and sort again based on single group with source and destination IP address, source and destination MAC address, and TCP/UDP port number.
- Queue schedule arithmetic, Strict Priority(SP) & combination schedule.
- Support CAR（Committed Access Rate）function. Manage the asynchronous upward and downward data stream from end

stage or up link. Input strategy control supplies the bandwidth control with minimal increment by 64kbps. It can satisfy the demand of discarding packets, time delay and time dithering when network congestion occurs, and supply the congestion avoiding function for the alignment.

Management

Switch management is described with the following statement:

- Supports SNMPv1/v2c/v3 and RMON.
- Supports ZXNM01 uniform network management platform.
- Supports CLI command lines, including Console, Telnet and SSH to access the switch.
- GUI method supports Web network management.
- Manage through ZGMP group.

Functions

Store and Forward Mode

ZXR10 2920/2928/2952 adopts Store and Forward mode and supports layer-2 switching at wire-speed. Full wire-speed switching is implemented at all ports.

ZXR10 2920/2928/2952 has the following functions:

- Megabit ports support port 10/100/1000M self-adapting and MDI/MDIX self-adapting.
- Kilomega ports support port 10/100/1000M self-adapting and MDI/MDIX self-adapting.
- Support 802.3x-compliant flow control (full duplex) and back-pressure flow control (half duplex).
- (VCT) function and faulty circuit test.
- Support 802.1q-compliant VLAN and private border VLAN. Maximum number of VLANs can be up to 4094.
- Support VLAN stacks function, and outer label is optional.
- Support GVRP dynamic VLAN.
- MAC addresses self-learning capability. The size of the MAC address table is 8K.
- Port MAC address bundling and address filtering.
- Support port security and segregating.
- Support the STP defined in the 802.1d, RSTP defined in the 802.1w, and MSTP defined in the 802.1s. The maximum number of the example can be up to 16.
- Support ZESR technology.

- Support LACP port bundling defined in 802.3ad and port static bundling. At most 15 port groups can be bundled and each group contains at most eight ports.
- Support multi-VLAN IGMP snooping & MVS controllable group broadcast technology.
- Support single port loop test.
- Support 802.1x transparent transmission and authentication.
- Port orientation support VBAS and DHCP-OPTION82.
- Support DHCP-snooping.
- Support Broadcast storm suppression.
- Port ingress and egress mirror, and flow-based mirror and statistics.
- Support ACL function of port and Trunk, and can be set according to time segment.
- Support IETF-DiffServ and IEEE-802.1p standard, the ports support 4 PRI queue. Ingress supports CAR. The queue attempering supports SP&combination(SP+WRR)attempering method. Egress is based on the queue, and discarding the toned tail.
- Port-based speed control includes input speed limit and output speed limit. Input speed limit strategy includes unicast, unknown unicast, broadcast and groupcast. Input speed limit is based on stream, and output speed limit is based on queue. The minimal is 64Kbps.
- Provide detailed port flow statistics.
- Support syslog.
- Support NTP client end.
- Configuration of NM static route.
- Support ZGMP group manage.
- SNMPv1/v2c/v3 and RMON.
- Support Console configuration, Telnet remote login.
- Support SSHv2. 0.
- Support WEB function.
- Support unified network management of ZXNM01.
- Uploading and downloading of TFTP version.

Technical Features and Parameters

ZXR10 2920/2928/2952 technical features and parameters are given in Table 6.

TABLE 6 TECHNICAL FEATURES AND PARAMETERS

model item	ZXR10 2920	ZXR10 2928	ZXR10 2952
Dimensions (HxWxD, mm)	43. 6×436× 200	43. 6×436× 200	43. 6×442× 280
Weigh (Fully equipped, kg)	≈2	≈2	≈2. 5
Maximum power consumption (W)	16	20	27
Power supply	AC power supply: 100V~240V, 48Hz~62Hz. Wave shape distortion <5% DC power supply: –57V to –40V		

Chapter 3

Structure and Principle

Overview

Introduction This chapter introduces the working principle, technical and hardware structural information on each of the ZXR10 2920/2928/2952.

Contents This chapter includes the following topics.

TABLE 7 TOPICS IN CHAPTER 3

Working Principle

ZXR10 2920/2928/2952 series are important parts of ZXR10 Ethernet switches that are launched by ZTE. They define a pure megabit L2+ user Ethernet switch. They are intended for gigabit upward access and used widely in large-scale enterprise network and top grade industry. This series of products features powerful functions and outstanding performance. Switch consists of:

- Control module
- Switching module
- Interface module

- Power supply module

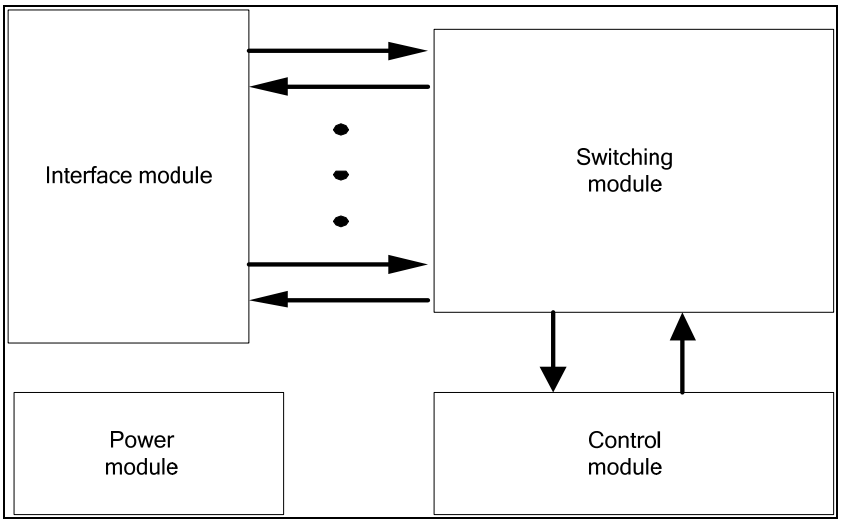
Control Module Control module consists of main processor and external functional chips to implement applications such as switching module control & manage for the system. It provides operational interfaces, such as serial ports and Ethernet interfaces for data operation and maintenance.

Switch module Switching module has Ethernet switching processing chips. Its primary function is simply switching traffic from multiple devices. This chip is interlinked with data packet transceiver and can directly provide hundred megabit or gigabit service interface to the users.

Interface module Interface module is composed of interface boards to accomplish the external user connection and transceivers packets. The interface module & switching module are interlinked by standard interface.

Power Module Power module adopts the 220 VAC or -48 VDC for power supply to offer required power supply for other parts of the system.

FIGURE 1 ZXR10 2920/2928/2952FI WORKING PRINCIPLE



ZXR10 2920/2928/2952 uses the "19(inch)" su-brack that is in compliance with the international standard. Sub-rack can be used as standalone equipment or installed in a standard cabinet.

Hardware Structure

ZXR10 2920/2928/2952 adopts the box structure, which is 1U high. It employs independent power supply and natural dissipation method. It has vents on the left and right sides of the box. The box is composed of a bottom case and a shell. It features light weight and simple structure. It allows an easy installation and un-installation.

On the front panel of ZXR10 2920/2928/2952, there are power indicators, RUN indicators, fixed Ethernet electrical interfaces, Ethernet optical interfaces, and one serial configuration port. The AC or DC power socket and power switch are located on the rear panel.

Major hardware of the ZXR10 2920/2928/2952 is the Ethernet switching main board, which is indispensable in any type of configuration.

ZXR10 2920

Front Panel

Front panel of the ZXR10 2920 is shown in Figure 2.

FIGURE 2 FRONT PANEL OF ZXR10 2920

Ethernet switching main board of ZXR10 2920 is KEBT.

Interfaces

ZXR10 2920 provides the following types of access ports:

- Sixteen fixed 10/100BASE-T Ethernet ports, support fullduplex or semiduplex, 10/100M & MDI/MDIX self-adaption function, VCT auto test.
- Two fixed 10/100/1000BASE-T interface.
- One expand slot, expansile dual-channel 1000M optical interface, double 1000M electrical interface, 1000M one optical & one electrical upward subboard.
- One Console port is to realize the management and configuration of various services.

Indicators

There are 32 indicators on the front panel of the ZXR10 2920, indicating the status of the 16 10/100Base-T ports. Every interface has two indicators, indicating semiduplex/fullduplex & LNK/ACT;four indicators show two 10/100/1000 BASE-T port & two indicators for each port showing LNK & LNK/ACT status;two system indicators show the system running work status.

- System indicators include power indicator (PWR) and running indicator (RUN).
  - After the system is powered up, the PWR indicator is on and the RUN indicator is off.
  - BootROM starts to load the version. If the version is unavailable, the states of indicators do not change. If the version is loaded normally, the RUN indicator flashes at 1Hz.

- If the power indicator (PWR) is flashing , it indicates that the switch is the main or standby role of the stack system. Flashing in the same frequency with RUN shows it is the main equipment. Flashing in the half frequency with RUN shows it is the standby equipment.

- 32 indicators corresponds to 10/100 Base-T port , each port with two:one is semiduplex/fullduplex, & the other is link activation indicator.
  - Semiduplex/fullduplex indicator is on in the condition of fullduplex, is off in the condition of semiduplex. , & is flashing in the condition of collision.
  - Link activation indicator is flashing when the link is activated.
- 4 interface indicators correspond to the 2 10/100/1000 Base-T interfaces. Every interface has two indicators. When one of the indicators is on, it indicates that the LINK is normal. When the other indicator is on, it indicates that the LINK is normal. If the indicator is flashing, it indicates that data sending or receiving is under way.

ZXR10 2928

Front Panel

Front panel of the ZXR10 2928 is shown in Figure 3.

FIGURE 3 FRONT PANEL OF ZXR10 2928

Ethernet switching main board of ZXR10 2928 is KEBT.

Interface

ZXR10 2928 provides the following types of access ports:

- Twenty-four 10/100BASE-T Ethernet ports. These ports support duplex/semiduplex, 10/100M & MDI/MDIX self adapter & VCT automatically check.
- Two fixed 10/100/1000BASE-T ports.
- One expand slot. It can expand double 1000M optical interface, double 1000M electrical interfaces, one optical & one electrical interfaces.
- One console port is to realize the management and configuration of various services.

Indicators

There are 48 indicators on the front panel of the ZXR10 2928, indicating the status of the 24 10/100 Base-T ports. Every interface has two indicators, indicating half-duplex/full-duplex and LNK/ACT;Four indicators indicate two 10/100/1000 Base-T port. Two system indicators indicate PWR & RUN.

- System indicators include power indicator (PWR) and running indicator (RUN).
  - After the system is powered on, PWR indicator is on and the RUN indicator is off.
  - BootROM starts to load the version. If the version is unavailable, the states of indicators do not change. If the version is loaded normally, the RUN indicator flashes at 1Hz.
  - If the power indicator (PWR) is flashing , it indicates that the switch is the main or standby role of the stack system. Flashing in the same frequency with RUN shows it is the main equipment. Flashing in the half frequency with RUN shows it is the standby equipment.
- 48 interface indicators correspond to the 24 10/100 Base-T interfaces. Every interface has two indicators:one is semiduplex/fullduplex indicator, the other is link activation indicator
  - Semiduplex/fullduplex indicator is on in the condition of fullduplex, is off in the condition of semiduplex & is flashing in the condition of collision.
  - Link activation indicator is flashing when the link is activated.
- 4 interface indicators correspond to the 2 10/100/1000 Base-T interfaces. Every interface has two indicators. When one of the indicators is on, it indicates that the LINK is normal. When the other indicator is on, it indicates that the LINK is normal. If the indicator is flashing, it indicates that data sending or receiving is underway

ZXR10 2952

Front panel Front panel of the ZXR10 2952 is shown in Figure 4.

FIGURE 4 FRONT PANEL OF ZXR102952

Ethernet switching main board of ZXR10 2952 is KEBF.

Interfaces ZXR10 2952 provides the following types of access ports:

- Forty-eight fixed 10/100BASE-T Ethernet ports. These ports support full-duplex/half-duplex, 10/100M & MDI/MDIX self-adaption & VCT self-check.
- Two fixed 10/100/1000BASE-T interface.

- Two fixed 1000BASE-X interface.
- One console port is to realize the management and configuration of various services.

Indicators

There are 48 indicators on the front panel of the ZXR10 2952, indicating the status of the 48 10/100 Base-T ports. Every interface has one indicators, indicating LNK and ACT. Four indicators show two 10/100/1000 BASE-T port & two indicators for each port showing LNK & LNK/ACT status;two indicators indicate 2 1000Base-X port, each port with one indicator, showing LNK/ACT status of the port;two system indicators show power indicator(PWR) & running indicator(RUN) .

- System indicators include power indicator (PWR) and running indicator (RUN).
  - After the system is powered on, PWR indicator is on and the RUN indicator is off.
  - BootROM starts to load the version. If the version is unavailable, the states of indicators do not change. If the version is loaded normally, the RUN indicator flashes at 1Hz.
  - If the power indicator (PWR) is flashing , it indicates that the switch is the main or standby role of the stack system. Flashing in the same frequency with RUN shows it is the main equipment. Flashing in the half frequency with RUN shows it is the standby equipment.
- 48 indicators respond to 48 10/100 Base-T port. Every port has 1 indicator indicating LNK/ACT. If the link indicator is on, it indicates that the LINK is normal. If the indicator is flashing, it indicates that data sending or receiving is underway.
- There are 2 indicators, indicating the status of the two 1000 Base-X ports. Every port has 1 indicator: If the link indicator is on, it indicates that the LINK is normal. If the indicator is flashing, it indicates that data sending or receiving is underway.
- 4 interface indicators correspond to the two 10/100/1000Base-T interfaces. Every interface has two indicators. When one of the indicators is on, it indicates that the LINK is normal. When the other indicator is on, it indicates that the LINK is normal. If the indicator is flashing, it indicates that data sending or receiving is underway.

ZXR10 2928-FI

Sub-board

FGEI、FGFI、FGFE can be chosen for ZXR10 2920/2928 according to the practical networking. Corresponding types & functions are shown in table5 ZXR10 .

TABLE5 ZXR10 2920/2928 SUBBOARD LIST

Subboard	Type	Function
FGEI	SF-2GE-2RJ45	2 gigabit Ethernet electrical port
FGFI	SF-2GE-2SFP	2 gigabit Ethernet light port
FGFE	SF-2GE-SFPRJ45	1 gigabit Ethernet light port+1 gigabit Ethernet electrical port

FGEI offer 2 gigabit ethernet upward electrical port, the type is SF-2GE-2RJ45，as shown in Figure 5.

FIGURE 5 FGEI SUBBOARD

Indicators

There are 4 indicators on the FGEI panel. Each gigabit ethernet electrical port has 2 indicators, & one is link activation indicator, & the other one is link status indicator.

- If the link activation indicator is flashing, it indicates that data sending or receiving is underway.
- When link status indicator is on, it indicates that the LINK is normal.

FGFI

FGFI subboard offer two gigabit Ethernet up-go light port, & the type is SF-2GE-2SFP，as shown in Figure 6.

Figure 6 SF-2GE-2SFP subboard（FGFI）

Indicators There are 2 indicators on the FGFIpanel: ACT1&ACT2 , corresponding to the two gigabit light port. When the indicator is on, it indicates that LINKis normal;if the indicator is flashing, it indicates that data sending or receiving is underway.

FGFE FGFI subboard offers 1 gigabit Ethernet up-go light port + 1 gigabit Ethernet up-go electrical port，& the type is SF-2GE-SFPRJ45, as shown in. figure 7

FIGURE 7 SF-2GE-SFPRJ45SUBBOARD（FGFE）

Indicators There are 3 indicators on the FGFIpanel. The gigabit Ethernet up-go light port has an indicator ACT. When the indicator is on, it indicates that LINKis normal;if the indicator is flashing, it indicates that data sending or receiving is underway. The gigabit Ethernet up-go electrical port has two indicators:one is link activation indicator, & the other one is link status indicator.

- If the link activation indicator is flashing, it indicates that data sending or receiving is underway.
- When link status indicator is on, it indicates that the LINK is normal.

Power Supply Module

Mode ZXR10 2920/2928/2952 supports two power supply modes:

- -48V DC power supply
- 110V/220V AC power supply

When the -48V DC power supply is adopted, use 48V DC power cables. When the AC power supply is adopted, use AC power cables. Both of the two modes support a backup power supply of 12v DC power supply. **FIGURE 8** and **FIGURE 9** respectively show rear panel of the switch when the -48V DC power supply and 110V/220V AC power supply are adopted.

FIGURE 8 **ZXR10 2920/2928/2952 BACK PANEL（DC POWER）**

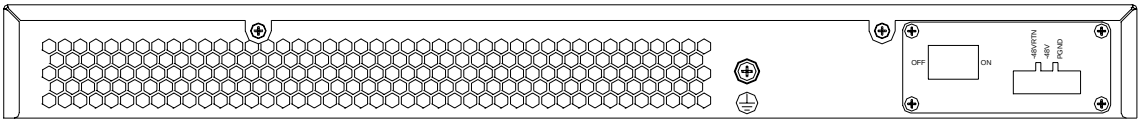
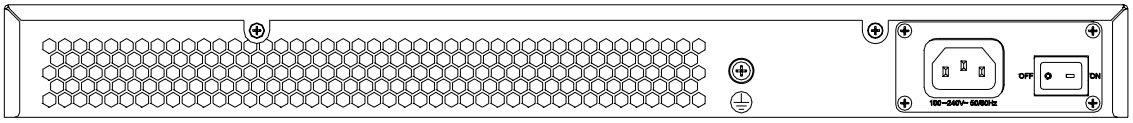


FIGURE 9 **ZXR10 2920/2928/2952 BACK PANEL（AC POWER）**



This page is intentionally blank.

Chapter 4

Installation and Debugging

Overview

Introduction This chapter provides an overview of installation and debugging processes of ZXR10 2920/2928/2952.

Contents This chapter includes the following topics.

TABLE 8 TOPICS IN CHAPTER 4

Equipment Installation

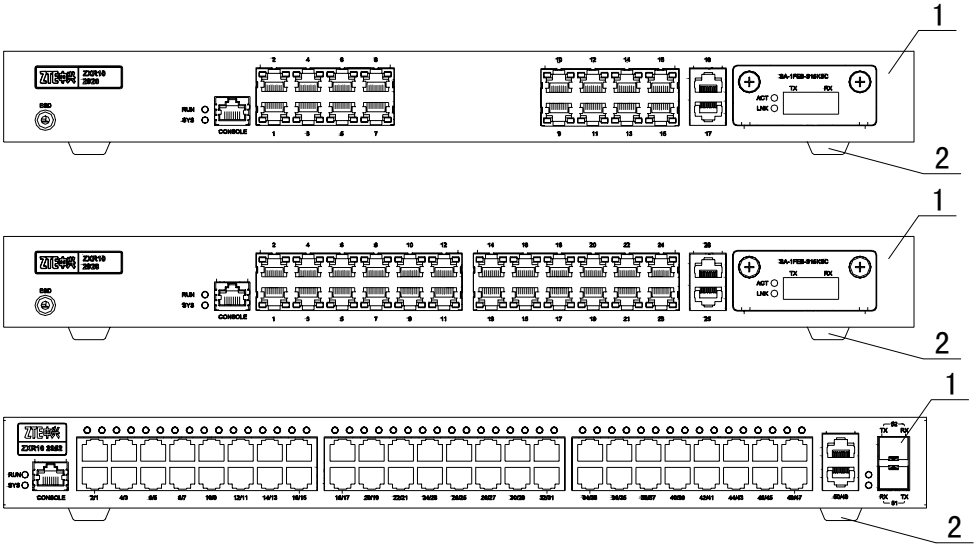
ZXR10 2920/2928/2952 can be placed on desktop and can be installed on a 19-inch standard cabinet.

19-inch standard cabinet can be provided by customer. If ZTE provides the cabinet, install cabinet as per 19-inch Standard Cabinet.

Switch Installation on Desktop

When switch is placed on desktop, install four plastic pads (the plastic pads and screws are part of the accessories) on bottom plate of switch. Four pads support switch and form a lower ventilation channel for power to cool down. It is shown in Figure 8.

FIGURE 8 INSTALLING PLASTIC PADS



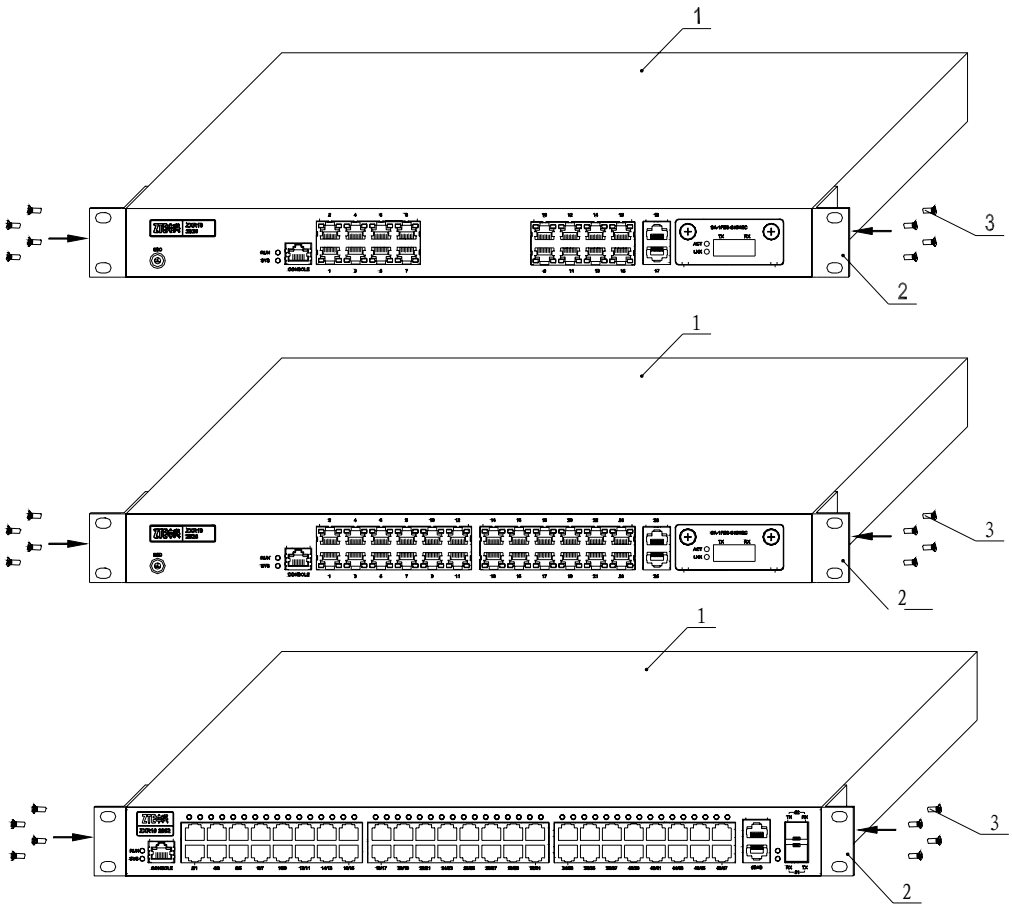
- 1 Case 2 Pad

Switch Installation onto a Cabinet

Installation Procedures

To install the switch into the 19-inch cabinet, install a flange to each of the two sides of the switch shell (the flange and screws are part of the accessories), as shown in Figure 9.

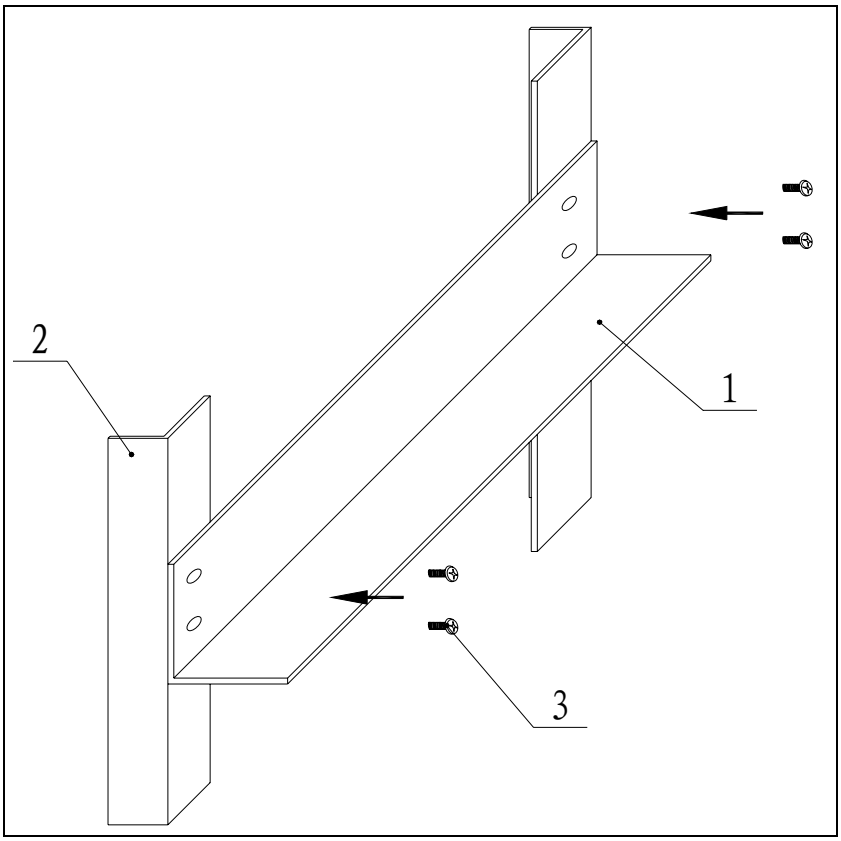
FIGURE 9 INSTALLING FLANGES



- 1 Case 2 Flange 3 Screw

Install two symmetrical brackets at both sides of the 19-inch cabinet to support the switch, as shown in Figure 10.

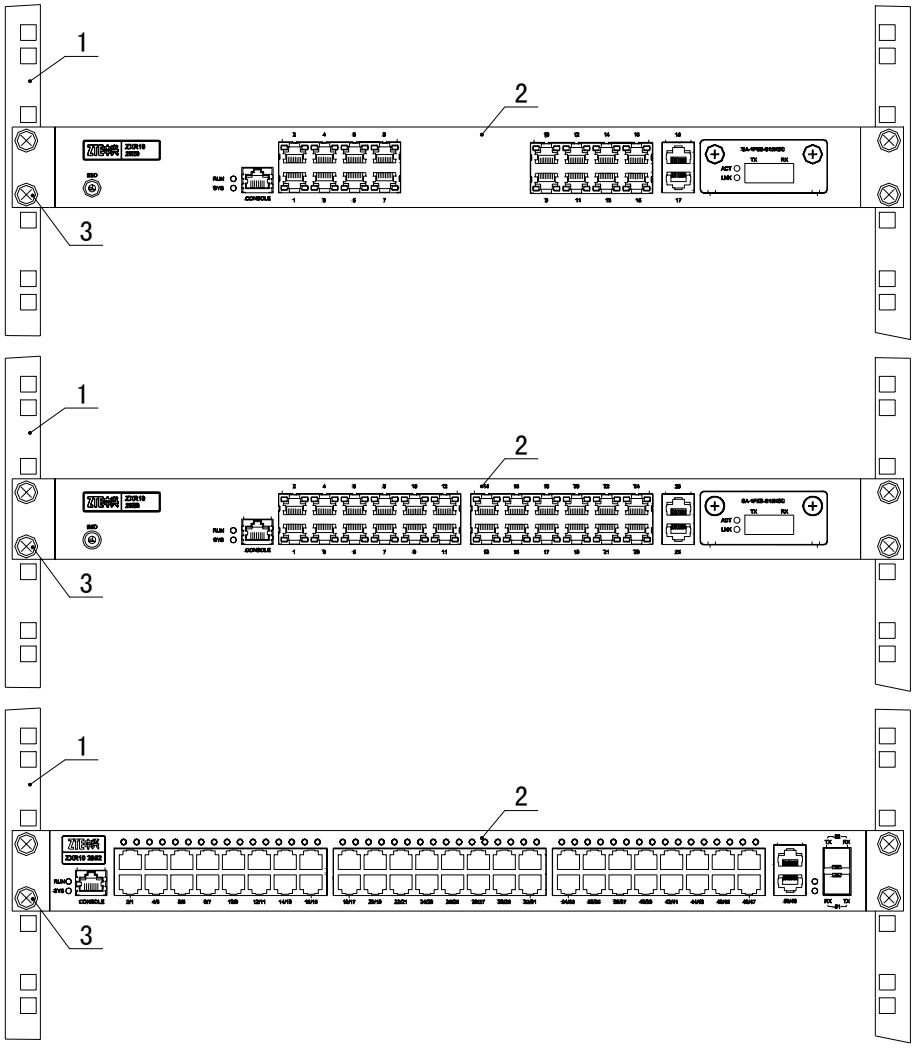
FIGURE 10 INSTALLING BRACKETS



- 1 Holder 2 Cabinet 3 Screw

After installation, push switch along with bracket, and fix flanges with screws onto cabinet, as shown in Figure 11.

FIGURE 11 FIXING THE SWITCH



- 1 Cabinet 2 Box 3 Screw

Cable Types

ZXR10 2920/2928/2952 consists of:

- Power cables
- Console cables
- Network cables
- Fiber optics.

Power Cables Installation

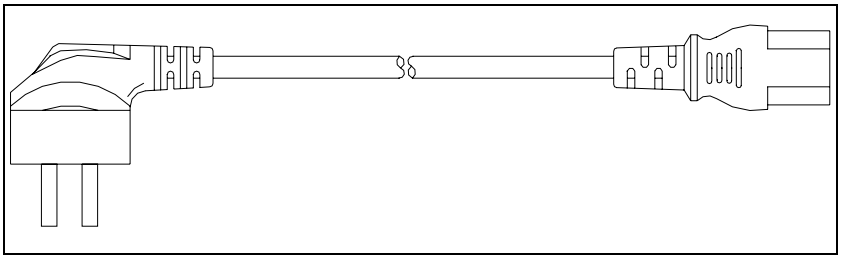
Power cables are classified as per power supply module:

- AC power cables
- DC power cables

AC power cable

An AC power cable looks the same as standard printer power cable, as shown in Figure 12.

FIGURE 12 AC POWER CABLE

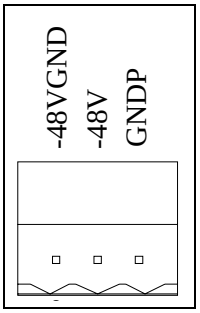


One end of the AC power cable connects the AC power socket of the ZXR10 2920/2928/2952 power module and the other end connects the 220 VAC power socket.

DC power socket

Appearance and description of -48V power socket on DC power supply module of ZXR10 2920/2928/2952 is shown in Figure 13.

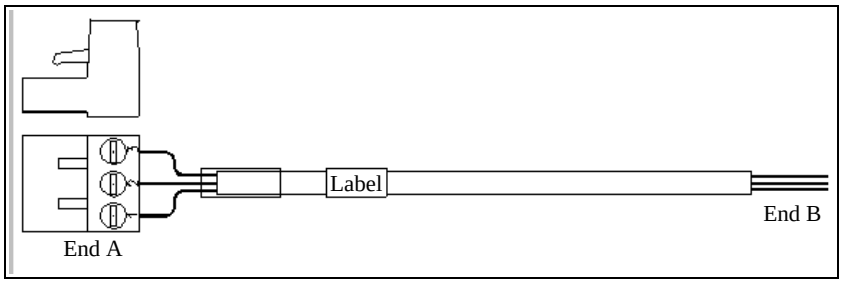
FIGURE 13 -48 POWER SOCKET



DC power Cable

DC power cable is a 3-core power cable, as shown in Figure 14.

FIGURE 14 DC POWER CABLE



Detail description of two ends of power cable is given in Table 9.

TABLE 9 DESCRIPTIONS OF POWER CABLES

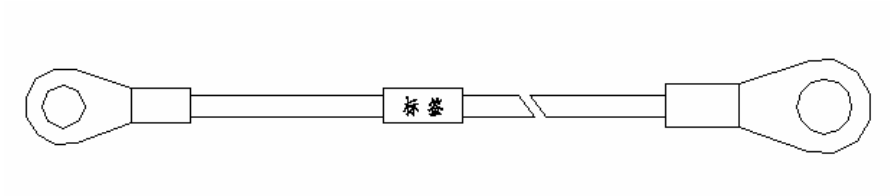
End A	End B	Power Signal
1	Brown	-48VGND
2	Blue	-48V
3	Yellow	GNDP

One end of the DC power cable is connected to the power socket on the DC power supply module of the ZXR10 2920/2928/2952, and the other end to the corresponding terminal of –48V DC power supply.

Grounding Power Cable

There is a grounding screw on the back of ZXR10 2920/2928/2952, figuring by ⏚. When connecting with kelly protect cable, one end of the cable is connected to the grouding screw, and the other end to the grouding protect of the cabinet of the ZXR10 2920/2928/2952. Grounding protect cable shape is shown in Figure 17 .

FIGURE 17 GROUNDING PROTECT CABLE



Console Cable Installation

Serial port cable connections

Serial port configuration cable is for configuration and routine maintenance of ZXR10 2920/2928/2952 switches.

ZXR10 2920/2928/2952 is delivered with serial port configuration cable. One end of the cable is a DB9 serial port,

which connects to serial port on computer. Other end is an RJ45 port, which connects to Console port of ZXR10 2920/2928/2952.

- Console cable is shown in FIGURE 18 .
- Linear ordering of serial port console cable is shown in TABLE 10 .

FIGURE 18 CONSOLE CABLE INSTALLATION

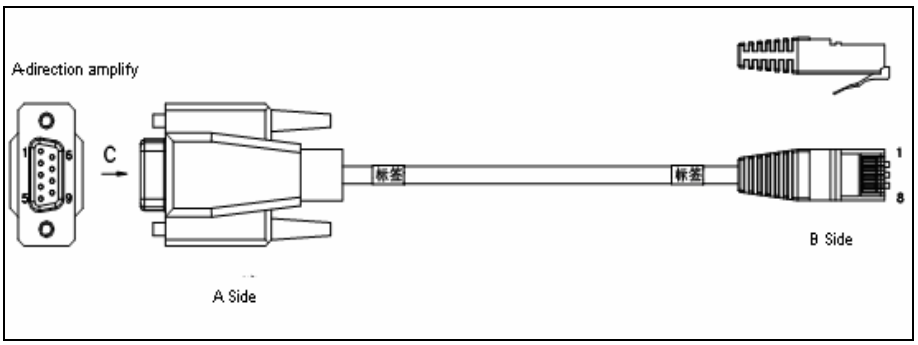


TABLE 10 LINEAR ORDERING OF SERIAL PORT CONSOLE CABLE

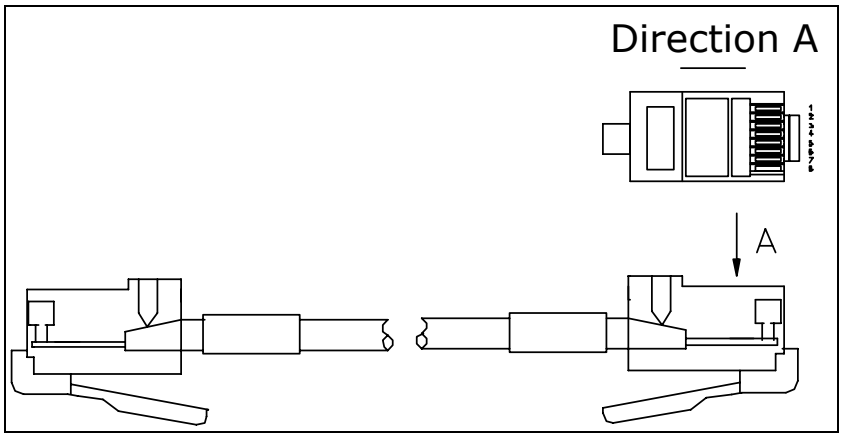
Side A	Color	Side B
2	White	3
3	Blue	6
5	White	4
	Orange	5
4	White	7
6	Green	2
7	White	8
8	Brown	1

Network Cable Installation

Both ends of network cable are crimped with RJ45 connectors, as shown in FIGURE 19 .

- Name of the cable connector: 8P8C straight crimping cable connector
- Specification: E5088-001023
- Technical parameters
  - Rated current 1.5A
  - Rated voltage 125V
  - Crimped with AWG24-28# round wire

FIGURE 19 NETWORK CABLE



Connectors, cables can be classified into two categories:

Straight-through RJ45

Straight-through RJ45 network cable, with pins at both ends in one-to-one correspondence. Specific pin outs are shown in Table 10.

TABLE 10 STRAIGHT-THROUGH NETWORK CABLE RJ45 LINEAR ORDERING

End A	Cable Color	End B
1	White-orange	1
2	Orange	2
3	White-green	3
6	Green	6
4	Blue	4
5	White-blue	5
7	White-brown	7
8	Brown	8

Crossover RJ45J cable

Crossover RJ45J cable, with two twisted pairs at both ends corresponding to each other in crossover mode. The specific connection relationship is shown in Table 11.

TABLE 11 CROSSOVER CABLE RJ45J'S LINEAR ORDERING

End A	Cable Color	End B
1	White-orange	3
2	Orange	6
3	White-green	1
6	Green	2
4	Blue	4
5	White-blue	5
7	White-brown	7
8	Brown	8

Optical Fiber

Each optical interface of ZXR10 2920/2928/2952 has two fibers to send and receive data respectively.

Note: Ensure proper connection to TX and RX marks on panel.

Classification

There are two kinds of optical fibers, single-mode and multi-mode optical fibers. Six types of optical fibers are available for configuration, as shown in Table 12.

TABLE 12 FIBER TYPES

Mode	Type of Connector to Switch	Type of Connector on the Peer End
Single-mode fiber	SC-PC connector (square flat connector)	FC/PC connector
		SC/PC connector
		ST/PC connector
		LC/PC connector
Multi-mode fiber	SC-PC connector (square flat connector)	FC/PC connector
		SC/PC connector
		ST/PC connector
		LC/PC connector

Fiber protection

For fiber cabinet layout of cabinet, make sure to protect fibers against any damages with plastic corrugated protection tubes.

- Fibers inside protection tube should not entangle with one another. They should be bent into a round shape at the bending position, if any.
- Labels at two ends of fiber should be clear and legible. Meanings of labels should clearly reflect corresponding

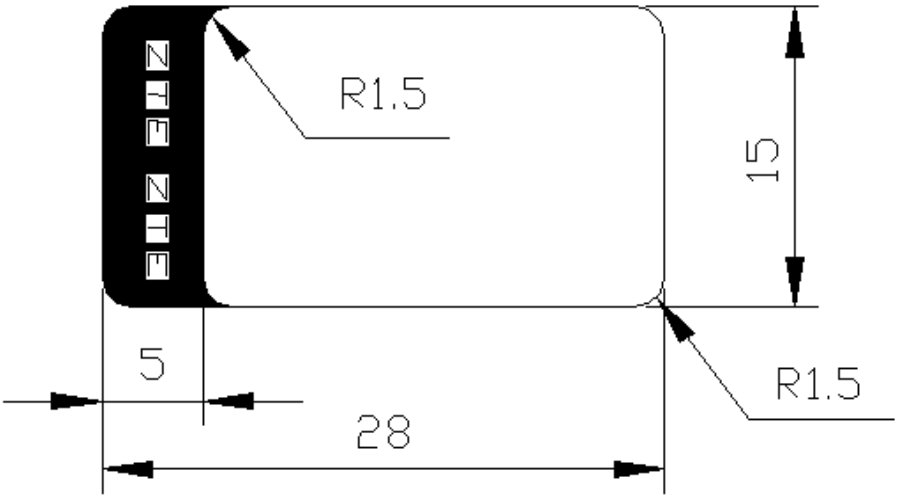
numbers and relationship between cabinets and between rows.

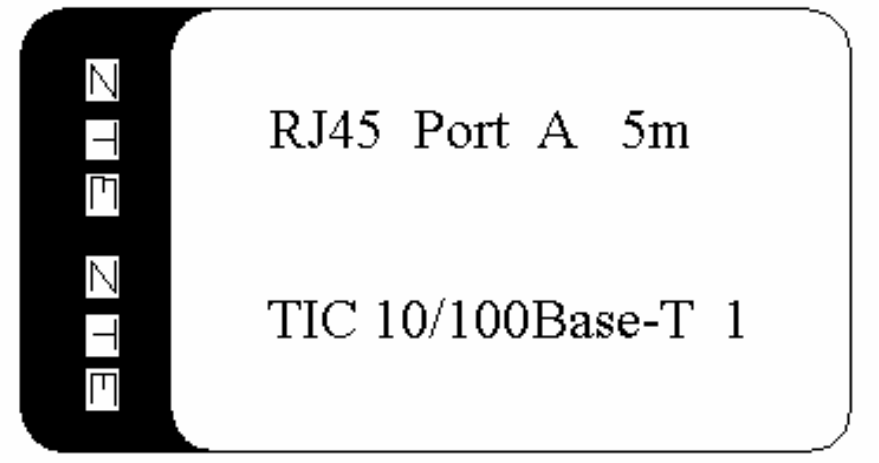
Labels

Pattern and meanings of the labels attached to the connector:

- Label attached to the connector is called transverse English label on panels and connectors. Structure and dimensions of the label is shown in FIGURE 20 .

FIGURE 20 TRANSVERSE ENGLISH LABEL ON PANELS AND CONNECTORS





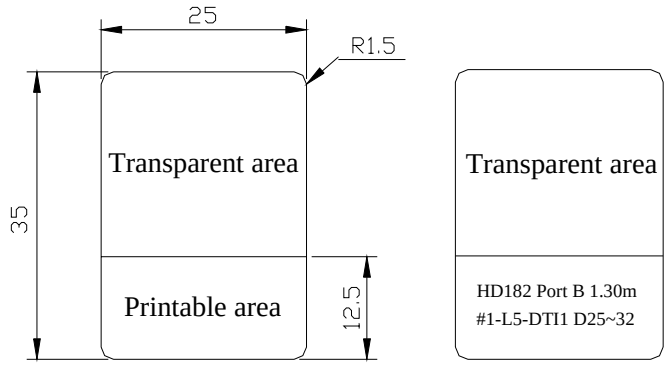
These contents are described in the following section:

- RJ45——Cable code
- Port A——End A of the cable connector, corresponding to End B or another end.
- 5m——Length of the finished cable. It refers to the straight line length of the cable from the connector at one end to the connector at the other end.
- TIC 10/100Base-T 1——Connection position, the first 10/100Base-T network port of the TIC board.

Pattern and meanings of the label attached to the cable:

- Label attached to the cable is called roll-type self-cover laser print label model II. Structure and dimensions of the label is shown in FIGURE 21 .

FIGURE 21 ROLL-TYPE SELF-COVER LASER PRINT LABEL MODEL II



Label Features

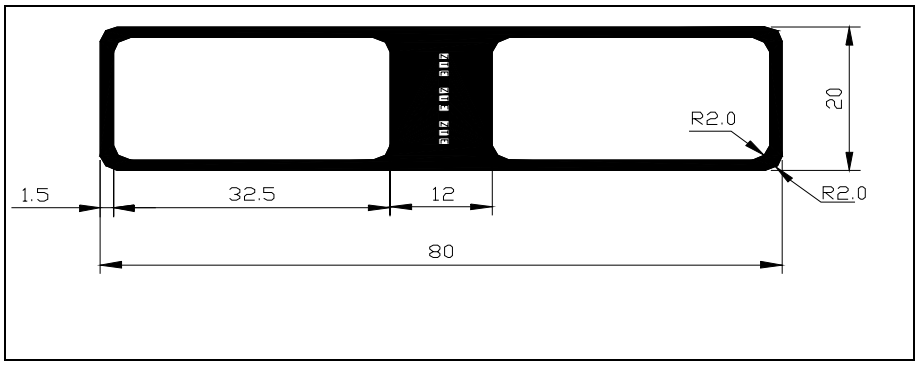
Contents of the label in the above figure have same meanings as those in FIGURE 20 . These two types of labels are used in different places.

- Transverse English label on panels and connectors is only applicable to the connectors where the attachment area is larger than the label area or to panels.
- Roll-up self-mulching laser printing label is rolled around the cable with its own scotch adhesive tapes. It is used when horizontal English label cannot be used because cable connector is small.

Before the cabinet equipment is delivered, all the internal interconnected cables shall be attached with flag-type direction labels.

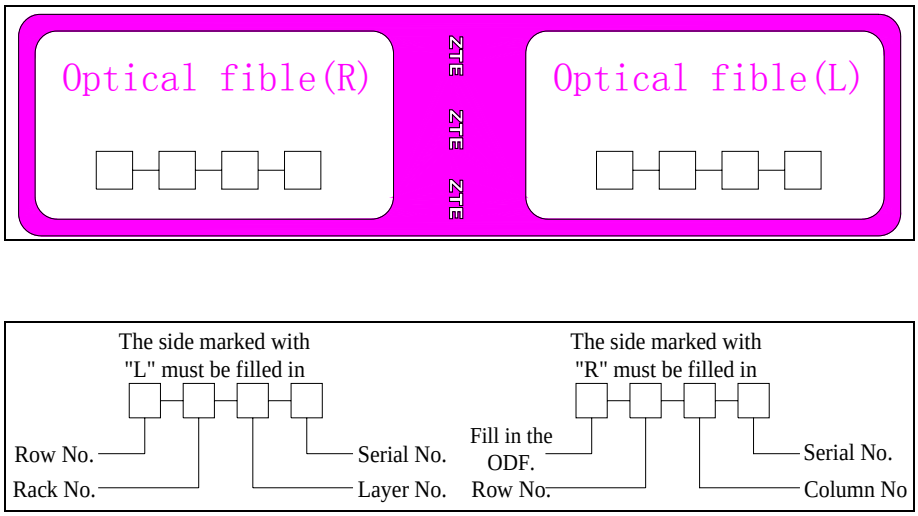
This label attached to the cable is called Transverse English Type I Label. Structure and dimensions of label is shown in Figure 15.

FIGURE 15 TRANSVERSE ENGLISH TYPE I LABEL



Meaning of the content and the structure of a fiber engineering label is shown in Figure 16.

FIGURE 16 PATTERN AND MEANINGS OF ENGINEERING LABEL ON OPTICAL FIBER



Engineering Labels

Two sides of the engineering label on the optical fiber are marked "L" and "R" with the specific meanings given as follows:

- When label is pasted on fiber at ZXR10 2920/2928/2952 side, row and column number of cabinet at side of connected remote optical interface device as well as the layer No. of the fiber in the cabinet and the fiber No. must be filled in the R area of the label.
- In this case, row and column Nos.of ZXR10 2920/2928/2952 where the fiber is located as well as the layer No. of the fiber and fiber number shall be filled in the L area of the label.

- If the label is attached on the optical interface equipment of the customer, contents filled on the label are just contrary to those at the ZXR10 2920/2928/2952 side.

Cable Lightning Protection Requirements

Lightning Protection

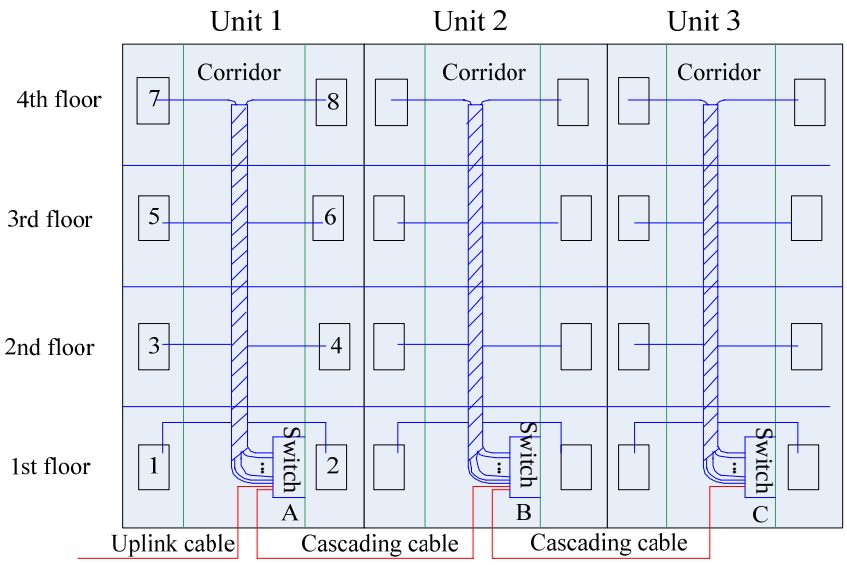
Lightning can be direct lightning strike and induction. Damage of direct lightning strike is hard to avoid. Following lightning protection requirements are proposed to reduce equipment failure rate in the areas where lightning is frequent.

Place the ethernet switch in the corridor, preferably on the first floor to avoid the direct sunshine, rains, and lightning. Ensure that all subscriber lines are distributed inside building to avoid lightning induction. Uplink, downlink, and cascading lines are distributed outside.

Switch cabling

Cabling of Ethernet switch in a four-floor building with three units is shown in Figure 17.

FIGURE 17 CABLING OF THE ETHERNET SWITCH IN A BUILDING



Explanation

Switch placement in fourth floor is explained below.

- Switch A is in Unit 1 and is convergence switch of the whole building. Switches B and C are access switches.
- Switches A, B, and C are cascaded. Cascading cables refers to connecting two switches. Cascading cable of switch A is the uplink cable of switch B, and cascading cable of switch B is uplink cable of switch C. Rest of subscriber lines are

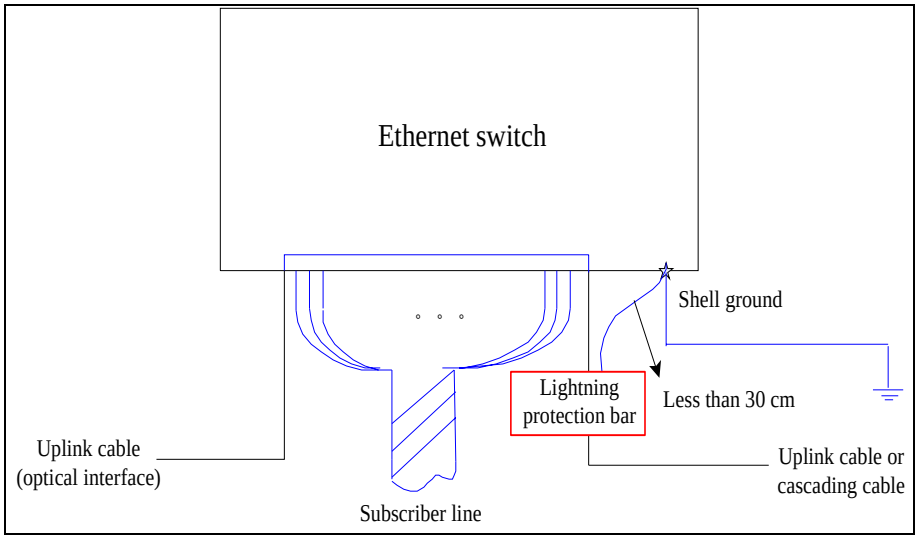
distributed inside the building and connected to subscriber terminals from bottom to top in the corridor.

- Lightning protection bars must be added for the uplink, downlink, and cascading Ethernet ports that are outdoors. Lightning protection bar must reach 6 KV or above and the current discharge capability must reach 5 KA. Grounding cable of lightning protection bar must have a diameter of 16 mm2 and a length less than 30 cm. It is recommended to use the optical port as uplink port for convergence switch in the building. If the electrical port is used, lightning protection bars must be added.

Convergence switch cabling

Cabling of a convergence switch is shown in Figure 18. Uplink port is optical port and lightning protection bars are added for downlink or cascaded cables. Lightning bars are connected to ground through shell. Rest of subscriber lines are distributed inside building.

FIGURE 18 CABLING OF A CONVERGENCE SWITCH



Explanation

Explanations are as follows:

- Grounding system with good ground grid is preferred for switch. Many residential buildings with proper grounding have a grounding resistance of 1 ohm. If the test shows that grounding system is not up to standard. It is recommended to equip an independent grounding post and the grounding cable must be of 16 mm2 in diameter and as short as possible. What ever grounding method is used, the grounding resistance must be less than 5 ohm and cannot exceed 10 ohm.
- It is prohibited that switch directly gets power from outdoor overhead power cable. If switch gets direct power from outdoor overhead power cables, special lightning protection measures must be taken into account. Lightning protection

socket and lightning protection bar, must be added to power supply. Lightning protection bar for power supply must have better lightning protection index than that for port cable.

Note: Ethernet switch suffers lightning strike due to grounding, power supply, and wiring. Lightning strike lead-in mechanism also varies a lot. Taking one measure does not prevent lightning strike. Therefore, several measures must be implemented at same time. Proper grounding, appropriate power supply, reasonable wiring, and suitable lightning protection measures will definitely reduce chances of switch damage resulted from lighting strike.

Chapter 5

Usage and Operation

Overview

Introduction This chapter provides an overview of configuration mode, command mode and command line use.

Contents This chapter includes the following topics.

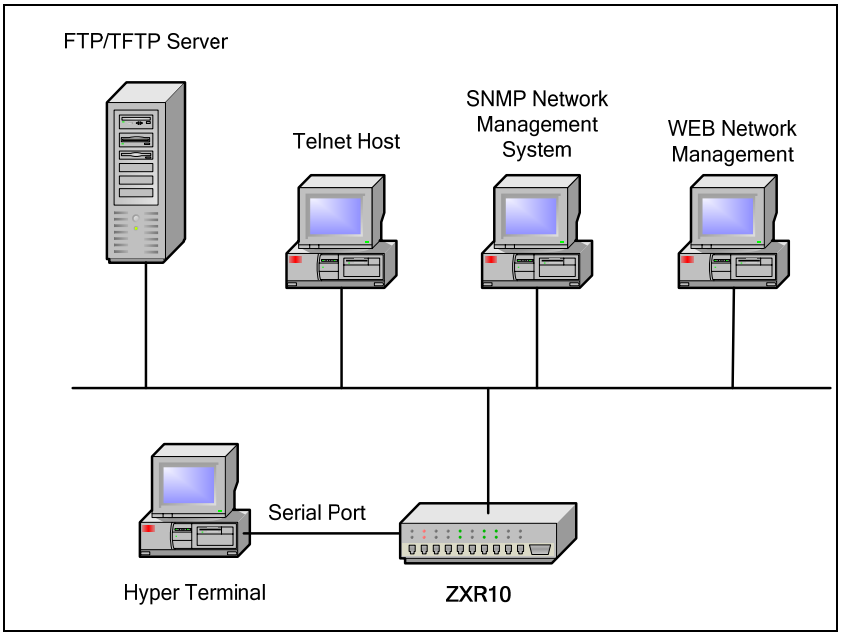
TABLE 13 TOPICS IN CHAPTER 5

Configuration Modes

ZXR10 2920/2928/2952 offers multiple configuration modes. A user can select configuration mode based on the connected network, as shown in Figure 19.

- Configuration through serial port connection
- Configuration through TELNET session
- Configuration through SNMP connection
- Configuration through WEB connection

FIGURE 19 ZXR10 2920/2928/2952 CONFIGURATION MODES



Configuration through Console Port Connection

Console Port Connection

Configuration through console port connection is the main configuration mode of the ZXR10 2920/2928/2952. The connection can be configured when the equipment is running.

Configuring through Telnet

Purpose This topic describes the configuration of ZXR10 2920/2928/2952 through Telnet.

Prerequisite Telnet mode is usually used when configuring the switch by telnet. Configure the switch through the host connecting to the local Ethernet interface logs in the telnet switch. Set username & password on the switch & make sure that local computer can ping the IP address of the layer-3 port in the switch. (Layer-3 port address configuration refers to section 7. 13)

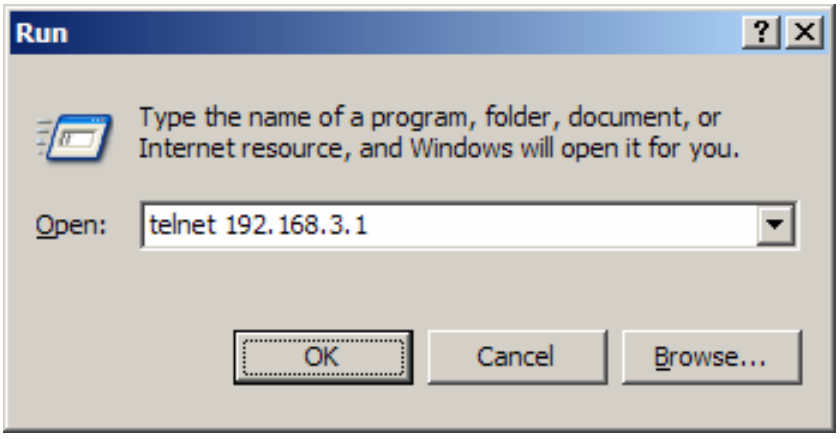
Create a new user using command **create user** <*name*> **admin|guest.** Set login password using command **set user local** <*name*> **login-password** [<*string*>].

Note: by default, the username & password is admin/zhongxing.

Steps To configure through telnet, perform the following steps.

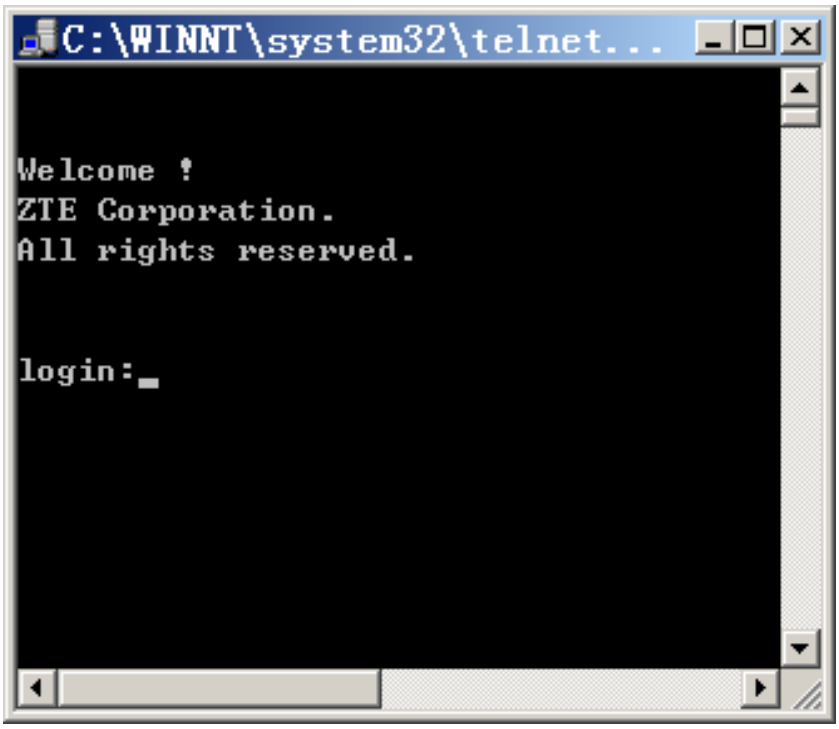
1. Run the telnet command on the host and input the IP address of the switch management Ethernet port, as shown in Figure 20.

FIGURE 20 RUN TELNET



2. Click **OK** to enter the interface as shown in Figure 21.

FIGURE 21 TELNET LOGIN



3. Type the correct user name and password at the prompt to enter into switch user mode.

END OF STEPS

Result Configuring of ZXR10 2920/2928/2952 through Telnet is completed successfully.

Simple Network Management Protocol (SNMP)

Overview Network Management Protocol (SNMP) is one of the most popular network protocols. An NM server can manage all devices on the network through this protocol.

Features of SNMP SNMP adopts the management based on the server and client. Background NM server serves as SNMP server and the foreground network device ZXR10 2920/2928/2952 serves as the SNMP client. Foreground and background share one MIB management database and the SNMP is used for communications.

NMS software supporting the SNMP shall be installed in the background NM server to manage and configure the ZXR10 2920/2928/2952.

Configuring through WEB Connection

Introduction Web is a long-distance management switchboard and is similar to Telnet. Users can access some Web services through a peer-to-peer arrangement rather than by going to a central server. The user should have the access along with password and management password for the switch, enable Web function.

Purpose This topic describes the configuration of Web connection.

Steps For the configuration of Web connection, perform the following steps.

1. To create user, use command **create user** <name> **admin|guest** in global configuration mode. This is shown in Table 14.

TABLE 14 CREATE USER COMMAND

Format	Mode	Function
create user <name> **admin|guest**	config	This creates user

Result: This creates user.

2. To configure user password, use command **set user local** <name> **login-password** <string> in global configuration mode. This is shown in Table 15.

TABLE 15 USER PASSWORD COMMAND

Format	Mode	Function
set user local <name> **login-password** <string>	config	This configures user password

Result: This configures user password.

3. To configure admin password, use command **set user local|radius** <name> **admin-password** <string> in global configuration mode. This is shown in Table 16.

TABLE 16 ADMIN PASSWORD

Format	Mode	Function
set user local|radius <name> **admin-password** <string>	config	This configures admin password

Result: This configures admin password.

4. To enable web function and to establish the monitor port, use command **set web enable** and **set web listen-port**

<80, 025-49151> in global configuration mode. This is shown in Table 17.

TABLE 17 WEB COMMANDS

Format	Mode	Function
set web enable	config	This enables web function
set web listen-port <80, 025-49151>		This establishes the monitor port

Result: This enables web function and establishes the monitor port.

Note: By default username is **admin**, password is **zhongxing** and http monitor port is 80.

END OF STEPS

Result Configuration of Web management is completed successfully.

Command Modes

Overview ZXR10 2920/2928/2952 allocates the commands to various modes based on the function. In order to authorize the facilitation to user's configuration and management for the switch only one command can be executed in the special mode only.

ZXR10 2920/2928/2952 command modes include:

- User mode
- Global configuration mode
- SNMP configuration mode
- Layer 3 configuration mode
- File system configuration mode
- NAS configuration mode
- Cluster management configuration mode
- Basic ACL configuration mode
- Global ACL configuration mode
- Extended ACL configuration mode
- L2 ACL configuration mode
- Hybrid ACL configuration mode

Configuring User Mode

Purpose This topic describes the configuration of user mode.

Steps For the configuration of user mode, perform the following steps.

1. When using HyperTerminal mode to log on to system, system enters into user mode automatically.

   Result: The prompt character in the user mode is the host name followed by ">", as shown below:

   ```
   zte>
   ```

   Note: By default host name is zte. Modify the host name by using the command **hostname**.

2. In the user mode, execute the command **exit** to exit the switch configuration.
3. In the user mode, execute the command **show** to display the system configuration and operation information.

   Note: The command show can be executed in any mode.

END OF STEPS

Result User mode has been configured.

Configuring Global Mode

Purpose This topic describes the global configuration mode.

Steps For the configuration of global mode, perform the following steps.

1. In user mode, enter the **enable** command and the corresponding password to enter the global configuration mode, as follows:

   ```
   zte>enable
   Password:***
   zte(cfg)#
   ```

2. In the global configuration mode, various functions of the switch can be configured. Use command **set user local|radius** <name> **admin-password** [<string>] to set the password for entering the global configuration mode to prevent the login of unauthorized users.

   Result: This sets the password for entering the global configuration mode.

3. To return to the user mode from the global configuration mode, use the **exit** command.

END OF STEPS

Result Global mode has been configured.

Configuring SNMP Mode

Purpose This topic describes the configuration of SNMP mode.

Steps For the configuration of SNMP mode, perform the following steps.

1. In the global configuration mode, use the command **config snmp** to enter the SNMP configuration mode, as shown below:

```
zte(cfg)#config snmp
zte(cfg-snmp)#
```

Note: In SNMP configuration mode, SNMP and RMON parameters can be set.

2. To return to the global configuration mode from the SNMP configuration mode, use command **exit** or press **Ctrl+Z**.

END OF STEPS

Result SNMP mode has been configured.

Configuring Layer 3 Mode

Purpose This topic describes the Layer 3 configuration mode.

Steps For the configuration of Layer 3 mode, perform the following steps.

1. In the global configuration mode, execute the command **config router** to enter the Layer 3 configuration mode, as shown in the following example:

```
zte(cfg)#config router
zte(cfg-router)#
```

Note: In the Layer 3 configuration mode, you can configure the Layer 3 port, static router, and ARP entities.

2. To return to the global configuration mode from the Layer 3 configuration mode, use command **exit** or press **Ctrl+Z**.

END OF STEPS

Result Layer 3 mode has been configured.

Configuring File System Mode

Purpose This topic describes the file system configuration mode.

Steps For the configuration of file system, perform the following steps.

1. In the global configuration mode, execute the command **config tffs** to enter the file system configuration mode, as shown below:

```
zte(cfg)#config tffs
zte(cfg-tffs)#
```

Note: In the file system configuration mode, switch file system can be operated, including adding file directory, deleting file or directory, modifying file name, displaying file or directory, changing file directory, uploading/downloading files through TFTP, copying files, formatting Flash, and so on.

2. To return to the global configuration mode from the file system configuration mode, use command **exit** or press **Ctrl+Z**.

END OF STEPS

Result File system mode has been configured.

Configuring NAS Mode

Purpose This topic describes the NAS configuration mode.

Steps For the configuration of NAS mode, perform the following steps.

1. In the global configuration mode, execute the command **config nas** to enter into NAS configuration mode, as shown below:

```
zte(cfg)#config nas
zte(cfg-nas)#
```

Note: In the NAS configuration mode, configuration of switch access service including user access authentication and management.

2. To return to the global configuration mode from the NAS configuration mode, use command **exit** or press **Ctrl+Z**.

END OF STEPS

Result NAS mode has been configured.

Configuring Cluster Management

Purpose This topic describes the cluster management configuration mode.

Steps For the configuration of cluster management, perform the following steps.

1. In the global configuration mode, execute command **config group** to enter the cluster management configuration mode, as shown below:

```
zte(cfg)#config group
zte(cfg-group)#
```

Note: In the cluster management configuration mode, configuration of switch cluster management service.

2. To return to the global configuration mode from the cluster management configuration mode, use command **exit** or press **Ctrl+Z**.

END OF STEPS

Result Cluster management is configured.

Configuring Basic ACL

Purpose This topic describes the basic ACL configuration mode.

Steps For the configuration of basic ACL, perform the following steps.

1. In the global configuration mode, execute command **config acl basic number** <1-99> to enter into basic ACL configuration mode, as shown below:

```
zte(cfg)#config acl basic number 10
zte(basic-acl-group)#
```

Note: In the basic ACL configuration mode, it is possible to add, delete, move the ACL rule for the specified ACL id.

2. To return to the global configuration mode from basic ACL configuration mode, use command **exit** or press **Ctrl + Z**.

END OF STEPS

Result Basic ACL is configured.

Configuring Extended ACL

Purpose This topic describes the extended ACL configuration mode.

Steps For the configuration of extended ACL, perform the following steps.

1. In the global configuration mode, execute command **config acl extend number** <100-199> to enter into extended ACL configuration mode, as shown in:

```
zte(cfg)#config acl extend number 100
zte(extend-acl-group)#
```

Note: Extended ACL configuration mode includes configuring ACL parameters and moving ACL rule sequence id.

2. To return to global configuration mode from the extended ACL configuration mode, use command **exit** or press **Ctrl+Z**.

END OF STEPS

Result Extended ACL is configured.

Configuring L2 ACL Mode

Purpose This topic describes the L2 ACL configuration mode.

Steps For the configuration of L2 ACL, perform the following steps.

1. In the global configuration mode, execute command **config acl link number** *<200-299>* to enter into L2 ACL configuration mode, as shown in:

```
zte(cfg)#config acl link number 200
zte(link-acl-group)#
```

Note: L2 ACL configuration mode includes configuring ACL parameters and moves ACL rule sequence id.

2. To return to global configuration mode from the L2 ACL configuration mode, use command **exit** or press **Ctrl+Z**.

END OF STEPS

Result L2 ACL is configured.

Configuring Hybrid ACL Mode

Purpose This topic describes the Hybrid ACL configuration mode.

Steps For the configuration of Hybrid ACL, perform the following steps.

1. In the global configuration mode, execute command **config acl hybrid number <**300-349**>** to enter into Hybrid ACL configuration mode, as shown in:

```
zte(cfg)# config acl hybrid number 333
zte(hybrid-acl-group)#
```

Note: Hybrid ACL configuration mode includes configuring ACL parameters and moves ACL rule sequence id.

2. To return to global configuration mode from the Hybrid ACL configuration mode, use command **exit** or press **Ctrl+Z**.

Using Command Line

Online Help In any command mode, enter a question mark (?) after DOS prompt of system, a list of available commands in command mode is displayed. With context-sensitive help function, keywords and parameter lists of any commands can be obtained.

Purpose This topic describes the configuration of online command help.

Steps For the configuration of online command help, perform the following steps.

1. Input **?** behind the prompt of any command mode to view all commands and brief descriptions of this mode.

   Result: Command mode is viewed.

   Example: An example given below shows ? behind the prompt of the command mode.

```
zte>?
  enable              enable configure mode
  exit                exit from user mode
  help                   description of the interactive
help system
  show                show config information
  list                print command list
zte>
```

2. Input the question mark behind a character or character string.

   Result: This will view the list of commands or keywords beginning with that character or character string.

   Example: An example given below shows the character string.

```
zte(cfg)#c?
config  clear  create
zte(cfg)#c
```

3. Input **?** behind the command, keyword and parameter.

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

   Example: An example is given below.

```
zte(cfg)#config ?
  snmp            enter SNMP config mode
 router           enter router config mode
 tffs             enter file system config mode
 nas              enter nas config mode
 group            enter group management config mode
 acl              enter acl config mode
zte(cfg)#config
```

4. If a wrong command, keyword or parameter is entered then press Enter.

   Result: It will show message “Command not found” will be displayed on the interface.

   Example: An example is given below:

```
zte(cfg)#conf ter
  %  Command not found (0x40000066)
zte(cfg)#
```

5. Online help is used to create user.

   Result: Online help creates user.

   Example: An example is given below:

```
zte(cfg)#cre?
create
zte(cfg)#create ?
  port                create descriptive name for port
  vlan                create descriptive name for vlan
  user                create user
zte(cfg)#create user
  %  Parameter not enough (0x40000071)
zte(cfg)#create user ?
  <string>              user name
zte(cfg)#create user wangkc
zte(cfg)#
```

END OF STEPS

Result Online command help has been configured.

Command Abbreviations

In ZXR10 2920/2928/2952, a command or keyword can be shortened into a character or string that can uniquely identify this command or keyword. For example, the command **exit** can be shortened as **ex**, and the command **show port** shortened as **sh po**.

History Commands

Input Command Input command can be recorded in the user interface, up to 10 history commands can be recorded and this function is useful for invoking a long or complicated command again.

Execute one of the following operations to re-invoke a command from the record buffer, as shown in Table 18.

TABLE 18 INVOKING A COMMAND

Command	Function
CTRL+P or ↑	Invoke a history command in the buffer forward

Command	Function
CTRL+N or ↓	Invoke a history command in the buffer backward

In the privileged mode, execute the show history command to list the commands input the latest in this mode.

Function Key

User Interface

ZXR10 2920/2928/2952 provides a lot of functional keys for the user interface to facilitate user operations. Functional keys are shown in Table 19.

TABLE 19 FUNCTIONAL KEYS

Functional Key	Usage
Ctrl-P or ↑	Recover the last command (Roll back in the historical records of commands).
Ctrl-N or ↓	Recover the next command (Roll forward in the historical records of commands).
Ctrl-B or ←	Move left in the command line currently indicated by the prompt.
Ctrl-F or →	Move right in the command line where the prompt is currently located.
Tab	Display commands starting with the character or string. If there is only one command, make this command a complete one.
Ctrl-A	Skip to the beginning of the command line.
Ctrl-E	Skip to the end of the command line.
Ctrl-K	Delete the characters from the cursor to the end.
Ctrl-H or Backspace	Delete the character on the left of the cursor.
Ctrl-C	Cancel the command and display the prompt character.
Ctrl-L	Clear screen.
Ctrl-Y	Recover the last command executed.
Ctrl-Z	Return to the global configuration mode.

When the command output exceeds one page, output is split into several pages automatically and the prompt "----- more ----- Press Q or Ctrl+C to break -----" appears at the bottom of current page. Press any key to turn pages or press **Q** or **Ctrl+C** to stop the output.

Chapter 6

System Management

Overview

Introduction This chapter introduces file system management FTP/TFTP configuration, file backup and restoration, software version upgrade.

Contents This chapter includes the following contents:

TABLE 20 TOPICS IN CHAPTER 6

File System

Flash memory In ZXR10 2920/2928/2952 Flash is the major storage device on the main control board. Software version file and configuration file of the ZXR10 2920/2928/2952 are saved in the Flash memory. Operations, such as version upgrading and configuration saving, should be conducted in the Flash memory.

There are three directories in Flash by default:

- The name of the version file is kernel.z.
- The name of the configuration file is running.cfg.
- The name of the directory file is config.txt.

Operating File System

Introduction ZXR10 2920/2928/2952 provides many commands for file operations. Command format is similar to DOS commands as present in Microsoft Windows Operating System.

Purpose This topic describes file system operation of ZXR10 2920/2928/2952.

Prerequisite To do file management, there must have an access to Command Line Interface (CLI). CLI is a text-based interface that can be accessed through a direct serial connection to device and through telnet connections.

Steps For file system operation, perform the following steps.

1. To enter the file system configuration mode, use command **config tffs** in global configuration mode. This is shown in Table 21.

TABLE 21 CONFIG TFFS COMMAND

Format	Mode	Function
config tffs	config	This enters into the file system configuration mode

Result: This enters into the file system configuration mode.

2. To create new directory, use command **md** <directory name> in file system configuration mode. This is shown in Table 22.

TABLE 22 MD COMMAND

Format	Mode	Function
md <directory name>	File system config	This creates new directory

Result: This creates new directory.

3. To delete a file or directory, use command **remove** <file-name> in file system configuration mode. This is shown in Table 23.

TABLE 23 REMOVE COMMAND

Format	Mode	Function
remove <file-name>	File system	This creates new directory

Format	Mode	Function
	config	

Result: This deletes a file or directory.

4. To rename a file, use command **rename** <file-name><file-name> in file system configuration mode. This is shown in Table 24.

TABLE 24 RENAME COMMAND

Format	Mode	Function
rename <file-name><file-name>	File system config	This renames the file

Result: This renames the file.

5. To modify the current directory, use command **cd** <directory name> in file system configuration mode. This is shown in Table 25.

TABLE 25 CD COMMAND

Format	Mode	Function
cd <directory name>	File system config	This modifies the current directory

Result: This modifies the current directory.

6. To displays the current directory list, use command **ls** in file system configuration mode. This is shown in Table 26.

TABLE 26 LS COMMAND

Format	Mode	Function
ls	File system config	This displays the current directory

Result: This displays the current directory.

7. To upload or download a version through TFTP, use command **tftp** <A. B. C. D> {**download|upload**} <name> in file system configuration mode. This is shown in Table 27.

TABLE 27 TFTP COMMAND

Format	Mode	Function
tftp <A. B. C. D> {**download|upload**} <name>	File system config	This uploads or downloads a version through TFTP

Result: This uploads or downloads a version through TFTP.

8. To copy a file, use command **copy** <source-pathname><dest-pathname> in file system configuration mode. This is shown in Table 28.

TABLE 28 COPY COMMAND

Format	Mode	Function
copy <source-pathname><dest-pathname>	File system config	This copies a file

Result: This copies a file.

9. To format the FLASH memory, use command **format** in file system configuration mode. This is shown in Table 29.

TABLE 29 FORMAT COMMAND

Format	Mode	Function
format	File system config	This formats the FLASH memory

Result: This formats the FLASH memory.

END OF STEPS

Result File system operation of ZXR10 2920/2928/2952 is configured.

Configuring ZXR10 2920/2928/2952 as an TFTP Client

Purpose This topic describes the background TFTP server configuration.

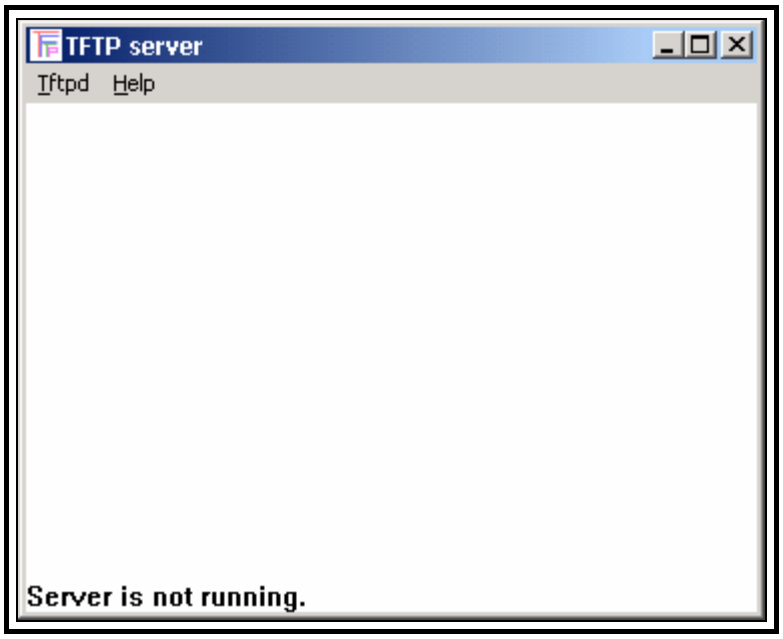
Prerequisite To configure background TFTP server, meet the following requirements.

- Start TFTP server on the background host, and access ZXR10 2920/2928/2952 as a TFTP client from the TFTP server.

Steps The following describes the background TFTP server configuration taking tftpd as an example.

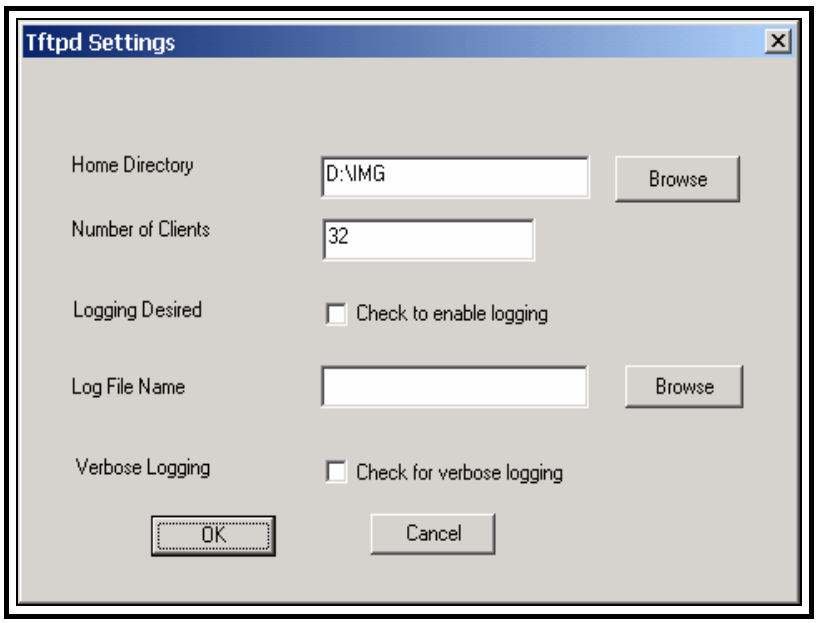
1. Run tftpd on the background host, and an interface as shown in Figure 22.

FIGURE 22 TFTPD INTERFACE



2. Select **Tftpd > Configure**, click **Browse** on the popup dialog box, and select a directory to store the version/configuration file, such as D:\IMG. The following dialog box will appear as shown in Figure 23.

FIGURE 23 CONFIGURE DIALOG BOX



3. Click **OK** in Figure 23 to finish the settings.

END OF STEPS

Result

Background of TFTP server is implemented. Start the TFTP server, and run copy on the switch to backup/restore files or import/export configurations.

Configuring Imports and Exports

Purpose This topic describes the import and export functions of configuration information of ZXR10 2920/2928/2952.

Steps For the configuration of import and export functions, perform the following steps.

1. The command **show running-config toFile** is used to export the execution result of **show running-config** to a config. txt and to save it in the FLASH memory.

   Result: This command exports and saves it in the FLASH memory.

   Example: This file can also be uploaded to the TFTP server to view a file.

   ```
   Zte(cfg-tffs)#tftp 192. 168. 1. 102 upload
   config. txt
   ```

   In normal condition, when rebooting the switch, use command **running. cfg file** to recover configurations.

   When switch can not find running. cfg file, it will check whether the config. txt file exists and when file exists, switch will use it to recover configurations.

   Config. txt file is used for version update. When the span between new version and old one is big, using running. cfg file of the primary version may cause mistakes after version update. Consider the following recommendations:

   - Create config. txt file before version update.
   - Use the newly downloaded version to reboot switch after deleting running. cfg file of old version.

   Important! Switch will use config. txt file to recover configurations. When command format is not modified or deleted in new version, configurations will be recovered successfully. If configurations is not recovered, recover them manually.

   - Use command **saveconfig** to create a running. cfg file for new version after update is finished.

2. The command **readconfig** is to read the configuration commands in the config. txt in the FLASH and sends them to the switch for resolution and execution.

   Result: Contents of the config. txt can be edited manually as needed and then downloaded to the switch by using the command **tftp**.

Example: This command downloads the file to the switch as shown below in the example.

```
zte(cfg-tffs)#tftp 192.    168.    1.    102 download
config.   txt
```

END OF STEPS

Result Import and export function has been configured.

Setting File Backup and Recovery

Purpose This topic describes the procedure of file backups and recovery.

Prerequisites To backup files and recover, meet the following requirements:

- To do Data backup and Recovery, there must have an access to Command Line Interface (CLI). CLI is a text-based interface that can be accessed through a direct serial connection to device and through telnet connections.
- Make sure the TFTP server is up and running as described above.

Steps For file backup and recovery, perform the following steps.

1. Use command **saveconfig** in global configuration mode. This is shown in Table 30.

   Note: When a command is used to modify the switch configuration, data is running in the memory of the switch. When the switch is restarted, all the contents newly configured will be lost.In order to save the current configuration into the FLASH memory,

TABLE 30 SAVECONFIG COMMAND

Format	Mode	Function
saveconfig	config	This saves the current configuration into the FLASH memory

Result: This saves the current configuration into the FLASH memory.

Example: The following shows the **saveconfig** command

```
zte(cfg)#saveconfig
```

To prevent damage to the configuration data, use command **tftp** in file system configuration mode. This is shown in below table:

Format	Mode	Function
tftp <A. B. C. D> {**download**|**upload**} <name>	File system config	This uploads or downloads a version through TFTP

Result: This command is used to back up a configuration file in the FLASH memory to the background TFTP Server.

Example: The following shows the back up of a configuration file in the FLASH MEMORY to the background of TFTP Server.

```
zte(cfg-tffs)#tftp 192.    168.    1.    102 upload
running.   cfg
```

This command can also be used **show running-config toFile** to write the configuration information into the config. txt and then back up the file to the TFTP server. For detailed method, refer to Configuring Imports and Exports .

2. Execute the following command to download the configuration file in background TFTP server to the FLASH memory.

```
zte(cfg-tffs)#tftp 192.    168.    1.    102 download
running.   cfg
```

3. Similar to the configuration file, use command **tftp** to upload the foreground version file to the background TFTP server.

   Example: This example shows the upload of the foreground version file to the background TFTP server.

```
Zte(cfg-tffs)#tftp 192.    168.    1.    102 upload
kernel.   z
```

4. Version file recovery is used to retransmit the background backup version file to the foreground through TFTP. Recovery is very important in the case of upgrading failure. The version recovery operation is basically the same with the version upgrade procedure.

END OF STEPS

Result File backup and recovery has been configured.

Software Version Upgrade

Introduction Software version upgrade is only made when the original version fails to support certain functions. Improper operation may lead to upgrade failure and hence system booting failure. Therefore, version upgrading must be done with the understanding of principle, operation and upgrade procedure of the ZXR10 2920/2928/2952 before start to upgrade the version.

Version Upgrading occurs in the following two cases:

- Version Upgrade in case of System Abnormality
- Version Upgrade in case of Normal System.

Viewing System Information

Purpose This topic describes the procedure for viewing system information.

Steps For system view, perform the following steps.

1. To view hardware and software versions of the System, use **show version** command in global configuration mode as shown in Table 31.

TABLE 31 SHOW VERSION COMMAND WINDOW

Format	Mode	Function
Show version	config	This display the version information about the software and hardware of system

Result: This shows the running software and hardware information of system.

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

```
zte(cfg)#version
    The System's Hardware Info:
      Switch's Mac Address: 00.    d0.    d0.    f0.    11.
22

      Module 0: ZXR10  5124; fasteth:  0; gbit: 24;

    The System's Software Info:
      Version number    : V1.   1.   11.   b
      Version make date: Jun 16 2006
      Version make time: 16:27:13

      System has run 0 years 2 days 3 hours 8 minutes 43
seconds

Zte(cfg)#
```

END OF STEPS

Result System information has been viewed.

Upgrading Version at Normality

Purpose This topic describes the procedure of software version upgrade for ZXR10 2920/2928/2952 in normal case.

Prerequisites To upgrade software version, meet the following requirements.

- Connect ZXR10 2920/2928/2952 console port (on the main control board) to the serial port of the background host with a console cable attached to the switch. Connect the management Ethernet port to the background host's network port with a straight through network cable. Make sure that both connections are correct.
- Set the IP address of the Ethernet port on the switch. Set the IP address of the background host used for upgrade. The two IP addresses must be in the same network segment so that the host can ping the switch.
- On the background host, start the TFTP server software and set Configuring ZXR10 2920/2928/2952 as an TFTP Client.

Steps For software version upgrade, perform the following steps.

1. View the information about the currently running image by using **show version** command in privileged mode as shown in Table 32.

TABLE 32 SHOW VERSION COMMAND WINDOW

Format	Mode	Function
Show version	Privileged mode	This indicated software version flash and image file present in directory

Result: This indicates new image file present in directory.

2. To delete the old version file in FLASH memory, use command **remove** <file-name> in file system configuration mode. This is shown in Table 33. If the FLASH memory has sufficient space, change the name of the old version file and keep it in FLASH memory.

TABLE 33 REMOVE COMMAND

Format	Mode	Function
remove <file-name>	File system config	This deletes the old version file in FLASH memory

Result: This deletes the old version file in the FLASH memory.

Example: The example of **remove** command is given below:

```
zte(cfg)#config tffs
zte(cfg-tffs)#remove kernel.   z
```

3. Use command **tftp** to upgrade the version. The following shows how to download the version file from the TFTP server to the FLASH memory:

```
zte(cfg-tffs)#tftp 192.    168.    1.    102 download
kernel.   z
.   .   .   .   .   .   .   .   .   .   .   .   .   .
 .   .   .   .   .   .   .   .   .   .   .   .   .   .
  .   .   .   .   .   .   .   .   .   .   .   .   .   .
   .   .   .   .   .   .   .   .   .   .   .   .   .   .
.   .   .   .   .   .   .   .   .   .   .   .   .   .
 .   .   .   .   .   .   .   .   .   .   .   .   .   .
  .   .   .   .   .   .   .   .   .   .   .   .   .   .
   .   .   .   .   .   .   .   .   .
  1, 979, 157 bytes downloaded
zte(cfg-tffs)#
```

4. Restart the switch. After successful startup, check the version under running and confirm whether the upgrading is successful.

END OF STEPS

Result Version upgrade has been installed.

Note When updating the version, there is configuration compatibility problem of old and new versions. running. cfg file is of binary and has poor compatibility. It is advised to test configuration recovery first, then check whether the configuration recovery needs to use config. txt file. When the old version has big span with the new one, use config. txt file to recover configuration. After upadate, check the recovered configurations are of same primary configurations or not. If they are not the same, configure according to facts and avoid the mistakes caused by update.

Upgrading Version at Abnormality

Purpose This topic describes the procedure of software version upgrade for ZXR10 2920/2928/2952 if it fails to start.

Prerequisite Connect Console port of the switch to the serial port of the background host using the self-contained configuration cable. Connect an Ethernet port of the switch to the network port of the background host using a network cable. Check whether the connections are correct.

Steps For software version upgrade, perform the following steps.

1. Restart the switch. At the HyperTerminal, press any key as prompted to enter the [VxWorks Boot] state.

```
Welcome to use ZTE eCarrier!!



Copyright(c) 2004-2006,   ZTE Co.   ,  Ltd.
System Booting.   .   .   .   .   .
CPU: DB-88E6218
Version: VxWorks5.   5.   1
BSP version: 1.   2/6-b
Creation date: Aug  1 2006,  09:40:27




Press any key to stop auto-boot.   .   .
 7
[ZxR10 Boot]:
```

2. Enter **c** in the [ZxR10 Boot] state and press **Enter** to enter the parameter modification status. Set the IP addresses of the Ethernet port and the TFTP server. Generally, these two addresses are set to the same network segment.

```
[ZxR10 Boot]:  c

'.    ' = clear field;   '-' = go to previous
field;  ^D = quit

boot device           : wbdEnd1           */Use
the default value.   /*
processor number      : 0                */ Use
the default value.   /*
host name             : tiger             */Use
the default value.   /*
file name             : vxWorks           */Use
the default value.   /*
inet on ethernet (e) : 10.   40.   89.   106
*/ IP address of the Ethernet port /*
inet on backplane (b):                    */Use
the default value.   /*
host inet (h)         : 10.   40.   89.   78
*/IP address of the TFTP server/*
gateway inet (g)       : 10.    40.    89.    78
*/Use the default value.   /*
user (u)              :                    (Use
the default value)
ftp password (pw) (blank = use rsh):      (Use
the default value)
flags (f)             : 0x80              */Use
the default value.   /*
target name (tn)      :                   */Use
the default value.   /*
startup script (s)    :                  */Use
the default value.   /*
other (o)             :                  */Use
the default value.   /*
[ZxR10 Boot]:
```

3. Set the IP address of the background host as the same with the IP address of the above TFTP server.
4. Start the TFTP server software on the background server and configure the TFTP server as per description in Configuring ZXR10 2920/2928/2952 as an TFTP Client.
5. In the [ZxR10 Boot] state, input zte to enter the [BootManager] state of the switch. Input **?** to display the command list for this state.

```
[ZxR10 Boot]: zte
Load wbdEnd Begin
W90N740 MAC0: 10MB - Full Duplex

Board 2818s !
Marvell has been initialized !
boot device          : wbdEnd
unit number          : 0
processor number     : 0
host name            : tiger
file name            : vxWorks
inet on ethernet (e) : 10.   40.   89.   106
host inet (h)        : 10.   40.   89.   78
gateway inet (g)     : 10.   40.   89.   78
flags (f)            : 0x80

Attached TCP/IP interface to wbdEnd0.
Warning! no netmask specified.
Attaching  network  interface  lo0.     .     .
done.
Attaching to TFFS.   .   .
test flash passed perfectly!
Welcome to boot manager!
Type for help

[BootManager]:?

ls                    */Display the current
directory list.   /*
pwd                   */Display the current
absolution path.    /*
devs                  */Display the FLASH
information.    /*
show                  */Display the switch
type and mac address.   /*
reboot                */Restart the switch.
/*
format                */Format the FLASH.   /*
del    file_name      */Delete the specified
file.   /*
md     dir_name       */Create a directory.
/*
mf     file_name      */Create a file.   /*
cd     absolue-pathname     */Change the
current directory.   /*
tftp   ip_address file_name */Download/upload
a version file through TFTP /*
update file_name      */Upgrade boot/*
rename  file_name newname   */Rename the file.
/*
```

6. In the [BootManager] state, use the command **tftp** to upgrade the version. The following shows how to download the version file from the TFTP server to the FLASH memory:

```
[BootManager]:tftp 10.   40.   89.   78 kernel.   z
Loading.   .   .    done!
[BootManager]:ls
snmpboots.   v3                 35
startcfg.   txt               1378
running.   cfg              231916
kernel.   z                1311339
[BootManager]:
```

7. In the [BootManager] state, execute the command **reboot** to restart the switch by using the new version. If the switch is started normally, use the command **version** to check whether the new version is running in the memory. When the switch is not started normally, it indicates the version upgrade fails. In this case, repeat the above upgrade procedure.

END OF STEPS

Result Software version upgrade has been completed.

This page is intentionally blank.

Chapter 7

Service Configuration

Overview

Introduction This chapter provides an overview of configuration methods for various services of ZXR10 2920/2928/2952.

Contents This chapter includes the following contents:

Configuring Basic Port Parameters

Introduction On the ZXR10 2920/2928/2952, configuration of the following port parameters: auto negotiation, duplex mode, rate, flow control, port priority, MAC address number restriction, and so on.

Purpose This topic describes the configuration of basic port parameters.

Steps For basic port parameters, perform the following steps.

1. To clear port name/statistics data, use **clear port** <*portlist*> {**name|statistics|description**}

TABLE 34 SET PORT COMMAND

Format	Mode	Function
clear port <*portlist*> {**name|statistics|description**}	Global config	This clear port name/statistics data.

Result: This clear port name/statistics data.

2. To create port description name, use command **create port** <*portname*> **name** <*name*> in global configuration mode. This is shown in Table 35.

TABLE 35 AUTO-SENSING COMMAND

Format	Mode	Function
clear port <*portlist*> {name|statistics|description}	Global config	This creates port description name.

Result: This creates port description name.

3. To enable or disable the port, use command **set port** <*portlist*> {**enable|disable**} in global configuration mode. This is shown in Table 36.

TABLE 36 WORK MODE COMMAND

Format	Mode	Function
set port <*portlist*> {enable|disable}	Global config	This enables or disables the port.

Result: This enables or disables the port.

4. To set the port auto, use command **set port** <*portlist*> **auto** {**enable|disable**} in global configuration mode. This is shown in Table 37.

TABLE 37 DUPLEX COMMAND

Format	Mode	Function
set port <*portlist*> auto {enable|disable}	Global config	This sets the port auto.

Result: This sets the port auto.

5. To set the port speedadvertise, use command **set port** <*portlist*>**speedadvertise**{**maxspeed|speed10|speed100|speed1000}** in global configuration mode. This is shown in Table 38.

TABLE 38 SPEED COMMAND

Format	Mode	Function
set <*portlist*> speedadvertise {maxspeed|speed10|speed100|speed1000}	Global config	This sets speed of the port.

Result: This sets speed of the port.

6. To set the working manner of the port, use command **set port** <*portlist*> **duplex {full|half}**.

Format	Mode	Function
set port <*portlist*> duplex {full|half}	Global config	This sets the working manner of the port.

7. To set the speed of the port, use command **set port** <*portlist*> **speed** {**10|100|1000**}.

Table 39 Set Port speed Commands

Format	Mode	Function
set port <*portlist*> speed {10|100|1000}}	Global config	This sets port's speed.

Result: This sets port's speed.

8. To set port <*portlist*> queue-schedule, use command **set port <*portlist*> queue-schedule { WRR0 |SP |WRR1-SP|WRR2-SP}.**
Table 40 Set port queue-schedule command

TABLE 40 PORT QUEUE-SCHEDULE COMMANDS

Format	Mode	Function
set port <portlist> **queue-scedule {WRR0|SP|WRR1-SP|WRR2-SP}**	Global config	This sets packet type of ingress direction

7. To set the priority of the source MAC address, use command **set port** <*portlist*> **sa-priority** {**enable|disable**}

TABLE 41 THE PRIORITY OF THE SOURCE MAC ADDRESS ON COMMAND

Format	Mode	Function
set port <portlist> **sa-priority {enable|disable}**	Global config	This sets the priority of the source MAC address.

Result: This sets the priority of the source MAC address.

8. To set the priority of the source VLAN, use command **set port** <*portlist*> **vlan-priority** {**enable|disable**}.

TABLE 42 QUEUE-SCHEDULE COMMAND

Format	Mode	Function
set port <portlist> **vlan-priority {enable|disable}**	Global config	This sets port's priority of the source VLAN.

Result: This sets port's queue-schedule profile.

9. To set the priority of a port, use command **set port** <portlist> **default-priority** <0-7> in global configuration mode. This is shown in Table 43.

TABLE 43 DEFAULT-PRIORITY COMMAND

Format	Mode	Function
set port <portlist> **default-priority** <0-7>	Global config	This sets the priority of a port

Result: This sets the priority of a port.

12. To set remapping-tag priority of a port, use command **set port** <portlist> **remapping-tag** <*0-7*>**priority** in global configuration mode. This is shown in Table 44.

TABLE 44 SET PORT SECURITY COMMAND

Format	Mode	Function

Format	Mode	Function
set port<*portlist***> remapping-tag <***0-7***> priority <***0-7***>**	Global config	This sets **remapping-tag priority** of a port.

Result: This sets **remapping-tag priority** of a port.

13. To set the port security, use command **set port** <*portlist*> **security** {**enable|disable**} in global configuration mode. This is shown in Table 45.

TABLE 45 MULTICAST-FILTER COMMAND

Format	Mode	Function
set port <*portlist***> security {enable|disable }**	Global config	This sets the multicast filter of a port

Result: This sets the port security.

14. To enable or disable the port unit-statistics, use command **set port** <*portlist*> **unit-statistics** {**enable |disable**} in global configuration mode. This is shown in Table 46.

TABLE 46 RATE ADVERTISEMENT COMMAND

Format	Mode	Function
set port <*portlist*> **unit-statistics** {**enable |disable**}	Global config	This sets the port unit-statistics

Result: This sets the port unit-statistics.

15. To set the multicast-filter, use command **set port** <portlist> **macaddress** {**on** <1-16>|**off**} in global configuration mode. This is shown in Table 47.

TABLE 47 MAC ADDRESS COMMAND

Format	Mode	Function
set port **<portlist>** macaddress **{**on **<1-16>|**off**}**	Global config	This sets multicast-filter

Result: This sets the number of MAC addresses.

16. To set port on Vlan, use command **set port** <*portname*> **description** <*string*> in global configuration mode. This is shown in Table 48.

TABLE 48 PROTOCOL-VLAN COMMAND

Format	Mode	Function
set port <*portname*> **description** <*string*>	Global config	This sets port description

Result: This sets port description.

17. To set port's macaddress, use command **set port** <*portlist*> **macaddress** {**on** <*1-16*> | **off** } in global configuration mode. This is shown in Table 49.

TABLE 49 PORT JUMBO COMMAND

Format	Mode	Function
set port <*portlist*> macaddress {on <*1-16*> | off }	Global config	This sets port's macaddress

Result: This sets port's macaddress.

18. To set the ACL info, use command **set port** <*portlist*> **acl** <*acl-number*> {**enable | disable**} in global configuration mode. This is shown in Table 50.

TABLE 50 CREATE PORT COMMAND

Format	Mode	Function
set port **<*portlist*>** acl **<*acl-number*>** **{**enable | disable**}**	Global config	This sets the ACL info

Result: This sets the ACL info.

19. To set port vlanjump, use command **set port** <*portlist*>**vlanjump** {**enable** [**defaultauthvlan**<*1-4094*>] | **disable** }in global configuration mode. This is shown in Table 51.

TABLE 51 PORT DESCRIPTION COMMAND

Format	Mode	Function
set port **<*portlist*>**vlanjump **{**enable **[**defaultauthvlan**<*1-4094*>**] |** disable	Global config	This sets port vlanjump

Result: This sets port vlanjump.

20. To set port trust-up, use command **set port** <*portlist*> **trust-up** {**enable | disable**}in global configuration mode. This is shown in Table 51.

TABLE 52 PORT DESCRIPTION COMMAND

Format	Mode	Function
set port ***<portlist>*** trust-up **{**enable | disable**}**	Global config	This sets port trust-up

Result: This sets port trust-up.

21. To set port trust-dscp, use command **set port** <*portlist*> **trust-dscp** {**enable | disable** }in global configuration mode. This is shown in Table 51.

TABLE 53 PORT DESCRIPTION COMMAND

Format	Mode	Function
set port <*portlist***>** **trust-dscp {enable | disable}**	Global config	This sets port trust-dscp

Result: This sets port trust-dscp.

Note: When setting megabit port trust-dscp, the switch also converts it to the corresponding UP. The flow is as follows:

When the IP message enterS from port A that trusts in DSCP, firstly, we get the default priority def[2:0](0-7, aggregately 3 bits). Then mapping the global DSCP-TC table according to DSCP value of the message, we can get the initial TC value TC[1:0](0-3, aggregately 2 bits) of the message. We adopt TC[1:0] as the [2:1]digit of UP, the last digit of port default priority def[0]as the new UP digit of the message(0-7, aggregately 3 bits). Finally, switch mapping the global UP-TC table according to the new UP, & get the queue that the message will enter.

Example:the DSCP of a item of message is 60, the entry default priority is 7, trust DSCP, DSCP-TC mapping table is 60-2. Then in the switch, the UP message converts to 5, & obtain the queue to enter according to global UP-TC table.

If port trust UP & DSCP at the same time, the gigabit port will trust DSCP firstly, & the megabit port will trust UP firstly.

END OF STEPS

Result Basic port parameters are configured.

Displaying Port Information

Purpose This topic describes the displaying of port information.

Steps To view of port information, perform the following steps.

1. To display the configuration and work state of the port, use command **show port** [<portlist>] in global configuration mode. This is shown in Table 54.

TABLE 54 SHOW PORT COMMAND

Format	Mode	Function
show port [<portlist>]	Global config	This displays the configuration and work state of the port

Result: This displays the configuration and work state of the port.

2. To displays Vlan information of the port, use command **show port** <portlist> **vlan** in global configuration mode. This is shown in Table 55.

TABLE 55 SHOW PORT VLAN COMMAND

Format	Mode	Function
show port <portlist> **vlan**	Global config	This displays Vlan information of the port

Result: This displays Vlan information of the port.

3. To display statistics information of the port in unit time, use command **show port** <portlist> **statistics 1min_unit|5min_unit** in global configuration mode. This is shown in Table 56.

TABLE 56 SHOW PORT STATISTICS TIME COMMAND

Format	Mode	Function
show port <portlist> **statistics 1min_unit|5min_unit**	Global config	This displays statistics information of the port in unit time

Result: This displays statistics information of the port in unit time.

4. To display the QoS configuration data of the port, use command **show port** <portlist> **qos** in global configuration mode. This is shown in Table 57.

TABLE 57 SHOW PORT QOS COMMAND

Format	Mode	Function

Format	Mode	Function
show port <portlist> **qos**	Global config	This displays the QoS configuration data of the port

Result: This displays the QoS configuration data of the port.

5. To display the bandwidth information of the port, use command **show port** <*portlist*> **bandwidth session** <*0-3*> in global configuration mode. This is shown in Table 58.

TABLE 58 SHOW PORT BANDWIDTH COMMAND

Format	Mode	Function
show port ***<portlist>*** bandwidth session ***<0-3>***	Global config	This displays the bandwidth information of the port

Result: This displays the bandwidth information of the port.

END OF STEPS

Result Port information is displayed.

Port Mirroring

Introduction Port mirroring is used to mirror data packets of the switch port (ingress mirroring port) to an ingress destination port (ingress monitoring port), or mirror the data packets of the switch port (egress mirroring port) to an egress destination port (egress monitoring port).

Through mirroring, data packets flowing in or out of a certain port can be monitored. Port mirroring provides an effective tool for the maintenance and monitoring of the switch.

Switch can be configured with only one ingress monitoring port and one egress monitoring port. Ingress monitoring port and egress monitoring port can be configured on same port. Whereas multiple source ingress monitoring ports and source egress monitoring ports can be configured at the same time.

Note: In default case, switch does not have mirroring port. The GOOD data packets received by ingress mirroring port are mirrored onto the monitoring ports, but data packets directly discarded on the ingress port (for example, because of CRC errors) are not mirrored. The source mirror port & the destination port must be in the same vlan.

Configuring Port Mirroring

Purpose

This topic describes the procedure of port mirroring configuration of ZXR10 2920/2928/2952.

Steps To mirror the ports, perform the following steps.

1. To add a mirroring port, use command **set mirror add source-port** <portlist> **{ingress|egress}** in global configuration mode. This is shown in Table 59.

TABLE 59 SET MIRROR COMMAND

Format	Mode	Function
set mirror add source-port <portlist> **{ingress|egress}**	Global config	This adds a mirroring port

Result: This adds a mirroring port.

2. To delete mirroring port, use command **set mirror delete source-port** <portlist> **{ingress|egress}** in global configuration mode. This is shown in Table 60.

TABLE 60 DELETE MIRRORING PORT COMMAND

Format	Mode	Function
set mirror delete source-port <portlist> **{ingress|egress}**	Global config	This deletes mirroring port

Result: This deletes mirroring port.

3. To set a monitoring port, use command **set mirror add dest-port** <portname> **{ingress|egress}** in global configuration mode. This is shown in Table 61.

TABLE 61 SET MIRROR DEST-PORT COMMAND

Format	Mode	Function
set mirror add dest-port <portname> **{ingress|egress}**	Global config	This sets a monitoring port

Result: This sets a monitoring port.

4. To delete destination monitoring port, use command **set mirror delete dest-port** <portname> **{ingress|egress}** in global configuration mode. This is shown in Table 62.

TABLE 62 SET MIRROR DELETE DEST-PORT COMMAND

Format	Mode	Function
set mirror delete dest-port <portname>	Global config	This deletes destination monitoring port

Format	Mode	Function
{ingress|egress}		

Result: This deletes destination port.

2. To display the port mirroring configuration, use command **show mirror** in global configuration mode. This is shown in Table 63.

TABLE 63 SHOW MIRROR COMMAND

Format	Mode	Function
show mirror	Global config	This displays port mirroring configuration

Result: This displays port mirroring configuration.

END OF STEPS]

Result Port mirroring is configured on ZXR10 2920/2928/2952.

Example To mirror data packets received by port 1 and port 16 onto the monitoring port 10, configuration is as follows:

```
zte(cfg)# set mirror add dest-port 10 ingress
zte(cfg)# set mirror add source-port 1, 16 ingress
```

Use the command **show mirror** to view the port mirroring configuration.

```
zte(cfg)#show mirror
  ingress mirror infomation
  --------------------------
     source port: 1 16
     dest port  : 10
  egress mirror infomation
  --------------------------
     source port: none
    dest port  : none
zte(cfg)#
```

To mirror the data packets received by port 2 and port 3 onto the monitoring port 4, configuration is as follows:

```
zte(cfg)# set mirror add dest-port 4 egress
zte(cfg)# set mirror add source-port 2, 3 egress
```

VLAN

Definition Virtual Local Area Network (VLAN) is a technology that divides a physical network into several logical (virtual) Local Area Networks (LANs). Each VLAN is identified by a VLAN ID (VID). Several VLANs share the switch & link of the physical local network.

Description Each VLAN is like an independent local area network logically. In the same VLAN, all the frame flow is limited in this VLAN. Cross-VLAN visit can only be implemented through forwarding on layer 3. This improve the network capability greatly. Reduce the whole flow of the physical local network.

ZXR102920/2928/2952 support tagged-based VLAN which is VLAN based on lable. This is the mode IEEE 802. 1Q defined, & the universal work mode. In this mode, VLAN partition is based on port's VLAN info(PVID:port VLAN ID)or the information in VLAN lable.

VLAN provides the following advantages:

- Lower broadcast traffic on the network
- Enhanced network security
- Streamlined network management

Configuring VLAN

Purpose This topic describes the configuration of VLAN on ZXR10 2920/2928/2952.

Steps For configuration of VLAN, perform the following steps.

1. To remove a VLAN name, use command **clear vlan** <vlanlist> **name** in global configuration mode. This is shown in Table 64.

TABLE 64 CLEAR VLAN COMMAND

Format	Mode	Function
clear vlan <vlanlist> **name**	Global config	This removes a VLAN name

Result: This removes a VLAN name.

2. To create a VLAN name, use command **create vlan** <1-4094> **name** <sting> in global configuration mode. This is shown in Table 65.

TABLE 65 CREATE VLAN COMMAND

Format	Mode	Function
create vlan <1-4094> **name** <string>	Global config	This creates a VLAN name

Result: This creates a VLAN name.

3. To set port PVID, use command **set port** <portlist> **pvid** <1-4094> in global configuration mode. This is shown in Table 66.

TABLE 66 SET PORT PVID COMMAND

Format	Mode	Function
set port <portlist> **pvid** <1-4094>	Global config	This sets port PVID

Result: This sets port PVID.

4. To set trunk PVID, use command **set trunk** < trunklist > **pvid** <1-4094> in global configuration mode. This is shown in Table 67.

TABLE 67 SET TRUNK PVID COMMAND

Format	Mode	Function
set trunk < trunklist > **pvid** <1-4094>	Global config	This sets trunk PVID

Result: This sets trunk PVID.

5. To Enable/Disable the VLAN, use command **set vlan** <vlanlist> **{enable|disable}** in global configuration mode. This is shown in Table 68.

TABLE 68 SET VLAN COMMAND

Format	Mode	Function
set vlan <vlanlist> **{enable|disable}**	Global config	This Enable/Disable the VLAN

Result: This Enable/Disable the VLAN.

6. To add a specified port to the VLAN, use command **set vlan** <vlanlist> **add port** <portlist> **[tag|untag]** in global configuration mode. This is shown in Table 69.

TABLE 69 SET VLAN ADD PORT COMMAND

Format	Mode	Function
set vlan <vlanlist> **add port <portlist>** [tag|untag]	Global config	This adds a specified port to the VLAN

Result: This adds a specified port to the VLAN.

7. To add a specified trunk to the VLAN, use command **set vlan** <vlanlist> **add trunk** <trunklist> **[tag|untag]** in global configuration mode. This is shown in Table 70.

TABLE 70 SET VLAN ADD TRUNK COMMAND

Format	Mode	Function
set vlan <vlanlist> **add trunk** <trunklist> **[tag|untag]**	Global config	This adds a specified trunk to the VLAN

Result: This adds a specified trunk to the VLAN.

8. To delete a specified port to the VLAN, use command **set vlan** <vlanlist> **delete port** <portlist> in global configuration mode. This is shown in Table 71.

TABLE 71 SET VLAN DELETE PORT COMMAND

Format	Mode	Function
set vlan <vlanlist> **delete port** <portlist>	Global config	This deletes a specified port to the VLAN

Result: This deletes a specified port to the VLAN.

9. To delete a specified trunk to the VLAN, use command **set vlan** <vlanlist> **delete trunk** <trunklist> in global configuration mode. This is shown in Table 72.

TABLE 72 SET VLAN DELETE TRUNK COMMAND

Format	Mode	Function
set vlan <vlanlist> **delete trunk** <trunklist>	Global config	This deletes a specified trunk to the VLAN

Result: This deletes a specified trunk to the VLAN.

10. To forbid port from VLAN, use command **set vlan** <vlanlist> **forbid port** <portlist> in global configuration mode. This is shown in Table 73.

TABLE 73 SET VLAN FORBID PORT COMMAND

Format	Mode	Function
set vlan <vlanlist> **forbid port** <portlist>	Global config	This forbids port from VLAN

Result: This forbids port from VLAN.

11. To permit port on VLAN, use command **set vlan** <vlanlist> **permit port** <portlist> in global configuration mode. This is shown in Table 74.

TABLE 74 SET VLAN PERMIT PORT COMMAND

Format	Mode	Function
set vlan <vlanlist> **permit port** <portlist>	Global config	This permits port on VLAN

Result: This permits port on VLAN.

12. To forbid trunk on VLAN, use command **set vlan** <vlanlist> **forbid trunk** <trunklist> in global configuration mode. This is shown in Table 75.

TABLE 75 SET VLAN FORBID TRUNK COMMAND

Format	Mode	Function
set vlan <vlanlist> **forbid trunk** <trunklist>	Global config	This forbids trunk on VLAN

Result: This forbids trunk on VLAN.

13. To permit trunk on VLAN, use command **set vlan** <vlanlist> **permit trunk** <trunklist> in global configuration mode. This is shown in Table 76.

TABLE 76 SET VLAN PERMIT TRUNK COMMAND

Format	Mode	Function
set vlan <vlanlist> **permit trunk** <trunklist>	Global config	This permits trunk on VLAN

Result: This permits trunk on VLAN.

14. To displays VLAN information, use command **show vlan** [<vlanlist>] in global configuration mode. This is shown in Table 77.

TABLE 77 SHOW VLAN COMMAND

Format	Mode	Function
show vlan [<vlanlist>]	Global config	This displays VLAN information

Result: This displays VLAN information.

END OF STEPS

Result VLAN is configured on ZXR10 2920/2928/2952.

Example This example shows the configuration of VLAN 100. Add untagged ports 1 and 2 and tagged ports 7 and 8. The detailed configuration is as follows:

Note: It is recommended to delete default VLAN before the configuration.

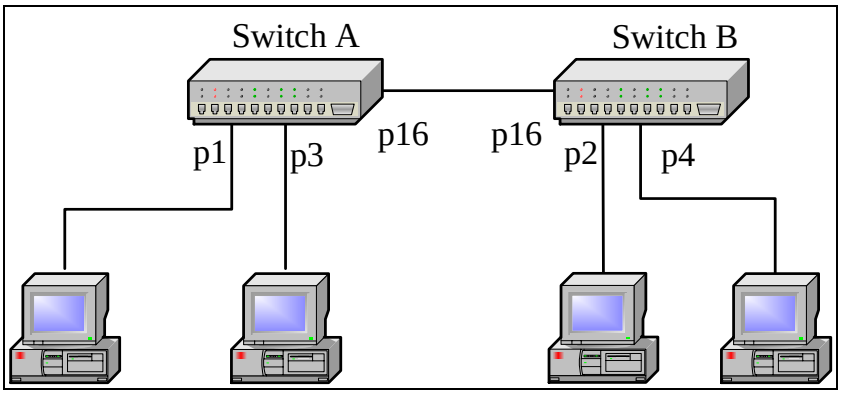
```
zte(cfg)#set vlan 100 add port 1, 2 untag
zte(cfg)#set vlan 100 add port 7, 8 tag
zte(cfg)#set port 1, 2 pvid 100
zte(cfg)#set vlan 100 enable
zte(cfg)#show vlan 100
  VlanId   :  100        Fid   :  100        Priority:  off
VlanStatus: enabled
  VlanName:
  Tagged ports  : 7-8
  Untagged ports: 1-2

zte(cfg)#
```

Configuration of VLAN transparent transmission

This example describes how Switch A is connected to switch B through port 16. Port 1 of switch A and port 2 of switch B belong to VLAN2, and port 3 of switch A and port 4 of switch B belong to VLAN3. Members of the same VLAN can communicate with each other. This is shown in Figure 24.

FIGURE 24 VLAN TRANSPARENT TRANSMISSION



Switch A configuration

```
zte(cfg)#set vlan 2 add port 16 tag
zte(cfg)#set vlan 2 add port 1 untag
zte(cfg)#set vlan 3 add port 16 tag
zte(cfg)#set vlan 3 add port 3 untag
zte(cfg)#set port 1 pvid 2
zte(cfg)#set port 3 pvid 3
zte(cfg)#set vlan 2-3 enable
```

Switch B configuration

```
zte(cfg)#set vlan 2 add port 16 tag
zte(cfg)#set vlan 2 add port 2 untag
zte(cfg)#set vlan 3 add port 16 tag
zte(cfg)#set vlan 3 add port 4 untag
zte(cfg)#set port 2 pvid 2
zte(cfg)#set port 4 pvid 3
zte(cfg)#set vlan 2-3 enable
```

Introduction to FDB

MAC Address Table

Media Access Control (MAC) address is the hardware identification of a network device, based on which the switch forwards packets. MAC address is unique, ensuring accurate packet forwarding.

Each switch maintains a MAC address table called forwarding database (FDB). FDB records one-to-one mapping relationship between MAC addresses and switch ports. Upon receiving a data frame, the switch decides whether to drop it or forward it to the proper port based on this table. The FDB is the basis and prerequisite for fast forwarding.

MAC Table Operations

MAC table operations include the configuration of MAC filter function, static address binding function, and MAC table aging time.

MAC filter function

MAC filter function is to enable the switch to discard the received data packets whose source or destination MAC address is the specified MAC address. There are 3 filter mode:according to source mac address filter, destination mac addressfilter & both of them.

Static address binding function

Static address binding function is to bind the specified MAC address with the switch port. After the binding, this MAC is kept away from the dynamic study.

MAC table aging time

MAC table aging time refers to the period from the latest update of dynamic MAC address in the FDB table to the deletion of this address.

Configuration of the MAC filter function and static address binding function prevents illegal access to the network and fraudulent use of key MAC addresses, and play an important role in ensuring the network security.

Configuring FDB

Purpose

This topic describes the configuration of FDB.

Steps

For the configuration of FDB, perform the following steps.

1. To add the static binding address to the address table, use command **set fdb add** <*xx. xx. xx. xx. xx. xx*> **vlan** <*1-4094*> {**port** <*portid*>|**trunk** <*trunkid*>} in global configuration mode. This is shown in Table 78.

TABLE 78 SET FDB ADD VLAN COMMAND

Format	Mode	Function
set fdb add <*xx. xx. xx. xx. xx. xx*> **vlan** <*1-4094*> {**port** <*portid*>|**trunk** <*trunkid*>}	Global config	This adds the static binding address to the address table

Result: This adds the static binding address to the address table.

2. To set the aging time of MAC address, use command **set fdb agingtime <40-1260>** in global configuration mode. This is shown in Table 79.

TABLE 79 SET FDB AGINGTIME COMMAND

Format	Mode	Function
set fdb agingtime <40-1260>	Global config	This sets the aging time of MAC address

Result: This sets the aging time of MAC address.

3. To delete a record in the table, use command **set fdb delete** <xx. xx. xx. xx. xx. xx> **vlan** <1-4094> in global configuration mode. This is shown in Table 80.

TABLE 80 SET FDB DELETE COMMAND

Format	Mode	Function

Format	Mode	Function
set fdb delete <xx. xx. xx. xx. xx. xx> **vlan** <1-4094>	Global config	This deletes a record in the table

Result: This deletes a record in the table.

4. To set the filter address of fdb, use command **set fdb filter<**xx. xx. xx. xx. xx. xx**>vlan**<1-4094> **{dest_mac|src_mac|both}**in global configuration mode. This is shown in Table 81.

TABLE 81 SET FDB FILTER COMMAND

Format	Mode	Function
set fdb filter <xx. xx. xx. xx. xx. xx>**vlan**<1-4094> **{dest_mac|src_mac|both}**	Global config	This sets the filter address of fdb

Result: This sets the filter address of fdb.

5. To display fdb information, use command **show fdb** [**static|dynamic|filter**] [**detail]** in global configuration mode. This is shown in Table 82.

TABLE 82 SHOW FDB COMMAND

Format	Mode	Function
show fdb [**static|dynamic|filter**] **{detail}**	Global config	This displays fdb information

Result: This displays fdb information.

6. To display the aging time of fdb address, use command **show fdb agingtime** in global configuration mode. This is shown in Table 83.

TABLE 83 SHOW FDB AGINGTIME COMMAND

Format	Mode	Function
show fdb agingtime	Global config	This displays the aging time of fdb address

Result: This displays the aging time of fdb address.

7. To display the MAC-based fdb information, use command **show fdb mac** <xx. xx. xx. xx. xx. xx> in global configuration mode. This is shown in Table 84.

TABLE 84 SHOW FDB MAC COMMAND

Format	Mode	Function
show fdb mac <xx. xx. xx. xx. xx. xx>	Global config	This displays the MAC-based fdb information

Result: This displays the MAC-based fdb information.

8. To display the port-based fdb information, use command **show fdb port** <portname> **{detail}** in global configuration mode. This is shown in Table 85.

TABLE 85 SHOW FDB PORT COMMAND

Format	Mode	Function
show fdb port <portname> **{detail}**	Global config	This displays the port-based fdb information

Result: This displays the port-based fdb information.

9. To display Trunk fdb information, use command **show fdb trunk** <trunkname> **[detail]**in global configuration mode. This is shown in Table 86.

TABLE 86 SHOW FDB TRUNK COMMAND

Format	Mode	Function
show fdb trunk <trunkname> **{detail}**	Global config	This displays Trunk fdb information

Result: This displays Trunk fdb information.

10. To display the VLAN-based fdb information, use command **show fdb vlan** <vlanname> **[detail]**in global configuration mode. This is shown in Table 87.

TABLE 87 SHOW FDB VLAN COMMAND

Format	Mode	Function
show fdb vlan <vlanname>**[detail]**	Global config	This displays VLAN-based fdb information

Result: This displays VLAN-based fdb information.

END OF STEPS

Result FDB is configured on the switch.

LACP Overview

LACP Link Aggregation Control Protocol (LACP) follows IEEE 802. 3ad standards.

Description Link aggregation means that physical links with same transmission media and transmission rate are "bound" together, making them look like one link logically. This concept is also known as Trunking. It allows parallel physical links between the switches or between the switch and server to increase the bandwidth in multiples and simultaneously. As a result, it becomes an import technology in broadening link bandwidth and creating link transmission flexibility and redundancy.

Aggregate Link Aggregated link is also called trunk. If a port of trunk is blocked or faulty, data packets will be distributed to other ports of this trunk for transmission. If this port recovers, data packets will be re-distributed to all the normal ports of this trunk for transmission.

ZXR10 2920/2928/2952 supports a maximum of 15 aggregation groups. In each aggregation group, number of links participating in aggregation does not exceed eight. Links participating in the aggregation must have same transmission media type and same transmission rate.

Configuring LACP

Purpose This topic describes the configuration of link aggregation.

Steps For configuration of link aggregation, perform the following steps.

1. To Enable/Disable the LACP function, use command **set lacp {enable|disable}** in global configuration mode. This is shown in Table 88.

TABLE 88 SET LACP COMMAND

Format	Mode	Function
set lacp {enable|disable}	Global config	This Enable/Disable the LACP function

Result: This Enable/Disable the LACP function.

Note: By default, the LACP function is disabled.

2. To add a specified port to the aggregation group, use command **set lacp aggregator** <trunkid> **add port** <portlist> in global configuration mode. This is shown in Table 89.

TABLE 89 SET LACP AGGREGATOR COMMAND

Format	Mode	Function
set lacp aggregator <trunkid> **add port** <portlist>	Global config	This adds a specified port to the aggregation group

Result: This adds a specified port to the aggregation group.

3. To delete a specified port to the aggregation group, use command **set lacp aggregator** <trunkid> **delete port** <portlist> in global configuration mode. This is shown in Table 90.

TABLE 90 SET LACP AGGREGATOR DELETE COMMAND

Format	Mode	Function
set lacp aggregator <trunkid> **delete port** <portlist>	Global config	This deletes a specified port to the aggregation group

Result: This deletes a specified port to the aggregation group.

4. To set aggregation mode of the aggregation group, use command **set lacp aggregator** <trunkid> **mode {dynamic|static|mixed}** in global configuration mode. This is shown in Table 91.

TABLE 91 SET LACP AGGREGATOR MODE COMMAND

Format	Mode	Function
set lacp aggregator <trunkid> **mode {dynamic|static|mixed}**	Global config	This sets aggregation mode of the aggregation group

Result: This sets aggregation mode of the aggregation group.

5. To set the mode used by the port to participate in the aggregation, use command **set lacp port** <portlist> **mode {active|passive}** in global configuration mode. This is shown in Table 92.

TABLE 92 SET LACP PORT MODE COMMAND

Format	Mode	Function
set lacp port <portlist> **mode {active|passive}**	Global config	This sets the mode used by the port to participate in the aggregation

Result: This sets the mode used by the port to participate in the aggregation.

6. To configure the timeout information of the port participating in the aggregation, use command **set lacp port** <portlist> **timeout {long|short}** in global configuration mode. This is shown in Table 93.

TABLE 93 SET LACP PORT TIMEOUT COMMAND

Format	Mode	Function
set lacp port <portlist> **timeout {long|short}**	Global config	This configures the timeout information of the port participating in the aggregation

Result: This configures the timeout information of the port participating in the aggregation.

5. To set the priority of LACP, use command **set lacp priority** <1-65535> in global configuration mode. This is shown in Table 94.

TABLE 94 SET LACP PRIORITY COMMAND

Format	Mode	Function
set lacp priority <1-65535>	Global config	This sets the priority of LACP

Result: This sets the priority of LACP.

6. To display the LACP configuration information, use command **show lacp** in global configuration mode. This is shown in Table 95.

TABLE 95 SHOW LACP COMMAND

Format	Mode	Function
show lacp	Global config	This displays the LACP configuration information

Result: This displays the LACP configuration information.

7. To display the aggregation information about the LACP aggregation group, use command **show lacp aggregator** [<trunkid>] in global configuration mode. This is shown in Table 96.

TABLE 96 SHOW LACP AGGREGATOR COMMAND

Format	Mode	Function
show lacp aggregator [<trunkid>]	Global config	This displays the aggregation information about the LACP aggregation group

Result: This displays the aggregation information about the LACP aggregation group.

8. To display the information of the port where the LACP is involved in the aggregation, use command **show lacp port** [<portlist >] in global configuration mode. This is shown in TABLE 99 .

TABLE 99 SHOW LACP PORT COMMAND

Format	Mode	Function
show lacp port [<portlist >] in	Global config	This displays the information of the port where the LACP is involved in the aggregation

Result: This displays the information of the port where the LACP is involved in the aggregation.

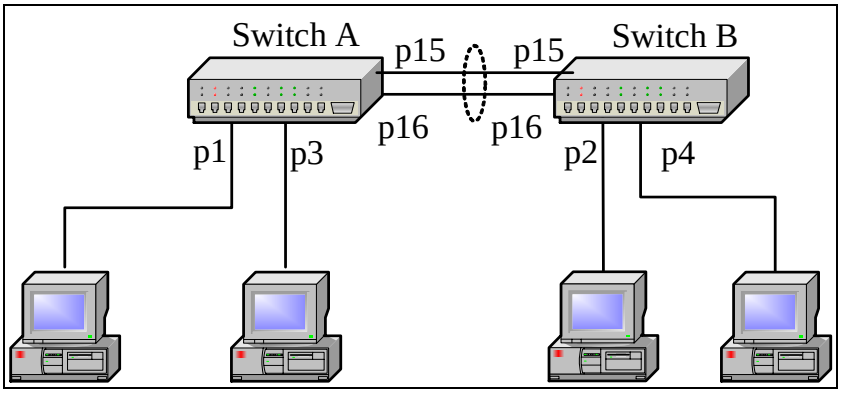
END OF STEPS

Result Link aggregation is configured.

Note After the configuration of the aggregation group, various settings can be performed on it, such as setting the PVID, adding it to the VLAN, setting the static binding MAC address, and so on.

Example This example describes that switch A and switch B are connected through aggregation port (binding the port 15 and port 16). Port 1 of switch A and port 2 of switch B belong to VLAN2. Port 3 of switch A and port 4 of switch B belong to VLAN2. Members of same VLAN can communicate with each other. This is shown in Figure 25.

FIGURE 25 LACP CONFIGURATION



Configuration of switch A

```
zte(cfg)#set lacp enable
zte(cfg)#set lacp aggregator 3 add port 15-16
zte(cfg)#set lacp aggregator 3 mode dynamic
zte(cfg)#set vlan 2 add trunk 3 tag
zte(cfg)#set vlan 2 add port 1 untag
zte(cfg)#set vlan 3 add trunk 3 tag
zte(cfg)#set vlan 3 add port 3 untag
zte(cfg)#set port 1 pvid 2
zte(cfg)#set port 3 pvid 3
zte(cfg)#set vlan 2-3 enable
```

Configuration of switch B

```
zte(cfg)#set lacp enable
zte(cfg)#set lacp aggregator 3 add port 15-16
zte(cfg)#set lacp aggregator 3 mode dynamic
zte(cfg)#set vlan 2 add trunk 3 tag
zte(cfg)#set vlan 2 add port 2 untag
zte(cfg)#set vlan 3 add trunk 3 tag
zte(cfg)#set vlan 3 add port 4 untag
zte(cfg)#set port 2 pvid 2
zte(cfg)#set port 4 pvid 3
zte(cfg)#set vlan 2-3 enable
```

IGMP Snooping

Drawback of IGMP snooping

Multicast address cannot appear in source address of the packet, switch cannot learn multicast address. When the switch receives a multicast message, it broadcasts the message to all the ports in the same VLAN. If no measure is taken, unwanted multicast message may be spreaded to each node of the network, thus causing a great waste of network bandwidth resource.

With IGMP Snooping function, IGMP communication between host and router is snooped, so that multicast packets are sent to the ports in the multicast forwarding table, instead of all ports. This restricts the wide spread of multicast messages in the LAN switch, reduces the waste of network bandwidth, and improves the utilization rate of the switch.

Configuring IGMP Snooping

Purpose

This topic describes the IGMP snooping configuration.

Steps

For configuration of IGMP snooping, perform the following steps.

1. To Enable/Disable the IGMP Snooping function, use command **set igmp snooping {enable|disable}** in global configuration mode. This is shown in Table 97.

TABLE 97 SET IGMP SNOOPING COMMAND

Format	Mode	Function
set igmp snooping {enable|disable}	Global config	This Enable/Disable the IGMP Snooping function

Result: This Enable/Disable the IGMP Snooping function.

2. To add the IGMP Snooping function for the specified VLAN, use command **set igmp snooping add vlan** <vlanlist> in global configuration mode. This is shown in Table 98.

TABLE 98 SET IGMP SNOOPING ADD VLAN COMMAND

Format	Mode	Function
set igmp snooping add vlan <vlanlist>	Global config	This adds the IGMP Snooping function for the specified VLAN

Result: This adds the IGMP Snooping function for the specified VLAN.

3. To set crossvlan monitor, use command **set igmp snooping crossvlan** {**enable|disable**} in global configuration mode. This is shown in Table 100.

TABLE 99 SET IGMP SNOOPING DELETE VLAN COMMAND

Format	Mode	Function
set igmp snooping delete vlan <vlanlist>	Global config	This deletes the IGMP Snooping function for the specified VLAN

Result: This sets crossvlan monitor.

4. To delete the IGMP Snooping function for the specified VLAN, use command **set igmp snooping delete vlan** <vlanlist> in global configuration mode. This is shown in Table 100.

TABLE 100 SET IGMP SNOOPING DELETE VLAN COMMAND

Format	Mode	Function
set igmp snooping delete vlan <vlanlist>	Global config	This deletes the IGMP Snooping function for the specified VLAN

Result: This deletes the IGMP Snooping function for the specified VLAN.

5. To Enable/Disable the IGMP fastleave function, use command **set igmp snooping fastleave {enable|disable}** in global configuration mode. This is shown in Table 101 .

TABLE 101 SET IGMP SNOOPING FASTLEAVE COMMAND

Format	Mode	Function
set igmp snooping fastleave {enable|disable}	Global config	This Enable/Disable the IGMP fastleave function

Result: This Enable/Disable the IGMP fastleave function.

6. To set the last member snooping interval, use command **set igmp snooping last-member-query** <10-250> in global configuration mode.

Result: This sets the last member snooping interval.

7. To Enable/Disable the IGMP snooping function for the specified VLAN, use command **set igmp snooping query vlan** <vlanlist> **{enable|disable}** in global configuration mode. This is shown in Table 101.

TABLE 101 SET IGMP SNOOPING QUERY VLAN COMMAND

Format	Mode	Function
set igmp snooping query vlan <vlanlist> **{enable|disable}**	Global config	This Enable/Disable the IGMP Snooping function for the specified VLAN

Result: This Enable/Disable the IGMP Snooping function for the specified VLAN.

8. To set the snooping interval, use command **set igmp snooping query-interval** <10-2147483647> in global configuration mode. This is shown in Table 102.

TABLE 102 SET IGMP SNOOPING QUERY INTERVAL COMMAND

Format	Mode	Function
set igmp snooping query-interval <10-2147483647>	Global config	This sets the snooping interval

Result: This sets the snooping interval.

9. To set the snooping interval, use command **set igmp snooping response-interval** <10-250> in global configuration mode. This is shown in Table 103.

TABLE 103 SET IGMP SNOOPING RESPONSE INTERVAL COMMAND

Format	Mode	Function
set igmp snooping response-	Global config	This sets the snooping interval

Format	Mode	Function
interval <10-250>		

Result: This sets the snooping interval.

10. To set multicast member/route timeout, use command **set igmp snooping timeout** <100-2147483647> **{host|router}** in global configuration mode. This is shown in Table 104.

TABLE 104 SET IGMP SNOOPING TIMEOUT COMMAND

Format	Mode	Function
set igmp snooping timeout <100-2147483647> **{host|router}**	Global config	This sets multicast member/route timeout

Result: This sets multicast member/route timeout.

11. To bind static multicast group to ports on Vlan, use command **set igmp snooping vlan <**1-4094> **add group** <A. B. C. D> [**port** <portlist> |**trunk** <trunklist>] in global configuration mode. This is shown in Table 105.

TABLE 105 STATIC MULTICAST GROUP TO PORTS COMMAND

Format	Mode	Function
set igmp snooping vlan <1-4094> **add group** <A. B. C. D>[**port** <portlist>| **trunk** <trunklist>]	Global config	This binds static multicast group to ports on Vlan

Result: This binds static multicast group to ports on Vlan.

12. To delete a static multicast group, use command **set igmp snooping vlan** <vlanname> **delete group** <A. B. C. D> in global configuration mode. This is shown in Table 106.

TABLE 106 SET IGMP SNOOPING VLAN DELETE COMMAND

Format	Mode	Function
set igmp snooping vlan <vlanname> **delete group** <A. B. C. D>	Global config	This deletes a static multicast group

Result: This deletes a static multicast group.

13. To bind static multicast group based on port or aggregation to ports on Vlan, use command **set igmp snooping vlan <**1-4094> **add group** <A. B. C. D> [**port** <portlist> |**trunk** <trunklist>] in global configuration mode. This is shown in Table 105.

TABLE 107 STATIC MULTICAST GROUP TO PORTS COMMAND

Format	Mode	Function
set igmp snooping vlan <1-4094> **add group** <A. B. C. D>[**port** <portlist>| **trunk** <trunklist>]	Global config	This binds static multicast group to ports on Vlan

Result: This binds static multicast group to ports on Vlan.

14. To unbind static multicast group from ports, use command **set igmp snooping vlan** <1-4094> **delete group** <A. B. C. D>[**port** <portlist>| **trunk** <trunklist>] in global configuration mode. This is shown in Table 108.

TABLE 108 SET IGMP SNOOPING VLAN DELETE GROUP PORT COMMAND

Format	Mode	Function
set igmp snooping vlan <1-4094> **delete group** <A. B. C. D>[**port** <portlist>|**trunk<**trunklist**>**	Global config	This unbinds static multicast group from ports

Result: This unbinds static multicast group from ports.

15. To add static multicast router port to a Vlan, use command **set igmp snooping vlan** <1-4094> **add smr** [**port** <portlist> | **trunk** <*trunklist*>] in global configuration mode. This is shown in Table 109.

TABLE 109 SET IGMP SNOOPING VLAN ADD SMR PORT COMMAND

Format	Mode	Function
set igmp snooping vlan <1-4094> **add smr** [**port** <portlist>	**trunk** <*trunklist*>]	Global config	This adds static multicast router port to a Vlan

Result: This adds static multicast router port to a Vlan.

16. To unbind static multicast group from ports, use command **set igmp snooping vlan** <1-4094> **delete**

group <A. B. C. D> [**port** <portlist>| **trunk** <trunklist>] in global configuration mode. This is shown in Table 108.

TABLE 110 SET IGMP SNOOPING VLAN DELETE GROUP PORT COMMAND

Format	Mode	Function
set igmp snooping vlan <1-4094> **delete group** <A. B. C. D>[**port** <portlist>| **trunk** <trunklist>]	Global config	This unbinds static multicast group from a VLAN

Result: This unbinds static multicast group from a VLAN.

17. To add maximum multicast group numbers to Vlan, use command **set igmp snooping add maxnum** <1-256> **vlan** <vlanlist> in global configuration mode. This is shown in Table 111.

TABLE 111 SET IGMP SNOOPING ADD MAXNUM VLAN COMMAND

Format	Mode	Function
set igmp snooping add maxnum <1-256> **vlan** <vlanlist>	Global config	This adds maximum multicast group numbers to Vlan

Result: This adds maximum multicast group numbers to Vlan.

18. To delete maximum multicast group number from Vlan, use command **set igmp snooping delete maxnum vlan** <vlanlist> in global configuration mode. This is shown in Table 112.

TABLE 112 SET IGMP SNOOPING DELETE MAXNUM VLAN COMMAND

Format	Mode	Function
set igmp snooping delete maxnum vlan <vlanlist>	Global config	This deletes maximum multicast group number from Vlan

Result: This deletes maximum multicast group number from Vlan.

4. To Enable/Disable the IGMP filter, use command **set igmp filter {enable|disable}** in global configuration mode. This is shown in Table 113.

TABLE 113 SET IGMP FILTER COMMAND

Format	Mode	Function
set igmp filter {enable|disable}	Global config	This Enable/Disable the IGMP filter

Result: This Enable/Disable the IGMP filter.

5. To add filter on Vlan multicast group, use command **set igmp filter add groupip** <A. B. C. D> **vlan** <vlanlist> in global configuration mode. This is shown in Table 114.

TABLE 114 SET IGMP FILTER ADD GROUPIP VLAN COMMAND

Format	Mode	Function
set igmp filter add groupip <A. B. C. D> **vlan** <vlanlist>	Global config	This adds filter on Vlan multicast group

Result: This adds filter on Vlan multicast group.

6. To delete source Ip of Vlan from filter, use command **set igmp filter delete groupip** <A. B. C. D> **vlan** <vlanlist> in global configuration mode. This is shown in Table 115.

TABLE 115 SET IGMP FILTER DELETE GROUPIP VLAN COMMAND

Format	Mode	Function
set igmp filter delete groupip <A. B. C. D> **vlan** <vlanlist>	Global config	This deletes source Ip of Vlan from filter

Result: This deletes source Ip of Vlan from filter.

7. To add the filter of multicast source address based on Vlan, use command **set igmp filter add sourceip** <A. B. C. D> **vlan** <vlanlist> in global configuration mode. This is shown in Table 116.

TABLE 116 SET IGMP FILTER ADD SOURCEIP VLAN COMMAND

Format	Mode	Function
set igmp filter add sourceip <A. B. C. D> **vlan** <vlanlist>	Global config	This adds the filter of multicast source address based on Vlan

Result: This adds the filter of multicast source address based on Vlan.

8. To delete filter of multicast source address based on Vlan, use command **set igmp filter delete sourceip** <A. B. C. D> **vlan** <vlanlist> in global configuration mode. This is shown in Table 117.

TABLE 117 SET IGMP FILTER DELETE SOURCEIP VLAN COMMAND

Format	Mode	Function
set igmp filter delete sourceip <A. B. C. D> **vlan** <vlanlist>	Global config	This deletes filter of multicast source address based on Vlan

Result: This deletes filter of multicast source address based on Vlan.

9. To display the configuration of IGMP snooping, use command **show igmp snooping** in global configuration mode. This is shown in Table 118.

TABLE 118 SHOW IGMP SNOOPING COMMAND

Format	Mode	Function
show igmp snooping	Global config	This displays the configuration of IGMP snooping

Result: This displays the configuration of IGMP snooping.

10. To display the configuration of IGMP snooping result, use command **show igmp snooping vlan** [<vlanname> [**host|router**]] in global configuration mode. This is shown in Table 119.

TABLE 119 SHOW IGMP SNOOPING VLAN COMMAND

Format	Mode	Function
show igmp snooping vlan [<vlanname> [**host|router**]]	Global config	This displays the configuration of IGMP snooping result

Result: This displays the configuration of IGMP snooping result.

11. To displays the configuration of IGMP filter, use command **show igmp filter** in global configuration mode. This is shown in Table 120.

TABLE 120 SHOW IGMP FILTER COMMAND

Format	Mode	Function
show igmp filter	Global config	This displays the configuration of IGMP filter

Result: This displays the configuration of IGMP filter.

12. To display the multicast snooping results, use command **show igmp filter vlan** <1-4094> in global configuration mode. This is shown in Table 121.

TABLE 121 SHOW IGMP FILTER VLAN COMMAND

Format	Mode	Function
show igmp filter vlan <1-4094>	Global config	This displays the multicast snooping results

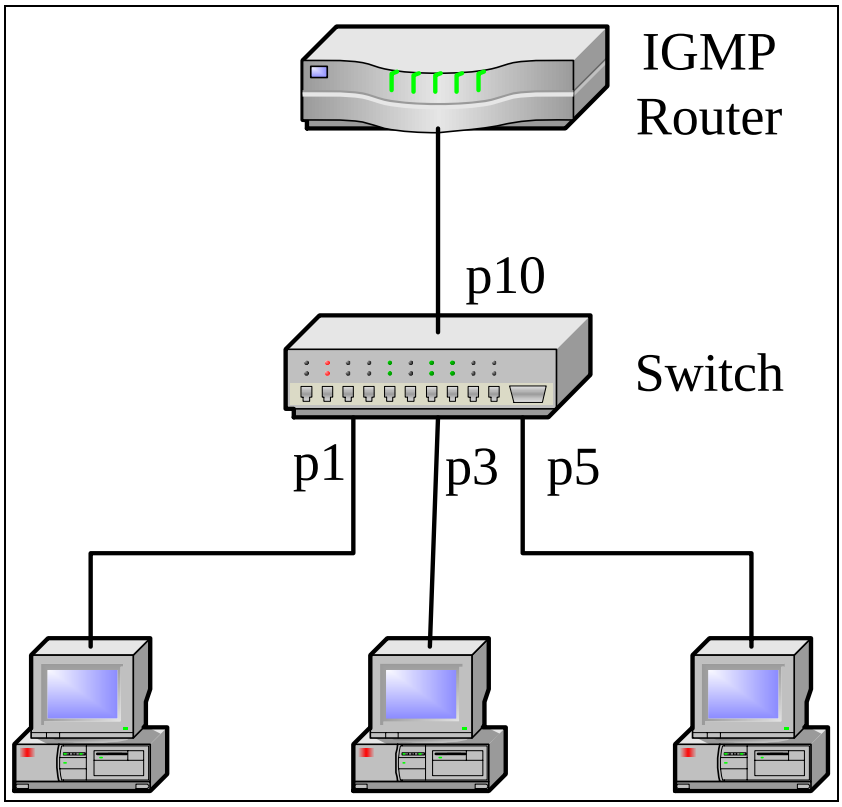
Result: This displays the multicast snooping results.

END OF STEPS

Result IGMP snooping has been configured

Example This example describes IGMP snooping function. Ports 1, 3, and 5 are connected to the host. Port 10 is connected to the router. The one-to-multiple communication mode is implemented. That is, port 10 can communicate with ports 1, 3, and 5, but ports 1, 3, and 5 cannot communicate with each other. The IGMP Snooping function of the switch is enabled and the snooping results are displayed. This is shown in Figure 26.

FIGURE 26 NETWORK TOPOLOGY



Configuration

```
zte(cfg)#set vlan 200 add port 1, 3, 5, 10 untag
zte(cfg)#set vlan 210 add port 1, 10 untag
zte(cfg)#set vlan 230 add port 3, 10 untag
zte(cfg)#set vlan 250 add port 5, 10 untag
zte(cfg)#set port 10 pvid 200
zte(cfg)#set port 1 pvid 210
zte(cfg)#set port 3 pvid 230
zte(cfg)#set port 5 pvid 250
zte(cfg)#set vlan 200, 210, 230, 250 enable
zte(cfg)#set igmp snooping enable
zte(cfg)#set igmp snooping add vlan 200, 210, 230, 250
zte(cfg)#set igmp snooping crossvlan disable
```

Multicast snooping result

```
zte(cfg)#show igmp snooping vlan

Num    VlanId    Group                          Last_Report
PortMember
1    210      224.   1.   1.   1         192.   168.   1.
1      1
2    230      224.   1.   1.   1         192.   168.   1.
2      3
3    250      224.   1.   1.   1         192.   168.   1.
3      5
```

Enable multi-VLAN IGMP snooping function of the switch and display the snooping results:

```
zte(cfg)#set igmp snooping crossvlan enable
zte(cfg)#show igmp snooping vlan
Num    VlanId    Group                          Last_Report
PortMember
1    210      224.   1.   1.   1         192.   168.   1.
1      1
2    230      224.   1.   1.   1         192.   168.   1.
2      3
3    250      224.   1.   1.   1         192.   168.   1.
3      5
4    200      224.   1.   1.   1         192.   168.   1.
3      1, 3, 5, 10
```

This example describes IGMP snooping and filter. Port 1, 3, 5 connected to the host. Port 10 is connected to the router. Port 1, 3, 5 join port 10 to Vlan 200. Port 1, 3, 5 on user transmits the group address separately for 230. 44. 45. 167, 230. 44. 45. 157 multicast joins the request, increases

multicast filtration group address 230. 44. 45. 167 on Vlan 200. Enable IGMP Snooping and IGMP on filter function. This is shown in Figure 26.

```
zte(cfg)#set vlan 200 add port 1, 3, 5, 10 untag
zte(cfg)#set port 1, 3, 5, 10 pvid 200
zte(cfg)#set vlan 200 enable
zte(cfg)#set igmp snooping enable
zte(cfg)#set igmp snooping add vlan 200
zte(cfg)#set igmp filter enable
zte(cfg)#set igmp filter groupip 230.    44.    45.    167
vlan 200
```

Display IGMP snooping and filter

```
zte(cfg)#show igmp snooping vlan
  Num    VlanId    Group                          Last_Report
PortMember
  1    200      230.   44.   45.   157    192.   168.   1.
1      1, 3, 5, 10

zte(cfg)#sho igmp filter
  IGMP Filter: enabled
  Index  FilterIpAddress     Vlan                      Port
    Type
  ----- ---------------- -------------- -------------- ---
    ------
  1      230.   44.   45.   167     200               ----
    --          Groupip

zte(cfg)#show igmp filter vlan 200
  Maximal group number: 256
  Current group number: 0
  The filter address list of this vlan:
  Index FilterIpAddress  Vlan   Type
  ----- ---------------- -----  ------
  1      230.   44.   45.   167     200    Groupip
```

Internet Protocol Television

Introduction to IPTV

Internet Protocol television (IPTV) is also called Interactive Network TV. IPTV is a method of distributing television content over IP that enables a more customized and interactive user experience. IPTV could allow people who were separated geographically to watch a movie together, while chatting and exchanging files simultaneously. IPTV uses a two-way

broadcast signal sent through the provider's backbone network and servers, allowing viewers to select content on demand, and take advantage of other interactive TV options. IPTV can be used through PC or "IP machine box + TV".

Configuring IPTV Global Parameters

Purpose This topic describes the configuration of IPTV.

Steps For the configuration of IPTV, perform the following steps.

1. To set the least view time, use command **iptv control log-time**<1-65534> in nas config mode. This is shown in Table 122.

TABLE 122 IPTV CONTROL LOG-TIME COMMAND

Format	Mode	Function
iptv control log-time<1-65534>	nas config mode	This sets the least view time

Result: This sets the least view time.

2. To set the max preview counts on global, use command **iptv control prvcount count** in nas config mode. This is shown in Table 123.

TABLE 123 IPTV CONTROL PRVCOUNT COUNT COMMAND

Format	Mode	Function
iptv control prvcount count	nas config mode	This sets the max preview counts on global

Result: This sets the max preview counts on global.

3. To set the least preview interval of global, use command **iptv control prvinterval** in nas config mode. This is shown

TABLE 124 IPTV CONTROL PRVINTERVAL COMMAND

Format	Mode	Function
iptv control prvinterval	nas config mode	This sets the least preview interval of global

Result: This sets the least preview interval of global.

4. To set the max preview time of global, use command **iptv control prvtime** in nas config mode. This is shown in Table 125.

TABLE 125 IPTV CONTROL PRVTIME COMMAND

Format	Mode	Function
iptv control prvtime	nas config mode	This sets the max preview time of global

Result: This sets the max preview time of global.

5. To set the period of global reset preview counts, use command **iptv control prvcount reset-period** in nas config mode. This is shown in Table 126.

TABLE 126 IPTV CONTROL PRVCOUNT RESET-PERIOD COMMAND

Format	Mode	Function
iptv control prvcount reset-period	nas config mode	This sets the period of global reset preview counts

Result: This sets the period of global reset preview counts.

6. To enable/disable IPTV, use command **iptv control {enable|disable}** in nas config mode. This is shown in Table 127.

TABLE 127 IPTV CONTROL COMMAND

Format	Mode	Function
iptv control {enable|disable}	nas config mode	This enable/disable IPTV

Result: This enable/disable IPTV.

END OF STEPS

Result IPTV has been configured.

Configuring IPTV Channels

Purpose This topic describes the configuration of IPTV channels.

Steps For the configuration of IPTV channels, perform the following steps.

1. To create channels of IPTV, use command **create iptv channel** <channellist> in nas config mode. This is shown in Table 128.

TABLE 128 CREATE IPTV CHANNEL COMMAND

Format	Mode	Function
create iptv channel	Nas config mode	This creates channels of IPTV

Format	Mode	Function
<channellist>		

Result: This creates IPTV channels.

2. To set the name of a channel, use command **iptv channel** <channellist> **name** in nas config mode. This is shown in Table 129.

TABLE 129 IPTV CHANNEL COMMAND

Format	Mode	Function
iptv channel <channellist> **name**	Nas config mode	This sets the name of a channel

Result: This sets the name of a channel.

3. To set a channel belonging to a multicast Vlan, use command **iptv channel** <channellist> **mvlan** in nas config mode. This is shown in Table 130.

TABLE 130 IPTV CHANNEL MVLAN COMMAND

Format	Mode	Function
iptv channel <channellist> **mvlan**	Nas config mode	This sets a channel belonging to a multicast Vlan

Result: This sets a channel belonging to a multicast Vlan.

4. To delete a channel, use command **clear iptv channel** <channellist> in nas config mode. This is shown in Table 131.

TABLE 131 CLEAR IPTV CHANNEL COMMAND

Format	Mode	Function
clear iptv channel <channellist>	Nas config mode	This deletes a channel

Result: This deletes a channel.

END OF STEPS

Result IPTV channels have been configured.

Configuring Channel Access Control (CAC)

Purpose This topic describes the configuration of CAC.

Steps For the configuration of CAC, perform the following steps.

1. To create rules of CAC, use command **create iptv cac-rule** <rule id> in nas config mode. This is shown in Table 132.

TABLE 132 CREATE IPTV CAC-RULE COMMAND

Format	Mode	Function
create iptv cac-rule <rule id>	Nas config mode	This creates rules of CAC

Result: This creates rules of CAC.

2. To set the name of CAC rule, use command **iptv cac-rule**<rulelist> **name** in nas config mode. This is shown in Table 133.

TABLE 133 IPTV CAC-RULE COMMAND

Format	Mode	Function
iptv cac-rule<rulelist> **name**	Nas config mode	This sets the name of CAC rule

Result: This sets the name of CAC rule.

3. To set maximum preview counts of rules, use command **iptv cac-rule** <rulelist> **prvcount** in nas config mode. This is shown in Table 134.

TABLE 134 IPTV CAC-RULE PRVCOUNT COMMAND

Format	Mode	Function
iptv cac-rule<rulelist> **prvcount**	Nas config mode	This sets maximum preview count of rules

Result: The sets maximum preview count of rules.

4. To set maximum preview time of rules, use command **iptv cac-rule** <rulelist> **prvtime** in nas config mode. This is shown in Table 135.

TABLE 135 IPTV CAC-RULE PRVTIME COMMAND

Format	Mode	Function
iptv cac-rule<rulelist> **prvtime**	Nas config mode	This sets max preview time of rules

Result: This sets maximum preview time of rules.

5. To set the least preview interval of rules, use command **iptv cac-rule** <rulelist> **prvinterval** in nas config mode. This is shown in Table 136.

TABLE 136 IPTV CAC-RULE PRVINTERVAL COMMAND

Format	Mode	Function
iptv cac-rule <rulelist> **prvinterval**	Nas config mode	This sets least preview interval of rules

Result: This sets the least preview interval of rules.

6. To set the right rule to channel, use command **iptv cac-rule** <rulelist> **right** in nas config mode. This is shown in Table 137.

TABLE 137 IPTV CAC-RULE RIGHT COMMAND

Format	Mode	Function
iptv cac-rule <rulelist> **right**	Nas config mode	This sets the right rule to channel

Result: This sets the right rule to channel.

7. To delete rules, use command **clear iptv cac-rule** <rulelist> in nas config mode. This is shown in Table 138.

TABLE 138 CLEAR IPTV CAC-RULE COMMAND

Format	Mode	Function
clear iptv cac-rule <rulelist>	Nas config mode	This deletes the rules

Result: This deletes the rules.

END OF STEPS

Result CAC has been configured.

Configuring Administrative Command of IPTV Users

Purpose This topic describes the configuration of administrative command of IPTV users.

Steps For the configuration of administrative command of IPTV users, perform the following step.

1. To delete online users of IPTV, use command **clear iptv client** on nas config mode. This is shown in Table 139.

TABLE 139 CLEAR IPTV CLIENT COMMAND

Format	Mode	Function
clear iptv client	Nas config mode	This deletes online users

Result: This deletes online users of IPTV.

END OF STEPS

Result Administrative commands of IPTV users have been configured.

Example This example describes how the user connects to port gei_1/1 which is a requesting user of multicast group 224. 1. 1. 1. Vlan ID of this multicast group is 100. Configuration is shown below:

```
ZXR10(config-nas)# iptv control enable
ZXR10(config-nas)# create iptv channel special 1 address
224.   1.   1.   1
ZXR10(config-nas)# iptv channel 1 mvlan 100
ZXR10(config-nas)# iptv channel 1 name cctv1
ZXR10(config-nas)# create iptv cac-rule 1 port gei_1/1
ZXR10(config-nas)# iptv cac-rule 1 right order 1
```

User in Vlan 1

User which connects to port gei_1/1 in Vlan 1 is the preview user of multicast group 224. 1. 1. 1. Max preview time is 2 minutes. Least preview interval is for 20 seconds. Max preview counts are 10. Vlan ID of multicast group is 100. Configuration is shown below.

```
ZXR10(config-nas)# iptv control enable
ZXR10(config-nas)# create iptv channel special 1 address
224.   1.   1.   1
ZXR10(config-nas)# iptv channel 1 mvlan 100
ZXR10(config-nas)# iptv channel 1 name cctv1
ZXR10(config-nas)# create iptv cac-rule 1 port gei_1/1
vlan 1
ZXR10(config-nas)# iptv cac-rule 1 prvcount 10
ZXR10(config-nas)# iptv cac-rule 1 prvtime 120
ZXR10(config-nas)# iptv cac-rule 1 prvinterval 20
ZXR10(config-nas)# iptv cac-rule 1 right preview 1
```

User which connects to port gei_1/1 wants to view all multicast groups in Vlan 100. Configuration is shown below.

```
ZXR10(config-nas)# iptv control enable
ZXR10(config-nas)# create iptv channel general 256
ZXR10(config-nas)# iptv channel 256 mvlan 100
ZXR10(config-nas)# create iptv cac-rule 1 port gei_1/1
ZXR10(config-nas)# iptv cac-rule 1 right order 256
```

Port gei_1/1 only permits receiving the requesting packets of multicast group 224. 1. 1. 1. Vlan ID of this multicast group is 100. Configuration is shown below.

```
ZXR10(config-nas)# iptv control enable
ZXR10(config-nas)# create iptv channel special 1 address
224.  1.  1.  1
ZXR10(config-nas)# iptv channel 1 mvlan 100
ZXR10(config-nas)# create iptv cac-rule 1 port gei_1/1
ZXR10(config-nas)# iptv cac-rule 1 right query 1
```

Maintenance and Diagnosis of IPTV

Purpose This topic describes the configuration of maintenance and diagnosis of IPTV.

Steps For the configuration of IPTV maintenance and diagnosis, perform the following steps:

1. To display the global configuration information of IPTV, use command **show iptv control** in privileged mode. This is shown in Table 140.

TABLE 140 SHOW IPTV CONTROL COMMAND

Format	Mode	Function
show iptv control	privileged mode	This displays the global configuration information of IPTV

Result: This displays the global configuration information of IPTV.

2. To display the channel information of IPTV, use command **show iptv channel** in privileged mode. This is shown in Table 141.

TABLE 141 SHOW IPTV CHANNEL COMMAND

Format	Mode	Function
show iptv channel	privileged mode	This displays the channel information of IPTV

Result: This displays the channel information of IPTV.

3. To display specific channel number and channel statistics information, use command **show iptv channel [id|name]** in privileged mode. This is shown in Table 142.

TABLE 142 SHOW IPTV CHANNEL ID/NAME COMMAND

Format	Mode	Function

Format	Mode	Function
show iptv channel [id|name	privileged mode	This displays specific channel number and channel statistics information

Result: This displays specific channel number and channel statistics information.

4. To display the CAC rule, use command **show iptv cac-rule** in privileged mode. This is shown in Table 143.

TABLE 143 SHOW IPTV CAC-RULE COMMAND

Format	Mode	Function
show iptv cac-rule	privileged mode	This displays CAC rule

Result: This displays CAC rule.

5. To display the CAC rule statistics, use command **show iptv cac-rule statistics** in privileged mode. This is shown in Table 144.

TABLE 144 SHOW IPTV CAC-RULE STATISTICS COMMAND

Format	Mode	Function
show iptv cac-rule statistics	privileged mode	This displays CAC rule statistics

Result: This displays CAC rule statistics.

6. To display online users of IPTV, use command **show iptv client** in privileged mode. This is shown in Table 145.

TABLE 145 SHOW IPTV CLIENT COMMAND

Format	Mode	Function
show iptv client	privileged mode	This displays online users of IPV

Result: This displays online users of IPTV.

7. To display online users of IPTV statistics, use command **show iptv client statistics** in privileged mode. This is shown in Table 145.

TABLE 146 SHOW IPTV CLIENT COMMAND

Format	Mode	Function
show iptv client statistics	privileged mode	This displays online users of IPV

Result: This displays online users of IPTV statistics.

END OF STEPS

Result Maintenance and diagnosis of IPTV has been configured.

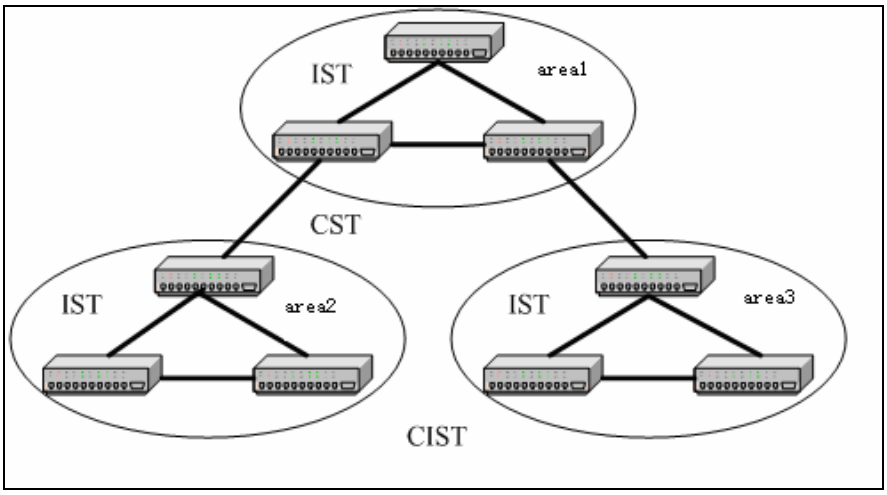
MSTP Mode

STP Spanning Tree Protocol (STP) is applicable to a loop network. It blocks some redundant paths with certain algorithms so that the loop network is pruned into a tree network without any loop, thus avoiding the hyperplasia and infinite loop of packets in the loop network.

RSTP Rapid Spanning Tree Protocol (RSTP) is on the basis of common STP, added with the mechanism that the port state can be rapidly changed from Blocking to Forwarding, which increases the topology convergence speed.

MSTP Multiple Spanning Tree Protocol (MSTP) is on the basis of RSTP and STP, added with the forwarding processing of frames with VLAN ID. The whole network topology structure can be planned into a Common and Internal Spanning Tree (CIST), which is divided into Common Spanning Tree (CST) and Internal Spanning Tree (IST), as shown in Figure 27.

FIGURE 27 MSTP TOPOLOGICAL STRUCTURE



In this whole MSTP topology structure, an IST can serve as a single bridge (switch). In this way, CTS can serve as an RSTP for the interaction of configuration information (BPDU). Multiple instances can be created in an IST area and these instances are valid only in this area. An instance is equivalent to an RSTP, except that the instance needs to perform BPDU interaction with bridges outside this area.

Spanning Tree Protocol (STP) can calculate accoding to the protocol. divide the ports into different parts:

Master:the port type introduced in MSTP protocol. When multiple different areas exist, the main port is the minimal pathcost port point to the root.

- Designated:the port transmits data to switch downward, & send STP protocol message to maintain the state of STP.
- Backup:the port receives the STP message. To prove that there exits a loop route to the port itself.
- Alternate:the port receives excess STP protocol message
- from other equipment . But when the original link abnormally lost, the port under this state can transfer to transmitting state, & maintain the network instead of the port lapsed.
- Edged:the port used to connect the terminal equipment, such as PC. The port set as the margin port do not participate in calculation when STP is turbulent & the state can switch fast.

According to port role, the state after the calculation being steady is shown in TABLE147 .

TABLE147 PORT ROLE & PORT STATE

Port role	Port state
Master	Forward
Root	Forward
Designated	Forward
Backup	Discard
Alternate	Discard
Edged	Forward

STP Spanning Tree Protocol (STP) is applicable to a loop network. It blocks some redundant paths with certain algorithms so that the loop network is pruned into a tree network without any loop, thus avoiding the hyperplasia and infinite loop of packets in the loop network.

BPDU Protection BPDU protect function is a particular protection for margin port. The margin port will not receive the protocol message . If there exists vicious protocol attack or Linux virtual bridge, receiving unlawful protocol message will bring to net shocking or topology changing abnormally. The port will be closed after using the protection. After a while, to check the net is normal or not. If it is normal, it will recovery to original state.

Root Protection Root protection is function is a particular protection for root switch. In the network that needs to appoint switch as root

switch, if there exists vicious protocol attack or Linux virtual bridge, it will bring to the change of the root & net abnormal. After using the root protection of the port, if the port receives the protocolinfo prior to root switch, it will transfer the port to blocking state, no longer transmit message, & discard the received protocol message to protect the status of the root switch.

Loop protection

Loop protection function is a particular protection for loop net topology. In the network that exists ring, redundant topology will be in the state of backup, & in the state of blocking after the port is steady. If there is no need to transfer to transmission state, it is possible to set port to loop protect. Once the port want to transform, it will inspire loop protection & set the port to blocking state.
When configuring one port, you can configure only one of the three protection:BPDU protection, root protection & loop protection.

Configuring STP

Purpose

This topic describes the STP configuration. In the default configuration, MSTP only has the instance with ins_id as 0. This instance always exists and cannot be manually deleted. This instance is mapped with VLANs 1 to 4094.

Steps

For the configuration of STP, perform the following steps.

1. To clear the STP instance, use command **clear stp instance** *<0-15>* in global configuration mode. This is shown in Table 151.

TABLE 147 SET STP COMMAND

Format	Mode	Function
clear stp instance ***<0-15>***	Global config	This clear the STP instance

Result: This clears the STP instance.

2. To clear the STP instance port cost, use command **clear stp instance** *<0-15>* **port** *<portname>* **cost** in global configuration mode. This is shown in Table 151.

TABLE 148 SET STP COMMAND

Format	Mode	Function
clear stp instance ***<0-15>*****port** **<**portname**>cost**	Global config	This clear the STP instance

Result: This clears the STP instance.

3. To clear the STP trunkcost, use command **clear stp instance** *<0-15>*trunk <trunkid>cost in global configuration mode. This is shown in Table 151.

TABLE 149 SET STP COMMAND

Format	Mode	Function
clear stp instance *<0-15>*trunk<trunkid>cost	Global config	This clear the STP instance trunkcost

Result: This clears the STP instance trunkcost.

4. To clear the STP name, use command **clear stp name***<0-15>*trunk <trunkid>cost in global configuration mode. This is shown in Table 151.

TABLE 150 SET STP COMMAND

Format	Mode	Function
clear stp name *<0-15>*	Global config	This clear the STP name

Result: This clears the STP name.

5. To Enable/Disable the STP, use command **set stp {enable|disable}** in global configuration mode. This is shown in Table 151.

TABLE 151 SET STP COMMAND

Format	Mode	Function
set stp {enable|disable}	Global config	This enable/disable the STP

Result: This is used to enable/disable the STP.

6. To set the STP aging time, use command **set stp agemax** <6-40> in global configuration mode. This is shown in Table 152.

TABLE 152 SET STP AGEMAX COMMAND

Format	Mode	Function
set stp agemax <6-40>	Global config	This sets the STP aging time

Result: This sets the STP aging time.

7. To set edge port, use command **set stp edge-port {add|delete} port** <portlist> in global configuration mode. This is shown in Table 153.

TABLE 153 SET STP EDGE PORT COMMAND

Format	Mode	Function
set stp edge-port {add|delete} port <portlist>	Global config	This sets edge port

Result: This sets edge port.

8. To set the STP forced version, use command **set stp forceversion {mstp|rstp|stp}** in global configuration mode. This is shown in Table 154.

TABLE 154 SET STP FORCEVERSION COMMAND

Format	Mode	Function
set stp forceversion {mstp|rstp|stp}	Global config	This sets the STP forced version

Result: This sets the STP forced version.

9. To set the STP forwarding delay time, use command **set stp forwarddelay** <4-30> in global configuration mode. This is shown in Table 155

TABLE 155 SET STP FORWARD DELAY COMMAND

Format	Mode	Function
set stp forwarddelay <4-30>	Global config	This sets STP forwarding delay time

Result: This sets STP forwarding delay time.

10. To set STP hello time, use command **set stp hellotime** <1-10> in global configuration mode. This is shown in Table 156.

TABLE 156 SET STP HELLOTIME COMMAND

Format	Mode	Function
set stp hellotime <1-10>	Global config	This sets hello time

11. To set stp hmd5 digest, use command **set stp hmd5-digest {CISCO|HUAWEI}** <0, 0x00. . 0-0xff. . f> in global configuration mode. This is shown in Table 157.

TABLE 157 SET STP HMD5 DIGEST COMMAND

Format	Mode	Function
set stp hmd5-digest {CISCO|HUAWEI}<0, 0x00. . 0-0xff. . f>	Global config	This sets stp hmd5 digest

Result: This sets hmd5 digest.

12. To set stp hmd5 key, use command **set stp hmd5-key {CISCO|HUAWEI}**<0, 0x00. . 0-0xff. . f> in global configuration mode. This is shown in Table 158.

TABLE 158 SET STP HMD5 KEY PORT COMMAND

Format	Mode	Function
set stp hmd5-key {CISCO|HUAWEI}<0, 0x00. . 0-0xff. . f>	Global config	This sets stp hmd5 key

Result: This sets stp hmd5 key.

13. To set the maximum number of hop between any two terminals of MST, use command **set stp hopmax** <1-40> in global configuration mode. This is shown in Table 159.

TABLE 159 SET STP HOPMAX COMMAND

Format	Mode	Function
set stp hopmax <1-40>	Global config	This sets the maximum number of hop between any two terminal of MST

Result: This sets the maximum number of hop between any two terminals of MST.

18. To set the bridge priority, use command **set stp instance** *<0-15>* **priority** *<0-61440>* in global configuration mode. This is shown in Table 160.

TABLE 160 SET STP INSTANCE BRIDGE PRIORITY COMMAND

Format	Mode	Function
set stp instance ***<0-15>*** priority ***<0-61440>***	Global config	This sets the bridge priority

Result: This sets the bridge priority.

15. To set port cost of the instance, use command **set stp instance** <0-15> **port** <portname> **cost** <1-200000000> in global configuration mode. This is shown in Table 161.

TABLE 161 SET STP INSTANCE PORT COST COMMAND

Format	Mode	Function
set stp instance <0-15> **port** <portname> **cost** <1-200000000>	Global config	This sets port cost of the instance

Result: This sets port cost of the instance.

16. To set the port priority of the instance, use command **set stp instance** <0-15> **port** <portname> **priority** <0-

240> in global configuration mode. This is shown in Table 162.

TABLE 162 SET STP INSTANCE PORT PRIORITY COMMAND

Format	Mode	Function
set stp instance <0-15> **port** <portname> **priority** <0-240>	Global config	This sets the port priority of the instance

Result: This sets the port priority of the instance.

17. To set port loop guard for STP instance, use command **set stp instance** *<0-15>* **port** *<portname>* **root-guard** {**enable|disable**} in global configuration mode. This is shown in Table 163.

TABLE 163 SET STP INSTANCE PORT LOOP GUARD COMMAND

Format	Mode	Function
set stp instance <0-15> **port** <portname>**root-guard {enable|disable}**	Global config	This sets port root guard for STP instance

Result: This sets port root guard for STP instance.

18. To set port loop guard for STP instance, use command **set stp instance** <0-15> **port** <portname>**loop-guard {enable|disable}** in global configuration mode. This is shown in Table 163.

TABLE 164 SET STP INSTANCE PORT LOOP GUARD COMMAND

Format	Mode	Function
set stp instance <0-15> **port** <portname>**loop-guard {enable|disable}**	Global config	This sets port loop guard for STP instance

Result: This sets port loop guard for STP instance.

19. To set trunk cost of the instance, use command **set stp instance** <0-15> **trunk** <trunkname> **cost** <1-200000000> in global configuration mode. This is shown in Table 165.

TABLE 165 SET STP INSTANCE TRUNK COST COMMAND

Format	Mode	Function
set stp instance <0-15> **trunk** <trunkname> **cost** <1-200000000>	Global config	This sets trunk cost of the instance

Result: This sets trunk cost of the instance.

20. To set the trunk priority of the instance, use command **set stp instance** <0-15> **trunk** < trunkid > **priority** <0-255> in global configuration mode. This is shown in Table 166.

TABLE 166 SET STP INSTANCE TRUNK PRIORITY COMMAND

Format	Mode	Function
set stp instance <0-15> **trunk** < trunkid > **priority** <0-255>	Global config	This sets the port priority of the instance

Result: This sets the port priority of the instance.

21. To set trunk root guard of the instance, use command **set stp instance** <0-15> **trunk** <trunkname> **root-guard {enable|disable}** in global configuration mode. This is shown in Table 167.

TABLE 167 SET STP INSTANCE TRUNK ROOT GUARD COMMAND

Format	Mode	Function
set stp instance <0-15> **trunk** <trunkname> **root-guard {enable|disable}**	Global config	This sets trunk root guard of the instance

Result: This sets trunk root guard of the instance.

22. To set trunk loop of the instance, use command **set stp instance** <0-15> **trunk** <trunkname>**loop-guard {enable|disable}** in global configuration mode. This is shown in Table 168.

TABLE 168 SET STP INSTANCE TRUNK LOOP-GUARD COMMAND

Format	Mode	Function
set stp instance <0-15> **trunk** <trunkname>**loop-guard {enable|disable}**	Global config	This sets trunk loop of the instance

Result: This sets trunk loop of the instance.

23. To set the mapping relation between the VLAN and instance, use command **set stp instance** <0-15>**[add|delete] vlan** <vlanlist>in global configuration mode. This is shown in Table 169.

TABLE 169 SET STP INSTANCE VLAN COMMAND

Format	Mode	Function
set stp instance <0-15>**[add|delete] vlan** <vlanlist>	Global config	This sets the mapping relation between the VLAN and instance

Result: This sets the mapping relation between the VLAN and instance.

9. To set MST area name, use command **set stp name** <name> in global configuration mode. This is shown in Table 170.

TABLE 170 SET STP NAME COMMAND

Format	Mode	Function
set stp name <name>	Global config	This sets MST area name

Result: This sets MST area name.

25. To enable/disable STP port, use command **set stp port** <portlist> **{enable|disable}** in global configuration mode. This is shown in Table 171.

TABLE 171 SET STP PORT COMMAND

Format	Mode	Function
set stp port <portlist> **{enable|disable}**	Global config	This enable/disable stp port

Result: This enable/disable STP port.

26. To set port's link type of the instance, use command **set stp port** <portlist> **linktype {point-point|shared}** in global configuration mode. This is shown in Table 172.

TABLE 172 SET STP PORT LINKTYPE COMMAND

Format	Mode	Function
set stp port <portlist> **linktype {point-point|shared}**	Global config	This sets port's link type of the instance

Result: This sets port's link type of the instance.

27. To set port packet type of the instance, use command **set stp port** <portlist> **packettype {IEEE|CISCO|HUAWEI| HAMMER|extend}}** in global configuration mode. This is shown in Table 173.

TABLE 173 SET STP PORT PACKETTYPE COMMAND

Format	Mode	Function
set stp port <portlist> **packettype {IEEE|CISCO|HUAWEI|HAMMER|extend}**	Global config	This sets port packet type of the instance

Result: This sets port packet type of the instance.

28. To check STP port protocol type, use command **set stp port** <portlist> **pcheck** in global configuration mode. This is shown in Table 174.

TABLE 174 SET STP PORT PCHECK COMMAND

Format	Mode	Function
set stp port <portlist> **pcheck**	Global config	This checks STP port protocol type

Result: This checks STP port protocol type.

29. To set BPDU guard, use command **set stp port** <portlist> **bpdu-guard**{**enable|disable**} in global configuration mode. This is shown in Table 175.

TABLE 175 SET STP PORT BPDU-GUARD COMMAND

Format	Mode	Function
set stp port <portlist> **bpdu-guard**{**enable|disable**}	Global config	This sets BPDU guard

Result: This sets BPDU guard.

30. To set STP BPDU guard interval, use command **set stp bpdu_interval** <10-65535> in global configuration mode. This is shown in Table 176.

TABLE 176 SET STP BPDU INTERVAL COMMAND

Format	Mode	Function
set stp bpdu_interval <10-65535>	Global config	This sets STP BPDU guard interval

Result: This sets STP BPDU guard interval.

31. To enable/disable STP relay, use command **set stp relay {enable|disable}** in global configuration mode. This is shown in Table 177.

TABLE 177 SET STP RELAY COMMAND

Format	Mode	Function
set stp relay {enable|disable}	Global config	This enables/disables STP relay

Result: This enables/disables STP relay.

32. To set the MST version, use command **set stp revision** <0-65535> in global configuration mode. This is shown in Table 178.

TABLE 178 SET STP REVISION COMMAND

Format	Mode	Function
set stp revision <0-65535>	Global config	This sets the MST version

Result: This sets the MST version.

33. To enable/disable STP trunk, use command **set stp trunk** <trunklist> **{enable|disable}** in global configuration mode. This is shown in Table 179.

TABLE 179 SET STP TRUNK COMMAND

Format	Mode	Function
set stp trunk <trunklist> **{enable|disable}**	Global config	This enable/disable stp trunk

Result: This enable/disable STP trunk.

34. To set trunk's link type of the instance, use command **set stp trunk** <trunklist> **linktype {point-point|shared}** in global configuration mode. This is shown in Table 180.

TABLE 180 SET STP TRUNK LINKTYPE COMMAND

Format	Mode	Function
set stp trunk <trunklist> **linktype {point-point|shared}**	Global config	This sets trunk link type of the instance

Result: This sets trunk link type of the instance.

35. To set trunk packet type of instance, use command **set stp trunk** < trunkid > **packettype {IEEE|CISCO|HUAWEI| HAMMER|extend}}** in global configuration mode. This is shown in Table 181.

TABLE 181 SET STP TRUNK PACKETTYPE COMMAND

Format	Mode	Function
set stp trunk < trunkid > **packettype {IEEE|CISCO|HUAWEI|HAMMER|extend}**	Global config	This sets trunk packet type of instance

Result: This sets trunk packet type of instance.

36. To display stp related configuration.

i. To display stp information, use command **show stp** in global configuration mode. This is shown in Table 182.

TABLE 182 SHOW STP COMMAND

Format	Mode	Function
show stp	Global config	This displays stp information

Result: This displays stp information.

ii. To display stp instance information, use command **show stp instance** [<0-15>] in global configuration mode. This is shown in Table 183.

TABLE 183 SHOW STP INSTANCE COMMAND

Format	Mode	Function
show stp instance [<0-15>]	Global config	This displays stp instance information

Result: This displays stp instance information.

iii. To display stp port information, use command **show stp port** [<portlist>] in global configuration mode. This is shown in Table 184.

TABLE 184 SHOW STP PORT COMMAND

Format	Mode	Function
show stp port [<portlist>]	Global config	This displays stp port information

Result: This displays stp port information.

iv. To display stp trunk information, use command **show stp trunk** <trunklist> in global configuration mode. This is shown in Table 185.

TABLE 185 SHOW STP TRUNK COMMAND

Format	Mode	Function
show stp trunk <trunklist>	Global config	This displays stp trunk information

Result: This displays stp trunk information.

v. To display stp relay information, use command **show stp relay** in global configuration mode. This is shown in Table 186.

TABLE 186 SHOW STP RELAY COMMAND

Format	Mode	Function
show stp relay	Global config	This displays stp relay information

Result: This displays stp relay information.

END OF STEPS

Result STP has been configured.

Example The following is an example of MSTP configuration.

Create instance 1, set up mapping relations with VLANs 10 to 20, and set the name as zte. The MST version is 10.

```
zte(cfg)#set stp instance 1 add vlan 10-20
zte(cfg)#set stp name zte
zte(cfg)#set stp revision 10
zte(cfg)#show stp
  The spanning_tree protocol is enabled!

  The STP ForceVersion is MSTP !
  Revision: 10     Name: zte
  Bpdu interval: 100
  Cisco key:     0x13ac06a62e47fd51f95d2ba243cd0346
  Cisco digest:  0x00000000000000000000000000000000
  Huawei key:    0x13ac06a62e47fd51f95d2ba243cd0346
  Huawei digest: 0x00000000000000000000000000000000
  Instance VlanMap
  -------- -------------------
  0        1-9, 21-4094
  1        10-20
Zte(cfg)#
```

Set the bridge priority and port priority of the instance.

```
zte(cfg)#set vlan 10 add port 2 untag
zte(cfg)#set stp instance 1 bridgeprio 7
zte(cfg)#set stp instance 1 port 2 priority 112
zte(cfg)#show stp instance 0
  RootID:
  Priority        : 32768        Address      : 00.    d0.
d0.   ff.   ff.   0a
  HelloTime(s)   : 2           MaxAge(s)   : 20
  ForwardDelay(s): 15

  Reg  RootID:
  Priority        : 32768        Address      : 00.    d0.
d0.   ff.   ff.   0a
  RemainHops     : 20

  BridgeID:
  Priority        : 32768        Address      : 00.    d0.
d0.   ff.   ff.   0a
  HelloTime(s)   : 2           MaxAge(s)   : 20
  ForwardDelay(s): 15          MaxHops     : 20

  Interface  PortId  Cost        Status   Role          Bound
GuardStatus
  --------- ------ --------- ------- ---------- ----- ----
-------
  2          128.    2   200000     Discard Designated MSTP
None
zte(cfg)#show stp instance 1
  RootID:
  Priority        : 1            Address      : 00.    d0.
d0.   ff.   ff.   0a
  HelloTime(s)   : 2           MaxAge(s)   : 20
  ForwardDelay(s): 15          RemainHops  : 20
  BridgeID:
  Priority        : 1            Address      : 00.    d0.
d0.   ff.   ff.   0a
  HelloTime(s)   : 2           MaxAge(s)   : 20
  ForwardDelay(s): 15          MaxHops     : 20

  Interface   PortId   Cost               Status     Role
GuardStatus
  --------- ------ --------- ------- ---------- ----------
-
  2         112.   2  200000    Discard Designated None
zte(cfg)#show stp port 2


The following ports are active!
  PortId      : 2             MSTI        : 00
    Priority    : 128           Cost        : 200000
```

```
The following ports are active!
  PortId      : 2             MSTI        : 00
    Priority    : 128           Cost        : 200000
    Status      : Forward       Role        : Designated
    EdgePort    : Disabled      GuardType   : None
    LinkType    : P2P           PacketType  : IEEE

  PortId      : 2             MSTI        : 01
    Priority    : 112           Cost        : 200000
    Status      : Forward       Role        : Designated
    EdgePort    : Disabled      GuardType   : None
    LinkType    : P2P           PacketType  : IEEE
```

ACL

Introduction

Packet filtering can help limit network traffic and restrict network use by certain users or devices. ACL's can filter traffic as it passes through a router and permit or deny packets at specified interfaces.

Description

An ACL is a sequential collection of permit and deny conditions that apply to packets. When a packet is received on an interface, the switch compares the fields in the packet against any applied ACL's to verify that the packet has the required permissions to be forwarded, based on the criteria specified in the access lists. It tests packets against the conditions in an access list one by one. The first match determines whether the switch accepts or rejects the packets because the switch stops testing conditions after the first match. The order of conditions in the list is critical. If no conditions match, the switch rejects the packets. If there are no restrictions, the switch forwards the packet; otherwise, the switch drops the packet.

Packet matching rules defined by the ACL are also used in other conditions where distinguishing traffic is needed. For instance, the matching rules can define the traffic classification rule in the QoS.

ACL Function

ZXR10 2920/2928/2952 provides ACL functions as follows:

- ZXR10 2920/2928/2952 provides three binding types including physical port, Trunk Groups and Vlan interface. When a physical port is added into a Trunk Group and has been bounded as ACL, current bound is to be released, a false message will return. When ACL is applied to Trunk Group, physical port will be bound with ACL automatically. Vlan interface also supports an ACL binding.

  Note: When a port/trunk itself belongs to a Vlan, choose mode to make sure that the received packets will be applied to a port/trunk bound ACL or a Vlan bound ACL.

- ACL rule can be added, deleted, sorted.
  - Rule can be added to a configured ACL. Regular ID number range is from 1-500 including Global ACL the number ranges from 1 to 16.
  - Configured ACL can be deleted regularly. If the specified ACL's access list number or rule number hasn't been configured, a false message will return.
  - Many rules of an ACL can be sorted and defined where the rule number is placed.
- An ACL can become effective according to configuring time range. After configuring absolute or relative time range on the switch, time range can be applied to the rule of ACL. This results in the rule to be in effect according to the time range identified.

Five Types of ACL

ZXR10 2920/2928/2952 provides the following five types of ACL's:

- Basic ACL: Only match source IP address.
- Extended ACL: Match the following items:
  - source IP address, destination IP address, IP protocol type, TCP source port number, TCP destination port number, UDP source port number, UDP destination port number, ICMP type, ICMP Code, DiffServ Code Point (DSCP), ToS and Precedence.
- L2 ACL: Match source MAC address, destination MAC address, source VLAN ID, L2 Ethernet protocol type and 802. 1p priority value.
- Hybrid ACL: Match the following items:
  - source IP address, destination IP address, IP protocol type, TCP source port number, TCP destination port number, UDP source port number, UDP destination port number, DiffServ Code Point (DSCP) L2 Ethernet protocol type, source MAC address, destination MAC address, source VLAN ID and 802. 1p priority value.
- Global ACL: Match the following items:
  - Physical port number, source IP address, destination IP address, IP protocol type, TCP source port number, TCP destination port number, UDP source port number, UDP destination port number, DiffServ Code Point (DSCP) L2 Ethernet protocol type, source MAC address, destination MAC address, source VLAN ID and 802. 1p priority value.

ACL Description

Each ACL has an access list number to identify. The access list number is a number. The access list number ranges of different types of ACL's are shown in Table 187.

TABLE 187 ACL DESCRIPTION

ACL Description	Access List Number
Basic ACL	The range is from 1 to 99
Extended ACL	The range is from 100 to 199
L2 ACL	The range is from 200 to 299
Hybrid ACL	The range is from 300 to 349
Global ACL	350

Each ACL has best 500 rules except that Global ACL has best 16 rules.

Configuring Basic ACL

Purpose This topic describes the basic ACL configuration number.

Steps For basic ACL configuration, perform the following steps.

1. To enter into basic ACL configuration, use command **config acl basic number** <acl-number> in global configuration mode. This is shown in Table 188.

TABLE 188 ACL BASIC NUMBER COMMAND

Format	Mode	Function
config acl basic number <acl-number>	global config	This enters into basic ACL configuration mode

Result: This enters into basic ACL configuration mode.

2. To configure the rules of ACL, use command **rule** <rule-id> {**permit** | **deny**} {<source-ipaddr wildcard> | **any**}[**fragment**] in ACL config mode. This is shown in Table 189.

TABLE 189 RULE COMMAND

Format	Mode	Function
rule <rule-id> {**permit** | **deny**} {<source-ipaddr wildcard> | **any**}[**fragment**]	ACL config	This configures ACL rules

Result: This configures ACL rules.

END OF STEPS

Result Basic ACL has been configured.

Configuring Extended ACL

Purpose This topic describes the configuration of extended ACL.

Steps For the configuration of extended ACL, perform the following steps.

1. To enter into extended ACL configuration, use command **config acl extend number** <acl-number> in global configuration mode. This is shown in Table 190.

TABLE 190 CONFIG ACL EXTEND COMMAND

Format	Mode	Function
config acl extend number <acl-number>	global config	This configures extended ACL

Result: This configures extended ACL

2. To configure the rules of ACL, use command **rule** <rule_id> {permit|deny} {<ip-protocol>| **ip | tcp | udp | icmp | arp**}{<source-ipaddr wildcard> | **any**} [<source-port sourceport-mask>]{<destination-ipaddr wildcard> | **any**} [<dest-port destport-mask>][**established** | **esblishing** | <icmp-type icmp-code>] [dscp] [**fragment**] in ACL config mode. This is shown in Table 191.

TABLE 191 RULE COMMAND

Format	Mode	Function
rule <rule_id> {permit|deny} {<ip-protocol>| **ip | tcp | udp | icmp | arp**}{<source-ipaddr wildcard> | **any**} [<source-port sourceport-mask>]{<destination-ipaddr wildcard> | **any**} [<dest-port destport-mask>][**established** | **esblishing** | <icmp-type icmp-code>] [dscp] [**fragment**]	ACL config	This configures ACL rules

Result: This configures ACL rules.

END OF STEPS

Result Basic ACL has been configured.

Configuring L2 ACL

Purpose This topic describes the configuration of L2 ACL.

Steps For the configuration of L2 ACL, perform the following steps.

1. To enter in L2 ACL configuration, use command **config acl link number** <acl-number> in global configuration mode. This is shown in Table 192.

TABLE 192 CONFIG ACL LINK COMMAND

Format	Mode	Function
config acl link number <acl-number>	global config	This enters into L2 ACL configuration mode

Result: This enters into L2 ACL configuration mode.

2. To configure the rules of ACL, use command **rule** <rule-id> {**permit | deny} {ip | arp | other | any** } [**ether-type** <protocol-number>] [<dsap-ssap>][cos] [source-vlanid] {<source-mac wildcard> | **any** |<destination-mac wildcard> | **any**} in ACL config mode. This is shown in Table 193

TABLE 193 RULE COMMAND

Format	Mode	Function
rule <rule-id> **{permit | deny} {ip | arp | other | any** } [**ether-type** <protocol-number>] [<dsap-ssap>][cos] [source-vlanid] {<source-mac wildcard> | **any** |<destination-mac wildcard> | **any**}	ACL config	This configures ACL rules

Result: This configures ACL rules.

END OF STEPS

Steps L2 ACL has been configured.

Configuring Hybrid ACL

Purpose This topic describes the configuration of Hybrid ACL.

Steps For the configuration of Hybrid ACL, perform the following steps.

1. To enter into Hybrid ACL, use command **config acl hybrid number** <acl-number> in global configuration mode. This is shown in Table 194

TABLE 194 CONFIG ACL HYBRID COMMAND

Format	Mode	Function
config acl hybrid number <acl-number>	global config	This enters into Hybrid ACL

Result: This enters into Hybrid ACL.

2. To configure the rules of ACL, use command **rule** <rule-id> {**permit|deny**} {< ip-protocol> | **ip | tcp | udp| arp**}{<source-ipaddr wildcard>|any} [<source-port sourceport-mask>]{<destination-ipaddr wildcard>|any} [<dest-port destport-mask>][**dscp] [fragment] [ether-type** <proto-number>] [cos][<source-vlanId>] [<source-mac wildcard >| **any**] [<destination-mac wildcard>| **any**] in ACL config mode. This is shown in

TABLE 195 RULE COMMAND

Format	Mode	Function
rule <rule-id> {**permit|deny**} {< ip-protocol>	**ip	tcp	udp| arp**}{<source-ipaddr wildcard>|any} [<source-port sourceport-mask>]{<destination-ipaddr wildcard>|any} [<dest-port destport-mask>][**dscp] [fragment] [ether-type** <proto-number>] [cos][<source-vlanId>] [<source-mac wildcard >| **any**] [<destination-mac wildcard>| **any**]	ACL config	This enters into ACL rules

Result: This enters into ACL rules.

END OF STEPS

Result Hybrid ACL has been configured.

Configuring Global ACL

Purpose This topic describes the configuration of global ACL.

Steps For the configuration of Global ACL, perform the following steps.

1. To enter into Global ACL configuration, use command **config acl global** in global configuration mode. This is shown in Table 196.

TABLE 196 CONFIG ACL GLOBAL COMMAND

Format	Mode	Function
config acl global	global config	This enters into Global ACL configuration mode

Result: This enters into Global ACL configuration mode.

2. To configure ACL rules, use command **rule** <rule-id> {**permit|deny**} **port** [<port-id> | **any**] {< ip-protocol> | **ip | tcp | udp| arp| any**}{<source-ipaddr wildcard>|any} [<source-port sourceport-mask>]{<destination-ipaddr wildcard>|any} [<dest-port destport-mask**>**]**[dscp] [fragment]** [**ether-type** <proto-number>] [**cos**][<source-vlanId>] [<source-mac wildcard >| **any**] [<destination-mac wildcard>| **any**] in ACL config mode. This is shown in Table 197.

TABLE 197 RULE COMMAND

Format	Mode	Function
rule <rule-id> {**permit|deny**} **port** [<port-id> | **any**] {< ip-protocol> | **ip | tcp | udp| arp| any**}{<source-ipaddr wildcard>|any} [<source-port sourceport-mask>]{<destination-ipaddr wildcard>|any} [<dest-port destport-mask>][**dscp**] [fragment] [ether-type <proto-number>] [**cos**][<source-vlanId>] [<source-mac wildcard >| **any**] [<destination-mac wildcard>| **any**]	ACL config	This configures ACL rules

Result: This configures ACL rules.

END OF STEPS

Result Global ACL has been configured.

Configuring Time-Range

Purpose This topic describes the configuration of time-range.

Steps For the configuration of time-range, perform the following step.

1. To configure time-range, use command **set time-range** <time-name> **range period|absolute** <start-time> **to** <end-time> **[daily | day-off | day-working | monday | tuesday | wednesday | thursday | friday | saturday | sunday]** in global configuration mode. This is shown in Table 198.

TABLE 198 SET TIME-RANGE COMMAND

Format	Mode	Function
set time-range <time-name> **range period|absolute <start-time> to** <end-time> **[daily | day-off | day-working | monday | tuesday | wednesday | thursday | friday | saturday | sunday]**	global config	This configures time-range

Result: This configures time-range.

- Configuration of time range per day: Specify the start time and end time per day.
- Configuration of period range: Specify the period as a date every week.
- Configuration of date range: Specify the start time and end time. If not configuring range, the date range refers from the effective date of the configuration to the maximum date of the system.

END OF STEPS

Result Time-range has been configured.

Configuring ACL to a Physical Port

Purpose This topic describes the configuration of ACL to a physical port.

Steps For the configuration of ACL to a physical port, perform the following step.

1. To configure ACL to a physical port, use the following command in global configuration mode as shown in Table 199.

TABLE 199 PORT COMMANDS

Format	Mode	Function
set port <portlist> **acl** <acl-number> **{enable | disable}**	global config	This enables/disables port ACL
set trunk <trunktlist> **acl** <acl-number> **{enable | disable}**	global config	This enables/disables trunk ACL
set vlan <valnlist> **acl** <acl-number> **{enable | disable}**	global config	This enables/disables Vlan ACL

Result: This enables/disables port, trunk and Vlan.

Note: A physical port can only have one ACL. It is necessary to release the current bound when you want to bind a new one in the case that an old one has applied to the physical port, otherwise, a false message will return.

END OF STEPS

Result ACL has been configured to a physical port.

Quality of Service (QoS)

Data Packet Priority

ZXR10 2920/2928/2952 provides QoS function and priority control function. Priority of the data packets can be determined by source MAC address priority of the data packets, VLAN priority, 802. 1P user priority, layer 3 DSCP priority, or the default port priority. The priority of a data packet is determined in the following sequence:

- Priority of the data packets sent by CPU (determined by CPU).
- Priority of MGMT data packets (management data packets such as the BPDU packets). Priority of the management packets is determined by the initialization.
- Priority of static source MAC address.
- VLAN priority.
- 802. 1P user priority.
- Layer 3 DSCP priority.
- Default port priority.

After data packet priority is determined by the previous priority determination policy, the later policies are ignored. To use the default port priority to decide the priority of the data packets received by the port, all the following conditions shall be satisfied.

- Data packets are not data packets sent by CPU or management data packets.
- Source MAC address of the data packets cannot be the static address or the port source priority function is disabled.
- Priority of VLAN that the data packets belong to is disabled or Priority of the VLAN of the port belongs to is disabled.
- 802. 1P user priority of the port is disabled, or the data packets are not TAG data packets.
- Port DSCP priority is disabled.

After the priority control policy of the switch is configured, if the switch receives the data frames, the data frames with higher priority can be transmitted first to ensure the key applications.

Configuring QoS

Purpose This topic describes the configuration of QoS including the data packet priority.

Steps For the configuration of QoS, perform the following steps.

1. To set the mapping of the user-priority to traffic-class, use command **set qos priority-map user-priority** <*0-7*> **traffic-class** <*0-3*> in global configuration mode. This is shown in Table 201.

TABLE 200 SET QOS DSCP COMMAND

Format	Mode	Function
set qos priority-map user-priority <*0-7*> **traffic-class** <*0-3*>	global config	This sets the mapping of user-priority to traffic-class

Result: This sets the mapping of user-priority to traffic-class.

2. To set the mapping of the DSCP to QoS profile, use command **set qos priority-map ip-priority** <*0-63*> **traffic-class** <*0-3*> in global configuration mode. This is shown in Table 201.

TABLE 201 SET QOS DSCP COMMAND

Format	Mode	Function
set qos priority-map ip-priority	global config	This sets the mapping of the

Format	Mode	Function
<*0-63*> traffic-class <*0-3*>		DSCP to QoS profile

Result: This sets the mapping of the DSCP to QoS profile.

3. To configure global queue schedule profile, use command **set qos queue-schedule queue0-weight** *<1-32>* **queue1-weight** *<1-32>* **queue2-weight** *<1-32>* **queue3-weight** *<1-32>* in global configuration mode. This is shown in Table 202.

TABLE 202 SET QOS QUEUE SCHEDULE COMMAND

Format	Mode	Function
set qos queue-schedule queue0-weight <*1-32*> queue1-weight <*1-32*> queue2-weight <*1-32*> queue3-weight <*1-32*>	global config	This configures global queue schedule profile

Result: This configures global queue schedule profile.

4. To configure the parameters of the flux monitor, use command **set qos policer counter-mode** {**L1 | L2 | L3**} in global configuration mode. This is shown in Table 203.

TABLE 203 SET QOS POLICER PARAMETERS COMMAND

Format	Mode	Function
set qos policer counter-mode {L1 | L2 | L3}	global config	This configures the parameters of flux monitor

Result: This configures the parameters of flux monitor.

Note:set counter mode of the qos policer. By default, it works in L2 mode.

5. To configure the promise speed parameters of the flux monitor, use command **set qos policer** *<0-255>* **parameters** *<1-25165824>*in global configuration mode. This is shown in Table 203.

TABLE 204 SET QOS POLICER PARAMETERS COMMAND

Format	Mode	Function
set qos policer counter-mode {L1 | L2 | L3}	global config	This configures the promise speed of flux monitor

Result: This configures the promise speed of flux monitor.

6. To configure the policer counter of the flux monitor, use command **set qos policer** *<0-255>* **counter** *<0-15>* {**enable | disable** }in global configuration mode. This is shown in Table 203.

TABLE 205 SET QOS POLICER PARAMETERS COMMAND

Format	Mode	Function
set qos policer <*0-255***> counter <***0-15***> {enable | disable }**	global config	This configures the promise speed of flux monitor

Result: This configures the policer counter of flux monitor.

7. To configure the overspeed disposal of the flux monitor, use command **set qos policer** *<0-255>* **exceed-action** {**no-operation | drop**}in global configuration mode. This is shown in Table 203.

TABLE 206 SET QOS POLICER PARAMETERS COMMAND

Format	Mode	Function
set qos policer <*0-255***> counter <***0-15***> {enable | disable }**	global config	This configures the overspeed disposol of flux monitor

Result: This configures the overspeed disposal of flux monitor.

8. To configure the ingress session rate of the flux monitor, use command **set bandwidth feport** *<portlist>* **ingress session** *<0-3>* **rate** *<64-100000>*in global configuration mode. This is shown in Table 203.

TABLE 207 SET QOS POLICER PARAMETERS COMMAND

Format	Mode	Function
set bandwidth feport <*portlist***> ingress session <***0-3***> rate <***64-100000***>**	global config	This configures the ingress session rate of flux monitor

Result: This configures the ingress session rate of flux monitor.

9. To configure the ingress session packet-type of the flux monitor, use command **set bandwidth feport** *<portlist>* **ingress session** *<0-3>* **packet-type** {**unknowmulticast | broadcast | unicast | multicast | MGMT | ARP | tcp-control | tcp-data | udp | non-tcpudp**} {**enable | disable**}in global configuration mode. This is shown in Table 203.

TABLE 208 SET QOS POLICER PARAMETERS COMMAND

Format	Mode	Function
set bandwidth feport <*portlist*> ingress session <*0-3*> packet-type {unknowmulticast | broadcast | unicast | multicast | MGMT | ARP | tcp-control | tcp-data | udp | non-tcpudp} {enable | disable}	global config	This configures the ingress session packet-type

Result: This configures the ingress session packet-type of flux monitor.

10. To configure the ingress session queue-priority of the flux monitor, use command **set bandwidth feport** <*portlist*> **ingress session** <*0-3*> **packet-type** {**unknowmulticast | broadcast | unicast | multicast | MGMT | ARP | tcp-control | tcp-data | udp | non-tcpudp**} {**enable | disable**}in global configuration mode. This is shown in Table 203.

TABLE 209 SET QOS POLICER PARAMETERS COMMAND

Format	Mode	Function
set bandwidth feport <*portlist*> ingress session <*0-3*> queue-priority <*queuelist*> {enable | disable }	global config	This configures the ingress session queue-priority

Result: This configures the ingress session queue-priority of flux monitor.

11. To configure the ingress session mgmt-no-ratelimit of the flux monitor, use command **set bandwidth feport** <*portlist*> **ingress session** <*0-3*> **mgmt-no-ratelimit** {**enable | disable**}in global configuration mode. This is shown in Table 203.

TABLE 210 SET QOS POLICER PARAMETERS COMMAND

Format	Mode	Function
set bandwidth feport <*portlist***> ingress session <***0-3***> mgmt-no-ratelimit {enable | disable}**	global config	This configures the ingress session mgmt-no-ratelimit

Result: This configures the ingress session mgmt-no-ratelimit of flux monitor.

12. To configure the ingress session of the flux monitor, use command **set bandwidth feport** <*portlist*> **ingress session** <*0-3*> {**enable | disable**}in global configuration mode. This is shown in Table 203.

TABLE 211 SET QOS POLICER PARAMETERS COMMAND

Format	Mode	Function
set bandwidth feport <*portlist***> ingress session <***0-3***> {enable | disable}**	global config	This configures the ingress session mgmt-no-ratelimit

Result: This configures the ingress session of flux monitor.

13. To configure the egress session of the flux monitor, use command **set bandwidth feport** <*portlist*> **egress** {{**on rate** <*64-1000000*>} | **off**}in global configuration mode. This is shown in Table 203.

TABLE 212 SET QOS POLICER PARAMETERS COMMAND

Format	Mode	Function
set bandwidth feport <*portlist***> egress {{on rate <***64-1000000***>} | off}**	global config	This configures the egress session

Result: This configures the egress session of flux monitor.

14. To configure the geport ingress session of the flux monitor, use command **set bandwidth geport** <*portlist*> **ingress** {{**on rate** <*2000-1000000*> } | **off** }in global configuration mode. This is shown in Table 203.

TABLE 213 SET QOS POLICER PARAMETERS COMMAND

Format	Mode	Function
set bandwidth geport <*portlist***> ingress {{on rate <***2000-1000000***> } | off }**	global config	This configures the geport ingress session

Result: This configures the geport ingress session of flux monitor.

14. To configure the geport ingress session of the flux monitor, use command **set bandwidth geport** <*portlist*> **ingress** {{**on rate** <*2000-1000000*> } | **off** }in global configuration mode. This is shown in Table 203.

TABLE 214 SET QOS POLICER PARAMETERS COMMAND

Format	Mode	Function
set bandwidth geport <*portlist***> ingress {{on rate <***2000-1000000***> } | off }**	global config	This configures the geport ingress session

Result: This configures the geport ingress session of flux monitor.

15. To configure the geport egress session of the flux monitor, use command **set bandwidth geport** <*portlist*> **egress** {**on rate** <*281-1000000*> [**burstsize** <*4-16380*>]} | **off** }in global configuration mode. This is shown in Table 203.

TABLE 215 SET QOS POLICER PARAMETERS COMMAND

Format	Mode	Function
set bandwidth geport <*portlist***> egress {on rate <***281-1000000***> [burstsize <***4-16380***>]} | off }**	global config	This configures the geport egress session

Result: This configures the geport egress session of flux monitor.

16. To configure the packet-type of geport ingress session of the flux monitor, use command **set bandwidth geport** <*portlist*> **packet-type** { **unicast | nounicast | multicast | broadcast** } {**enable | disable** }in global configuration mode. This is shown in Table 203.

TABLE 216 SET QOS POLICER PARAMETERS COMMAND

Format	Mode	Function
set bandwidth geport <*portlist***> packet-type { unicast | nounicast | multicast | broadcast } {enable | disable }**	global config	This configures the packet-type of geport ingress session

Result: This configures the packet-type of geport ingress session of flux monitor.

17. Remarking the VLAN is to remark the VLAN attribution of the designated flow. To remark the VLAN, use command **set policy vlan-remark in acl** *<1-349>* **rule** *<1-500> <1-4094>* {**untagged|tagged|all**} {**nested|replaced**} in global configuration mode. This is shown in Table 217.

TABLE 217 SET POLICY VLAN REMARK COMMAND

Format	Mode	Function
set policy vlan-remark in acl ***<1-349>*** rule ***<1-500> <1-4094>*** **{**untagged|tagged|all**}** **{**nested|replaced**}**	global config	This remarks the VLAN

Result: This remarks the VLAN.

18. To bind the rule of flux monitor, use command **set policy policing in acl** <1-350> **rule** <1-500> **policer** <0-255> in global configuration mode. This is shown in

TABLE 218 SET POLICY POLICING IN ACL COMMAND

Format	Mode	Function
set policy policing in acl <1-350> **rule** <1-500> **policer** <0-255>	global config	This binds the rule of flux monitor

Result: This binds the rule of flux monitor.

19. Flow mirror is to copy the designated data flow to the monitor port, use it to monitor the network and eliminate trouble. To configure the mirror for the traffic, use command **set policy mirror in acl** <1-350> **rule** <1-500> {**cpu|analyze-port**} in global configuration mode. This is shown in Table 219.

TABLE 219 SET POLICY MIRROR COMMAND

Format	Mode	Function
set policy mirror in acl <1-350> **rule** <1-500> {**cpu|analyze-port**}	global config	This configures the mirror for the traffic

Result: This configures the mirror for the traffic.

20. Flow redirection is to redirect the designated data flow to the egress port designated by users, and monitor the flow. To redirect the data flow, use command **set policy redirect in acl** *<1-349>* **rule** *<1-500>* {**cpu|port** *<portname>*} in global configuration mode. This is shown in Table 220.

TABLE 220 SET POLICY REDIRECT COMMAND

Format	Mode	Function
set policy redirect in acl <*1-349***> rule <***1-500***> {cpu|port <***portname***>}**	global config	This redirects the data flow

Result: This redirects the data flow.

21. To set policy statistics, use command **set policy statistics in acl** *<1-349>* **rule** *<1-500>* **counter** *<0-31>* in global configuration mode. This is shown in Table 222.

TABLE 221 SET POLICY QOS REMARK COMMAND

Format	Mode	Function
set policy statistics in acl **<***1-349***>** rule **<***1-500***>** counter **<***0-31***>**	global config	This sets policy statistics

Result: This sets policy statistics.

22. Remarking the flow is to remark the QoS attribution of the designated flow. This happens after the primary QoS marking on the port. To remark the flow, use command **set police remark in acl <***1-349***> rule <***1-500***> up <***0-7***>** in global configuration mode. This is shown in Table 222.

TABLE 222 SET POLICY QOS REMARK COMMAND

Format	Mode	Function
set police remark in acl <*1-349***> rule <***1-500***> up <***0-7***>**	global config	This remarks the flow of traffic

Result: This remarks the flow of traffic.

23. To clear QoS policy counter, use command **clear qos policy-counter** <0-31> in global configuration mode. This is shown in Table 223.

TABLE 223 CLEAR QOS POLICY COUNTER COMMAND

Format	Mode	Function
clear qos policy-counter <0-31>	global config	This clears QoS policy counter

Result: This clear QoS policy counter.

3. To delete mirror for the traffic, use command **clear policy mirror in acl** <1-349> **rule** <1-100> in global configuration mode. This is shown in Table 224.

TABLE 224 CLEAR POLICY MIRROR COMMAND

Format	Mode	Function
clear policy mirror in acl <1-349> rule <1-100>	global config	This deletes mirror for the traffic

Result: This deletes mirror for the traffic.

25. To delete Vlan remark for the traffic, use command **clear policy vlan-remark in acl** <1-349> **rule** <1-100> in global configuration mode. This is shown in Table 225.

TABLE 225 CLEAR POLICY VLAN COMMAND

Format	Mode	Function
clear policy vlan-remark in acl <1-349> **rule** <1-100>	global config	This clears Vlan remark for the traffic

Result: This clears Vlan remark for the traffic.

26. To delete QoS policing for the traffic, use command **clear policy policing in acl** <1-349> **rule** <1-100> in global configuration mode. This is shown in Table 226.

TABLE 226 CLEAR POLICY POLICING COMMAND

Format	Mode	Function
clear policy policing in acl <1-349> **rule** <1-100>	global config	This deletes QoS policing for the traffic

Result: This deletes QoS policing for the traffic.

27. To clear remark for the traffic, use command **clear policer remark in acl** *<1-349>* **rule** *<1-500>* in global configuration mode. This is shown in Table 227.

TABLE 227 CLEAR POLICY QOS REMARK COMMAND

Format	Mode	Function
clear policer remark in acl ***<1-349>*** rule ***<1-500>***	global config	This clears remark for the traffic

Result: This clears remark for the traffic.

28. To clear statistics for the traffic, use command **clear policy statistics in acl** <1-349> **rule** <1-100> in global configuration mode. This is shown in Table 228.

TABLE 228 CLEAR POLICY STATISTICS COMMAND

Format	Mode	Function
clear policy statistics in acl <1-349> **rule** <1-100>	global config	This clears statistics for the traffic

Result: This clears statistics for the traffic.

29. To clear redirect for the traffic, use command **clear policy redirect in acl** <1-349> **rule** <1-100> in global configuration mode. This is shown in Table 229.

TABLE 229 CLEAR POLICY REDIRECT COMMAND

Format	Mode	Function
clear policy redirect in acl <1-349> **rule** <1-100>	global config	This clears redirect for the traffic

Result: This clears redirect for the traffic.

30. To view user-priority to the QoS profiles mapping session, use command **show qos priority-map user-priority** in global configuration mode. This is shown in Table 230.

TABLE 230 SHOW QOS DSCP COMMAND

Format	Mode	Function
show qos priority-map user-priority	global config	This view dscp to the Qos profiles mapping session

Result: This views user-priority to the QoS profiles mapping session.

4. To view ip-priority to the QoS profiles mapping session, use command **show qos priority-map ip-priority** in global configuration mode. This is shown in Table 231.

TABLE 231 SHOW QOS QUEUE PROFILE COMMAND

Format	Mode	Function
show qos priority-map ip-priority	global config	This views queue schedule profile

Result: This views user-priority to the QoS profiles mapping session.

5. To view qos queue-schedule, use command **show qos queue-schedule** [**wrr0 | sp | wrr1-sp | wrr2-sp**] in global configuration mode. This is shown in Table 233.

TABLE 232 SHOW QOS POLICER COMMAND

Format	Mode	Function
show qos queue-schedule **[**wrr0 | sp | wrr1-sp | wrr2-sp]	global config	This views qos policer

Result: This view qos queue-schedule.

33. To view qos policer, use command **show qos policer** [<0-255>] in global configuration mode. This is shown in Table 233.

TABLE 233 SHOW QOS POLICER COMMAND

Format	Mode	Function
show qos policer [<0-255>]	global config	This views qos policer

Result: This view qos policer.

34. To view qos policy counter, use command **show qos counter** [<0-31>] in global configuration mode. This is shown in Table 234.

TABLE 234 SHOW QOS POLICY COUNTER COMMAND

Format	Mode	Function
show qos counter [<0-31>]	global config	This views qos policy counter

Result: This views qos policy counter.

6. To view policy for traffic, use command **show policy [mirror | redirect | qos-remark | vlan-remark |statistic | policing** [<0-255>]] in global configuration mode. This is shown in Table 235.

TABLE 235 SHOW POLICY COMMAND

Format	Mode	Function
show policy [mirror | redirect | qos-remark | vlan-remark |statistic | policing [<0-255>]]	global config	This views policy for traffic

Result: This views policy for traffic.

END OF STEPS

Result QoS including data packet priority has been configured.

Example This example shows overall situation of QoS profile. Value is {TC=5, DP=1, UP=5, DSCP=33}.

```
zte(cfg)#set qos profile 66 tc 5 dp 1 up 5 dsc 33
zte(cfg)#show qos profile 66
  ProfileIndex      tc      dp       up     dscp
  -------------    ----   ----    ----   -----
  66                  5       1        5       33
```

To set up→profile mapping is 5→55, set dscp→profile mapping is 33→66.

```
  zte(cfg)#set qos up-to-profile 5 55
 zte(cfg)#set qos dscp-to-profile 33 66
 zte(cfg)#show qos up-to-profile 5
   up    ProfileIndex
 ----   -------------
5        55
 zte(cfg)#show qos dscp-to-profile 33
  dscp    ProfileIndex
 ----   -------------
  33        66
```

Config QoS Queue Profile

Modify queue schedule profile 2 which has queue 4, 5, 6, 7 and change this mode to sdwrr1, the weight respectively is 5, 10, 15, 20.

```
zte(cfg)#set qos queue-schedule 2 4 sdwrr 1 5

zte(cfg)#set qos queue-schedule 2 5 sdwrr 1 10

zte(cfg)#set qos queue-schedule 2 6 sdwrr 1 15

zte(cfg)#set qos queue-schedule 2 7 sdwrr 1 20

zte(cfg)#show qos queue-profile 2
 Queue schedule profile:2
  QueueNumber  Mode     Weight
  ----------- ------   ------
     0      sdwrr-0     1
     1      sdwrr-0     2
     2      sdwrr-0     3
     3      sdwrr-0     4
     4      sdwrr-1     5
     5      sdwrr-1     10
     6      sdwrr-1     15
     7      sdwrr-1     20
```

Private Virtual LAN Overview

Features of VLAN

Packets of different users are separated to improve network security. A VLAN can be allocated to each user. This has its limits:

- Current IEEE 802. 1Q standard supports up to 4094 VLANs, which restrict the user capacity and network expansion.
- Each VLAN corresponds to an IP subnet which leads to waste of IP address resources.
- Planning and management of enormous VLANs and IP subnets add complexity to network management.

There are two types of PVLAN ports:

- Promiscuous port
- Isolated port

Promiscuous port

A promiscuous port communicates with all other PVLAN ports. The promiscuous port is the port that communicates with external routers, network management devices, backup servers, administrative workstations, and other devices.

Isolated port An isolated port has complete separation from other ports within the same PVLAN. The isolate port communicates with the promiscuous port only, but not with any other isolate port. Isolated port forwards traffic to all promiscuous ports only.

ZXR10 2920/2928/2952 supports 8 PVLANs groups, each group having customized isolate ports and at most 8 promiscuous ports.

Configuring PVLAN

Purpose This topic describes the configuration of PVLAN in ZXR10 2920/2928/2952 .

Steps For the configuration of PVLAN, perform the following steps.

1. To configure the isolate ports and promiscuous ports of PVLAN to isolate trunk and sharing port/trunk, use command **set pvlan session** <1-4> **add promiscuous** { **port**<portid>|**trunk**<trunkid>} **isolate** {**port** <portlist>|**trunk** <trunklist>} in global configuration mode. This is shown in Table 236.

TABLE 236 SET PVLAN SESSION COMMAND

Format	Mode	Function
set pvlan session <1-4> **add promiscuous** { **port**<portid>|**trunk**<trunkid>} **isolate** {**port** <portlist>|**trunk** <trunklist>}	global config	This configures isolate ports and promiscuous ports of PVLAN

Result: This configures isolate ports and promiscuous ports of PVLAN.

2. To delete the isolate ports and promiscuous ports of PVLAN, use command **set pvlan session** <1-4> **delete isolate** {**port** <portlist>|**trunk** <trunklist>} in global configuration mode. This is shown in Table 237.

TABLE 237 SET PVLAN SESSION DELETE COMMAND

Format	Mode	Function
set pvlan session <1-4> **delete isolate** {**port** <portlist>|**trunk** <trunklist>}	global config	This deletes the isolate ports and promiscuous ports of PVLAN

Result: This deletes the isolate ports and promiscuous ports of PVLAN.

3. To modify promiscuous ports/trunk in the PVLAN, use command **set pvlan session** <1-4> **modify promiscuous** {**port**<portid>|**trunk**<trunkid>} in global configuration mode. This is shown in Table 238.

TABLE 238 SET PVLAN SESSION MODIFY COMMAND

Format	Mode	Function
set pvlan session <1-4> **modify promiscuous** {**port**<portid>|**trunk**<trunkid>}	global config	This modifies promiscuous ports/trunk in the PVLAN

Result: This modifies promiscuous ports/trunk in the PVLAN.

4. To clear PVLAN session, use command **set pvlan session** <1-4> **clear-config** in global configuration mode. This is shown in Table 239.

TABLE 239 SET PVLAN SESSION CLEAR COMMAND

Format	Mode	Function
set pvlan session <1-4> **clear-config**	global config	This clears PVLAN session

Result: This clears PVLAN session.

5. To view PVLAN, use command **show pvlan** in global configuration mode. This is shown in Table 240.

TABLE 240 SHOW PVLAN COMMAND

Format	Mode	Function
show pvlan	global config	This views PVLAN

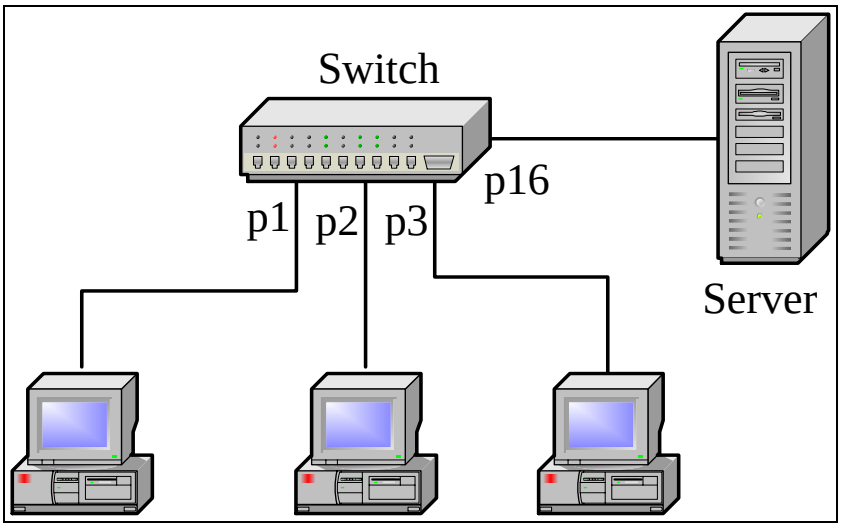
Result: This views PVLAN.

END OF STEPS

Result PVLAN has been configured.

Example This example describes how to add shared port 16 and isolated ports 1, 2, and 3 to the PVLAN. This is shown in Figure 28.

FIGURE 28 PLVAN CONFIGURATION EXAMPLE



Configuration

```
zte(cfg)#set pvlan session 1 add promis port 16 isolate-
port 1-3
zte(cfg)#show pvlan
  pvlan session   : 1
   promiscuous-port: 16
   isolated-port   : 1-3
   isolated-trunk  :

   pvlan session   : 2
   promiscuous-port:
   isolated-port   :
   isolated-trunk  :

   pvlan session   : 3
   promiscuous-port:
   isolated-port   :
   isolated-trunk  :

   pvlan session   : 4
   promiscuous-port:
   isolated-port   :
   isolated-trunk  :

zte(cfg)#
```

In PLVAN 2 session add trunk 16 with isolation port trunk 1, 2 and 3.

```
zte(cfg)#set pvlan session 2 add promis trunk 16 isolate-
trunk 1, 2, 3
zte(cfg)#show pvlan
  pvlan session   : 1
  promiscuous-port: 16
  isolated-port   : 1-3
  isolated-trunk  :

  pvlan session   : 2
  promiscuous-port: T16
  isolated-port   :
  isolated-trunk  : 1-3

  pvlan session   : 3
  promiscuous-port:
  isolated-port   :
  isolated-trunk  :

  pvlan session   : 4
  promiscuous-port:
  isolated-port   :
  isolated-trunk  :


zte(cfg)#
```

802. 1x Transparent Transmission

IEEE 802. 1x

IEEE 802. 1x is a port-based network access control protocol. Port-based network access control is a way to authenticate and authorize the users connected to the LAN equipment. This type of authentication provides a point-to-pint subscriber identification method in the LAN.

ZXR10 2920/2928/2952 provides 802. 1x transparent transmission function that allows the transparent transmission of 802. 1x protocol packets from the client to the authentication server for authentication.

Configuring 802. 1x Transparent Transmission

Purpose This topic describes the configuration of 802. 1x transparent transmission in ZXR10 2920/2928/2952.

Steps For configuration of 802. 1x transparent transmission, perform the following steps.

1. To enable/disable the 802. 1x transparent transmission function, use command **set 802. 1xrelay {enable|disable}** in global configuration mode. This is shown in Table 241.

TABLE 241 SET 802. 1X RELAY COMMAND

Format	Mode	Function
set 802. 1xrelay {enable|disable}	global config	This enable/disable the 802. 1x transparent transmission function

Result: This enable/disable the 802. 1x transparent transmission function.

2. To display the configuration of 802. 1x transparent transmission, use command **show 802. 1xrelay** in global configuration mode. This is shown in Table 242.

TABLE 242 SHOW 802. 1X RELAY COMMAND

Format	Mode	Function
show 802. 1xrelay	global config	This displays the configuration of 802. 1x transparent transmission

Result: This displays the configuration of 802. 1x transparent transmission.

END OF STEPS

Result 802. 1 x transparent transmissions in ZXR10 2920/2928/2952have been configured.

Layer 3 Configuration

Introduction to Layer 3 ZXR10 2920/2928/2952 provides few layer 3 functions for the remote configuration and management. To realize the remote access, an IP port must be configured on the switch. If the IP

port of the remote configuration host and that of the switch are not in the same network segment, it is also necessary to configure the static route.

Static route is a simple unicast route protocol. The next-hop address to a destination network segment is specified by user, where next hop is also called bridge. Static route involves destination address, destination address mask, next-hop address, and egress interface. Destination address and destination address mask describe the destination network information. The next-hop address and egress interface describe the way that switch forwards destination packet.

ZXR10 2920/2928/2952 allows addition and deletion of entries in the static ARP table. ARP table records mapping between IP address of each node in same network and MAC address. When sending IP packets, switch first checks whether destination IP address is in the same network segment. If yes, switch checks whether there is a peer end IP address and MAC address mapping entry in ARP table.

- If yes, switch directly sends the IP packets to this MAC address.
- If MAC address corresponding to peer end IP address cannot be found in ARP table, an ARP Request broadcast packet is sent to the network to query peer end MAC address.

Generally, entries of the ARP table on the switch are dynamic. Static ARP table entry is configured only when the connected host cannot respond to the ARP Request.

To configure the layer 3 function, use command **config router** to enter into layer 3 configuration mode first.

Configuring IP Port

Purpose This topic describes the configuration of IP port on ZXR10 2920/2928/2952.

Steps For the configuration of IP port, perform the following steps.

1. To set IP address and mask address of layer 3 port, use command **set ipport** <0-63> **ipaddress** {<A. B. C. D/M>|<A. B. C. D> < A. B. C. D>} in router config mode. This is shown in Table 243.

TABLE 243 SET IPPORT COMMAND

Format	Mode	Function
set ipport <0-63> **ipaddress** {<A. B. C. D/M>|<A. B. C. D> < A. B. C. D>}	router config	This sets IP address and mask address of layer 3 port

Result: This sets IP address and mask address of layer 3 port.

2. To bind the Vlan for layer 3 port, use command **set ipport** <0-63> **vlan** <vlanname> in router config mode. This is shown in Table 244.

TABLE 244 SET IPPORT VLAN COMMAND

Format	Mode	Function
set ipport <0-63> **vlan** <vlanname>	router config	This binds the Vlan for layer 3 port

Result: This binds the Vlan for layer 3 port.

3. To set the MAC address of layer 3 port, use command **set ipport** <0-63> **mac** <xx. xx. xx. xx. xx. xx> in router config mode. This is shown in Table 245.

TABLE 245 SET IPPORT MAC COMMAND

Format	Mode	Function
set ipport <0-63> **mac** <xx. xx. xx. xx. xx. xx>	router config	This sets the MAC address of layer 3 port

Result: This sets the MAC address of layer 3 port.

4. To enable/disable the layer 3 port, use command **set ipport** <0-63> **{enable|disable}** in router config mode. This is shown in Table 246.

TABLE 246 SET IPPORT ENABLE/DISABLE COMMAND

Format	Mode	Function
set ipport <0-63> **{enable|disable}**	router config	This enable/disable the layer 3 port

Result: This enable/disable the layer 3 port.

END OF STEPS

Result IP port on ZXR10 2920/2928/2952 has been configured.

Note: When modifying the configuration of an IP port, set the port to disable state first, and then modify the configuration. The new settings will overwrite the original ones.

Use the command **clear ipport** to clear one or all the parameters of the port. Before clearing parameters, set the port to disable state first.

Example Configure an IP port on the switch. Set the IP address of the port to 192. 1. 1. 1 and the mask to 24 digits. Bind the port to VLAN 100. The port uses the default address of the switch. The detailed configuration is as follows:

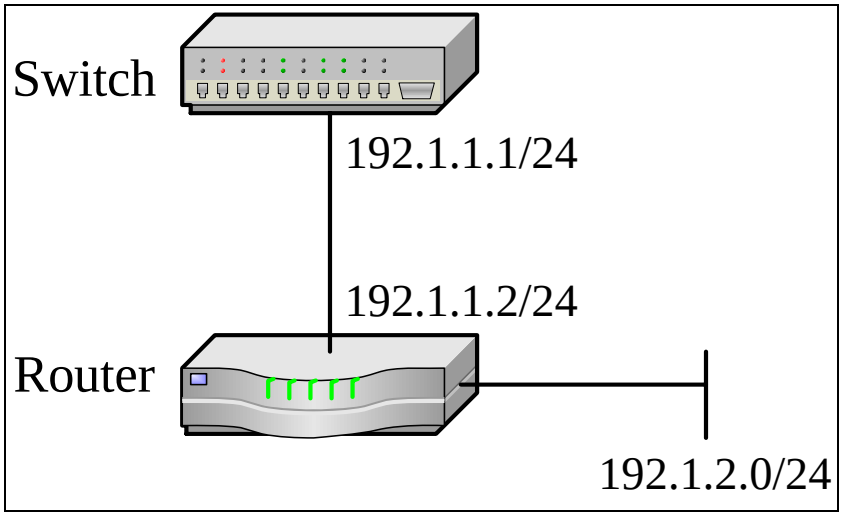
```
zte(cfg)#config router
zte(cfg-router)#set ipport 1 ipaddress 192. 1. 1.
1/24
zte(cfg-router)#set ipport 1 vlan 100
zte(cfg-router)#set ipport 1 enable
zte(cfg-router)#exit
zte(cfg)#
```

After the configuration is completed, use command **show ippor** to view the IP port configuration.

Static Route Configuration

After an IP port is configured, if the remote user to be connected is not in the network segment of the interface, use command **iproute** {<A. B. C. D/M>|<A. B. C. D> < A. B. C. D>} < A. B. C. D> [<1-15>]to set a static route to the remote network.

FIGURE 29 STATIC ROUTE



Remote host is located in the network segment 192. 1. 2. 0/24, which is not the same as the switch. This is shown in Figure 29.

To enable the communication between switch and host on the network segment 192. 1. 2. 0/24, configure the following static route.

```
zte(cfg)#config router
zte(cfg-router)#iproute 192.    1.    2.    0/24 192.    1.
1.   2
```

Use command **show iproute** to view the direct routes and static routes on the switch.

Command result displays destination network segment, next-hop address, route metric and egress interface of the static route. The following shows the result.

```
zte(cfg-router)#show iproute
  Type     IpAddress           Mask                  Gateway
Metric IPport
  ------ --------------- --------------- --------------- -
----- ------
  direct 192.    1.    1.    0        255.    255.    252.    0
192.   1.   1.   1        0      0
  static 192.    1.    2.    0        255.    255.    255.    0
192.   1.   1.   2        0      0
  Total: 2
```

Use command **clear iproute** to delete one or more static routes.

Configuring ARP Table Entry

Purpose This topic describes the configuration of ARP table entry.

Steps For the configuration of ARP table entry, perform the following steps.

1. To add a static ARP table entry, use command **arp add** <A. B. C. D> <xx. xx. xx. xx. xx. xx> <0-63> <vlanname> in router config mode. This is shown in Table 247.

TABLE 247 ARP ADD COMMAND

Format	Mode	Function
arp add <A. B. C. D> <xx. xx. xx. xx. xx. xx> <0-63> <vlanname>	router config	This adds a static ARP table entry

Result: This adds a static ARP table entry.

2. To delete a static ARP table entry, use command **arp delete** <A. B. C. D> in router config mode. This is shown in Table 248.

TABLE 248 ARP DELETE COMMAND

Format	Mode	Function
arp delete <A. B. C. D>	router config	This deletes a static ARP table entry

Result: This deletes a static ARP table entry.

3. To delete all static ARP table entry, use command **clear arp** in **clear arp** in router config mode. This is shown in Table 249.

TABLE 249 CLEAR ARP COMMAND

Format	Mode	Function
clear arp	router config	This deletes all static ARP table entry

Result: This deletes static ARP table entry.

4. To delete the ipport configuration, use command **clear ipport** *<0-63>* [**mac|ipaddress** {*<A. B. C. D/M>*|*<A. B. C. D>* *<A. B. C. D>*}|**vlan** *<vlanname>*]in router config mode. This is shown in Table 250.

TABLE 250 ARP IPPORT TIMEOUT COMMAND

Format	Mode	Function
arp ipport <0-63> **timeout** <1-1000>	router config	This sets ARP table entry aging time of the IP port

Result: This deletes the ipport configuration.

5. To delste the iproute configuration, use command **clear iproute** [{*<A. B. C. D/M>*|*<A. B. C. D>* *<A. B. C. D>*} *<A. B. C. D>*]in router config mode. This is shown in Table 250.

TABLE 251 ARP IPPORT TIMEOUT COMMAND

Format	Mode	Function
arp ipport <0-63> **timeout** <1-1000>	router config	This sets ARP table entry aging time of the IP port

Result: This deletes the iproute configuration.

6. To add the iproute, use command **add iproute** {*<A. B. C. D/M>*|*<A. B. C. D>* *<A. B. C. D>*} *<A. B. C.*

D> [<*1-15*>]in router config mode. This is shown in Table 250.

TABLE 252 ARP IPPORT TIMEOUT COMMAND

Format	Mode	Function
Add iproute {<*A. B. C. D/M*>|<*A. B. C. D*> <*A. B. C. D*>} <*A. B. C. D*> [<*1-15*>]	router config	This sets ARP table entry aging time of the IP port

Result: This adds the iproute.

7. To view ARP table entries, use command **show arp [static|dynamic|invalid|ipport**<0-63> **static|dynamic|invalid} |ipaddress** <A. B. C. D>] in router config mode. This is shown in Table 253.

TABLE 253 SHOW ARP COMMAND

Format	Mode	Function
show arp [static|dynamic|invalid|ipport<0-63> **static|dynamic|invalid} |ipaddress** <A. B. C. D>]	router config	This views ARP table entries

Result: This views ARP table entries.

8. To view ARP info, use command **show arp** [**static|dynamic|invalid|ipport** <*0-63*> [**static|dynamic|invalid**] **|ipaddress** <A. B. C. D>] in router config mode. This is shown in Table 253.

TABLE 254 SHOW ARP COMMAND

Format	Mode	Function
show arp [static|dynamic|invalid|ipport <*0-63***> [static|dynamic|invalid] |ipaddress <**A. B. C. D**>]**	router config	This views ARP table entries

Result: This views ARP info.

9. To view ipport, use command **show ipport** [<*0-63*>] in router config mode. This is shown in Table 253.

TABLE 255 SHOW ARP COMMAND

Format	Mode	Function
show ipport **[<*0-63*>]**	router config	This views ARP table entries

Result: This views ipport.

10. To view ARP info, use command **show arp iproute** in router config mode. This is shown in Table 253.

TABLE 256 SHOW ARP COMMAND

Format	Mode	Function
show arp iproute	router config	This views ARP table entries

Result: This views ARP iproute.

END OF STEPS

Result ARP table entry has been configured.

This page is intentionally blank.

Chapter 8

Access Service

Introduction

With the rapid expansion of Ethernet construction scale, to meet fast increase of subscribers and requirement of diversified broadband services, Network Access Service (NAS) is embedded on the switch to improve authentication and management of access subscribers and better support billing, security, operation, and management of broadband network.

NAS uses the 802. 1x protocol and RADIUS protocol to realize the authentication and management of access subscribers. It is highly efficient, safe, and easy to operate.

IEEE 802. 1x is called port-based network access control protocol. Its protocol system includes three key parts:

Client System

Client system is generally a user terminal system installed with client software. A subscriber originates the IEEE802. 1x protocol authentication process through this client software. To support the port-based network access control, client system must support Extensible Authentication Protocol Over LAN (EAPOL).

Authentication System

Authentication system is generally network equipment that supports IEEE802. 1x protocol, for example, switch. Corresponding to ports of different subscribers (ports could be physical ports or MAC address, VLAN, or IP address of user equipment). Authentication system has two logical ports: controlled port and uncontrolled port.

- Uncontrolled port is always in the state that the bidirectional connections are available. It is used to transfer EAPOL frames and can ensure that client can always send or receive authentication.
- Control port is enabled only when authentication is passed. It is used to transfer network resource and services. Controlled port can be configured as bidirectional controlled or input controlled to meet requirement of different applications. If subscriber authentication is not passed, this subscriber cannot visit services provided by authentication system.

Controlled port and uncontrolled port in the IEEE 802. 1x protocol are logical ports. There are no such physical ports on equipment. IEEE 802. 1x protocol sets up a local authentication for each subscriber that other subscribers cannot use. Thus, there will not be such a problem that the port is used by other subscribers after port is enabled.

Authentication Server

Authentication server is generally a RADIUS server. This server can store a lot of subscriber information, such as VLAN that the subscriber belongs to, CAR parameters, priority, subscriber access control list, and so on. After authentication of a subscriber is passed, authentication server will pass information of this subscriber to authentication system, which will create a dynamic access control list. Subsequent flow of subscriber will be monitored by above parameters. Authentication system communicates with RADIUS server through RADIUS protocol.

RADIUS is a protocol standard used for the authentication, authorization, and exchange of configuration data between the Radius server and Radius client.

Client/Server Mode

RADIUS adopts Client/Server mode. Client runs on NAS. It is responsible for sending subscriber information to specified Radius server and carrying out operations according to the result returned by the server.

Radius Authentication Server is responsible for receiving subscriber connection request, verifying the subscriber identity, and returning the configuration information required by the customer. A Radius Authentication Server can serve as a RADIUS customer proxy to connect to another Radius Authentication Server.

Radius Accounting Server

Radius Accounting Server is responsible for receiving the subscriber billing start request and subscriber billing stop request, and completing the billing function.

NAS communicates with Radius Server through RADIUS packets. Attributes in RADIUS packets are used to transfer detailed authentication, authorization, and billing information. Attributes used by this switch are primarily standard attributes defined in rfc2865, rfc2866, and rfc2869.

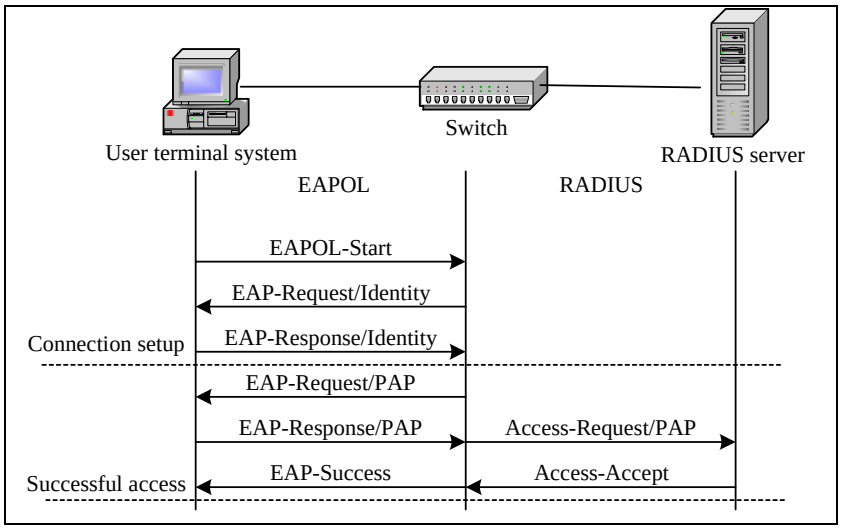
EAP protocol is used between switch and subscriber. Three types of identity authentication methods are provided between the RADIUS servers: PAP, CHAP, and EAP. Any of the methods can be used according to different service operation requirements.

Password Authentication Protocol (PAP)

PAP is a simple plain text authentication mode. NAS requires subscriber to provide username and password and subscriber returns subscriber information in the form of plain text. Server checks whether this subscriber is available and whether password is correct according to subscriber configuration and returns different responses. This authentication mode features poor security and username and password transferred may be easily stolen.

Process of using the PAP mode for identity authentication is shown in Figure 30.

FIGURE 30 USING PAP MODE FOR IDENTITY AUTHENTICATION

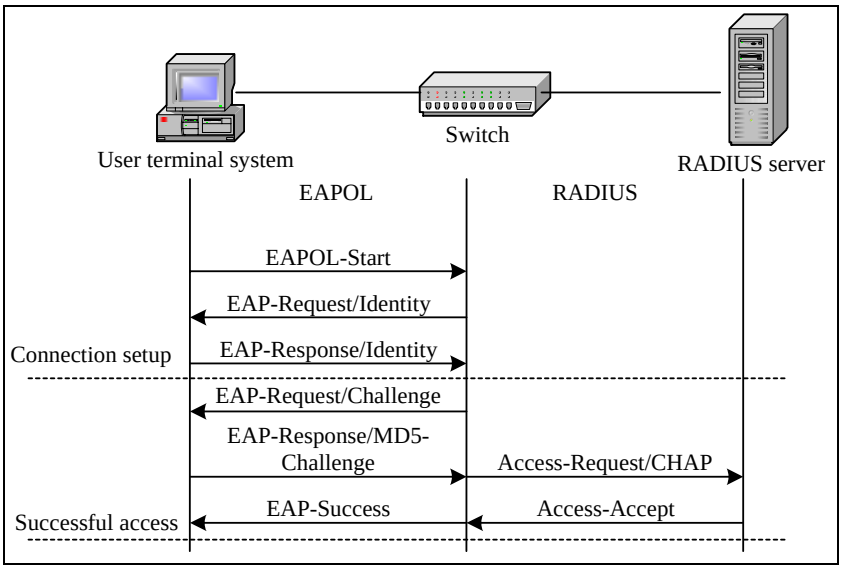


CHAP CHAP is an encrypted authentication mode and avoids transmission of user's real password upon the setup of connection. NAS sends a randomly generated Challenge string to user. User encrypts Challenge string by using own password and MD5 algorithm and returns username and encrypted Challenge string (encrypted password).

Server uses user password it stores and MD5 algorithm to encrypt Challenge string. It compares this Challenge string with encrypted password of the server and returns a response accordingly.

Process of using the CHAP mode for identity authentication is shown in

FIGURE 31 USING CHAP MODE FOR IDENTITY AUTHENTICATION

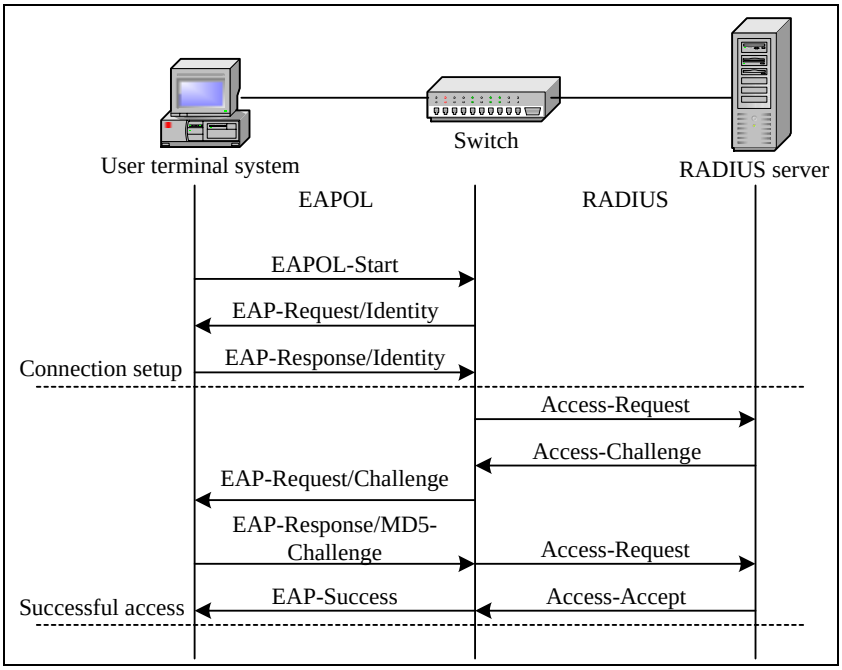


Extensible Authentication Protocol - Message Digest 5 (EAP-MD5)

EAP is an authentication method that transparently transmits EAP packets .It includes EAP-MD5 and PEAP.The following example explains EAP-MD5.

EAP-MD5 is a CHAP identity authentication mechanism used in the EAP framework structure. Process of using the EAP-MD5 mode for identity authentication is shown in

FIGURE 32 USING EAP-MD5 MODE FOR IDENTITY AUTHENTICATION



Configuring 802. 1x

Purpose This topic describes the configuration of 802. 1x on ZXR10 2920/2928/2952.

Steps For the configuration of 802. 1x, perform the following steps.

1. To enable/disable port 802. 1x function, use command **aaa-control port** <portlist> **dot1x {enable|disable}** in nas config mode. This is shown in Table 257.

TABLE 257 AAA CONTROL PORT COMMAND

Format	Mode	Function
aaa-control port <portlist> **dot1x {enable|disable}**	nas config	This enable/disable port 802. 1x function

Result: This enable/disable port 802. 1x function.

2. To configure the authentication control mode of the port, use command **aaa-control port** <portlist> **port-mode {auto|force-unauthorized| force-authorized}** in nas config mode. This is shown in Table 258.

TABLE 258 AAA CONTROL PORT MODE COMMAND

Format	Mode	Function
aaa-control port <portlist> **port-mode {auto|force-unauthorized| force-authorized}**	nas config	This configures the authentication control mode of the port

Result: This configures the authentication control mode of the port.

Note: The available modes include:

- Auto: Subscriber access from the port configured as "auto" must go through authentication. Subscriber access is successful only when authentication is successful.
- Force-authorized: Subscriber can be connected to network through this port without authentication.
- Force-unauthorized: Subscriber cannot be connected to network through this port.

Note: The default authentication control mode is "auto".

3. To allow/prohibit multi-subscriber access of the port, use command **aaa-control port** <portlist> **multiple-hosts {enable|disable}** in nas config mode. This is shown in Table 259.

TABLE 259 AAA CONTROL PORT MULTIPLE HOST COMMAND

Format	Mode	Function
aaa-control port <portlist> **multiple-hosts {enable|disable}**	nas config	This allows/prohibits multi-subscriber access of the port

Result: This allows/prohibits multi-subscriber access of the port.

4. To set the maximum number of subscribers connected through the port, use command **aaa-control port** <portlist> **max-hosts** <0-64> in nas config mode. This is shown in Table 260.

TABLE 260 AAA CONTROL PORT MAX HOSTS COMMAND

Format	Mode	Function
aaa-control port <portlist> **max-hosts** <0-64>	nas config	This set the maximum number of subscribers connected through port

Result: This sets the maximum number of subscribers connected through port.

Note: A port can allow access of multiple subscribers and each subscriber has own independent authentication and billing processes. The **aaa-control port max-hosts** command is valid only when the port allows access of multiple subscribers.

5. To enable/disable re-authentication mechanism, use command **dot1x re-authenticate {enable|disable}** in nas config mode. This is shown in Table 261.

TABLE 261 DOT1X RE-AUTHENTICATION COMMAND

Format	Mode	Function
dot1x re-authenticate {enable|disable}	nas config	This enable/disable re-authentication mechanism

Result: This enable/disable re-authentication mechanism.

6. To set the re-authentication interval, use command **dot1x re-authenticate period** <1-4294967295> in nas config mode. This is shown in Table 262.

TABLE 262 DOT1X RE-AUTHENTICATION PERIOD COMMAND

Format	Mode	Function
dot1x re-authenticate period <1-4294967295>	nas config	This sets the re-authentication interval

Result: This sets the re-authentication interval.

Important! To judge whether access subscriber maintains connection all time, NAS can periodically request re-authentication of this subscriber. Re-authentication needs to initiate a complete authentication process for each on-line subscriber. If number of subscribers is large, there will be a lot of authentication packets, which brings a heavy burden to the switch.

7. To enable/disable abnormal off-line detection mechanism of the port, use command **aaa-control port** <portlist> **keepalive {enable|disable}** in nas config mode. This is shown in Table 263.

TABLE 263 AAA CONTROL PORT KEEPALIVE COMMAND

Format	Mode	Function
aaa-control port <portlist> **keepalive {enable|disable}**	nas config	This enable/disable abnormal off-line detection mechanism of the port

Result: This enable/disable abnormal off-line detection mechanism of the port.

8. To set the abnormal off-line detection period of the port, use command **aaa-control port** <portlist> **keepalive period** <1-3600> in nas config mode. This is shown in Table 264.

TABLE 264 AAA CONTROL PORT KEEPALIVE PERIOD

Format	Mode	Function
aaa-control port <portlist> **keepalive period** <1-3600>	nas config	This sets the abnormal off-line detection period of the port

Result: This sets the abnormal off-line detection period of the port.

Note: The following are the main features of abnormal off-line detection mechanism.

- Besides re-authentication mechanism, NAS module also introduces abnormal off-line detection mechanism to judge whether subscriber still keeps the connection. Abnormal off-line detection mechanism only requires a

few packet interactions to determine whether the subscriber is still on line.

- Abnormal off-line detection mechanism is implemented in this way: Device takes the initiative to send a detection request periodically to the client. EAPOL/EAP RepId packet defined in the 802. 1x protocol is used as request packet. When EAPOL/EAP RepId response is received from client, it means that subscriber is still on line. Otherwise, the subscriber is off line.

9. To set authentication mode of the port, use command **aaa-control port** <portlist> **protocol {pap|chap|eap}** in nas config mode. This is shown in Table 265.

TABLE 265 AAA CONTROL PROTOCOL COMMAND

Format	Mode	Function
aaa-control port <portlist> **protocol {pap|chap|eap}**	nas config	This sets authentication mode for the port

Result: This sets authentication mode for port.

Note: During the subscriber access authentication, there are three subscriber identity authentication methods between the authentication server and the authentication system: PAP, CHAP, and EAP. The default one is EAP.

END OF STEPS

Result 802. 1x on ZXR10 2920/2928/2952 has been configured.

Configuring Protocol Parameters of 802. 1x

Purpose This topic describes the configuration of protocol parameters or 802. 1x on ZXR10 2920/2928/2952.

Steps For the configuration of protocol parameters, perform the following steps.

1. To set interval between first authentication failure of authentication system and next authentication request, use command **dot1x quiet-period** <0-65535> in nas config mode. This is shown in Table 266.

TABLE 266 DOT1X QUIET PERIOD COMMAND

Format	Mode	Function
dot1x quiet-period <0-65535>	nas config	This sets interval between first authentication failure of authentication system and next authentication request

Result: This sets interval between first authentication failure of authentication system and next authentication request.

2. To set time that authentication system needs to wait before it can resend EAPOL data packet because it does not receive the response from the client, use command **dot1x tx-period** <1-65535> in nas config mode. This is shown in Table 267.

TABLE 267 DOT1X QUIET PERIOD COMMAND

Format	Mode	Function
dot1x quiet-period <0-65535>	nas config	This set time that authentication system needs to wait before it can resend EAPOL data packet

Result: This set time that authentication system needs to wait before it can resend EAPOL data packet.

3. To set timeout time for authentication system to receive data packets from authentication client system, use command **dot1x supplicant-timeout** <1-65535> in nas config mode. This is shown in Table 268.

TABLE 268 DOT1X SUPPLICANT TIMEOUT COMMAND

Format	Mode	Function
dot1x supplicant-timeout <1-65535>	nas config	This set timeout time for authentication system to receive data packets from authentication client system

Result: This set timeout time for authentication system to receive data packets from authentication client system.

4. To set timeout time for authentication system to receive data packets from authentication server, use command **dot1x server-timeout** <1-65535> in nas config mode. This is shown in Table 269.

TABLE 269 DOT1X SERVER TIMEOUT COMMAND

Format	Mode	Function
dot1x server-timeout <1-65535>	nas config	This set timeout time for authentication system to receive data packets from authentication server

Result: This set timeout time for authentication system to receive data packets from authentication server.

5. To set maximum times of request resending when timer expires before authentication system receives Challenge response from client, use command **dot1x max-request** <1-10> in nas config mode. This is shown in Table 270.

TABLE 270 DOT1X MAX REQUEST COMMAND

Format	Mode	Function
dot1x max-request <1-10>	nas config	This set maximum times of request resending when timer expires before authentication system receives Challenge response from client

Result: This set maximum time of request resending when timer expires before authentication system receives Challenge response from client.

Note: 802. 1x realizes the access control by exchanging EAPOL data packets between client system and authentication system and RADIUS data packets between authentication system and authentication server. During exchange of data packets, the following parameters are used for control purpose:

- QuietPeriod refers to the period before which authentication system will not receive authentication request from client system after first authentication failure. This function can prevent the subscriber's continuous authentication attempts.
- TxPeriod refers to the time after which authentication system will resend EAPOL data packets to client system when it does not receive the response from client system.
- Supplicant Timeout and serverTimeout respectively refer to the time during which authentication system shall receive data packet from client system and authentication server.

- Max-request refers to maximum times of request resending when timer expires before authentication system receives Challenge response from client system.

6. To display the 802. 1x configuration of the port, use command **show aaa-control port** [<portlist>] in nas config mode. This is shown in Table 271.

TABLE 271 SHOW AAA CONTROL PORT COMMAND

Format	Mode	Function
show aaa-control port [<portlist>]	nas config	This displays the 802. 1x configuration of the port

Result: This displays the 802. 1x configuration of the port.

7. To display the 802. 1x protocol parameters, use command **show dot1x** in nas config mode. This is shown in Table 272.

TABLE 272 SHOW DOT1X COMMAND

Format	Mode	Function
show dot1x	nas config	This displays the 802. 1x protocol parameters

Result: This displays the 802. 1x protocol parameters.

END OF STEPS

Result Protocol parameters or 802. 1x has been configured on ZXR10 2920/2928/2952.

Configuring RADIUS

Purpose This topic describes the RADIUS configuration of ZXR10 2920/2928/2952.

Steps For the configuration of RADIUS, perform the following steps.

1. To add/delete an ISP domain, use command **radius isp** <ispname> **{enable|disable}** in nas config mode. This is shown in Table 273.

TABLE 273 RADIUS ISP COMMAND

Format	Mode	Function
radius isp <ispname> **{enable|disable}**	nas config	This add/delete an ISP domain

Result: This add/delete an ISP domain.

Important! In RADIUS configuration, concept of isp-domain is introduced. Different domains may be operated by different ISPs. Access equipment identifies domain that subscriber belongs to according to domain name in subscriber name (username@DomainName) input by the subscriber and sends authentication and billing requests of subscriber to authentication server and billing server of the corresponding domain. Each domain has its own RADIUS server. After a domain is deleted, all the configurations related to this domain are deleted.

2. To add authentication server to domain, use command **radius isp** <ispname> **add authentication** <A. B. C. D> [<0-65535>] in nas config mode. This is shown in Table 274.

TABLE 274 RADIUS ISP ADD AUTHENTICATION COMMAND

Format	Mode	Function
radius isp <ispname> **add authentication** <A. B. C. D> [<0-65535>]	nas config	This add authentication server to domain

Result: This add authentication server to domain.

3. To delete the authentication server from domain, use command **radius isp** <ispname> **delete authentication** <A. B. C. D> in nas config mode. This is shown in Table 275.

TABLE 275 RADIUS ISP DELETE AUTHENTICATION COMMAND

Format	Mode	Function
radius isp <ispname> **delete authentication** <A. B. C. D>	nas config	This deletes the authentication server from domain

Result: This deletes the authentication server form domain.

Note: A domain can be configured with up to three authentication servers. Priority of server is determined by configuration order. First server configured enjoys highest priority, and last server has lowest priority. When a server is deleted, priorities of related servers rise in sequence.

4. To add an accounting server to the domain, use command **radius isp** <ispname> **add accounting** <A. B. C. D> [<0-65535>] in nas config mode. This is shown in Table 276.

TABLE 276 RADIUS ISP ADD ACCOUNTING COMMAND

Format	Mode	Function
radius isp <ispname> **add accounting** <A. B. C. D> [<0-65535>]	nas config	This adds an accounting server to the domain

Result: This adds an accounting server to the domain.

5. To delete an accounting server from the domain, use command **radius isp** <ispname> **delete accounting** <A. B. C. D> in nas config mode. This is shown in Table 277.

TABLE 277 RADIUS ISP DELETE ACCOUNTING COMMAND

Format	Mode	Function
radius isp <ispname> **delete accounting** <A. B. C. D>	nas config	This deletes an accounting server from the domain

Result: This deletes an accounting server from the domain.

Note: A domain can be configured with up to three accounting servers. Priority of the server is determined by configuration order. First server configured enjoys highest priority, and last server has lowest priority. When a server is deleted, priorities of the related servers rise in sequence.

6. To set the IP address of the client in the domain, use command **radius isp** <ispname> **client** <A. B. C. D> in nas config mode. This is shown in Table 278.

TABLE 278 RADIUS ISP CLIENT COMMAND

Format	Mode	Function
radius isp <ispname> **client** <A. B. C. D>	nas config	This sets the IP address of the client in the domain

Result: This sets the IP address of the client in the domain.

Note: IP address of client in domain must be IP address of an interface on the switch.

7. To set shared password, use command **radius isp** <ispname> **sharedsecret** <string> in nas config mode. This is shown in Table 279.

TABLE 279 RADIUS ISP SHAREDSECRET

Format	Mode	Function
radius isp <ispname> **sharedsecret** <string>	nas config	This sets shared password

Result: This sets shared password.

Note: Shared password is used for data encryption between RADIUS client and RADIUS server. Setting of shared password must be consistent on the client and server.

8. To specify a default domain, use command **radius isp** <ispname> **defaultisp {enable|disable}** in nas config mode. This is shown in Table 280.

TABLE 280 DEFAULT ISP DEFAULT ISP COMMAND

Format	Mode	Function
radius isp <ispname> **defaultisp {enable|disable}**	nas config	This specifies a default domain

Result: This specifies a default domain.

Note: Only one domain can be specified as default domain in system. System will send subscriber authentication requests without domain name specified on RADIUS authentication server in default domain.

9. To set full account of domain, use command **radius isp** <ispname> **fullaccount {enable|disable}** in nas config mode. This is shown in Table 281.

TABLE 281 RADIUS ISP FULLACCOUNT COMMAND

Format	Mode	Function
radius isp <ispname> **fullaccount {enable|disable}**	nas config	This sets full account of domain

Result: This sets full account of domain.

Note: When it is specified to use full account, RADIUS client uses "username@DomainName" as subscriber name to request authentication of RADIUS server. If it is not specified to use full account, subscriber name will not contain domain name.

10. To configure domain description, use command **radius isp** <ispname> **description** <string> in nas config mode. This is shown in Table 282.

TABLE 282 RADIUS ISP DESCRIPTION COMMAND

Format	Mode	Function
radius isp <ispname> **description** <string>	nas config	This configures domain description

Result: This configures domain description.

11. Configuration of RADIUS parameters:

i. To set server response timeout time, use command **radius timeout** <1-255> in nas config mode. This is shown in Table 283.

TABLE 283 RADIUS TIMEOUT COMMAND

Format	Mode	Function
radius timeout <1-255>	nas config	This sets server response

Result: This sets server response.

ii. To set number of retransmissions upon server response timeout, use command **radius retransmit** <1-255> in nas config mode. This is shown in Table 284.

TABLE 284 RADIUS RETRANSMIT COMMAND

Format	Mode	Function
radius retransmit <1-255>	nas config	This sets number of retransmission upon server response timeout

Result: This sets number of retransmission upon server response timeout.

iii. To set NAS server name, use command **radius nasname** <nasname> in nas config mode. This is shown in Table 285.

TABLE 285 RADIUS NASNAME COMMAND

Format	Mode	Function
radius nasname <nasname>	nas config	This sets NAS server name

Result: This sets NAS server name.

12. To Enable/Disable billing function of port, use command **aaa-control port** <portlist> **accounting {enable|disable}** in nas config mode. This is shown in Table 286.

TABLE 286 AAA CONTROL PORT COMMAND

Format	Mode	Function
aaa-control port <portlist> **accounting {enable|disable}**	nas config	This Enable/Disable billing function of port

Result: This Enable/Disable billing function of port.

13. To delete accounting of packet, use command **clear accounting-stop** { **session-id** <session-id> | **user-name** <user-name> | **isp-name** <isp-name> | **server-ip** <A. B. C. D>} in nas config mode. This is shown in Table 287.

TABLE 287 CLEAR ACCOUNTING STOP COMMAND

Format	Mode	Function
clear accounting-stop { **session-id** <session-id> | **user-name** <user-name> | **isp-name** <isp-name> | **server-ip** <A. B. C. D>}	nas config	This deletes accounting of packet

Result: This deletes accounting of packet.

14. To display RADIUS configuration, use command **show radius** [{**ispName** [<ispname>] } | {**accounting-stop** [**session-id** <session-id>] [**user-name** <user-name>] [**isp-name** <isp-name>] [**server-ip** <A. B. C. D>] }] in nas config mode. This is shown in Table 288.

TABLE 288 SHOW RADIUS COMMAND

Format	Mode	Function
show radius [{**ispName** [<ispname>] } | {**accounting-stop** [**session-id** <session-id>] [**user-name** <user-name>] [**isp-name** <isp-name>] [**server-ip** <A. B. C. D>] }]	nas config	This displays RADIUS configuration

Result: This displays RADIUS configuration.

END OF STEPS

Result RADIUS has been configured on ZXR10 2920/2928/2952.

Example This example describes how to enable 802. 1x function of port 1. Set quiet-period to 60 seconds, tx-period to 30 seconds,

supp-timeout to 30 seconds, and server-timeout to 30 seconds. Enable keepalive function and set keepalive interval to 10 seconds.

```
zte(cfg-nas)#aaa-control port 1 dot1x enable
zte(cfg-nas)#dot1x quiet-period 60
zte(cfg-nas)#dot1x tx-period 30
zte(cfg-nas)#dot1x supplicant-timeout 30
zte(cfg-nas)#dot1x server-timeout 30
zte(cfg-nas)#aaa-control port 1 keepalive enable
zte(cfg-nas)#aaa-control port 1 keepalive period 10

zte(cfg-nas)#show aaa-control 1
  PortId                                          :     1
PortControl                                       : auto
  Dot1x                                           :
enabled         AuthenticationProtocol: eap
  KeepAlive                                       :
enabled         KeepAlivePeriod                   : 10
  Accounting                                      :
disabled        MultipleHosts                     :
disabled
  MaxHosts    :  0                       HistoryHostsTotal
             : 0
  OnlineHosts                                        : 0

zte(cfg-nas)#show dot1x
  TxPeriod     : 30                           QuietPeriod
              : 60
  SuppTimeout                  :                        30
              ServerTimeout    : 30
  ReAuthPeriod                 :                      3600
              ReAuthenticate   : disabled
  MaxReq                       : 2
zte(cfg-nas)#
```

Enable re-authentication function and set re-authentication period to 3600 seconds.

```
zte(cfg-nas)#dot1x re-authenticate enable
zte(cfg-nas)#dot1x re-authenticate period 3600

zte(cfg-nas)#show dot1x
  TxPeriod     : 30                          QuietPeriod
             : 60
  SuppTimeout                  :                          30
             ServerTimeout     : 30
  ReAuthPeriod                 :                        3600
             ReAuthenticate    : enabled
  MaxReq                       : 2
zte(cfg-nas)#
```

Set the authentication control state of port 1 to auto and authentication mode to CHAP. Enable multi-subscriber access. Maximum number of subscriber accessed is 5.

```
zte(cfg-nas)#aaa-control port 1 port-mode auto
zte(cfg-nas)#aaa-control port 1 protocol chap
zte(cfg-nas)#aaa-control port 1 multiple-hosts enable
zte(cfg-nas)#aaa-control port 1 max-hosts 5

zte(cfg-nas)#show aaa-control 1
  PortId                       :                           1
             PortControl                              : auto
  Dot1x                        :                       enabled
             AuthenticationProtocol                   : chap
  KeepAlive                    :                       enabled
             KeepAlivePeriod          : 10
  Accounting                   :                     disabled
             MultipleHosts                            :
enabled
  MaxHosts                     :                           5
             HistoryHostsTotal                        : 0
  OnlineHosts                    : 0
```

Configure RADIUS domain 188 according to the following requirements:

- Authentication server address and accounting server address: 10. 40. 92. 212 and 10. 40. 92. 215
- Share Password: 123456
- Client IP address: 10. 40. 92. 100. Use default domain.

```
zte(cfg-nas)#radius isp 188 enable
zte(cfg-nas)#radius isp 188 add authentication 10.    40.
92.   212
zte(cfg-nas)#radius isp 188 add authentication 10.    40.
92.   215
zte(cfg-nas)#radius isp 188 add accounting 10.   40.   92.
215
zte(cfg-nas)#radius isp 188 add accounting 10.   40.   92.
212
zte(cfg-nas)#radius isp 188 sharedsecret 123456
zte(cfg-nas)#radius isp 188 client 10.   40.   92.   100
zte(cfg-nas)#radius isp 188 defaultisp enable

zte(cfg-nas)#show radius 188
  Client                :  10.      40.      92.      100
             IspName      : 188
  DefaultIsp   : Yes             Description :
  FullAccounts      : No               SharedSecret:
123456
  Authentication servers  Auth-port
  ----------------------  ---------
  10.   40.   92.   212             1812
  10.   40.   92.   215             1812
  Accounting servers      Acct-port
  ----------------------  ---------
  10.   40.   92.   215             1813
  10.   40.   92.   212             1813

zte(cfg-nas)#
```

QinQ Overview

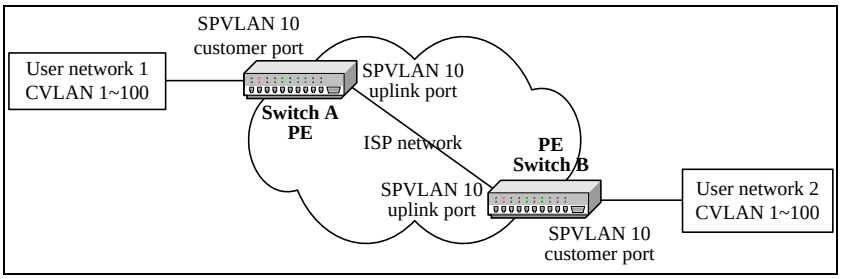
QinQ description

QinQ is IEEE 802. 1Q tunneling protocol and is also called VLAN stacking. QinQ technology is the addition of one more VLAN tag (outer tag) to the original VLAN tag (inner tag). Outer tag can shield the inner tag.

QinQ does not need protocol support. Simple Layer 2 Virtual Private Network (L2VPN) can be realized through QinQ. QinQ is especially suitable for small-size LAN that takes layer 3 switch as its backbone.

Figure 33 shows typical networking of the QinQ technology. Port connected to user network is called Customer port. Port connected to ISP network is called Uplink port. Edge access equipment of ISP network is called Provider Edge (PE).

FIGURE 33 QINQ NETWORKING



SPVLAN: Service Provider VLAN CVLAN: Customer VLAN

User Network

User network is generally connected to PE through Trunk VLAN mode. Internal Uplink ports of the ISP network are symmetrically connected through the Trunk VLAN mode.

- When a packet is sent form user network 1 to customer port of switch A because PORTBASE VLAN-based customer port does not identify the tag when receiving the packet, customer port processes the packet as an untagged packet no matter whether this data packet is attached with VLAN tag or not. Packet is forwarded by VLAN 10, which is determined by the PVID.
- Uplink port of switch A inserts outer tag (VLAN ID: 10) when forwarding data packet received from customer port. Tpid of this tag can be configured on switch. Inside ISP network, packet is broadcast along port of VLAN 10 until it reaches switch B.
- Switch B finds out that port connected to user network 2 is a customer port. Thus, it removes outer tag in compliance with conventional 802. 1Q protocol to recover original packet and sends packet to user network 2.
- In this way, data between user network 1 and user network 2 can be transmitted transparently. VLAN IDs of user network can be planned regardless of conflict with VLAN IDs in ISP network.

Configuring QinQ

Purpose

This topic describes the PVLAN configuration on ZXR10 2920/2928/2952.

Steps

For the PVLAN configuration, perform the following steps.

1. To add/delete a Customer port, use command **set qinq customer port** <portlist> **{enable|disable}** in global configuration mode. This is shown in Table 289.

TABLE 289 SET QINQ CUSTOMER PORT COMMAND

Format	Mode	Function
set qinq customer port <portlist> **{enable|disable}**	global config	This add/delete a customer port

Result: This add/delete a customer port.

2. To add/delete an uplink port, use command **set qinq uplink port** <portlist> **{enable|disable}** in global configuration mode. This is shown in Table 290.

TABLE 290 SET QINQ UPLINK PORT COMMAND

Format	Mode	Function
set qinq uplink port <portlist> **{enable|disable}**	global config	This add/delete a uplink port

Result: This add/delete a uplink port.

3. To set tpid of the outer tag, use command **set qinq tpid** <tpid> in global configuration mode. This is shown in Table 291.

TABLE 291 SET QINQ TPID COMMAND

Format	Mode	Function
set qinq tpid <tpid>	global config	This set tpid of the outer tag

Result: This set tpid of the outer tag.

4. To display QinQ configuration, use command **show qinq** in global configuration mode. This is shown in Table 292.

TABLE 292 SHOW QINQ COMMAND

Format	Mode	Function
show qinq	global config	This displays QinQ configuration

Result: This displays QinQ configuration.

END OF STEPS

Result PVLAN has been configured on ZXR10 2920/2928/2952.

Note When QinQ is configured, customer port and uplink port of SPVLAN can be set as an untagged port, or as a tagged port.

Example This example describes that suppost customer port of switch A is port 1 and uplink port is port 24. Customer port of switch B is port 1 and uplink port is port 24. This is shown in Figure 33.

```
zte(cfg)#set vlan 10 enable
zte(cfg)#set vlan 10 add port 1, 24
zte(cfg)#set port 1, 24 pvid 10
zte(cfg)#set qinq customer port 1 enable
zte(cfg)#set qinq uplink port 24 enable
```

Configuration of switch B is same as that of switch A.

SQinQ Overview

SQinQ (Selective QinQ) is based on QinQ technology. Selective QinQ configuration enables packets to be tagged with external tags according to tag they already carry.

SQinQ uses same terms as QinQ to describe its features:

- Customer port: port connected to Client Network;
- Uplink port: port connected to Service Provider Network
- PE (Provider Edge): accessing equipment at the edge of Service Provider Network.
- Client Network is accessed to PE via Trunk VLAN.
- Uplink Ports inside Service Provider Network are connected via Trunk VLAN symmetrically.
- By matching specific ACL traffic rules in ports, SQinQ functions can set different Service Provider's VLAN tags for packets.
- Packets are transmitted in Service Provider Network. Vlan Tags of Service Provider would be strip off when packets leave Service Provider Vlan.

SQinQ configuration is determined as per following conditions:

Customer Port Strategy Configuration

Normally, a set of Customer Vlans is set in one Uplink Port. Several sets of Customer Vlans can be in one Uplink Port when it is confirmed that all Vlans in this port are different with each other. Configuration of SQinQ in Customer Port only makes sense for packets which carrying 802. 1Q tag and for designated Customer Vlan. As to the Customer Vlan which carries 802. 1P tag or untag, they are all handled as normal Vlan.

Note: SQinQ would not work in good condition when QinQ is already configured. Reason is that port could not recognize Customer Vlan Tag any more when QinQ is configured on this port. Consequently, SQinQ would not get any Customer Vlan information.

SQinQ does not support binding with Trunk directly so far. However, binding with Trunk could be supported indirectly: adding ports bound with the function of SQinQ to a Trunk in which ports must belong to same SQinQ Session.

Service Provider Vlan Configuration

It is necessary to operate Service Provider Network after Customer Port configuration. Packets can be exchanged successfully. Configure all ports in Service Provider Network as Tag Ports and all Customer Ports as Untag Ports.

All the packets exchanged in Service Provider Network carry two layers of Tag which are Uplink Tag and Customer Tag. When packets leaving Service Provider Network, there is only one layer of Tag left: Customer Tag.

Configuring SQinQ

Purpose

This topic describes the configuration of SQinQ strategy policy.

Steps

For the configuration of SQinQ, perform the following steps.

1. To configure SQinQ session, use command **set sqinq-session** <1-256> **customer-vlan** <vlanlist> **uplink-vlan** <1-4094> in global configuration mode. This is shown in Table 293.

TABLE 293 SET SQINQ SESSION COMMAND

Format	Mode	Function
set sqinq-session <1-256> **customer-vlan** <vlanlist> **uplink-vlan** <1-4094>	global config	This configures SQinQ session

Result: This configures SQinQ session.

2. To set Qos remark, use command set policy **qos-remark in sqinq-session** <1-256> **profile** <0-71> **up {no-change|enable-modify|disable-modify} dscp {no-change|enable-modify |disable-modify}** in global configuration mode. This is shown in Table 294.

TABLE 294 QOS REMARK IN SQINQ COMMAND

Format	Mode	Function
qos-remark in sqinq-session <1-256> **profile** <0-71> **up {no-change|enable-modify|disable-modify} dscp {no-change|enable-modify |disable-modify}**	global config	This sets Qos remark

Result: This sets Qos remark.

3. To clear Qos remark, use command **clear policy qos-remark in sqinq-session** <1-256> in global configuration mode. This is shown in Table 295.

TABLE 295 CLEAR POLICY QOS COMMAND

Format	Mode	Function
clear policy qos-remark in sqinq-session <1-256>	global config	This clears Qos remark

Result: This clears Qos remark.

4. To monitor traffic, use command **set policy policing in sqinq-session** <1-256> **policer** <0-255> in global configuration mode. This is shown in Table 296.

TABLE 296 SET POLICY POLICING COMMAND

Format	Mode	Function
set policy policing in sqinq-session <1-256> **policer** <0-255>	global config	This monitors traffic

Result: This monitors traffic.

5. To clear traffic monitor, use command **clear policy policing in sqinq-session** <1-256> in global configuration mode. This is shown in Table 297.

TABLE 297 CLEAR POLICY POLICING COMMAND

Format	Mode	Function
clear policy policing in sqinq-session <1-256>	global config	This clears traffic monitor

Result: This clears traffic monitor.

6. To redirect policy for traffic, use command **set policy redirect in sqinq-session** <1-256> **port** < portname> in global configuration mode. This is shown in Table 298.

TABLE 298 SET POLICY REDIRECT COMMAND

Format	Mode	Function
set policy redirect in sqinq-session <1-256> **port** < portname>	global config	This redirects policy for traffic

Result: This redirects policy for traffic.

7. To clear redirect policy, use command **clear policy redirect in sqinq-session** <1-256> in global configuration mode. This is shown in Table 299.

TABLE 299 CLEAR POLICY REDIRECT COMMAND

Format	Mode	Function
clear policy redirect in sqinq-session <1-256>	global config	This clears redirect policy

Result: This clears redirect policy.

8. To set policy of statistics, use command **set policy statistics in sqinq-session** <1-256> **counter** <0-31> in global configuration mode. This is shown in Table 300.

TABLE 300 SET POLICY STATISTICS COMMAND

Format	Mode	Function
set policy statistics in sqinq-session <1-256> **counter** <0-31>	global config	This sets policy of statistics

Result: This sets policy of statistics.

9. To clear policy of statistics, use command **clear policy statistics in sqinq-session** <1-256> in global configuration mode. This is shown in Table 301.

TABLE 301 CLEAR POLICY STATISTICS COMMAND

Format	Mode	Function
clear policy statistics in sqinq-session <1-256>	global config	This clears policy of statistics

Result: This clears policy of statistics.

10. To apply SQinQ session to port, use command **set port** <portlist> **sqinq-session** <sessionlist> **{enable|disable}** in global configuration mode. This is shown in Table 302.

TABLE 302 SET PORT SQINQ SESSION COMMAND

Format	Mode	Function
set port <portlist> **sqinq-session** <sessionlist> **{enable|disable}**	global config	This applies SQinQ session to port

Result: This applies SQinQ session to port.

11. To clear SQinQ session in port, use command **clear sqinq-session** <sessionlist> in global configuration mode. This is shown in Table 303.

TABLE 303 CLEAR SQINQ SESSION COMMAND

Format	Mode	Function
clear sqinq-session <sessionlist>	global config	This clears SQinQ session in port

Result: This clear SQinQ session in port.

12. To view parameters of SQinQ session use command **show sqinq-session** [<sessionlist>] in global configuration mode. This is shown in Table 304.

TABLE 304 SHOW SQINQ SESSION COMMAND

Format	Mode	Function
show sqinq-session [<sessionlist>]	global config	This views parameters of SQinQ session

Result: This views parameters of SQinQ session.

END OF STEPS

Result SQinQ strategy policy has been configured.

Example This example describes that there are two switches of ZXR10-5124 (Switch A and Switch B) in Service Provider Network. Port 24 of Switch A is connected to port 24 of Switch B. Vlan1-200 is in port 1 through 6 of Switch A which communicate with port 1 through 3 of Switch B in which Uplink vlanid assigned as 100. Vlan201-4094 is in port 1 through 6 of Switch A which communicates with port 4 though 6 of Switch B in which Uplink vlanid assigned as 200. Customer Port of Switch A is untag port only for Vlan1.

Configuration of Switch A

```
zte(cfg)#set sqinq-session 1 customer-vlan 1-200 uplink-vlan 100
zte(cfg)#set port 1-6 sqinq-session 1 enable
zte(cfg)#set vlan 100 enable
zte(cfg)#set vlan 100 add port 1-6 untag
zte(cfg)#set vlan 100 add port 24 tag
zte(cfg)#set sqinq-session 2 customer-vlan 201-4094 uplink-vlan 200
zte(cfg)#set port 1-6 sqinq-session 2 enable
zte(cfg)#set vlan 200 enable
zte(cfg)#set vlan 200 add port 1-6 untag
zte(cfg)#set vlan 200 add port 24 tag
```

Configuration of Switch B

```
zte(cfg)#set sqinq-session 1 customer-vlan 1-200 uplink-
vlan 100
zte(cfg)#set port 1-3 sqinq-session 1 enable
zte(cfg)#set vlan 100 enable
zte(cfg)#set vlan 100 add port 1-3 untag
zte(cfg)#set vlan 100 add port 24 tag
zte(cfg)#set sqinq-session 2 customer-vlan 201-4094
uplink-vlan 200
zte(cfg)#set port 4-6 sqinq-session 2 enable
zte(cfg)#set vlan 200 enable
zte(cfg)#set vlan 200 add port 4-6 untag
zte(cfg)#set vlan 200 add port 24 tag
```

Syslog Overview

Syslog Information Center

Syslog is a key part of Ethernet switch. It is the information center of system software module. Syslog manages and classify most output information so that the information can be filtered effectively to support network manager and developer monitoring network running circumstance and diagnosing network fault.

Syslog log system classifies log information to eight levels according to the Levels. This is shown in Table 324.

TABLE 305 SYSLOG INFORMATION

Level	Description
Emergencies	Very much emergent error
Alerts	Error needing to correct immediately
Critical	Critical error
Errors	Error needing to note but not critical
Warnings	Warnings, maybe error exist
Notifications	Information that needs notification
Informational	Normal suggestion information
Debugging	Debugging information

Configuring Syslog

Purpose This topic describes the configuration of Syslog on ZXR10 2920/2928/2952.

Steps For the configuration of Syslog, perform the following steps.

1. To enable/disable syslog, use command **set syslog** in global configuration mode. This is shown in Table 306.

TABLE 306 SET SYSLOG COMMAND

Format	Mode	Function
set syslog	global config	This enable/disable syslog

Result: This enable/disable syslog.

Note: By default syslog is disabled. Syslog is enabled when there is much log information, the system performance will degrade.

2. To define syslog information level, use command **set syslog level** in global configuration mode. This is shown in Table 307.

TABLE 307 SET SYSLOG LEVEL COMMAND

Format	Mode	Function
set syslog level	global config	This defines syslog information level

Result: This defines syslog information level.

Note: Default level of syslog information is informational. If level of syslog information is configured to emergencies, the information will be sent firstly.

3. To setup syslog information receiving server, use command **set syslog {add | delete} server** in global configuration mode. At most five IP addresses of syslog server can be configured. This is shown in Table 308.

TABLE 308 SET SYSLOG SERVER COMMAND

Format	Mode	Function
set syslog {add | delete} server	global config	This setups syslog information receiving server

Result: This setups syslog information receiving server.

4. To enable/disable module of syslog, use command **set syslog module** in global configuration mode. This is shown in Table 309.

TABLE 309 SET SYSLOG MODULE COMMAND

Format	Mode	Function
set syslog module	global config	This enable/disable module of syslog

Result: This enable/disable module of syslog.

5. To display configuration of syslog, use command **show syslog status** in global configuration mode. This is shown in Table 310.

TABLE 310 SHOW SYSLOG STATUS COMMAND

Format	Mode	Function
show syslog status	global config	This displays configuration of syslog

Result: This displays configuration of syslog.

END OF STEPS

Result Syslog has been configured on ZXR10 2920/2928/2952.

Example In this example, syslog in switch is enabled, level of information is informational and all functional modules are enabled. IP address of server is 192. 168. 1. 1 and name of server is Srv1.

Configuration

```
zte(cfg)#set syslog level informational
zte(cfg)#set syslog add server 1 ipaddress 192. 168.
1. 1 name Srv1
zte(cfg)#set syslog module all enable
zte(cfg)#set syslog enable
zte(cfg)#show syslog status
  Syslog status: enable
  Syslog alarm level: informational
  Syslog enabled modules:
  alarm         cmdlog
  Syslog server IP            Name
  1             192.  168.  1.  1  Srv1

zte(cfg)#
```

Configuring NTP

Network Time Protocol NTP (Network Time Protocol) is used by Ethernet switches to synchronize time with other network devices. ZXR10 2920/2928/2952 provides function of NTP client and synchronizes time with the NTP servers in network.

Purpose This topic describes the configuration of NTP.

Steps For the configuration of NTP, perform the following steps.

1. To enable/disable NTP, use command **set ntp** in global configuration mode. This is shown in Table 311.

TABLE 311 SET NTP COMMAND

Format	Mode	Function
set ntp	global config	This enable/disable NTP

Result: This enable/disable NTP.

Note: Only after configuring this command, the following commands can be configured. To synchronize time with NTP server, configuring IP address of NTP server is also required.

2. To setup NTP server IP address, use command **set ntp server** in global configuration mode. This is shown in Table 312.

TABLE 312 SET NTP SERVER COMMAND

Format	Mode	Function
set ntp server	global config	This setups NTP server IP address

Result: This setups NTP server IP address.

Note: At present only one NTP server can be configured. If several NTP servers are configured, the latter will cover the former.

3. To configure source IP address which is used when switch sends time synchronization request of NTP protocol, use command **set ntp source** in global configuration mode. This is shown in Table 313.

TABLE 313 SET NTP SOURCE COMMAND

Format	Mode	Function
set ntp source	global config	This configure source IP address which is used when switch sends time synchronization request of NTP protocol

Result: This configures source IP address which is used when switch send time synchronization request of NTP protocol.

Note: By default, switch doesn't configure source address, when NTP send time synchronization request, IP address that the message need is decided by network layers.

4. To view NTP status, use command **show ntp** in global configuration mode. This is shown in Table 314.

TABLE 314 SHOW NTP COMMAND

Format	Mode	Function
show ntp	global config	This views NTP status

Result: This views NTP status.

END OF STEPS

Result NTP has been configured.

Example: In this example, switch will synchronize time with NTP server whose IP address is 202. 10. 10. 10.

Configuration

```
zte(cfg)#set ntp server 202.   10.   10.   10
zte(cfg)#set ntp enable
zte(cfg)#show ntp
  ntp protocol is enable
  ntp protocol version : 3
  ntp server address   : 202.   10.   10.   10
  ntp source address   : None
  ntp is_synchronized  : No
  ntp rcv stratum      : 16
  no reference clock.
zte(cfg)#
```

In the output, ntp is_synchronized represents whether switch has synchronized time with NTP server.

GARP/GVRP Overview

GARP uses Protocols GARP (Generic Attribute Registration Protocol) uses different protocols to dynamically distribute attribute information, such as VLAN and MAC address of multicast for members in switch network.

GVRP GVRP (GARP VLAN Registration Protocol) is a kind of protocol defined by GARP. GVRP can dynamically maintenance information of VLAN in switches.

One switch which supports GVRP can receive information of VLAN registration from other switches and dynamically update local information of VLAN registration including current VLANs in switch and interfaces in these VLANs.

One switch which supports GVRP also can send local information of VLAN registration to other switches.

Configuring GARP

Purpose This topic describes the configuration of GARP.

Steps For the configuration of GARP, perform the following steps.

1. To enable/disable GARP, use command **set garp** in global configuration mode. This is shown in Table 315.

TABLE 315 SET GARP COMMAND

Format	Mode	Function
set garp	global config	This enable/disable GARP

Result: This enable/disable GARP.

Note: By default GARP is disabled.

2. To set timer of GARP, use command **set garp timer {hold|join|leave|leaveall}** <timer_value> in global configuration mode. This is shown in Table 316.

TABLE 316 SET GARP TIMER COMMAND

Format	Mode	Function
set garp timer {hold|join|leave|leaveall} <timer_value>	global config	This sets timer of GARP

Result: This sets timer of GARP.

Note: There are four kinds of timer including hold timer, join timer, leave timer, and leave all timer.

3. To show GARP information and timer setup status, use command **show garp** in global configuration mode. This is shown in Table 317.

TABLE 317 SHOW GARP COMMAND

Format	Mode	Function
show garp	global config	This shows GARP information and timer setup status

Result: This shows GARP information and timer setup status.

Note: All timers which enable GARP must be exactly same otherwise application protocol can't work normally.

END OF STEPS

Result GARP has been configured.

Configuring GVRP

Purpose This topic describes the configuration of GVRP.

Steps For the configuration of GVRP, perform the following steps.

1. To enable/disable GVRP, use command **set gvrp** in global configuration mode. This is shown in Table 318.

TABLE 318 SET GVRP COMMAND

Format	Mode	Function
set gvrp	global config	This enable/disable GVRP

Result: This enable/disable GVRP.

Note: By default, GVRP is disabled. GVRP is only enabled when GARP is enabled.

2. To enable/disable GVRP in port, use command **set gvrp port** <portlist> **{enable|disable}** in global configuration mode. This is shown in Table 319.

TABLE 319 SET GVRP PORT COMMAND

Format	Mode	Function
set gvrp port <portlist> **{enable|disable}**	global config	This enable/disable GVRP in port

Result: This enable/disable GVRP in port.

Note: By default, GVRP in port is disabled. After enabling GVRP in port, the port can receive packets of GVRP protocol.

3. To configure type of GVRP registration in port, use command **set gvrp port** <portlist> **registration {normal|fixed|forbidden}** in global configuration mode. This is shown in Table 320.

TABLE 320 SET GVRP PORT REGISTRATION COMMAND

Format	Mode	Function
set gvrp port <portlist> **registration {normal|fixed|forbidden}**	global config	This configure type of GVRP registration in port

Result: This configures type of GVRP registration in port.

Note: By default, system port GVRP registration status is normal, this command is to setup port GVRP registration type. There are three types of registration types:

Normal: Switches handle the receipt information of GARP. Switches can dynamically create, register and withdraw VLAN.

Fixed: Switches ignore all information of GARP but are still in registration status. Permit manually creating and registering VLAN, and prevent withdrawing VLAN. Other ports can’t register VLANs which are received from the port.

Forbidden: Ignore all information of GARP, withdraw all VLANs except VLAN1 and prevent creating and registering other VLANs in port.

4. To enable/disable GVRP in trunk port, use command **set gvrp trunk** <trunklist> **{enable|disable}** in global configuration mode. This is shown in Table 321.

TABLE 321 SET GVRP TRUNK COMMAND

Format	Mode	Function
set gvrp trunk <trunklist> **{enable|disable}**	global config	This enable/disable GVRP in trunk port

Result: This enable/disable GVRP in trunk port.

Note: By default, GVRP in trunk port is disabled**.** After enabling GVRP in trunk port, the port can receive packets of GVRP protocol.

5. To configure trunk port and GVRP registration type, use command **set gvrp trunk** <trunklist> **registration {normal|fixed|forbidden}** in global configuration mode. This is shown in Table 322.

TABLE 322 SET GVRP TRUNK REGISTRATION COMMAND

Format	Mode	Function
set gvrp trunk <trunklist> **registration {normal|fixed|forbidden}**	global config	This configures trunk port and GVRP registration type

Result: This configures trunk port and GVRP registration type.

Note: By default, type of GVRP registration in trunk port is normal. There are three kinds of registration type in trunk port. Functions of them are same as that in port.

6. To show GVRP configuration information, use command **show gvrp** in global configuration mode. This is shown in Table 323.

TABLE 323 SHOW GVRP COMMAND

Format	Mode	Function
show gvrp	global config	This shows GVRP configuration information

Result: This shows GVRP configuration information.

END OF STEPS

Result GVRP has been configured.

Example

In this example, enable/disable GARP and set GARP timer.

Configuration

```
zte(cfg)#set garp enable
zte(cfg)#set garp disable

zte(cfg)#set garp timer hold 100
zte(cfg)#set garp timer join 200
zte(cfg)#set garp timer leave 600
zte(cfg)#set garp timer leaveall 10000
```

In this example, show GARP configuration status.

```
zte(cfg)#show garp
  GARP is enabled!
  GARP Timers:
  Hold Timeout      :100 millisecond
  Join Timeout      :200 millisecond
  Leave Timeout     :600 millisecond
  LeaveAll Timeout  :10000 millisecond
```

In this example, enable/disable GVRP, enable/disable GVRP in port and configure type of registration in port.

```
zte(cfg)#set gvrp enable
zte(cfg)#set gvrp disable

zte(cfg)#set gvrp port 2 enable
zte(cfg)#set gvrp port 2 disable

zte(cfg)#set gvrp port 2 registration fixed
zte(cfg)#set gvrp port 2 registration forbidden
zte(cfg)#set gvrp port 2 registration normal
```

In this example, enable/disable GVRP in trunk port and configure type of registration in trunk port.

```
zte(cfg)#set gvrp trunk 2 enable
zte(cfg)#set gvrp trunk 2 disable

zte(cfg)#set gvrp trunk 2 registration fixed
zte(cfg)#set gvrp trunk 2 registration forbidden
zte(cfg)#set gvrp trunk 2 registration normal
```

In this example, show GVRP configuration status.

```
zte(cfg)#show gvrp
  GVRP is enabled!

  PortId Status   Registration LastPduOrigin
  ------ -------- ------------ -----------------
  2         Enabled   Fixed          00.    00.    00.    00.
00.   00
  T2        Enabled   Normal         00.    00.    00.    00.
00.   00
```

DHCP Snooping/Option82

DHCP (Dynamic Host Configuration Protocol) is a protocol that the network host sends request to server to get host configuration in dynamic mode.

DHCP Server and Client

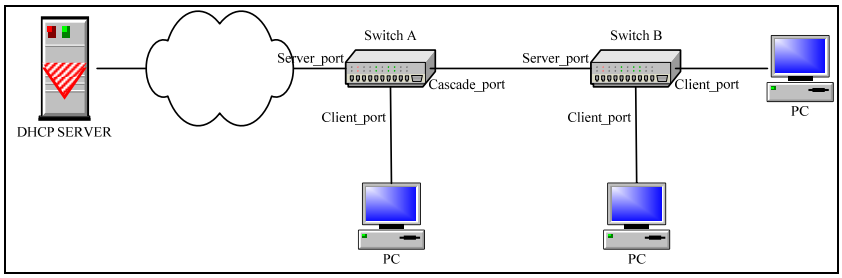
As having no IP address, DHCP servers interact in broadcasting way, and course is transparent. There is no authentication between DHCP server and client. There may be DHCP servers that establish a private and illegal way, which causes confusion to part of the hosts of their address distribution, gateway and DNS parameters, and make it impossible for the hosts to connect to the external network.

Strengthening of Network

There will be IP deceiving, MAC address deceiving and user ID deceiving from illegal client, and exhaustion of DHCP server address. DHCP Snooping and Option82 are designed to solve these safety problems. DHCP Snooping, namely DHCP packet filtering, is to detect legality of DHCP packets based on some special rules and filter illegal packets. Use Option82 technique to provide more additional information, and then strengthen the network safety ability.

Typical applications of DHCP Snooping and Option82 are shown in Figure 34.

FIGURE 34 TYPICAL NETWORK OF DHCP



DHCP Snooping Function

Set attribute of the port on switch connecting to users directly as Client. Set attribute of the port up-connecting to server as Server, and that of port cascade connecting as Cascade. Enable DHCP Snooping function, and DHCP response packets coming into switch from the port except Server port will be filtered. This method solves the problem caused by private DHCP server. Switch generates and maintains an information table of users who succeed to get host configuration, which make it effective to distinguish and prevent the illegal users of IP or MAC address deceiving from accessing.

Enable IP source guard function on the base of DHCP Snooping. It can stop IP data flow with illegal address, and it also can prevent flux attack caused by embezzling neighbor IP address.

DHCP Option82

Enable DHCP Option82 function, and request DHCP packets sent by users will add Option82 according to user configurations. It makes it possible for hosts to interact with more special information with DHCP Server. Using Circuit ID sub-option, switch provides user access link information, which is good for server to distribute and manage address. Server limits the amount of user IP address that distributed to each Remote ID labeled switch, which prevent IP address from exhausting. With incident user ID option of Option82, DHCP server does not need to use the un-authorized or off-standard client identify field. Correlating user MAC address and Remote ID makes server to prevent illegal users of other Remote ID who use same MAC address to deceive from accessing.

Configuring Global DHCP

Purpose

This topic describes the DHCP global configuration on ZXR10 2920/2928/2952 to support snooping and Option82 function.

Steps

For the global configuration of DHCP, perform the following steps.

1. To enable/disable the system of DHCP function, use command **set dhcp {enable|disable}** in global configuration mode. This is shown in Table 324.

TABLE 324 SET DHCP COMMAND

Format	Mode	Function
set dhcp {enable|disable}	global config	This enable/disable the system of DHCP function

Result: This enable/disable the system of DHCP function.

Note: System DHCP function is disabled by default. This command is used to enable or disabled the function globally.

2. To configure DHCP attribute of port, use command **set dhcp port** <portname> **{server|cascade|client}** in global configuration mode. This is shown in Table 325.

TABLE 325 SET DHCP PORT COMMAND

Format	Mode	Function
set dhcp port <portname> **{server|cascade|client}**	global config	This configures DHCP attribute of port

Result: This configures DHCP attribute of port.

Important! There are three kinds of attributes of the port: server (port connecting to DHCP server), cascade (cascade connecting port) client (port connecting to client). Attribute is client by default.

3. To display DHCP information and attribute of the ports, use command **show dhcp** in global configuration mode. This is shown in Table 326.

TABLE 326 SHOW DHCP COMMAND

Format	Mode	Function
show dhcp	global config	This displays DHCP information and attribute of the ports

Result: This displays DHCP information and attribute of the ports.

END OF STEPS

Result DHCP global has been configured on ZXR10 2920/2928/2952 and to support snooping and Option82 function.

Note DHCP global configurations are indispensable precondition to use Snooping and Option82 function. Port attribute should be set accurately; otherwise it will impact DHCP interaction.

Configuring DHCP Snooping

Purpose This topic describes the DHCP snooping configuration on ZXR10 2920/2928/2952.

Steps For the DHCP snooping configuration, perform the following steps.

1. To enable/disable DHCP Snooping function based on port, use command **set dhcp snooping {add|delete} port** <portlist> in global configuration mode. This is shown in Table 327.

TABLE 327 SET DHCP SNOOPING COMMAND

Format	Mode	Function
set dhcp snooping {add|delete} port <portlist>	global config	This enable/disable DHCP Snooping function based on port

Result: This enable/disable DHCP Snooping function based on port.

Note: DHCP snooping function is disabled by default. This command is to enable or disable DHCP Snooping function on port. Only in the condition that the global DHCP function is enabled can this function be enabled. DHCP function on the ports connecting to user and that connecting to server should be enabled at same time.

2. To display DHCP Snooping configurations, use command **show dhcp snooping** in global configuration mode. This is shown in Table 328.

TABLE 328 SHOW DHCP SNOOPING COMMAND

Format	Mode	Function
show dhcp snooping	global config	This displays DHCP Snooping configurations

Result: This displays DHCP Snooping configurations.

3. To display information of DHCP Snooping dynamic binding table, use command **show dhcp snooping binding [port** <portname>**]** in global configuration mode. This is shown in Table 329.

TABLE 329 SHOW DHCP BINDING PORT COMMAND

Format	Mode	Function
show dhcp snooping binding [port <portname>**]**	global config	This displays information of DHCP Snooping dynamic binding table

Result: This displays information of DHCP Snooping dynamic binding table.

Note: Display information of the host that get dynamic configurations on DHCP Snooping enabled port recorded by switch

4. To clear information of DHCP Snooping dynamic binding table/item, use command **clear dhcp snp-bind-entry** {**all|port** <portname>|**mac** <xx. xx. xx. xx. xx. xx>} in global configuration mode. This is shown in Table 330.

TABLE 330 CLEAR DHCP SNP BIND COMMAND

Format	Mode	Function
clear dhcp snp-bind-entry {**all|port** <portname>|**mac** <xx. xx. xx. xx. xx. xx>}	global config	This clears information of DHCP Snooping dynamic binding table/item.

Result: This clears information of DHCP Snooping dynamic binding table/item.

Important! There are three kinds of modes to clear information of DHCP Snooping dynamic binding table/item: clear all, based on port and based on MAC address.

Note: All items in table are dynamic generated and cleared. Only when network trouble appears and dynamic host configurations fail to recover, users are advertised to clear table items by hand. Otherwise it will impact DHCP interaction.

END OF STEPS

Result DHCP snooping has been configured on ZXR10 2920/2928/2952.

Configuring IP Source Guard

Purpose This topic describes IP source guard configuration on ZXR10 2920/2928/2952.

Steps For the configuration of IP source guard, perform the following steps.

1. To enable/disable IP source guard function based on port, use command **set dhcp ip-source-guard {add|delete} port** <portlist> in global configuration mode. This is shown in Table 331.

TABLE 331 SET DHCP IP SOURCE GUARD COMMAND

Format	Mode	Function
set dhcp ip-source-guard {add|delete} port <portlist>	global config	This enable/disable IP source guard function based on port.

Result: This enable/disable IP source guard function based on port.

2. To display IP source guard configuration, use command **show dhcp ip-source-guard** in global configuration mode. This is shown in Table 332.

TABLE 332 SHOW DHCP IP SOURCE GUARD COMMAND

Format	Mode	Function
show dhcp ip-source-guard	global config	This displays IP source guard configuration

Result: This displays IP source guard configuration.

END OF STEPS

Result IP source guard has been configured on ZXR10 2920/2928/2952.

Configuring DHCP Option82

Purpose This topic describes the Option82 configuration on ZXR10 2920/2928/2952.

Steps For the configuration of Option82, perform the following steps.

1. To configure access-node-identifier, use command **set dhcp option82 ani** <string> in global configuration mode. This is shown in Table 333.

TABLE 333 SET DHCP OPTION82 COMMAND

Format	Mode	Function
set dhcp option82 ani <string>	global config	This configures access node identifier

Result: This configures access node identifier.

2. To enable/disable Option82 function based on port, use command **set dhcp option82 {add|delete} port**

<portlist> in global configuration mode. This is shown in Table 334.

TABLE 334 SET DHCP OPTION82 COMMAND

Format	Mode	Function
set dhcp option82 {add|delete} port <portlist>	global config	This enable/disable Option82 function based on port

Result: This enable/disable Option82 function based on port.

Note: Option82 function is disabled by default. Command is to enable/disable Option82 function on port. When global DHCP function is enable then this function is enabled.

3. To enable/disable DHCP Option82 Circuit_ID sub-option based on port, use command **set dhcp option82 sub-option port** <portname> **circuit-ID {on \|{cisco\|china-tel\|dsl-forum}\|off}** in global configuration mode. This is shown in Table 335.

TABLE 335 SET DHCP OPTION82 SUB-OPTION COMMAND

Format	Mode	Function
set dhcp option82 sub-option port <portname> **circuit-ID {on |{cisco|china-tel|dsl-forum}|off}**	global config	This enable/disable DHCP Option82 Circuit_ID sub-option based on port

Result: This enable/disable DHCP Option82 Circuit_ID sub-option based on port.

Important! ZXR10 2920/2928/2952 supports three forms of Circuit_ID sub-option: Cisco form, CHINA-TEL form and DSL-Forum form.

4. To enable/disable DHCP Option82 Subscriber_ID sub-option based on port, use command **set dhcp option82 sub-option port** <portname> **Subscriber-ID {on** <string>**\|off}** in global configuration mode. This is shown in Table 336.

TABLE 336 SET DHCP OPTION82 COMMAND

Format	Mode	Function
set dhcp option82 sub-option port <portname> **Subscriber-ID {on** <string>**|off}**	global config	This enable/disable DHCP Option82 Subscriber_ID sub-option based on port

Result: This enable/disable DHCP Option82 Subscriber_ID sub-option based on port.

5. To configure expanding option of DHCP Option82 based on port, use command **set dhcp option82 sub-option port** <portname> **reserve {on tag** <1-255> **value** <string>**|off}** in global configuration mode. This is shown in Table 337.

TABLE 337 SET DHCP OPTION82 SUB-OPTION PORT COMMAND

Format	Mode	Function
set dhcp option82 sub-option port <portname> **reserve {on tag** <1-255> **value** <string>**|off}**	global config	This configures expanding option of DHCP Option82 based on port.

Result: This configures expanding option of DHCP Option82 based on port.

Note: ZXR10 2920/2928/2952 supports Circuit_ID, Remote_ID and Subscriber_ID. These three sub-options, tags are 1, 2 and 6 in order. Circuit_ID supports three forms. Remote_ID is enabled by default and does not need to configure it. Besides, switches support a sub-option which uses in expanding.

6. To display DHCP Option82 configuration information, use command **show dhcp Option82** in global configuration mode. This is shown in Table 338.

TABLE 338 SHOW DHCP OPTION82 COMMAND

Format	Mode	Function
show dhcp Option82	global config	This displays DHCP Option82 configuration information

Result: This displays DHCP Option82 configuration information.

7. To display DHCP Option82 access-node-identifier, use command **show dhcp Option82 ani** in global configuration mode. This is shown in Table 339.

TABLE 339 SHOW DHCP OPTION82 ANI COMMAND

Format	Mode	Function
show dhcp Option82 ani	global config	This displays DHCP Option82 access-node-identifier

Result: This displays DHCP Option82 access node identifier.

8. To display DHCP Option82 configuration information based on port, use command **show dhcp Option82 port**

<portname> in global configuration mode. This is shown in Table 340.

TABLE 340 SHOW DHCP OPTION82 PORT COMMAND

Format	Mode	Function
show dhcp Option82 port <portname>	global config	This displays DHCP Option82 configuration information based on port

Result: This displays DHCP Option82 configuration information based on port.

9. To clear configuration of DHCP Option82 access-node-identifier, use command **clear dhcp Option82 ani** in global configuration mode. This is shown in Table 341.

TABLE 341 CLEAR DHCP OPTION82 ANI COMMAND

Format	Mode	Function
clear dhcp Option82 ani	global config	This clears configuration of DHCP Option82 access-node-identifier

Result: This clears configuration of DHCP Option82 access-node-identifier.

END OF STEPS

Result Option82 has been configured on ZXR10 2920/2928/2952.

Example This example shows the following instance of DHCP global configuration.

```
zte(cfg)#set dhcp enable
zte(cfg)#set dhcp port 1 server
zte(cfg)#set dhcp port 24 cascade
zte(cfg)#set dhcp disable
```

The following instance shows DHCP Snooping configuration.

```
zte(cfg)#set dhcp snooping add port 1-8，24
zte(cfg)#set dhcp snooping delete port 5
```

The following instance shows the configuration information of DHCP Snooping.

```
zte(cfg)#show dhcp snooping
  DHCP snooping is enabled on the following port(s):
  portID    portType
  ------    --------
  1         Server
  2         Client
  3         Client
  4         Client
  6         Client
  7         Client
  8         Client
  24        Cascade

zte(cfg)#
```

The following instance shows DHCP Option82 configuration.

```
zte(cfg)#set dhcp option82 add port 1-8, 24
zte(cfg)#set dhcp option82 delete port 5
zte(cfg)#set dhcp option82 ani nanjing68
zte(cfg)#set dhcp option82 sub-option port 7 circuit-ID on
china-tel
zte(cfg)#set dhcp option82 sub-option port 7 subscriber-ID
on yuhuatai
```

The following instance shows DHCP Option82 configuration information.

```
zte(cfg)#show dhcp option82
  DHCP option82 is enabled on the following port(s):
  portID    portType
  ------    --------
  1         Server
  2         Client
  3         Client
  4         Client
  6         Client
  7         Client
  8         Client
  24        Cascade

zte(cfg)#show dhcp option82 port 7
  DHCP option82 information on port 7:

  circuit-ID: Enabled
    format: CHINA-TEL

  remote-ID: Enabled
    format: Cisco

  subscriber-ID: Enabled
    value: yuhuatai

  reserve sub-option: Disabled

zte(cfg)#
```

VBAS Overview

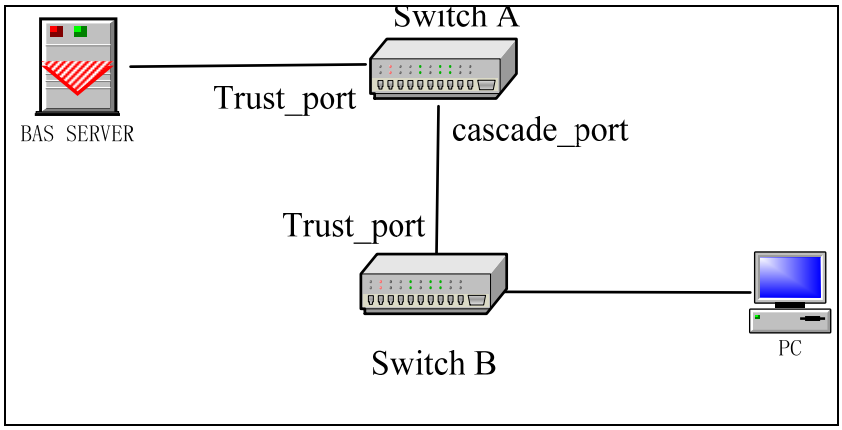
VBAS itself is not physical equipment, is a standard protocol, which is developed by Guangdong Institute of China Telecom. VBAS is to solve the problem of wideband user identifier. When BAS gets user identifier by inquiring correspondence relationship of users MAC dialing to the switch and port, then sends user name, password and identifier information to RADIUS, it can realize the position of the user.

Layer 2 communication mode takes place between BAS and switches, that is, information query and response data packets of VBAS are encapsulated into Ethernet data frames in layer 2 directly, and use protocol number 0x8200 to identify.

Note Only trust ports can receive VBAS packets for switches and VBAS response packets only can be sent from trust ports.

Port connecting to user network is called cascade port and port connecting to BAS server is called trust port. Typical network of VBAS is shown in

FIGURE 35 TYPICAL NETWORK OF VBAS



Configuring VBAS

Purpose This topic describes the configuration of VBAS.

Steps For the configuration of VBAS, perform the following steps.

1. To enable/disable global VBAS function, use command **set vbas {enable|disable}** in global configuration mode. This is shown in Table 342.

TABLE 342 SET VBAS COMMAND

Format	Mode	Function
set vbas {enable|disable}	global config	This enable/disable global VBAS function

Result: This enable/disable global VBAS function.

Note: VBAS function is disabled by default. This command is to enable/disable VBAS globally.

2. To enable/disable trust port VBAS function, use command **set vbas trust-port** <portlist> **{enable|disable}** in global configuration mode. This is shown in Table 343.

TABLE 343 SET VBAS TRUST PORT COMMAND

Format	Mode	Function
set vbas trust-port <portlist> **{enable|disable}**	global config	This enable/disable trust port VBAS function

Result: This enable/disable trust port VBAS function.

Note: By default port is no trusted.

3. To enable/disable cascade port VBAS function, use command **set vbas cascade-port** <portlist> **{enable|disable}** in global configuration mode. This is shown in Table 344.

TABLE 344 SET VBAS CASCADE PORT COMMAND

Format	Mode	Function
set vbas cascade-port <portlist> **{enable|disable}**	global config	This enable/disable cascade port VBAS function

Result: This enable/disable cascade port VBAS function.

4. To display VBAS configuration, use command **show vbas** in global configuration mode. This is shown in Table 345.

TABLE 345 SHOW VBAS COMMAND

Format	Mode	Function
show vbas	global config	This displays VBAS configuration

Result: This displays VBAS configuration.

END OF STEPS

Result VBAS has been configured.

Example This example describes how to trust port of switch A is port 1, cascade port is port 2, and trust port of switch B is port 1. This is shown in Figure 35.

Configuration of Switch A

```
zte(cfg)#set vbas enable
zte(cfg)#set vbas trust-port 1 enable
zte(cfg)#set vbas cascade-port 2 enable
```

Configuration of Switch B

```
zte(cfg)#set vbas enable
zte(cfg)#set vbas trust-port 1 enable
```

Show Configuration of Switch A

```
zte(cfg)#show vbas
vbas enable
trust port    :1
cascade port  :2
```

Show Configuration of Switch B

```
zte(cfg)#show vbas
vbas enable
trust port    :1
cascade port  :
```

sFlow Monitoring Overview

Description of sFlow

Sample Flow (sFlow) is a technique to monitor data transmission of network equipments such as routers and switches. sFlow monitors flow of 10-gigabit or even bigger speed, and has advantages of timely, actual, low-cost and being upgraded. sflow is an expert format, and adds more information of monitored data packets. It uses sFlow proxy embedded in network equipments to send the sampled data packets to the sFlow collectors. sFlow collectors analyzes and processes the packets then gets information of current network.

Configuring sFlow

Purpose

This topic describes the configuration of sFlow on ZXR10 2920/2928/2952/5116-FI/5124-FI.

Steps

For the configuration of sFlow, perform the following steps.

1. To set proxy IP address of sFlow, use command **set sflow agent-address** <A. B. C. D> in global configuration mode. This is shown in Table 346.

TABLE 346 SET SFLOW AGENT ADDRESS COMMAND

Format	Mode	Function
set sflow agent-address <A. B. C. D>	global config	This sets proxy IP address of sFlow

Result: This sets proxy IP address of sFlow.

Note: Proxy IP address should be layer 3 poet IP address of switches. If there are no enabled layer 3 ports on the switches, proxy IP address of sFlow can not be set.

2. To set IP address of sFlow collector, use command **set sflow collector-address** <A. B. C. D> in global configuration mode. This is shown in Table 347.

TABLE 347 SET SFLOW COLLECTOR ADDRESS COMMAND

Format	Mode	Function
set sflow collector-address <A. B. C. D>	global config	This sets IP address of sFlow collector

Result: This sets IP address of sFlow collector.

3. To enable sample flow function on port, use command in global configuration mode, **set sflow{ingress|egress}port**<portlist>**{on frequency**<20000-100000000>**|off}**<20000-100000000> is the sample frequency of port with data packets as its unit. This is shown in Table 348.

TABLE 348 SET SFLOW PORT COMMAND

Format	Mode	Function
set sflow{ingress|egress}port<portlist>**{on frequency**<20000-100000000>**|off}**<20000-100000000>	global config	This enables sample flow function on port.

Result: This enables sample function on port.

4. To set ingress sample mode of sFlow function, use command **set sflow ingress sample-mode {forward|good}** in global configuration mode. This is shown in Table 349.

TABLE 349 SET SFLOW INGRESS COMMAND

Format	Mode	Function
set sflow ingress sample-mode {forward|good}	global config	This sets ingress sample mode of sFlow function

Result: This sets ingress sample mode of sFlow function.

5. To set sample frequency reload-mode on port of sFlow function, use command **set sflow {ingress|egress} reload-mode {continuous|cpu}** in global configuration mode. This is shown in Table 350.

TABLE 350 SET SFLOW RELOAD MODE COMMAND

Format	Mode	Function
set sflow {ingress|egress} reload-mode {continuous|cpu}	global config	This sets sample frequency reload-mode on port of sFlow function

Result: This sets sample frequency reload-mode on port of sFlow function.

Parameters Description:

- **Continuous** mode is continuous reload-mode, is using same sample frequency in each sample time.
- **Cpu** mode is cpu control mode, is each time it finishes to sample, cpu will generate a random sample frequency.

6. To clear sFlow configurations, use command **set sflow clear-config** in global configuration mode. This is shown in Table 351.

TABLE 351 SET SFLOW CLEAR CONFIG COMMAND

Format	Mode	Function
set sflow clear-config	global config	This clear sFlow configurations

Result: This clears sFlow configurations.

END OF STEPS

Result sFlow has been configured on ZXR10 2920/2928/2952/5116-FI/5124-FI.

Examples In the following instance, it shows configurations of IP addresses of sFlow proxy and collector, and it enables the sample flow function on port 1.

```
zte(cfg)#set sflow agent-address 192.   168.   1.   1
zte(cfg)#set sflow collector-address 192.   168.   1.   2
zte(cfg)#set sflow ingress port 1 on frequency 20000
zte(cfg)#set sflow egress port 2 on frequency 20000
zte(cfg)#
```

Use command **show sflow** to view sFlow.

```
zte(cfg)#show sflow
  Agent address    :192.   168.   1.   1
  Collector address:192.   168.   1.   2
  Ingress:
  Reload Mode: Continuous
  Sample Mode: All
  PortId  Port Freq   CPU Freq    Counter
  ------  ----------  ----------  ---------
  1       20000       None           18459

  Egress:
  Reload Mode: Continuous
  PortId  Port Freq   CPU Freq    Counter
  ------  ----------  ----------  ---------
  2       20000       None           19998

zte(cfg)#
```

When counter of port is decreased to 0, data packets coming into port will be sampled to cpu. When port does not link up, value of counter is 0.

ZESR Overview

Disadvantage of STP

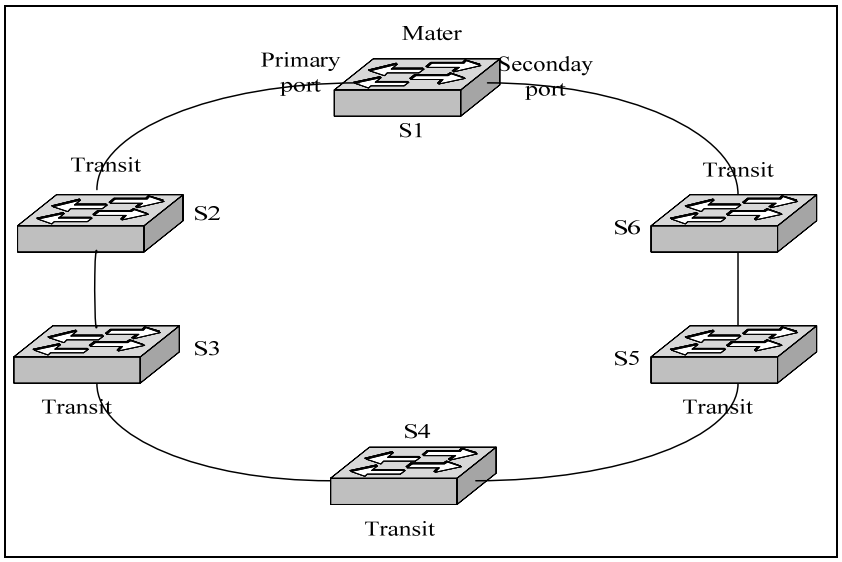
There is disadvantage of STP; its convergence speed is slow. To make up for it, and considering that most of core networks are annular and each switch has two ports to link into the ring in this topology structure, so it only needs to block a port in ring to avoid loop. When link trouble occurs, free the port from blocked to protect the service flow.

ZESR features

ZTE Ethernet Switching Ring supports fast convergence well when the topology of ring Ethernet link changes. ZESR is a master switch in an annular network, and others are transits. Each switch has two port connected into ring, and one of the port is designated as primary port, other as secondary port. Master switch sends ring detection frames to detect whether loop is good. When loop is good, master switch blocks its secondary port. When master switch detects that loop is down, it turns its secondary port into forwarding state, which ensures loop to be normal.

Figure 36 shows the typical network of ZESR. S1 is master, and other switches are transits. Master has a primary port and a secondary port in ring. When loop is good, secondary port on master is blocked. When loop is down, master turns on its secondary port.

FIGURE 36 NETWORK OF ZESR



Configuring ZESR

Purpose This topic describes the configuration of ZESR.

Steps For the configuration of ZESR, perform the following steps.

1. To set node equipment mode in ZESR domain, use command **set zesr domain** <domainId> **mode {master|transit}** in global configuration mode. This is shown in Table 352.

TABLE 352 SET ZESR DOMAIN COMMAND

Format	Mode	Function
set zesr domain <domainId> **mode {master|transit}**	global config	This sets node equipment mode n ZESR domain

Result: This sets node equipment mode in ZESR domain.

2. To set primary port in ZESR domain, use command **set zesr domain** <domainId> **primary port** <portname> in global configuration mode. This is shown in Table 353.

TABLE 353 SET ZESR DOMAIN PRIMARY PORT COMMAND

Format	Mode	Function
set zesr domain <domainId> **primary port** <portname>	global config	This sets primary port in ZESR domain

Result: This sets primary port in ZESR domain.

3. To set secondary port in ZESR domain, use command **set zesr domain** <domainId**>** **secondary port** <portname> in global configuration mode. This is shown in Table 354.

TABLE 354 SET ZESR DOMAIN SECONDARY PORT COMMAND

Format	Mode	Function
set zesr domain <domainId> **secondary port** <portname>	global config	This sets secondary port in ZESR domain

Result: This sets secondary port in ZESR domain.

4. To set primary trunk port in ZESR domain, use command **set zesr domain** <domainId> **primary trunk** <trunkname> in global configuration mode. This is shown in Table 355.

TABLE 355 SET ZESR DOMAIN PRIMARY TRUNK COMMAND

Format	Mode	Function
set zesr domain <domainId> **primary trunk** <trunkname>	global config	This sets primary trunk port in ZESR domain

Result: This sets primary trunk port in ZESR domain.

Note: Set trunk port as primary port on switches in ZESR domain

5. To set secondary trunk port in ZESR domain, use command **set zesr domain** <domainId> **secondary trunk** <trunkname> in global configuration mode. This is shown in Table 356.

TABLE 356 SET ZESR DOMAIN SECONDARY TRUNK COMMAND

Format	Mode	Function
set zesr domain <domainId> **secondary trunk** <trunkname>	global config	This sets secondary trunk port in ZESR domain

Result: This sets secondary trunk port in ZESR domain.

Note: Set trunk port as the secondary port on switches in ZESR domain.

6. To add control VLAN in ZESR domain, use command **set zesr domain** <domainId> **add control_vlan** <vlanname> in global configuration mode. This is shown in Table 357.

TABLE 357 SET ZESR DOMAIN VLAN COMMAND

Format	Mode	Function
set zesr domain <domainId> **add control_vlan** <vlanname>	global config	This adds VLAN in ZESR domain

Result: This adds VLAN in ZESR domain.

Note: Add control VLAN in ZESR domain, and ports configured in ring should be added into control VLAN and set as Tagged. Control VLAN is opened by users. ZESR function can not be enabled if control VLAN is not enabled.

7. To add protect VLAN in ZESR domain, use command **set zesr domain** <domainId> **add protect_vlan** <vlanlist> in global configuration mode. This is shown in Table 358.

TABLE 358 SET ZESR DOMAIN ADD PROTECT VLAN COMMAND

Format	Mode	Function
set zesr domain <domainId> **add protect_vlan** <vlanlist>	global config	This add protect VLAN in ZESR domain

Result: This add protect VLAN in ZESR domain.

Note: Add protect VLAN in ZESR domain. Protect VLAN is the user data VLAN in the domains.

8. To delete control VLAN in ZESR domain, use command **set zesr domain** <domainId> **delete control_vlan** <vlanname>in global configuration mode. This is shown in Table 359.

TABLE 359 SET ZESR DOMAIN 'DELETE COMMAND

Format	Mode	Function
set zesr domain <domainId> **delete control_vlan** <vlanname>	global config	This deletes control VLAN in ZESR domain

Result: This deletes control VLAN in ZESR domain.

9. To delete protect VLAN in ZESR domain, use command **set zesr domain** <domainId> **delete protect_vlan** <vlanlist> in global configuration mode. This is shown in Table 360.

TABLE 360 SET ZESR DOMAIN DELETE VLAN COMMAND

Format	Mode	Function
set zesr domain <domainId> **delete protect_vlan** <vlanlist>	global config	This deletes protect VLAN in ZESR domain

Result: This deletes protect VLAN in ZESR domain.

10. To enable/disable ZESR function in ZESR domain, use command **set zesr domain** <domainId> **{enable|disable}** in global configuration mode. This is shown in Table 361.

TABLE 361 SET ZESR DOMAIN COMMAND

Format	Mode	Function
set zesr domain <domainId> **{enable|disable}**	global config	This enable/disable ZESR function in ZESR domain

Result: This enable/disable ZESR function in ZESR domain.

Note: Enable/disable ZESR function in ZESR domain. ZESR function in ZESR domains is disabled by default. When enabling ZESR function, parameters in domains should be set actually. ZESR function can not be enabled if parameter is not integrated, meanwhile ZESR control VLAN should be enabled by users, and add ports in the ring as Tagged ports into control VLAN. To distinguish with STP function, ports in ZESR ring are not managed by STP. Before ZESR function is enabled, STP function in ring should be disabled.

11. To clear ZESR domain configurations, use command **clear zesr domain** <domainId> in global configuration mode. This is shown in Table 362.

TABLE 362 CLEAR ZESR DOMAIN COMMAND

Format	Mode	Function
clear zesr domain <domainId>	global config	This clears ZESR domain configurations

Result: This clears ZESR domain configurations.

Note: Clearing parameters configuration in ZESR domain can be processed when ZESR function is disabled in ZESR domain.

12. To display ZESR domain configuration, use command **show zesr domain** <domainId> in global configuration mode. This is shown in Table 363.

TABLE 363 SHOW ZESR DOMAIN COMMAND

Format	Mode	Function
show zesr domain <domainId>	global config	This displays ZESR domain configuration

Result: This displays ZESR domain configuration.

Note: This command displays configuration in signal ZESR domain.

13. To display configurations in all ZESR domains, use command **show zesr domain** in global configuration mode. This is shown in Table 364.

TABLE 364 SHOW ZESR COMMAND

Format	Mode	Function
show zesr domain	global config	This displays configuration in all ZESR domains

Result: This displays configuration in all ZESR domains.

Note: This command displays configuration in all ZESR domains.

END OF STEPS

Result ZESR has been configured.

Example This example describes instance configuration in ZESR domain.

```
zte(cfg)#set zesr domain 2 mode transit
zte(cfg)#set zesr domain 2 primary port 5
zte(cfg)#set zesr domain 2 secondary port 6
zte(cfg)#set zesr domain 2 add control_vlan 100
zte(cfg)#set zesr domain 2 add protect_vlan 110-115
zte(cfg)#set zesr domain 2 enable
```

The following instance shows configuration information in ZESR domain.

```
zte(cfg)#show zesr domain 1
 ZESR domains  1
 ------------------------------------------------
 Ring state     : Up
 Domain enabled : Yes     Node mode  : Master
 Primary port   : 3       Port state : Forward
 Secondary port : 4       Port state : Block
 ZESR Domain Control Vlan   : 10
 ZESR Domain protected vlan : 1, 20-30
```

In the following instance, it sets the switch as master, and set primary and secondary ports as trunk ports.

```
zte(cfg)#show zesr domain 2
 ZESR domains  2
 ------------------------------------------------
 Ring state     : Down
 Domain enabled : No      Node mode  : Transit
 Primary port   : T1      Port state : Forward
 Secondary port : T2      Port state : Forward
 ZESR Domain Control Vlan   : 100
 ZESR Domain protected vlan : 110-115
```

In the following instance, it shows the information of the enabled transit.

```
zte(cfg)#show zesr domain 1
 ZESR domains  1
 ------------------------------------------------
 Ring state     : Down
 Domain enabled : Yes     Node mode  : Transit
 Primary port   : 3       Port state : Forward
 Secondary port : 4       Port state : Forward
 ZESR Domain Control Vlan   : 10
 ZESR Domain protected vlan : 1, 20-30
```

Chapter 9

Network Management

Overview

Introduction This chapter provides and overview of network management functions of the ZXR10 2920/2928/2952, such as Remote-Access, SSH, SNMP, RMON and cluster management.

Contents This chapter includes the following contents:

Remote Access Overview

Network Management Users

Remote-Access is a restrictive mechanism used for network management users to log in through Telnet, that is, it is used to restrict the access. This function is to enhance the security of the network management system.

After this function is enabled, a network management is specified for user to access the switch only from a specified IP address by configuring the related parameters. In this case, user cannot access the switch from other IP addresses. When this function is disabled, the network management user can access the switch through Telnet from any IP address.

Configuring Remote-Access

Purpose

This topic describes the configuration of Remote-Access.

Steps

For the configuration of Remote-Access, perform the following steps.

1. To enable/disable restrictive remote access, use command **set remote-access {any|specific}** in global configuration mode. This is shown in Table 365.

TABLE 365 SET REMOTE ACCESS COMMAND

Format	Mode	Function
set remote-access {any|specific}	global config	This enable/disable restrictive remote access

Result: This enable/disable restrictive remote access.

Note: By default, restrictive access is disabled.

2. To configure IP address that allows remote access, use command **set remote-access ipaddress** <A. B. C. D> [<A. B. C. D>] in global configuration mode. This is shown in Table 366.

TABLE 366 SET REMOTE ACCESS IPADDRESS COMMAND

Format	Mode	Function
set remote-access ipaddress <A. B. C. D> [<A. B. C. D>]	global config	This configures IP address that allows remote access.

Result: This configures IP address that allows remote access.

3. To delete all IP addresses that allow remote access, use command **clear remote-access all** in global configuration mode. This is shown in Table 367.

TABLE 367 CLEAR REMOTE ACCESS ALL COMMAND

Format	Mode	Function
clear remote-access all	global config	This deletes all IP addresses that allow remote access

Result: This deletes all IP addresses that allow remote access.

4. To delete an IP address that allows remote access, use command **clear remote-access ipaddress** <A. B. C. D> [<A. B. C. D>] in global configuration mode. This is shown in Table 368.

TABLE 368 CLEAR REMOTE ACCESS IPADDRESS COMMAND

Format	Mode	Function
clear remote-access ipaddress <A. B. C. D> [<A. B. C. D>]	global config	This deletes an IP address that allows remote access

Result: This deletes an IP address that allows remote access.

5. To display Remote-Access configuration information, use command **show remote-access** in global configuration mode. This is shown in Table 369.

TABLE 369 SHOW REMOTE ACCESS COMMAND

Format	Mode	Function
show remote-access	global config	This displays Remote-Access configuration information

Result: This displays Remote-Access configuration information.

END OF STEPS

Result Remote-Access has been configured.

Remote-Access Configuration Examples

Example 1 Only allows network management user to access the switch from 10. 40. 92. 0/24 through Telnet.

```
zte(cfg)#set remote-access specific
zte(cfg)#set remote-access ipaddress 10.    40.    92.    0
255.   255.   255.   0
zte(cfg)#show remote-access
  Whether check remote manage address: YES
  Allowable remote manage address list:
    10.   40.   92.   0/255.   255.   255.   0
zte(cfg)#
```

Example 2 Only allows network management user to access the switch from 10. 40. 92. 212 through Telnet.

```
zte(cfg)#set remote-access specific
zte(cfg)#set remote-access ipaddress 10.   40.   92.   212
zte(cfg)#show remote-access
  Whether check remote manage address: YES
  Allowable remote manage address list:
    10.   40.   92.   212/255.   255.   255.   255
zte(cfg)#
```

Example 3 Allow network management user to access switch from any IP address through Telnet.

```
zte(cfg)#set remote-access any
zte(cfg)#show remote-access
  Whether check remote manage address: NO
  Allowable remote manage address list:
    none
zte(cfg)#
```

SSH Overview

SSH Purpose Secure shell (SSH) is a protocol created by Network Working Group of the IETF, offers secure remote access and other secure network services over an insecure network.

Purpose of the SSH protocol is to solve the security problems in interconnected networks, and to offer a securer substitute for Telnet and Rlogin (Although the present development of the SSH protocol has far exceeded the remote access function scope), therefore, the SSH connection protocol shall support interactive session.

SSH is to encrypt all transmitted data, even if these data is intercepted, no useful information can be obtained.

SSH Proctocol Versions At present, SSH protocol has two incompatible versions: SSH v1. x and SSH v2. x. This switch only supports SSH v2. 0 and uses the password authentication mode. SSH uses port 22.

Configuring SSH

Purpose This topic describes the configuration of SSH.

Steps For the configuration of SSH, perform the following steps.

1. To enable/disable SSH, use command **set ssh {enable|disable}** in global configuration mode. This is shown in Table 370.

TABLE 370 SET SSH COMMAND

Format	Mode	Function
set ssh {enable|disable}	global config	This enable/disable SSH

Result: This enable/disable SSH.

- By default, SSH function is disabled. SSH configures remote access to the switch. User name and password for login (or remote RADIUS login mode) shall be configured on the switch, and the local host shall be able to ping the IP port address on the switch normally.
- This switch only supports SSH login of a single user, allowing for three login attempts. After three login attempts, connection with the user is automatically terminated. After user login, **set ssh disable** command is to terminate connection with user and prohibit user from logging in through SSH. However, if user is in Diffie-Hellman key exchange state, command is disabled.

2. To display SSH configuration and user login status, use command **show ssh** in global configuration mode. This is shown in Table 371.

TABLE 371 SHOW SSH COMMAND

Format	Mode	Function
show ssh	global config	This displays SSH configuration and user login status

Result: This displays SSH configuration and user login status.

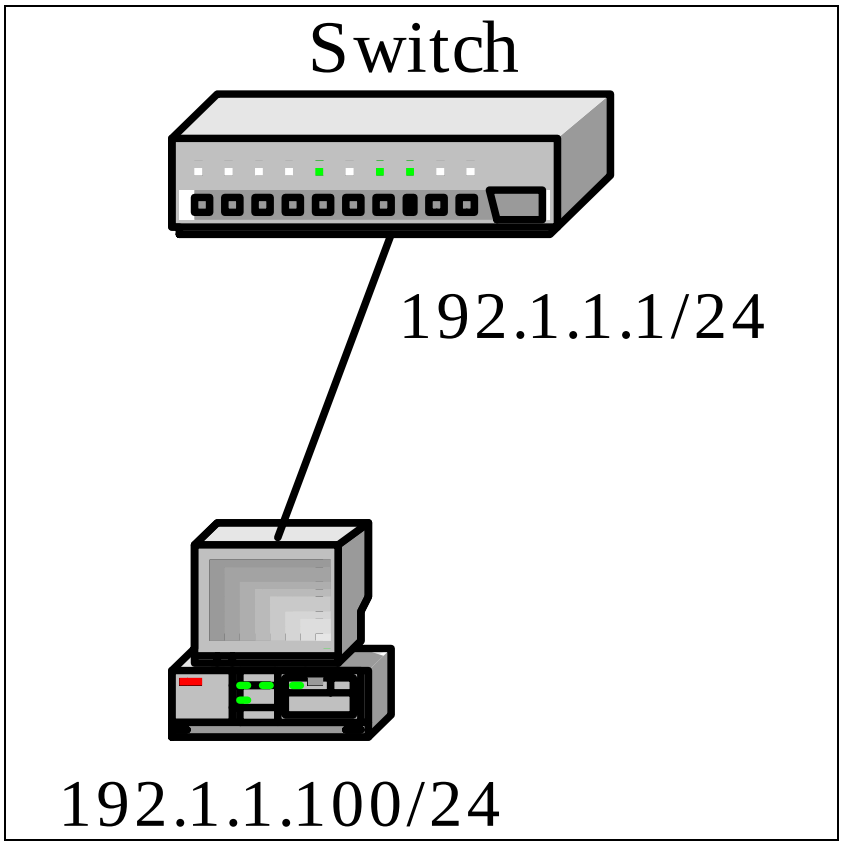
END OF STEPS

Result SSH has been configured.

Example One host attempts to access switch through SSH. Switch is configured with a layer 3 port. IP address of the port is 192.

1. 1. 1/24, and the IP address of the host is 192. 1. 1. 100/24. This is shown in

FIGURE 37 SSH CONFIGURATION



Specific configuration of the switch is as follows:

```
zte(cfg)#creat user zte guest
zte(cfg)#loginpass zte
zte(cfg)#set ssh enable
```

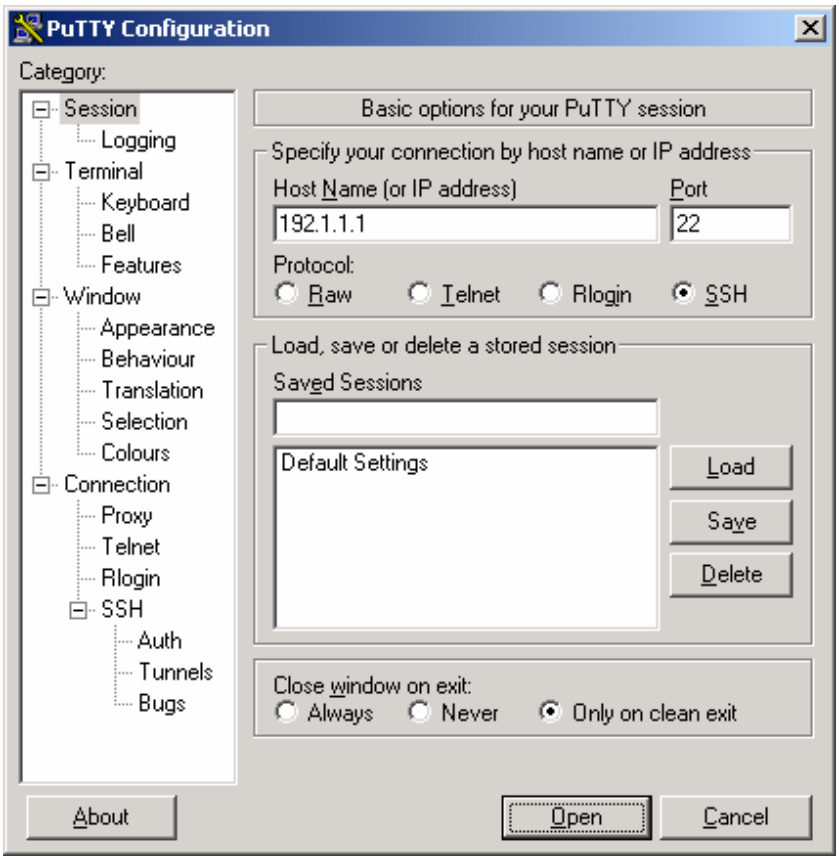
Configuring SSH v2. 0

Purpose This topic describes the client using SSH v2. 0 can configure free software Putty developed by Simon Tatham to access the switch.

Steps For the configuration of SSH v2. 0, perform the following steps:

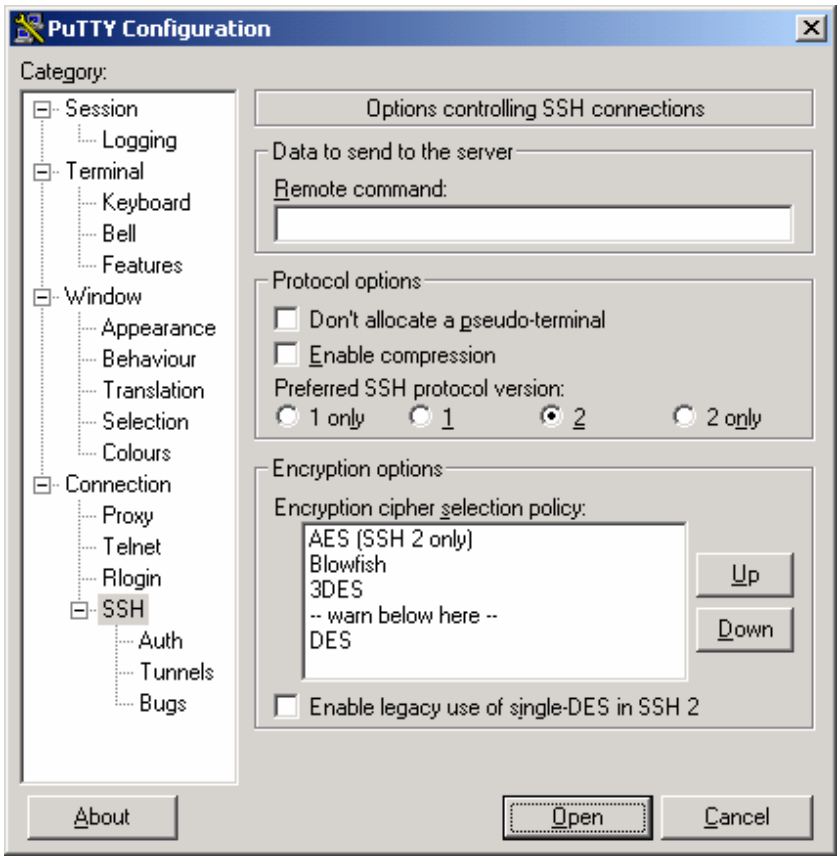
1. Set the IP address and port number of SSH Server, as shown in Figure 38 Setting IP Address And Port Number Of SSH Server.

FIGURE 38 SETTING IP ADDRESS AND PORT NUMBER OF SSH SERVER



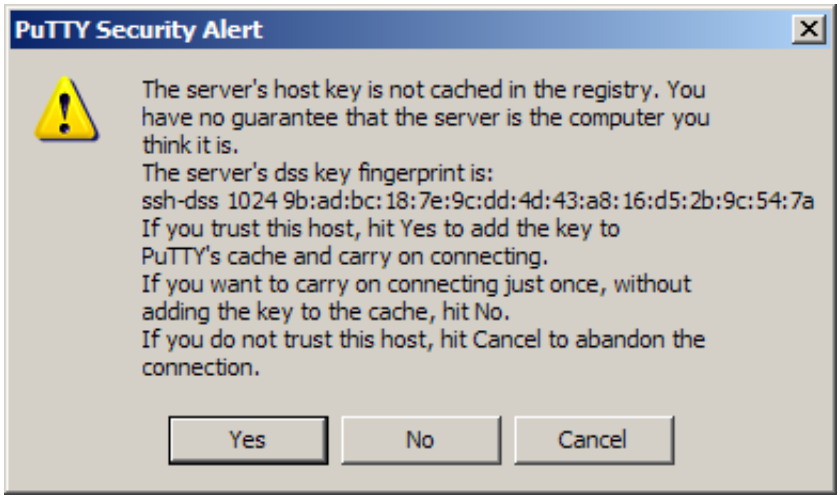
2. Set the SSH version number, as shown in Figure 39.

FIGURE 39 SETTING SSH VERSION NUMBER



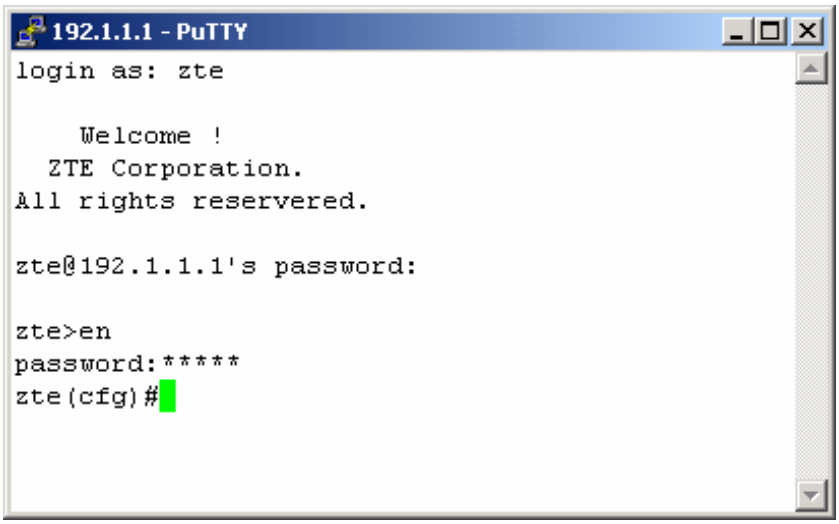
3. For the first time to log in, user confirmation is needed, as shown in Figure 40.

FIGURE 40 PUTTY SECURITY ALERT



4. SSH login result is shown in Figure 41.

FIGURE 41 LOGIN RESULT



END OF STEPS

Result SSH login has started successfully

SNMP Overview

SNMP is the most popular network management protocol currently. It involves a series of protocol suite and specifications:

- MIB
- SMI
- SNMP

They collect network management information from network devices. SNMP also enables devices to report problems and errors to network management stations. Any network administrator can use SNMP to manage switches.

SNMP adopts the "Management process—Agent process" model to monitor and control all types of managed network devices. The SNMP network management needs three key elements:

Managed Devices Managed devices can communicate over the Internet. Each device contains an agent.

Network Management Station (NMS) The network management process shall be able to communicate over the Internet.

SNMP The protocol used for the exchange of management information between the switching agent process and the NMS, that is, SNMP.

An NMS collects data by polling the agents that reside in managed devices. Agents in managed devices can report errors to NMSs at any time before NMSs poll them. These errors are called traps. When a trap occurs to a device, the NMS can be used to query the device (suppose it is reachable) and obtain more information.

All variables in the network are stored in MIB. SNMP monitors network device status by querying the related object values in the agent MIB. ZXR10 2920/2928/2952 implements the standard MIB defined in rfc1213, rfc1493, rfc2674 and rfc2819.

Configuring SNMP

Purpose This topic describes the configuration of SNMP.

Steps For the configuration of SNMP, perform the following steps.

1. To create communication name and set access authority, use command **create community** in SNMP config mode. This is shown in Table 372.

TABLE 372 CREATE COMMUNITY COMMAND

Format	Mode	Function
create community	SNMP config	This creates communication name and set access authority

Result: This creates communication name and set access authority

- Community string offers a user confirmation mechanism for remote network administrators to configure switches. The "public" indicates that switch only allows for read only access, while "private" indicates that the read/write authority to the switch is permitted.
- If community string created with this command already exists, newly created string overwrites the original one.

2. To create a view and specify whether the view contains a mib subtree, use command **create view** in SNMP config mode. This is shown in Table 373.

TABLE 373 CREATE VIEW COMMAND

Format	Mode	Function
create view	SNMP config	This creates a view

Result: This creates a view and specifies whether the view contains a mib subtree.

- A view is an object subset of the MIB. Parameter <*mib-oid*> specifies mib subtree. If the excluded or included mib subtree is not specified, it includes 1. 3. 6. 1 by default.
- When view created with this command already exists, newly created view overwrites original one.

3. To set specific community name that view contains, use command **set community view** in SNMP config mode. This is shown in Table 374.

TABLE 374 SET COMMUNITY VIEW COMMAND

Format	Mode	Function
set community view	SNMP config	This sets specific community name that view contains

Result: This sets specific community name that view contains.

- Community and view must be created. One community can only correspond to one view, but one view can correspond to multiple communities.

4. To set group name and its security level, use command **set group** in SNMP config mode. This is shown in Table 375.

TABLE 375 SET GROUP COMMAND

Format	Mode	Function
set group	SNMP config	This sets group name and its security level

Result: This sets group name and its security level.

- There are three levels of group: no authentication and no encrypting, authentication and no encrypting, authentication and encrypting. Group can be configured as three views: reading, writing and informing. If it is not specified, it will take "zte View" as the default view, including reading, writing and informing. It is allowed to configure on switch with same group name and different security level.

5. To set user name, group it belonging to and its security attribute, use command **set user** in SNMP config mode. This is shown in Table 376.

TABLE 376 SET USER COMMAND

Format	Mode	Function
set user	SNMP config	This sets user name, group it

Format	Mode	Function
		belongs to and its security attribute

Result: This sets user name, group it belongs to and its security attribute.

- Security attribute of user includes authentication and cryptogram, arithmetic of authentication and encrypting (MD5\SHA\DES). Security level of user and group should be accordant.

6. To set engine identifier, use command **set engineID** in SNMP config mode. This is shown in Table 377.

TABLE 377 SET ENGINEID COMMAND

Format	Mode	Function
set engineID	SNMP config	This sets engine identifier

Result: This sets engine identifier.

Note: EngineID identifies a SNMP entity uniquely. When it is changed, configurations of primary engineID don't work any longer.

7. To set the address, community name and version of trap or inform host, use command **set host** in SNMP config mode. This is shown in Table 378.

TABLE 378 SET HOST COMMAND

Format	Mode	Function
set host	SNMP config	This sets address

Result: This set address community name and version of trap or inform host.

- Host is destination IP address sending by trap or inform. It can designate the version of trap and inform and community or user.

8. To enable/disable SNMP trap, use command **set trap** in SNMP config mode. This is shown in Table 379.

TABLE 379 SET TRAP COMMAND

Format	Mode	Function
set trap	SNMP config	This enable/disable SNMP trap

Result: This enable/disable SNMP trap.

- When it is enabled, operation as described in 5) above occurs, a trap is sent to the management console. The cold start and warm start traps are sent to management

console only after the system is started. In general, there is a delay of several minutes.

9. To delete a community name, use command **clear community** in SNMP config mode. This is shown in Table 380.

TABLE 380 CLEAR COMMUNITY COMMAND

Format	Mode	Function
clear community	SNMP config	This deletes a community name

Result: This deletes a community name.

10. To delete a view name, use command **clear view** in SNMP config mode. This is shown in Table 381.

TABLE 381 CLEAR VIEW COMMAND

Format	Mode	Function
clear view	SNMP config	This deletes a view name

Result: This deletes a view name.

11. To delete a group name, use command **clear group** in SNMP config mode. This is shown in Table 382.

TABLE 382 CLEAR GROUP COMMAND

Format	Mode	Function
clear group	SNMP config	This deletes a group name

Result: This deletes a group name.

12. To delete a user name, use command **clear suer** in SNMP config mode. This is shown in Table 383.

TABLE 383 CLEAR SUER COMMAND

Format	Mode	Function
clear suer	SNMP config	This deletes a user name

Result: This deletes a user name.

13. To delete a trap, use command **clear host** in SNMP config mode. This is shown in Table 384.

TABLE 384 CLEAR HOST COMMAND

Format	Mode	Function
clear host	SNMP config	This deletes a trap

Result: This deletes a trap.

14. To view SNMP configuration, use command **show snmp** in SNMP config mode. This is shown in Table 385.

TABLE 385 SHOW SNMP COMMAND

Format	Mode	Function
show snmp	SNMP config	This views SNMP configuration

Result: This views SNMP configuration.

END OF STEPS

Result SNMP has been configured.

Example This example describes basic configuration of SNMPv1 and SNMPv2c

Suppose that IP address of network management server is 10. 40. 92. 105, switch has a layer 3 port with IP address of 10. 40. 92. 200, and switch is managed through network management server.

Create a community named "zte" with read/write authority and view named "vvv", and then associate the community "zte" with view "vvv". Specify IP address of the host receiving traps as 10. 40. 92. 105, and community as "zte".

```
zte(cfg)#config router
zte(cfg-router)#set  ipport  0  ipaddress  10.    40.    92.
200 255.   255.   255.   0
zte(cfg-router)#set ipport 0 vlan 2
zte(cfg-router)#set ipport 0 enable
zte(cfg-router)#exit

zte(cfg)#config snmp
zte(cfg-snmp)#create community zte private
zte(cfg-snmp)#create view vvv
zte(cfg-snmp)#set community zte view vvv
zte(cfg-snmp)#set host 10.   40.   92.   105 trap v1 zte

zte(cfg-snmp)#show snmp community
  CommunityName  Level      ViewName
  -------------- --------- ------------
  zte              private    vvv

zte(cfg-snmp)#show snmp view
  ViewName     Exc/Inc  MibFamily
  ----------- -------- ------------------------
  vvv           Include  1.   3.   6.   1

zte(cfg-snmp)#show snmp host
  HostIpAddress            Comm/User       Version     type
SecurityLevel
  ---------------- ----------- ------- ------ ------------
-
  10.    40.    92.    77          zte            Ver.    1
Trap   -
zte(cfg-snmp)#
```

This example describes basic configuration of SNMPv3

Suppose that IP address of network management server is 10. 40. 92. 77, switch has a layer 3 port with IP address of 10. 40. 92. 200, and switch is managed through network management server in user security model.

Create a user named “zteuser” belonging to group named “ztegroup”, with security level of authentication and encrypting, and reading, writing and informing view are default. Specify IP address of host receiving traps as 10. 40. 92. 77, and user as “zteuser”.

```
  zte(cfg)#config router
zte(cfg-router)#set  ipport  1  ipaddress  10.    40.    92.
11/24
zte(cfg-router)#set ipport 1 vlan 1
zte(cfg-router)#set ipport 1 enable
zte(cfg-router)#exit

zte(cfg)#config snmp
zte(cfg-snmp)# set group ztegroup v3 priv
zte(cfg-snmp)#  set  user  zteuser  ztegroup  v3  md5-auth  zte
               des56-priv zte
zte(cfg-snmp)#  set  host  10.    40.    89.    77  inform  v3
zteuser priv

zte(cfg-snmp)#show snmp group
  groupName: ztegroup
  secModel : v3                         readView  : zteView
  secLevel : AuthAndPriv              writeView : zteView
  rowStatus: Active                     notifyView: zteView

zte(cfg-snmp)#show snmp user
  UserName   : zteuser
  GroupName  : ztegroup(v3)
  EngineID   : 830900020300010289d64401
  AuthType    : Md5                           StorageType:
NonVolatile
  EncryptType: Des_Cbc                        RowStatus   :
Active

zte(cfg-snmp)#show snmp host
  HostIpAddress             Comm/User        Version   type
SecurityLevel
  ---------------- ----------- ------- ------ ------------
-
  10.    40.    89.    77         zteuser        Ver.    3
Inform  AuthAndPriv

zte(cfg-snmp)#
```

RMON Overview

Definition Remote Monitoring (RMON) defines standard network monitoring function and communication interface between management

console and remote monitor. RMON offers an efficient and high availability method to monitor behaviors of subnets in case of reducing oad of other agents and management stations.

RMON specifications refers to the definition of RMON MIB. ZXR10 2920/2928/2952 supports four groups of RMON MIB.

History History records periodic statistics sample of information that can be obtained from statistics group.

Statistics Statistics maintains basic application and error statistics of each subnet that the agent monitors.

Event Event is a table related to all events generated by RMON agents.

Alarm Alarm allows operators of management console to set sampling interval and alarm threshold for any count or integer recorded by RMON agents.

All these groups store data collected by monitor and derived data and statistics. Alarm group is based on implementation of event group. These data can be obtained through MIB browser.

RMON control information can be configured through MIB browser, and a HyperTerminal or remote Telnet command line. RMON sampling information and statistics are obtained through MIB browser.

Configuring RMON

Purpose This topic describes the configuration of RMON through a HyperTerminal or remote Telnet.

Steps For the configuration of RMON, perform the following steps.

1. To enable/disable RMON function, use command **set rmon {enable|disable}** in SNMP config mode. This is shown in Table 386.

TABLE 386 SET RMON COMMAND

Format	Mode	Function
set rmon {enable|disable}	SNMP config	This enable/disable RMON function

Result: This enable/disable RMON function.

Note: By default, RMON function is disabled. Sampling of etherStatsTable information in etherHistoryTable and statistics groups in history group can be implemented only when RMON function is enabled. During the sampling, data sampling stops if the RMON function is disabled.

2. To create/configure instances of history group, use command **set history** <1-65535> {**datasource**<portname>|**bucketRequested** <1-65535>|**owner** <string>|**interval** <1-3600>| **status**

{**valid|underCreation| createRequest|invalid**}} in SNMP config mode. This is shown in Table 387.

TABLE 387 SET HISTORY COMMAND

Format	Mode	Function
set history <1-65535> {**datasource**<portname>|**bucketRequested** <1-65535>|**owner** <string>|**interval** <1-3600>|**status** {**valid|underCreation|createRequest|invalid**}}	SNMP config	These create/configure instances of history group

Result: These create/configure instances of history group.

The command line configuration of the history group is to configure the historyControlTable in the history group. The configuration involves:

- historyControlDataSource: It is the ifIndex oid in rfc1213 interface group, for example, the oid of port 16 is 1. 3. 6. 1. 2. 1. 2. 2. 1. 1. 16. In command line configuration, enter the port number 16 directly.
- historyControlBucketsRequested: By default, it is 50.
- historyControlOwner.
- historyControlInterval. By default, it is 1, 800 seconds.
- historyControlStatus: It can be "valid", "underCreation", "createRequest" and "invalid". When it is set to "invalid", the instance is deleted. The control status can be set to "valid" only when the data source is specified.

3. To create/configure instances of the statistics group, use command **set statistics** <1-65535> {**datasource** <portname>|**owner** <string>|**status** {**valid|underCreation|createRequest| invalid**}} in SNMP config mode. This is shown in Table 388.

TABLE 388 SET STATISTICS COMMAND

Format	Mode	Function
set statistics <1-65535> {**datasource** <portname>|**owner** <string>|**status** {**valid|underCreation|createRequest| invalid**}}	SNMP config	This create/configure instances of the statistics group

Result: This create/configures instances of the statistics group

Command line configuration of statistics group is to configure etherStatsTable in statistics group. Configuration involves:

- etherStatsDataSource: It is the same as that of the history group. When configuring the data source through the command line, enter the port number directly.
- etherStatsOwner
- etherStatsStatus: It can be "valid", "underCreation", "createRequest" and "invalid". When it is set to "invalid", the instance is deleted. Control status can be set to "valid" only when data source is specified.

4. To create/configure instances of the event group, use command **set event** <1-65535> **{description** <string>|**type {none|log|snmptrap| logandtrap} | owner** <string>|**community** <string>| **status {valid|underCreation| createRequest|invalid}}** in SNMP config mode. This is shown in Table 389.

TABLE 389 SET EVENT COMMAND

Format	Mode	Function
set event <1-65535> **{description** <string>|**type {none|log|snmptrap| logandtrap}	owner** <string>|**community** <string>| **status {valid|underCreation| createRequest|invalid}}**	SNMP config	These create/configure instances of the event group

Result: These create/configure instances of the event group.

Command line configuration of event group is to configure eventTable in event group. The configuration involves:

- eventDescription.
- eventType: It can be "none(1)", "log(2)", "snmp-trap(3)" and "log-and-trap(4)". When the "log" is selected, a log instance is created for each event in the logTable. When the "snmp-trap" is selected, for each event, the monitor sends an SNMP trap to one or more management stations. When the "log-and-trap" is selected, the log is created and a trap is sent.
- eventOwner.
- eventCommunity.
- eventStatus: It can be "valid", "underCreation", "createRequest" and "invalid". When it is set to "invalid", event instance is deleted.

5. To create/configure instances of the alarm group, use command **set alarm** <1-65535> {**interval** <1-65535>|**variable** <mib-oid>|**sampletype {absolute|delta}|startup {rising|falling|both}|threshold** <1-65535> **eventindex**

<1-65535> {**rising|falling}|owner** <string>|**status {valid|underCreation|createRequest| invalid}}** in SNMP config mode. This is shown in Table 390.

TABLE 390 SET ALARM COMMAND

Format	Mode	Function
set alarm <1-65535> {**interval <1-65535>|variable** <mib-oid>**|sampletype {absolute|delta}|startup {rising|falling|both}|threshold** <1-65535> **eventindex** <1-65535> **{rising|falling}|owner** <string>**|status {valid|underCreation|createRequest| invalid}}**	SNMP config	These create/configure instances of the alarm group

Result: These create/configure instances of the alarm group.

Command line configuration of alarm group is to configure alarmTable in the alarm group. The configuration involves:

- alarmInterval.
- alarmVariable: It indicates the object identifier of a specific variable to be sampled in the local mib, for example, for sampling the etherHistoryBroadcastPkts, the variable value shall be 1. 3. 6. 1. 2. 1. 16. 2. 2. 1. 7. x. x, where, "x. x" indicates the sampling bucket of an instance of the history group.
- alarmSampleType: The "absolute" indicates the absolute value, and "delta" indicates the relative value.
- alarmStartupAlarm: It can be "risingAlarm(1)", "fallingAlarm(2)" and "risingOrFallingAlarm(3)", which indicate that, after the instance becomes effective, the first sampling starts when the rising sampling value exceeds the threshold, the falling sampling value is lower than the threshold or both cases occur simultaneously.
- alarmRisingThreshold.
- alarmFallingThreshold.
- alarmRisingEventIndex.
- alarmFallingEventIndex.
- alarmOwner.
- alarmStatus: It can be "valid", "underCreation", "createRequest" and "invalid". When it is set to "invalid", the alarm instance is deleted.

Alarm variable can be configured only when object to be sampled specified by alarm variable can sample data. Status can be set to "valid" only when alarm variable is configured successfully.

6. To query RMON status and configuration information, use the follwing commands in SNMP config mode as shown in Table 391.

TABLE 391 SHOW RMON COMMANDS

Format	Mode	Function
show rmon	SNMP config	This displays RMON status
show history	SNMP config	This displays configuration information about history group
show statistic	SNMP config	This displays configuration information about statistic group
show event	SNMP config	This display configuration information about event group
show alarm	SNMP config	This display configuration information about alarm group

Result: This displays RMON status, history group, statistics group, event group and alarm group

END OF STEPS

Result RMON through a HyperTerminal or remote Telnet has been configured.

Example Following examples describe how to set event 2, history 2, alarm 2 and statistics 1 respectively.

```
zte(cfg-snmp)#set event 2 description It'sJustForTest!!
zte(cfg-snmp)#set event 2 type logandtrap
zte(cfg-snmp)#set event 2 community public
zte(cfg-snmp)#set event 2 owner zteNj
zte(cfg-snmp)#set event 2 status valid

zte(cfg-snmp)#set history 2 datasource 16
zte(cfg-snmp)#set history 2 bucket 3
zte(cfg-snmp)#set history 2 interval 10
zte(cfg-snmp)#set history 2 owner zteNj
zte(cfg-snmp)#set history 2 status valid

zte(cfg-snmp)#set rmon enable

zte(cfg-snmp)#set alarm 2 interval 10
zte(cfg-snmp)#set alarm 2 variable 1.   3.   6.   1.   2.
1.   16.   2.   2.   1.   6.   2.   1
zte(cfg-snmp)#set alarm 2 sample absolute
zte(cfg-snmp)#set alarm 2 startup rising
zte(cfg-snmp)#set alarm 2 threshold 8 eventindex 2 rising
zte(cfg-snmp)#set  alarm  2  threshold  15  eventindex  2
falling
zte(cfg-snmp)#set alarm 2 owner zteNj
zte(cfg-snmp)#set alarm 2 status valid

zte(cfg-snmp)#set statistics 1 datasource 16
zte(cfg-snmp)#set statistics 1 owner zteNj
zte(cfg-snmp)#set statistics 1 status valid
```

Query configuration information about event 2:

```
zte(cfg-snmp)#show event 2
  EventIndex  : 2             Type       : log-and-trap
  Community   : public        Status     : valid
  Owner       : zteNj
  Description : It'sJustForTest!!

zte(cfg-snmp)#
```

Query configuration information about history 2:

```
zte(cfg-snmp)#show history 2
  ControlIndex : 2              BucketsRequest: 3
  Interval     : 10             BucketsGranted: 3
  ControlStatus: valid          ControlOwner  : zteNj
  DataSource    : 1.    3.    6.    1.    2.    1.    2.    2.
1.   1.   16
zte(cfg-snmp)#
```

Query configuration information about alarm 2:

```
zte(cfg-snmp)#show alarm 2
  AlarmIndex   : 2          SampleType: absolute
  Interval     : 10         Value     : 16
  Threshold(R) : 8          Startup   : risingAlarm
  Threshold(F) : 15         Status    : valid
  EventIndex(R): 2          Variable  : 1.   3.   6.   1.
2.   1.   16.   2.   2.   1.   6.   2.   1
  EventIndex(F): 2          Owner     : zteNj

zte(cfg-snmp)#
```

Query configuration information about statistics 1:

```
zte(cfg-snmp)#show statistics 1
  StatsIndex: 1
  DropEvents    : 0         BroadcastPkts       : 0
  Octets        : 0          MulticastPkts       : 0
  Pkts          : 0          Pkts64Octets        : 0
  Fragments     : 0         Pkts65to127Octets   : 0
  Jabbers       : 0         Pkts128to255Octets  : 0
  Collisions    : 0         Pkts256to511Octets  : 0
  CRCAlignErrors: 0        Pkts512to1023Octets : 0
  UndersizePkts : 0        Pkts1024to1518Octets: 0
  OversizePkts  : 0           DataSource(port) : 1.    3.
6.   1.   2.   1.   2.   2.   1.   1.   16
  Status         : valid          Owner                :
zteNj

zte(cfg-snmp)#
```

After above configuration, when number of etherHistoryPkts of first bucket of port 16 rises over 8 or number falls below 15, event with index of 2 is triggered. Event with index of 2 sends a trap to management station, and creates a log simultaneously. This log can be queried in logTable of event group.

Cluster Management Overview

Cluster Definition

Cluster is a combination consisting of a set of switches in a specific broadcast domain. This set of switches forms a unified management domain, providing an external public network IP address and management interface, as well as the ability to manage and access each member in the cluster.

Management switch which is configured with a public network IP address is called a command switch. Other switches serve as member switches. In normal cases, a member switch is not configured with a public network IP address. A private address is allocated to each member switch through the class DHCP function of the command switch. The command switch and member switches form a cluster (private network).

Command Switch

It is recommended to isolate broadcast domain between public network and private network on the command switch and shield direct access to private address. Command switch provides an external management and maintenance channel to manage cluster in a centralized manner.

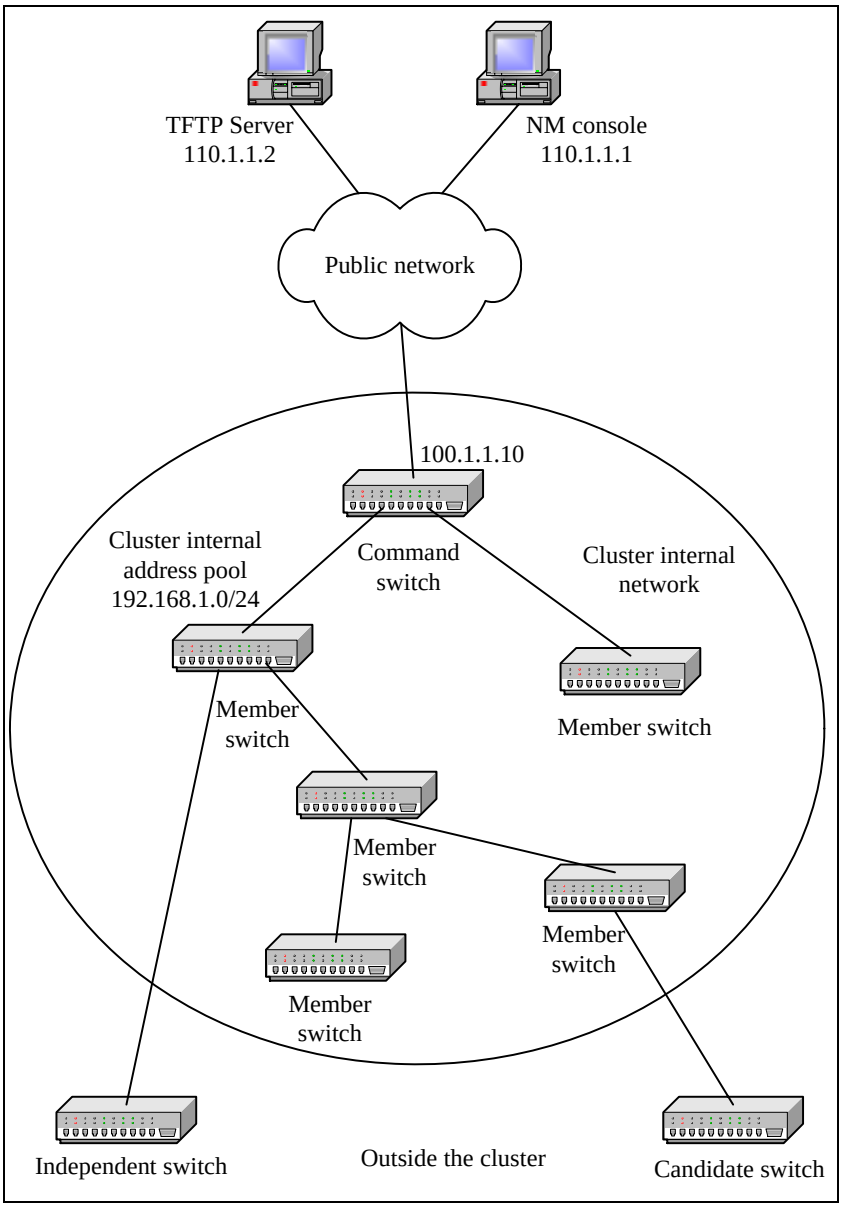
In general, broadcast domain where a cluster is located consists of switches in these roles: Command switch, member switches, candidate switches and independent switches.

Independent Switches

One cluster has only one command switch. Command switch can automatically collect device topology and set up a cluster. After a cluster is set up, the command switch provides a cluster management channel to manage member switches. Member switches serve as candidate switches before they join the cluster. Switches that do not support cluster management are called independent switches.

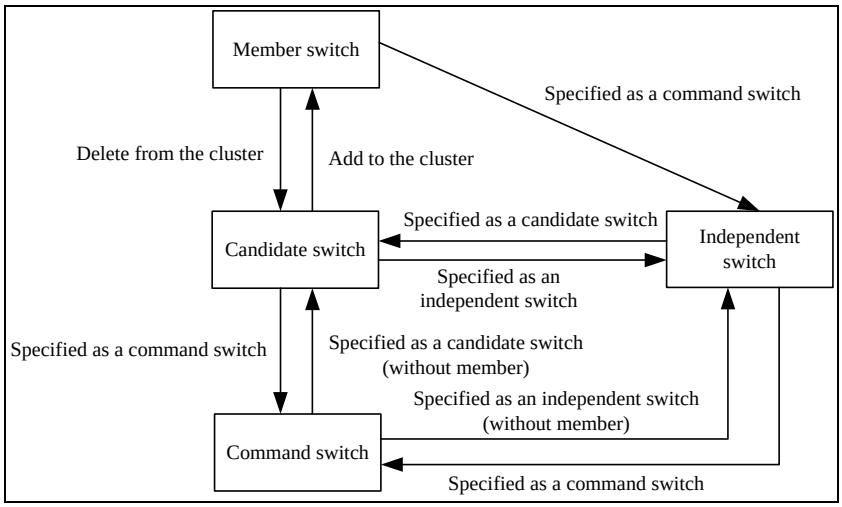
Cluster management networking is shown in Figure 42.

FIGURE 42 CLUSTER MANAGEMENT NETWORK



Changeover rule of four roles of switches within a cluster is shown in

FIGURE 43 SWITCH ROLE CHANGEOVER RULE



Configuring a ZDP

Purpose This topic describes ZDP configuration. ZDP (Discovery Protocol) is a protocol used to discover the related information about direct neighbor node, including adjacent device ID, device type, version and port information. This protocol supports the refreshing and aging of neighbor device information table.

Prerequisite To configure cluster management function, meet the following requirement.

- To configure cluster management function, use command **config group** to enter into cluster management configuration mode.

Steps For the configuration of ZDP, perform the following steps.

1. To enable/disable ZDP function, use command **set zdp {enable|disable}** in group config mode. This is shown in Table 392.

TABLE 392 SET ZDP COMMAND

Format	Mode	Function
set zdp {enable|disable}	group config	This enable/disable ZDP function

Result: This enable/disable ZDP function.

Note: By default, system ZDP function is enabled. When system ZDP function is disabled, contents of neighbor device information table are cleared, and ZDP packets processing is suspended.

2. To enable/disable port ZDP function, use command **set zdp port** <portlist> **{enable|disable}** in group config mode. This is shown in Table 393.

TABLE 393 SET ZDP PORT COMMAND

Format	Mode	Function
set zdp port <portlist> **{enable|disable}**	group config	This enable/disable port ZDP function

Result: This enable/disable port ZDP function.

3. To enable/disable trunk ZDP function, use command **set zdp trunk** <trunklist> **{enable|disable}** in group config mode. This is shown in Table 394.

TABLE 394 SET ZDP TRUNK COMMAND

Format	Mode	Function
set zdp trunk <trunklist> **{enable|disable}**	group config	This enable/disable trunk ZDP function

Result: This enable/disable trunk ZDP function.

Important! By default, ZDP functions of all ports/trunks are enabled. When ZDP function of a port/trunk is disabled, contents of neighbor device information table of port/trunk are cleared, and ZDP packets processing is suspended.

Note: A port/trunk can collect and send ZDP information normally only when both ZDP function of port/trunk and system ZDP function are enabled.

4. To set time interval for sending ZDP packets, use command **set zdp holdtime** <10-255> in group config mode. This is shown in Table 395.

TABLE 395 SET ZDP HOLDTIME COMMAND

Format	Mode	Function
set zdp holdtime <10-255>	group config	This set time interval for sending ZDP packets

Result: This sets the time interval for sending ZDP packets.

Note: ZDP holdtime value should be bigger than time value, here give the advice that the holdtime value is three times of time value.

5. To set time interval for sending ZDP packets, use command **set zdp timer** <5-255> in group config mode. This is shown in Table 396.

TABLE 396 SET ZDP TIMER COMMAND

Format	Mode	Function
set zdp timer <5-255>	group config	This set time interval for sending ZDP packets

6. To display ZDP configuration, use command **show zdp** in group config mode. This is shown in Table 397.

TABLE 397 SHOW ZDP COMMAND

Format	Mode	Function
show zdp	group config	This displays ZDP configuration

Result: This displays ZDP configuration.

7. To display neighbor device information table, use command **show zdp neighbour [detail]** in group config mode. This is shown in Table 398.

TABLE 398 SHOW ZDP NEIGHBOR COMMAND

Format	Mode	Function
show zdp neighbour [detail]	group config	This displays neighbor device information table

Result: This displays neighbor device information table.

END OF STEPS

Result ZDP has been configured.

Configuring ZTP

Background Topology protocol (ZTP) is a protocol used to collect network topology information. With neighbor device information table collected through ZDP, ZTP sends and forwards ZTP topology collection packets through the relevant port in the specified VLAN to collect the topology information in the network (hop count) within a specific range and to create a topology information table which is used for knowing network topology status and managing the cluster.

Purpose This topic describes the configuration of ZTP.

Steps For the configuration of ZTP, perform the following steps.

1. To enable/disable the system ZTP function, use the following command **set ztp {enable|disable}** in group config mode. This is shown in Table 399.

TABLE 399 SET ZTP COMMAND

Format	Mode	Function
set ztp {enable|disable}	group config	This enable/disable the system ZTP function

Result: This enable/disable the system ZTP function.

Note: By default, system ZTP function is enabled. When system ZTP function is disabled, contents of switch topology information table are cleared, and ZTP packets processing is suspended.

2. To enable/disable port ZTP function, use command **set ztp port** <portlist> **{enable|disable}** in group config mode. This is shown in Table 400.

TABLE 400 SET ZTP PORT COMMAND

Format	Mode	Function
set ztp port <portlist> **{enable|disable}**	group config	This enable/disable port ZTP function

Result: This enable/disable port ZTP function.

3. To enable/disable trunk ZTP function, use command **set ztp trunk** <trunklist> **{enable|disable}** in group config mode. This is shown in Table 401.

TABLE 401 SET ZTP TRUNK COMMAND

Format	Mode	Function
set ztp trunk <trunklist> **{enable|disable}**	group config	This enable/disable trunk ZTP function

Result: This enable/disable trunk ZTP function.

Important! By default, ZTP function of all ports/trunks is enabled. If ZTP function of a port/trunk is disabled, ZTP packets processing of port/trunk is suspended.

Note: A port/trunk can collect and send ZTP information normally only when both ZTP function of the port/trunk and system ZTP function are enabled.

4. To configure ZTP parameters use the following commands in group config mode as shown in Table 402.

TABLE 402 SET ZTP COMMANDS

Format	Mode	Function
set ztp vlan<1-4094>	group config	This configures a VLAN for collecting topology information.
set ztp hop <1-128>	group config	This sets range (hop count) of collecting topology information.
set ztp timer <0-60>	group config	This sets time interval for collecting topology information periodically.
set ztp hopdelay <1-1000>	group config	This sets hop delay for forwarding topology requests.
set ztp portdelay <1-100>	group config	This sets port delay for forwarding topology requests.

Result: This configures vlan and sets range, set time, set hop delay and set port delay for topology.

- By default, specified VLAN for collecting topology information is VLAN 1, and topology collecting range is four hops. By default, time interval for collecting topology information is 0 minute, that is, topology information is not collected periodically.
- When switch is configured to be a command switch, VLAN for collecting topology information serves as management VLAN of command switch. In this case, it is not allowed to change specified VLAN for collecting topology information.
- When network delay is high, hop delay and port delay of topology forwarding shall be modified to adapt current network status.
- To collect network topology information within a larger range, administrator can increase hop counts.

5. To manually start collecting topology information, use command **ztp start** in group config mode. This is shown in Table 403.

TABLE 403 ZTP START COMMAND

Format	Mode	Function
ztp start	group config	This starts collecting topology information manually

Result: This starts collecting topology information manually.

Note: To know network topology information at any time, user can manually start topology information collection procedure, without depending on automatic topology information collection

6. To display ZTP configuration, use command **show ztp** in group config mode. This is shown in Table 404.

TABLE 404 SHOW START COMMAND

Format	Mode	Function
show ztp	group config	This displays ZTP configuration

Result: This displays ZTP configuration.

7. To display details of specified device according to MAC address, use command **show ztp mac** in group config mode. This is shown in Table 405.

TABLE 405 ZTP MAC COMMAND

Format	Mode	Function
show ztp mac	group config	This displays detail of specified device according to MAC address

Result: This displays detail of specified device according to MAC address.

8. To display topology information table, use command **show ztp device** [<idlist>] in group config mode. This is shown in Table 406.

TABLE 406 SHOW ZTP DEVICE COMMAND

Format	Mode	Function
show ztp device [<idlist>]	group config	This displays topology information table

Result: This displays topology information table.

Note: Device ID offered by topology information table is the temporary ID that is generated based on current topology information collection result. With the purpose of facilitating display and cluster management, it is effective to current topology information collection result only.

END OF STEPS

Result ZTP has been configured.

Configuring Cluster

Purpose This topic describes the cluster configuration. Unique ID of a cluster consists of VLAN where cluster is located and MAC address of command switch.

Steps For the configuration of cluster, perform the following steps.

1. To set candidate switches, use command **set group candidate** in group config mode. This is shown in Table 407.

TABLE 407 SET GROUP CANDIDATE COMMAND

Format	Mode	Function
set group candidate	group config	This sets candidate switches

Result: This sets candidate switches.

2. To set independent switches, use command **set group independent** in group config mode. This is shown in Table 408.

TABLE 408 SET GROUP INDEPENDENT COMMAND

Format	Mode	Function
set group independent	group config	This sets independent switches

Result: This sets independent switches

3. To set a command switch, specify a layer 3 port number for cluster management and set IP address pool for user cluster management, use command **set group commander ipport** <0-63> **ip-pool** < A. B. C. D/M > in group config mode. This is shown in Table 409.

TABLE 409 SET GROUP COMMAND

Format	Mode	Function
set group commander ipport <0-63> **ip-pool** < A. B. C. D/M >	group config	This sets a command switch

Result: This sets a command switch; specify a layer 3 number for cluster management and sets IP address pool for user cluster management.

- After a candidate switch is added to the cluster by command switch and becomes a member switch,

member switch cannot change itself to a candidate switch or command switch.

- In setting command switch, VLAN to which the layer 3 port is bound shall be the specified VLAN for collecting topology information. Once a switch is configured to be a command switch, specified VLAN for collecting topology information cannot be changed.
- Command switch is allowed to be a candidate switch or independent switch only when the cluster has no member switch.

END OF STEPS

Result Cluster management Unique ID of cluster has been configured.

Configuring a Cluster Member

Purpose This topic describes the configuration of cluster member to add/delete.

Steps For the configuration of cluster member, perform the following steps.

1. To add a member based on device MAC address, use command **set group add mac** <xx. xx. xx> in group config mode. This is shown in Table 410.

TABLE 410 SET GROUP ADD MAC COMMAND

Format	Mode	Function
set group add mac <xx. xx. xx>	group config	This adds a member based on device MAC address

Result: This adds a membe based on device MAC address.

2. To add a member based on device MAC address and specify member ID, use command **set group add mac** <xx. xx. xx> <1-255> in group config mode. This is shown in Table 411.

TABLE 411 SET GROUP ADD MAC COMMAND

Format	Mode	Function
set group add mac <xx. xx. xx> <1-255>	group config	This adds a member based on device MAC address and specify member ID

Result: This adds a member based on device MAC address and specify member ID.

3. To add a member based on temporary device ID obtained from collected topology information, use command **set group add device** <idlist> in group config mode. This is shown in Table 412.

TABLE 412 SET GROUP ADD DEVICE COMMAND

Format	Mode	Function
set group add device <idlist>	group config	This adds a member based on temporary device ID obtained from collected topology information

Result: This adds a member based on temporary device ID obtained from collected topology information.

4. To delete a device with specified member ID from cluster, use command **set group delete member** <idlist> in group config mode. This is shown in Table 413.

TABLE 413 SET GROUP DELETE MEMBER COMMAND

Format	Mode	Function
set group delete member <idlist>	group config	This deleted a device with specified member ID from cluster

Result: This deletes a device with specified member ID from cluster.

END OF STEPS

Result Cluster member has been add/delet.

Note: When a device is added to cluster but member ID is not specified, system automatically allocates a unique ID to the member.

Configuring Cluster Parameters

Purpose This topic describes the configuration of cluster parameters.

Steps For the configuration of cluster parameters, perform the following steps.

1. To set cluster name, use command **set group name** <name> in group config mode. This is shown in Table 414.

TABLE 414 SET GROUP NAME COMMAND

Format	Mode	Function
set group name	group config	This sets cluster

Format	Mode	Function
<name>		name

Result: This sets cluster name.

2. To set a time interval for handshake between command switch and member switch, use command **set group handtime** <1-300> in group config mode. This is shown in Table 415.

TABLE 415 SET GROUP HANDTIME COMMAND

Format	Mode	Function
set group handtime <1-300>	group config	This sets a time interval for handshake between command switch and member switch

Result: This sets a time interval for handshake between command switch and member switch.

3. To set effective holding time of information about switches in cluster, use command **set group holdtime** <1-300> in group config mode. This is shown in Table 416.

TABLE 416 SET GROUP HOLDTIME COMMAND

Format	Mode	Function
set group holdtime <1-300>	group config	This sets effective holding time of information about switches in cluster

Result: This sets effective holding time of information about switches in cluster.

4. To set IP address of internal public SYSLOG Server of cluster, use command **set group syslogsvr** < A. B. C. D > in group config mode. This is shown in Table 417.

TABLE 417 SET GROUP SYSLOGSVR COMMAND

Format	Mode	Function
set group syslogsvr < A. B. C. D >	group config	This sets IP address of internal public SYSLOG Server of cluster

Result: This sets IP address of internal public SYSLOG Server of cluster.

5. To set IP address of internal public TFTP Server of cluster, use command **set group tftpsvr** < A. B. C. D > in group config mode. This is shown in Table 418.

TABLE 418 SET GROUP TFTPSVR COMMAND

Format	Mode	Function
set group tftpsvr < A. B. C. D >	group config	This sets IP address of internal public TFTP Server of cluster

Result: This sets IP address of internal public TFTP Server of cluster.

END OF STEPS

Result Cluster parameters have been configured.

Note: Above parameters can be configured for command switch only.

Effective holding time of cluster means that when command switch detects communication failure of a member switch (or a member switch detects that of command switch), and communication is recovered within effective holding time, member status is normal; if the communication is not recovered after effective holding time, command switch displays that member is in DOWN state. After communication is recovered, member is added to cluster automatically and is displayed in UP status.

If IP address of TFTP Server of cluster is configured, member switch can access TFTP Server by directly accessing command switch.

Configuring Access and Control Cluster Members

Purpose This topic describes the configuration of access and control cluster members.

Steps For the configuration of access and control cluster members, perform the following steps.

1. To switch from command switch to a specified member switch, use command **rlogin member** <1-255> in privileged mode. This is shown in Table 419.

TABLE 419 RLOGIN MEMBER COMMAND

Format	Mode	Function
rlogin member <1-255>	privileged mode	This switches from command switch to a specified member switch

Result: This switches from command switch to a specified member switch.

2. To switch from a member switch to command switch, use command **rlogin commander** in privileged mode. This is shown in Table 420.

TABLE 420 RLOGIN COMMANDER COMMAND

Format	Mode	Function
rlogin commander	privileged mode	This switches from a member switch to command switch

Result: This switches from a member switch to command switch.

3. To download/upload versions through TFTP on command switch, use command **tftp commander {download|upload}** <name> in privileged mode. This is shown in Table 421.

TABLE 421 TFTP COMMANDER COMMAND

Format	Mode	Function
tftp commander {download|upload} <name>	privileged mode	This download/upload version through TFTP on command switch

Result: This download/upload version through TFTP on command switch.

4. To save configuration of specified member switch, use command **save member** {<idlist>|**all**} in privileged mode. This is shown in Table 422.

TABLE 422 SAVE MEMBER COMMAND

Format	Mode	Function
save member {<idlist>|**all**}	privileged mode	This saves configuration of specified member switch

Result: This saves configuration of specified member switch.

5. To delete configuration of specified member switch, use command **erase member** {<idlist>|**all**} in privileged mode. This is shown in Table 423.

TABLE 423 ERASE MEMBER COMMAND

Format	Mode	Function
erase member {<idlist>|**all**}	privileged mode	This deletes configuration of

Format	Mode	Function
		specified member switch

Result: This deletes configuration of specified member switch.

6. To restart specified member switch, use command **reboot member** {<idlist>|**all**} in privileged mode. This is shown in Table 424.

TABLE 424 REBOOT MEMBER COMMAND

Format	Mode	Function
reboot member{<idlist>|**all**}	privileged mode	This restarts specified member switch

Result: This restarts specified member switch.

END OF STEPS

Result Access and control cluster members have been configured.

Displaying Cluster Configuration

Purpose This topic describes the display of cluster configuration and cluster member information.

Steps For the display of cluster configuration, perform the following steps.

1. To display cluster configuration information, use command **show group** in global config mode. This is shown in Table 425.

TABLE 425 SHOW GROUP COMMAND

Format	Mode	Function
show group	global config	This displays cluster configuration information

Result: This displays cluster configuration information.

2. To display candidate switches that can be added to cluster, use command **show group candidate** in global config mode. This is shown in Table 426.

TABLE 426 SHOW GROUP CANDIDATE COMMAND

Format	Mode	Function
show group candidate	global config	This displays candidate switches that can be added

Format	Mode	Function
		to cluster

Result: This displays candidate switches that can be added to cluster.

3. To display cluster member information, use command **show group member** [<1-255>] in global config mode. This is shown in Table 427.

TABLE 427 SHOW GROUP MEMBER COMMAND

Format	Mode	Function
show group member [<1-255>]	global config	This displays cluster member information

Result: This displays cluster member information.

END OF STEPS

Result Cluster configuration and member information has been displayed.

Example This example describes the initial configuration of switches is default configuration. Set the VLAN where public network IP address of command switch in cluster is located to 2525, IP address to 100. 1. 1. 10/24, gateway address to 100. 1. 1. 1, cluster management VLAN to 4000, private address pool to 192. 168. 1. 0/24, and IP address of TFTP Server of whole cluster to 110. 1. 1. 2. This is shown in Figure 42.

Detail configuration is as follows:

Configure public network IP address of command switch and gateway.

```
WYXX(cfg)#set vlan 2525 enable
WYXX(cfg)#set vlan 2525 add port 1-16 tag

WYXX(cfg)#config router
WYXX(cfg-router)#set ipport 25 ipaddress 100.    1.    1.
10/24
WYXX(cfg-router)#set ipport 25 vlan 2525
WYXX(cfg-router)#set ipport 25 enable

WYXX(cfg-router)#iproute 0.   0.   0.   0/0 100.   1.   1.
1
```

Create a cluster on layer 3 port 1 of command switch and VLAN 1 (default VLAN).

```
WYXX(cfg)#config group
WYXX(cfg-group)#set group commander ipport 1 ip-pool 192.
168.   1.   1/24

Cmdr.   WYXX(cfg-group)#ztp start
Cmdr.   WYXX(cfg-group)#show ztp device
  Last collection vlan : 1
  Last collection time : 188 ms
   Id  MacAddress         Hop   Role  Platform
  ---  ----------------- ---  -----  ---------
    0  00.   d0.   d0.   fc.   08.   6c    0  cmdr   ZXR10
2928
    1  00.   d0.   d0.   fc.   08.   d6    1  candi  ZXR10
2928
    2  00.   d0.   d0.   fc.   08.   cf    1  candi  ZXR10
5116-FI
    3  00.   d0.   d0.   fc.   08.   fa    1  candi  ZXR10
5116
    4  00.   d0.   d0.   fc.   08.   d5    1  candi  ZXR10
2928-FI
    5  00.   d0.   d0.   fc.   09.   3a    1  candi  ZXR10
2818S

Cmdr.   WYXX(cfg-group)#set group add device 1-5
  Adding device id : 1    .    .    .      Successed to add
member!
  Adding device id : 2    .    .    .      Successed to add
member!
  Adding device id : 3    .    .    .      Successed to add
member!
  Adding device id : 4    .    .    .      Successed to add
member!
  Adding device id : 5    .    .    .      Successed to add
member!

Cmdr.   WYXX(cfg-group)#show group member
  MbrId MacAddress        IpAddress           Status
  ----- ----------------- ------------------- ----------
  1     00.   d0.   d0.   fc.   08.   d6 192.   168.   1.
2/24      Up
  2     00.   d0.   d0.   fc.   08.   cf 192.   168.   1.
3/24      Up
  3     00.   d0.   d0.   fc.   08.   fa 192.   168.   1.
4/24      Up
  4     00.   d0.   d0.   fc.   08.   d5 192.   168.   1.
5/24      Up
  5     00.   d0.   d0.   fc.   09.   3a 192.   168.   1.
6/24      Up
```

Switch to each member switch and add all ports to VLAN 4000 (taking member 4 as an example)

```
Cmdr.   WYXX(cfg)#set vlan 4000 enable
Cmdr.   WYXX(cfg)#set vlan 4000 add port 1-16 tag

Cmdr.   WYXX(cfg)#rlogin member 4
  Trying  .   .   .   Open
  Connecting .   .   .

Membr_4.   zte>enable

Membr_4.   zte(cfg)#set vlan 4000 enable
Membr_4.   zte(cfg)#set vlan 4000 add port 1-16 tag
```

Delete cluster created on VLAN 1.

```
Cmdr.   WYXX(cfg-group)#set group delete member 1-5
  Deleting member id : 1   .   .   .     Successed to del
member!
  Deleting member id : 2   .   .   .     Successed to del
member!
  Deleting member id : 3   .   .   .     Successed to del
member!
  Deleting member id : 4   .   .   .     Successed to del
member!
  Deleting member id : 5   .   .   .     Successed to del
member!

Cmdr.   WYXX(cfg-group)#set group candidate
WYXX(cfg-group)#
```

Create a cluster on VLAN 4000.

```
WYXX(cfg-group)#set ztp vlan 4000

WYXX(cfg-group)#set group commander ipport 1 ip-pool 192.
168.   1.   1/24

Cmdr.   WYXX(cfg-group)#ztp start
Cmdr.   WYXX(cfg-group)#show ztp device
  Last collection vlan : 4000
  Last collection time : 176 ms
   Id  MacAddress         Hop   Role  Platform
  ---  ----------------- ---  -----  ---------
    0  00.   d0.   d0.   fc.   08.   6c    0  cmdr   ZXR10
2928
    1  00.   d0.   d0.   fc.   08.   d6    1  candi  ZXR10
2928
    2  00.   d0.   d0.   fc.   08.   cf    1  candi  ZXR10
5116-FI
    3  00.   d0.   d0.   fc.   08.   fa    1  candi  ZXR10
5116
    4  00.   d0.   d0.   fc.   08.   d5    1  candi  ZXR10
2928-FI
    5  00.   d0.   d0.   fc.   09.   3a    1  candi  ZXR10
2818S

Cmdr.   WYXX(cfg-group)#set group add device 1-5
  Adding device id : 1    .    .    .      Successed to add
member!
  Adding device id : 2    .    .    .      Successed to add
member!
  Adding device id : 3    .    .    .      Successed to add
member!
  Adding device id : 4    .   .   .     Successed to add
member!
  Adding device id : 5    .   .   .     Successed to add
member!

Cmdr.  WYXX(cfg-group)#show group member
  MbrId MacAddress        IpAddress           Status
  ----- --------------- ---------------- ----------
  1     00.  d0.  d0.  fc.  08.  d6 192.  168.  1.  2/24
Up
  2     00.  d0.  d0.  fc.  08.  cf 192.  168.  1.  3/24
Up
  3     00.  d0.  d0.  fc.  08.  fa 192.  168.  1.  4/24
Up
  4     00.  d0.  d0.  fc.  08.  d5 192.  168.  1.  5/24
Up
  5     00.  d0.  d0.  fc.  09.  3a 192.  168.  1.  6/24
Up
```

Set IP address of TFTP Server in cluster to 110. 1. 1. 2.

```
Cmdr. WYXX(cfg-group)#set group tftpsvr 110. 1. 1. 2
```

Set IP address of cluster SYSLOG Server as 110. 1. 1. 3.

```
Cmdr. WYXX(cfg-group)#set group syslogsvr 110. 1. 1. 3
```

Download version kernel. Z on member 4.

```
Membr_4. zte(cfg-tffs)#tftp commander download kernel. Z
```

Web Management Overview

Web Management Description

ZXR10 2920/2928/2952 provides an embedded WEB server stored in flash memory. It allows users to manage the switch remotely using a standard WEB browser (give the advice that the browser version should be above IE 4. 0, with a distinguish rate of 1024*768) through the network.

Logging On Using Web Management

Purpose

This topic describes procedure to login web management of ZXR10 2920/2928/2952.

Prerequisites

To login to web management, meet the following requirements.

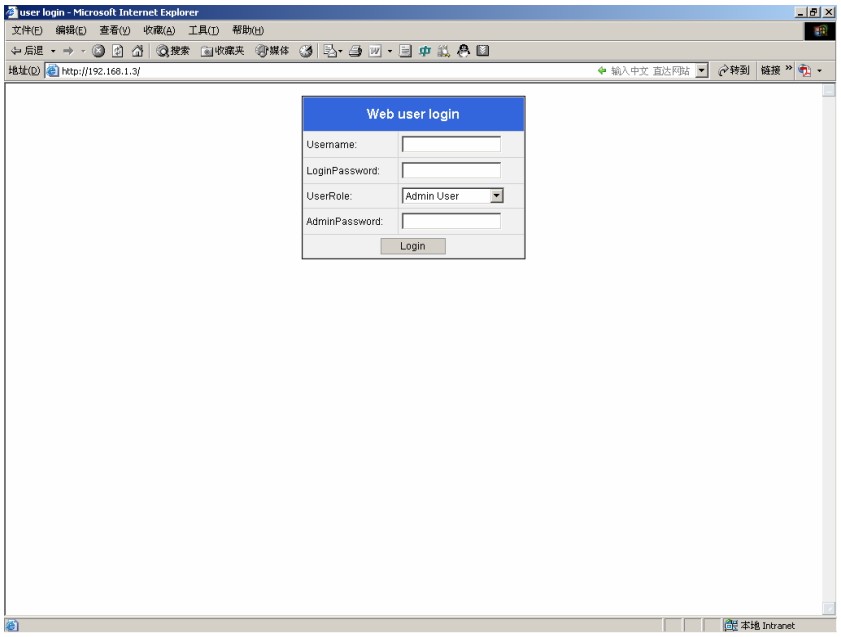
- Enable the web through hyper terminal.
- ZXR10 2609/2818S/2826S/2852S supports web server. It allows users to use standard web browser. Internet Explorer 4. 0 is required for the access of web management.

Steps

To login to web management of switch, perform following steps.

1. To use web management interface, open a web browser and enter IP address of switch as shown in Figure 44.

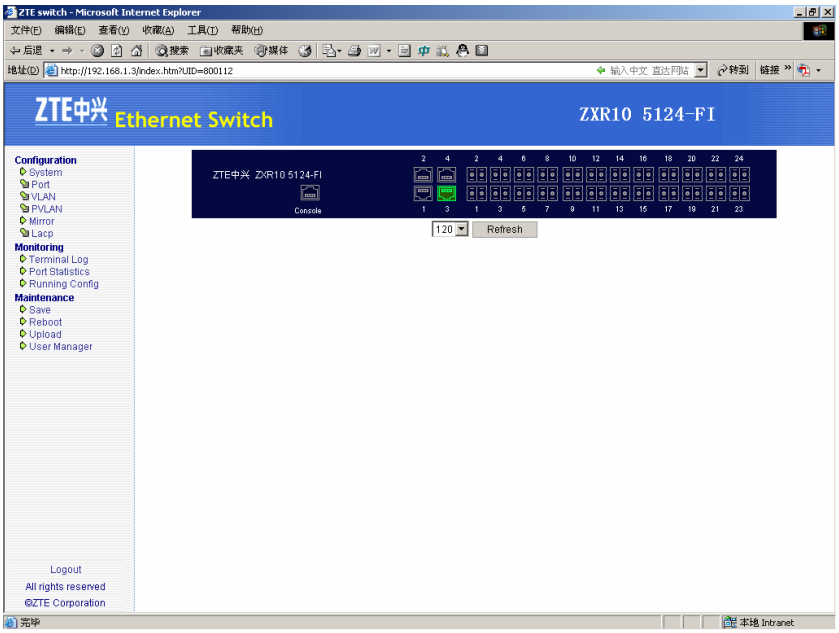
FIGURE 44 WEB USER LOGIN



2. Enter Username and login Password. By default username is **admin** and password is **zhongxing**.
3. Select **User Role**. It could be Admin User or Normal User. In Normal User there is no need of Admin Password. Without Admin Password, admin user is not accessible.
4. Click <**Login**> button, and log in the main system.

   Result: Ethernet switch is displayed as shown in Figure 45.

FIGURE 45 SYSTEM INTERFACE



END OF STEPS

Result Logging on using Web management is implemented.

Configuring a System

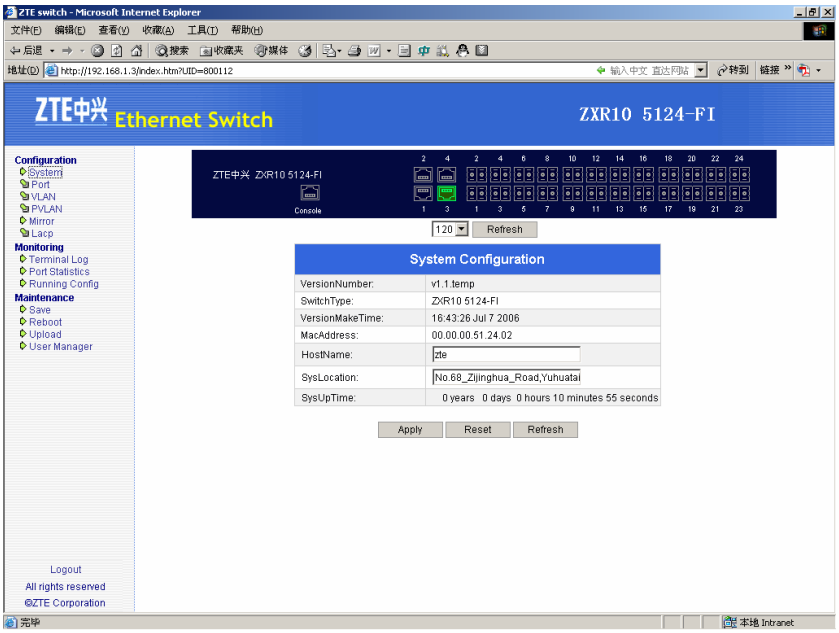
Purpose This topic describes the structure of switch configuration.

Steps For system configuration, perform the following steps.

1. Click the catalog tree in the left of the system main page **Configuration** > **System** to open system information page.

   Result: System configuration is displayed showing all the parameters as shown in Figure 46.

FIGURE 46 SYSTEM CONFIGURATION



Detail of system configuration is given in Table 428.

TABLE 428 SYSTEM CONFIGURATION DETAIL

Parameters	Detail
Version Number	Versin number detail
Switch Type	Type of switch
Version Make Time	When version is made
Mac Address	Hardware address of the switch
Host Name	System name
Sys Location	System location
Sys Up Time	Time the system has run since its start up

2. Host name and Sys location is change by clicking on it. Name and address is typed in columns.
3. Click **Apply**.

   Result: Host name and address is changed.

END OF STEPS

Result Structure of switch has been configured.

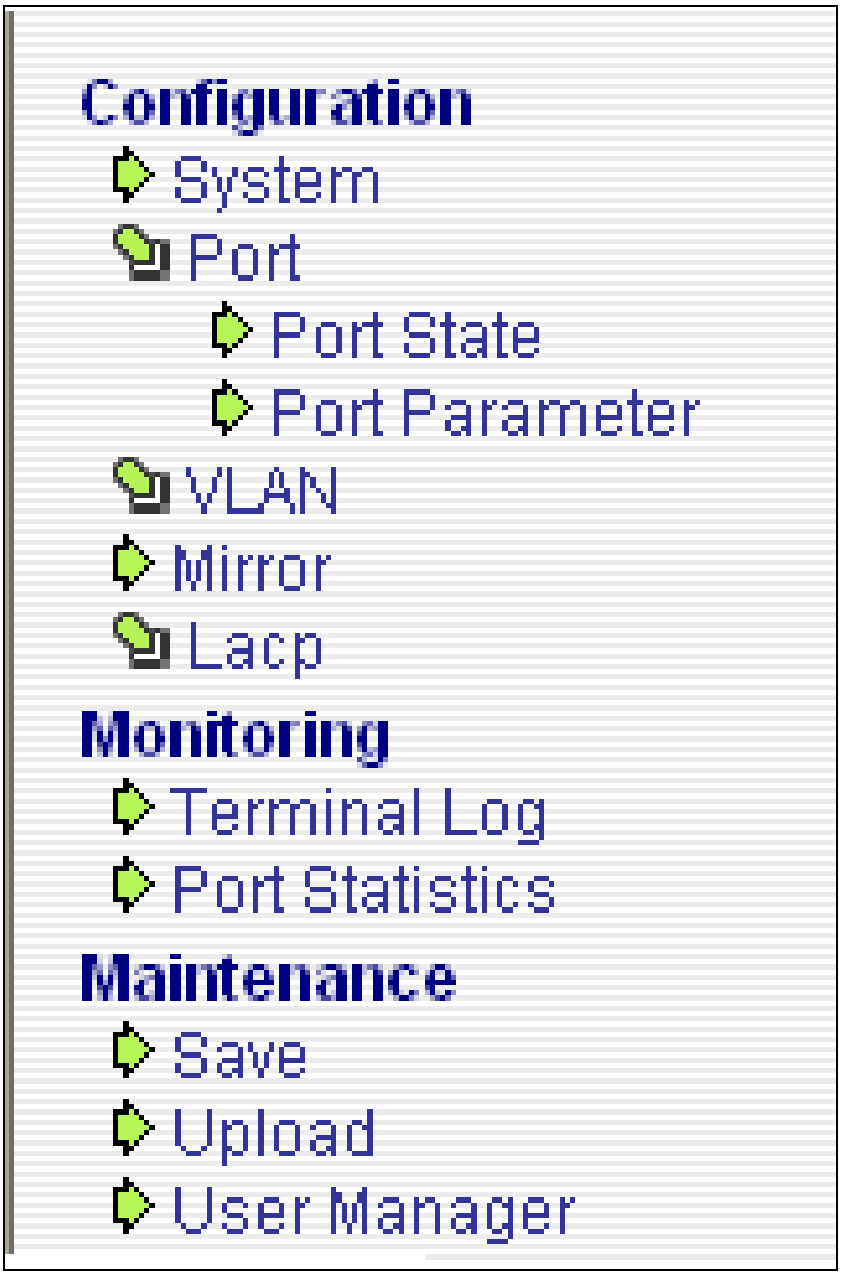
Configuring Port and Parameters

Purpose This topic describes the port status and parameters.

Steps For port status, perform following steps.

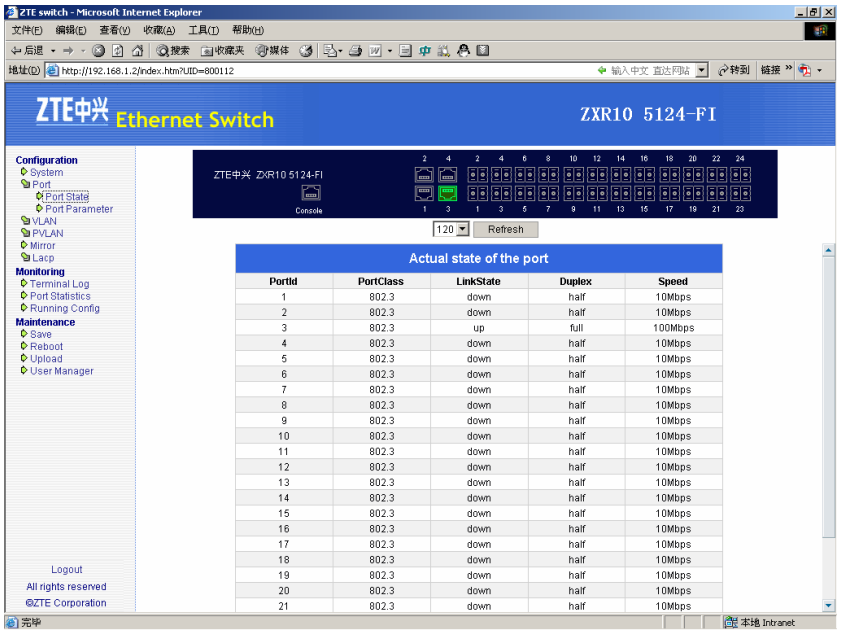
1. Click on **Configuration** > **Port** > **Port State** from configuration mode as show in Figure 47.

FIGURE 47 PORT STATE AND PARAMETERS



Result: Port status appears as shown in Figure 48.

FIGURE 48 PORT STATE INFORMATION



- Detail of Port status of Figure 48 is given below in Table 429.

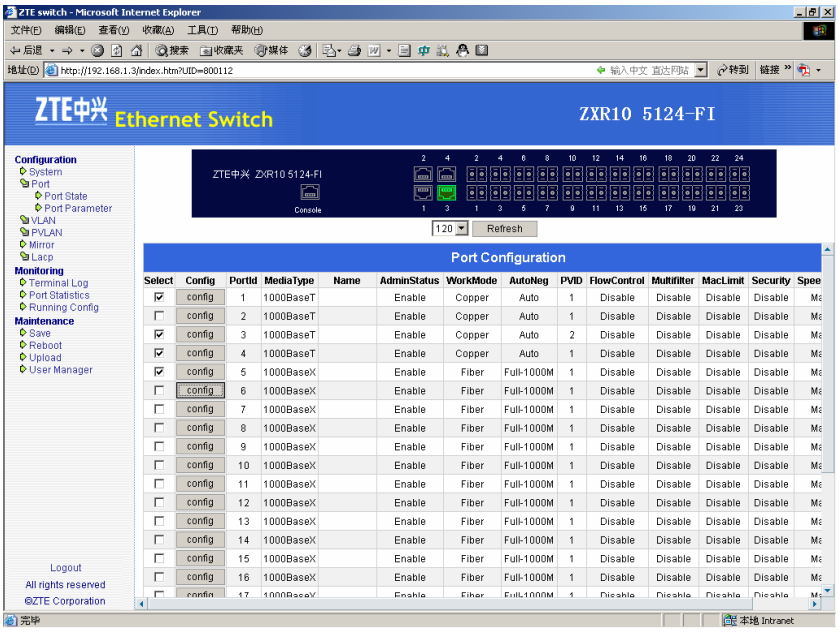
TABLE 429 PORT PARAMETERS DETAIL

Parameters	Description
Port Class	Ethernet standard
Link State	Link state (linkup or linkdown) of port
Duplex	Working duplex state of port
Speed	Working speed of port

Note: When port state is linkdown, the items "Duplex" and "Speed" are meaningless.

2. Click catalog tree in the left of system main page **Configuration** > **Port** > **Port Parameter** to open the port configuration information page, as shown in Figure 49.

FIGURE 49 PORT CONFIGURATION INFORMATION

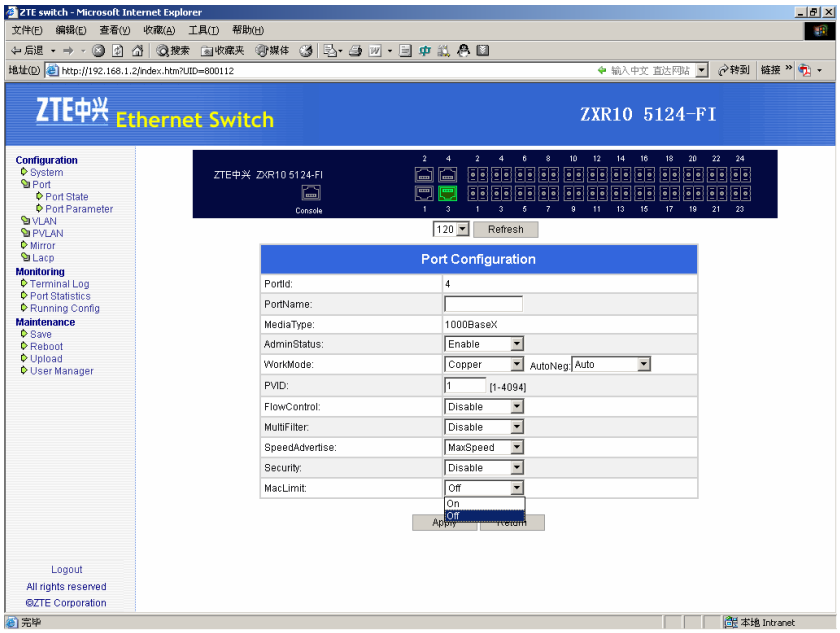


- The page shows the following information of the port:

Parameters	Description
Media Type	Media type of the port
Port Name	Port name
Admin Statu	Port Enable
Work Mode	Work mode of the port
Auto Neg	Work mode of the port that is work speed and duplex
PVID	VLAN ID is default on the port
Flow Control	Flow control enable on the port
Multi Filter	Multicast filtration enable on the port
Mac Limit	Limit the MAC address learning on the port
Security	Security enable on the port
Speed Advertise	Speed advertise on the port

3. For single port configuration, click **Config** button in the port row in the port configuration information page list to open the configuration page of the port need to be configured, as shown in Figure 50.

FIGURE 50 SINGLE PORT CONFIGURATION



4. In the page some attributes of the selected port can be configured. After configuration, click **Apply** button to submit.

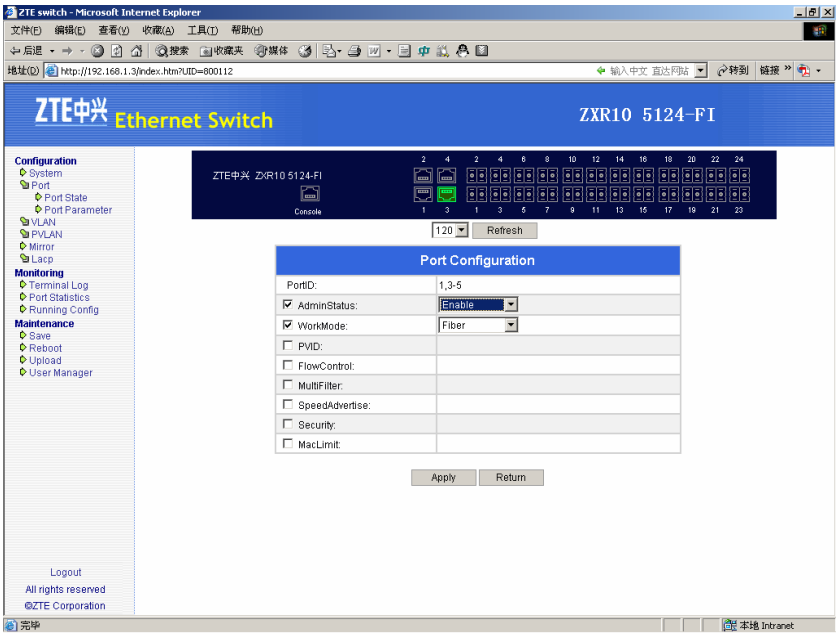
   Result: Configuration of selected port is accessible.

   Note: When security is enabling, Mac Limit is not supported.

   Important! Ensure that changes made to a port is not web management terminal, this can effect in terminating web management session.

5. For batch ports configuration select some ports in the port configuration information page list and at the same time user can choose **Select All** for all ports to be selected, then click **Apply** button to open the batch ports configuration page, as shown in Figure 51.

FIGURE 51 BATCH PORT CONFIGURATION



6. Click check boxes before the attributes to configure, and click **Apply** button to submit.

END OF STEPS

Result: Batch Ports are accessible.

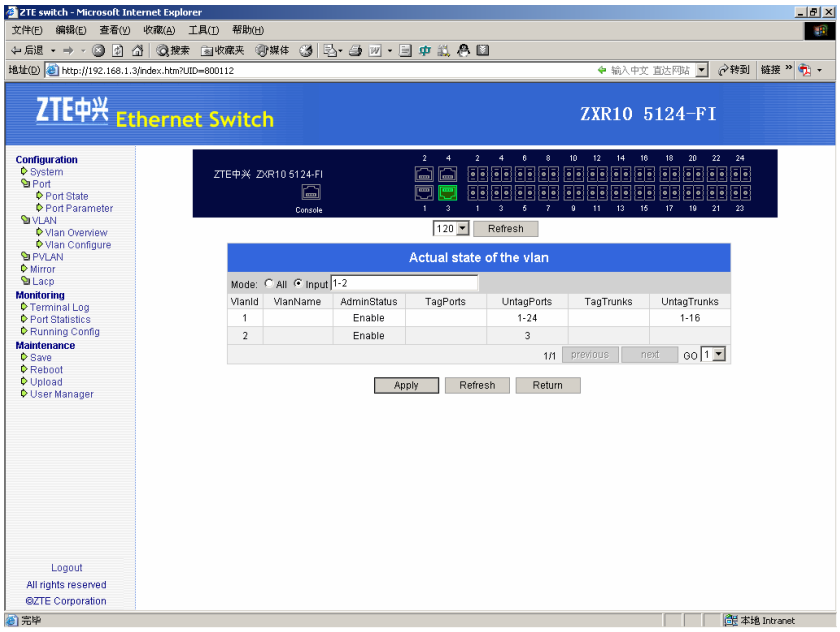
Configuring Vlan Management

Purpose This topic describes the configuration of Vlan management.

Steps For the configuration Vlan management, perform the following steps.

1. Click the catalog tree in the left of system main page **Configuration** > **VLAN** > **Vlan Overview** to open VLAN information page. This shows recent operated VLAN information. If there is on operation on the VLAN, it shows VLAN as default. This is shown in Figure 52.

FIGURE 52 VLAN INFORMATION



- Table 430 defines parameters shown in Figure 52.

TABLE 430 PARAMETERS DESCRIPTION

Parameters	Description
Vlan Name	Name of Vlan
Admin Status	Enable/Disable admin status
Tagged Port	Select ports which are to be tagged
Untagged Port	Select ports which are to be untagged
Tagged Trunk	Select ports which are to be tagged trunk
Untagged Trunk	Select ports which are to be untagged trunk

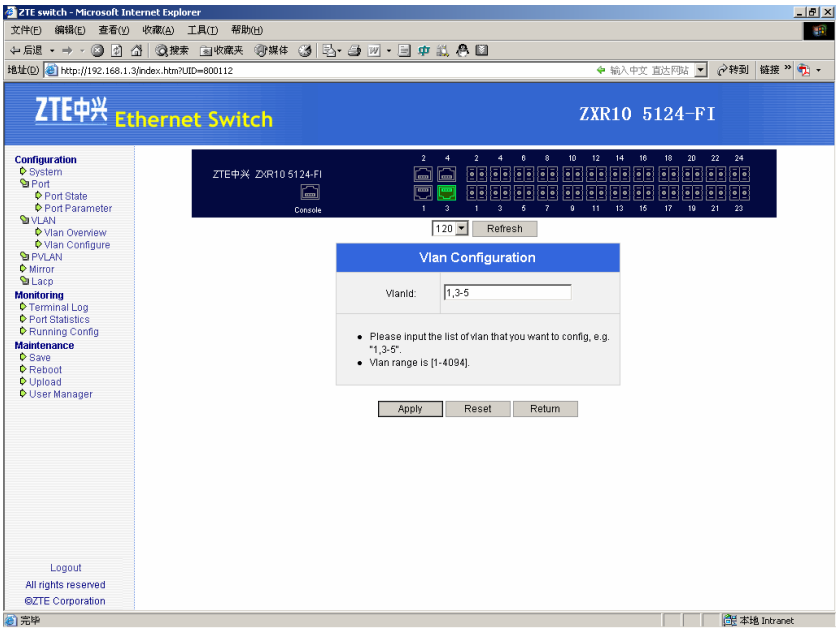
2. To show specified VLAN information select the radio box **Input** in the VLAN information page, then input the wanted VLAN number in text column, such as "1, 3-5"; or select the radio box **All**. Click **Apply** button to submit

   Result: Vlan information is displayed.

   Important! When there are more than 20 items, it will show them page by page with the page number on the left of the bottom. If there are more than one page, use the **previous** or **next** button to switch, or choose the page number directly in the **Go** column.

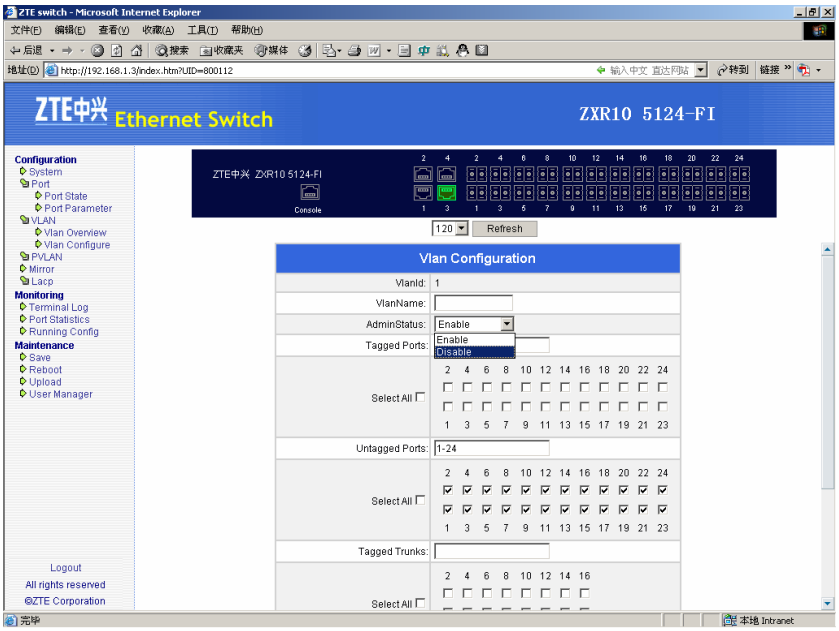
3. Click the catalog tree in the left of the system main page **Configuration** > **VLAN** > **Vlan Configure** to open VLAN number input page, as shown in Figure 53.

FIGURE 53 VLAN NUMBER INPUT



4. Input the VLAN number, format is like "1, 3-5" in the VLAN number input page, and click **Apply** button to enter single VLAN or batch VLANs configuration page.
5. Single VLAN configuration page is shown in Figure 54.

FIGURE 54 SINGLE VLAN



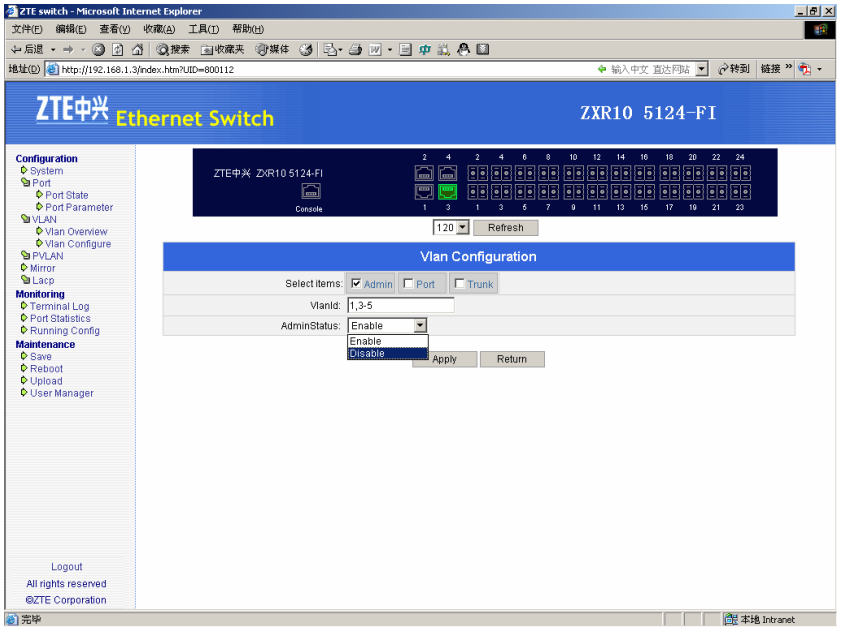
6. After configuring some attributes of the Vlan, click **Apply** button to submit.

   Result: Vlan is configured

Note: When configure port or trunk in the VLAN, user can insert port or trunk number in the text column following it, in the format such like "1, 3-5"; user can also select corresponding check boxes of the items wanted in the VLAN.

7. Batch VLANs configuration page is shown in Figure 55.

FIGURE 55 BATCH VLAN



8. Select and configure some attributes of the Vlan in the page, then click **Apply** button to submit.

   Result: Batch Vlan is configured.

END OF STEPS

Result VLAN has been configured.

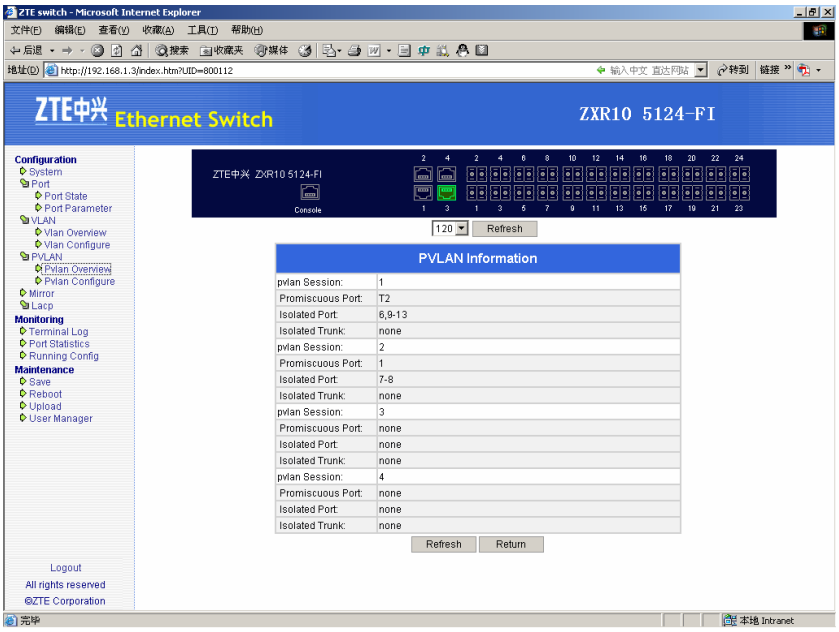
Configuring PVLAN

Purpose This topic describes the configuration of PVLAN.

Steps For the configuration PVLAN, perform the following steps.

1. Click the catalog tree in the left of the system main page **Configuration** > **PVLAN** > **PVLAN Overview** to open PVLAN information page, as shown in Figure 56.

FIGURE 56 PVLAN INFORMATION



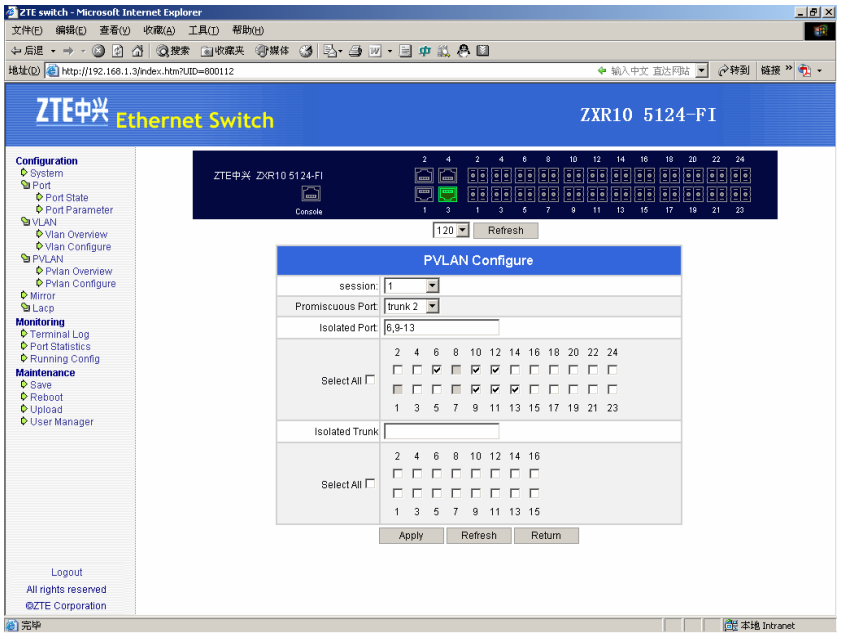
- Table 431 defines parameters shown in Figure 56.

TABLE 431 PVLAN PARAMETERS DESCRIPTION

Parameters	Description
PVlan Session	Pvlan session
Promiscuous Port	Prmoiscuous port
Isolated Port	Isolated port
Isolated Trunk	Isolated trunk

2. Click the catalog tree in the left of the system main page **Configuration** > **PVLAN** > **Pvlan Configure** to open the PVLAN configuration page, as shown in Figure 57.

FIGURE 57 PVLAN CONFIRUATION



3. After configuring attributes in this page, click **Apply** button to submit.

END OF STEPS

Result PVLAN has been configured.

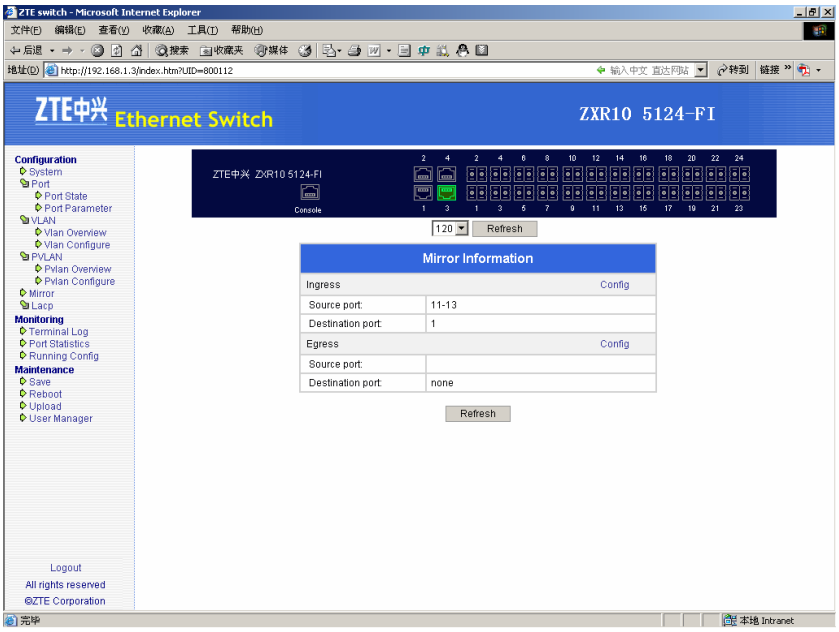
Configuring Mirroring Management

Purpose This topic describes the port mirroring management.

Steps For the port mirroring management, perform the following steps.

1. Click the catalog tree in the left of the system main page **configuration** > **mirror** to open mirror information page, as shown in Figure 58.

FIGURE 58 MIRRORING INFORMATION



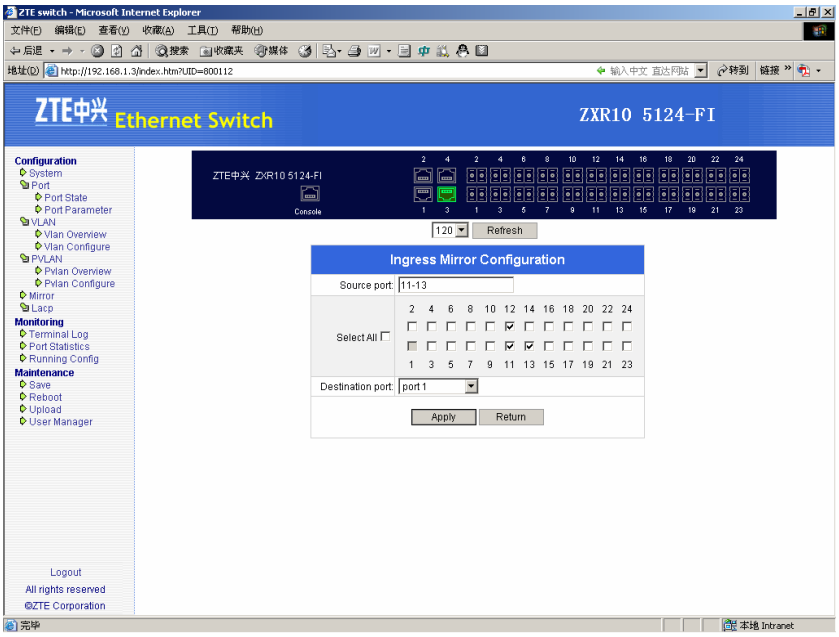
- The page shows the following information of port mirror including ingress and egress as shown in Table 432.

TABLE 432 PORT MIRROR DETAIL

Parameters	Description
Source port	Source port of the mirror
Destination port	Destination port of the mirror

2. Click **Config** link on the right of Ingress column to open the ingress port mirror configuration page, as shown in Figure 59.

FIGURE 59 INGRESS PORT MIRROR

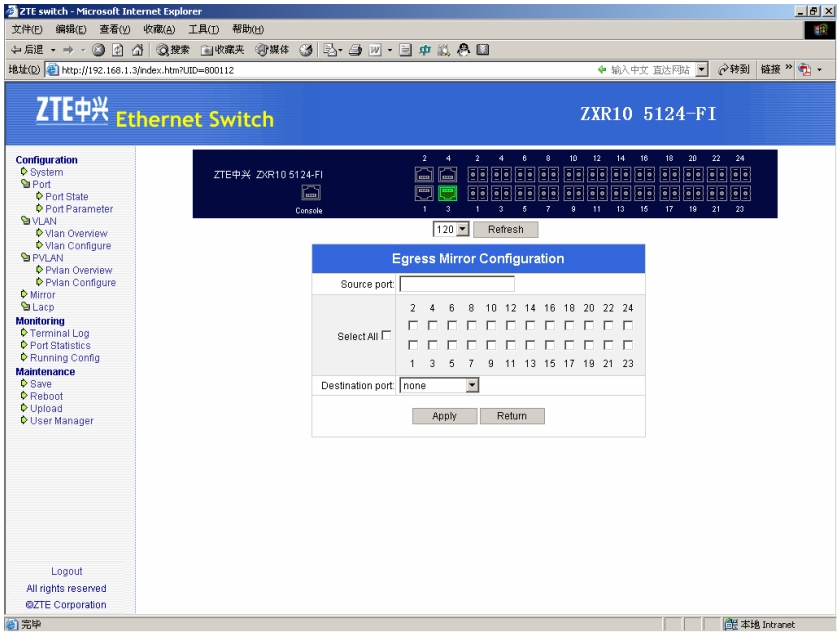


3. Configure destination and source port of ingress port mirror, then click **Apply** button to submit.

   Result: This configures destination and source port of ingress port mirror.

4. Click **Config** link on the right of Egress column to open the egress port mirror configuration page, as shown in Figure 60.

FIGURE 60 EGRESS PORT MIRROR



5. Configure destination and source port of egress port mirror, then click **Apply** button to submit.

   Result: This configures destination and source port of egree port mirror.

END OF STEPS

Result Mirroring management has been configured.

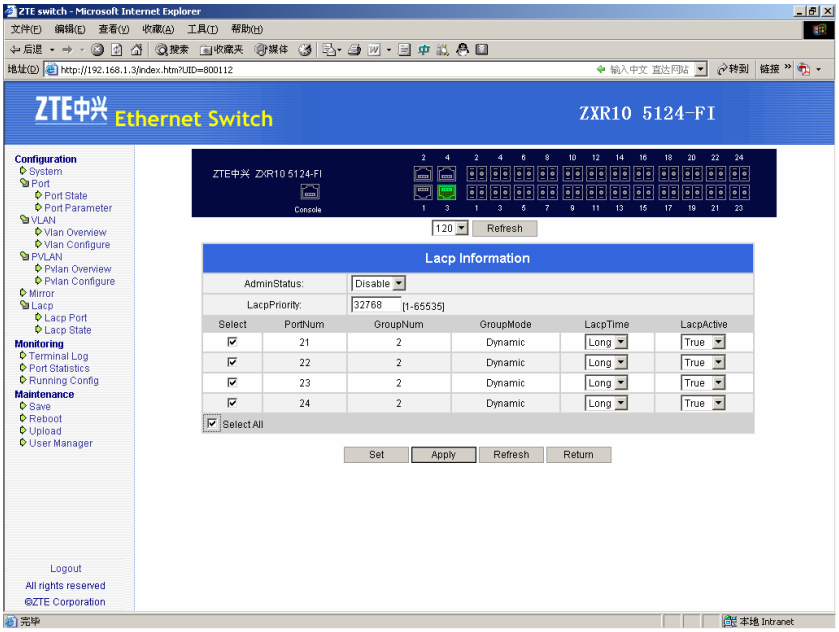
Configuring LACP Management

Purpose This topic describes the configuration of LACP management.

Steps For the configuration of LACP management, perform the following steps.

1. Click catalog tree in the left of the system main page **Configuration** > **Lacp** > **Lacp Port** to open LACP basic attributes page, as shown in Figure 61.

FIGURE 61 LACP BASIC ATTRIBUTE



- This page includes LACP basic information as shown in Table 433.

TABLE 433 LACP BASIC INFORMATION DETAIL

Parameters	Description
Admin Status	LACP enable status
Lacp Priority	LACP priority

- Information of assembling port is shown in Table 434.

TABLE 434 ASSEMBLING PORT INFORMATION

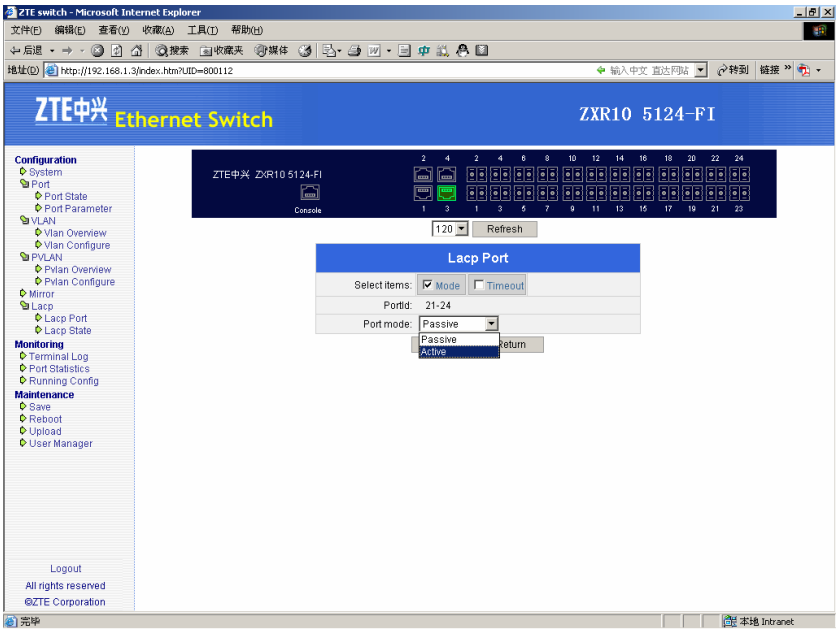
Parameters	Description
Group Num	Assembling group number that assembling port belongs to
Group Mode	Assembling mode that assembling port belongs to
Lacp Time	Overtime of assembling port
LacpActiv	Active/passive mode of assembling port

2. To configure basic attributes "AdminStatus" and "LacpPriority" of LACP, and attributes "LacpTime" and "LacpActive" of assembling port in the page.
3. After configuration click **Apply** button to submit.

Result: This configures basic attribute of LACP.

4. To configure batch assembling port attributes, select the check boxes of assembling ports **Select All**, all ports are selected, then click **Set** button to open batch assembling ports configuration page, as shown in Figure 62.

FIGURE 62 BATCH ASSEMBLING PORTS CONFIGURATION

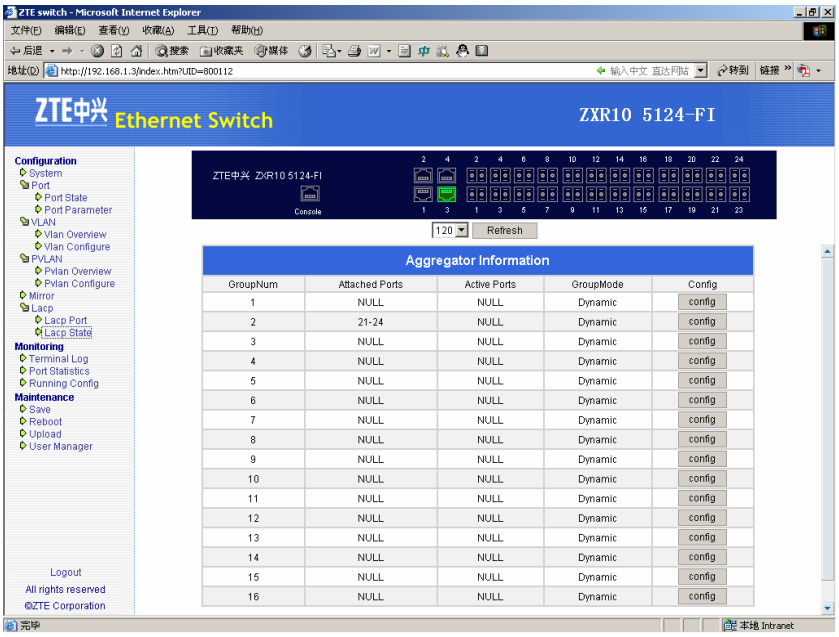


5. To configure assembling port attributes in the page, click **Apply** button to submit.

   Result: This configures assembling port attributes.

6. Click the catalog tree in the left of system main page **Configuration** > **Lacp** > **Lacp State** to open assembling group information page, as shown in Figure 63.

FIGURE 63 ASSEMBLING GROUP INFORMATION



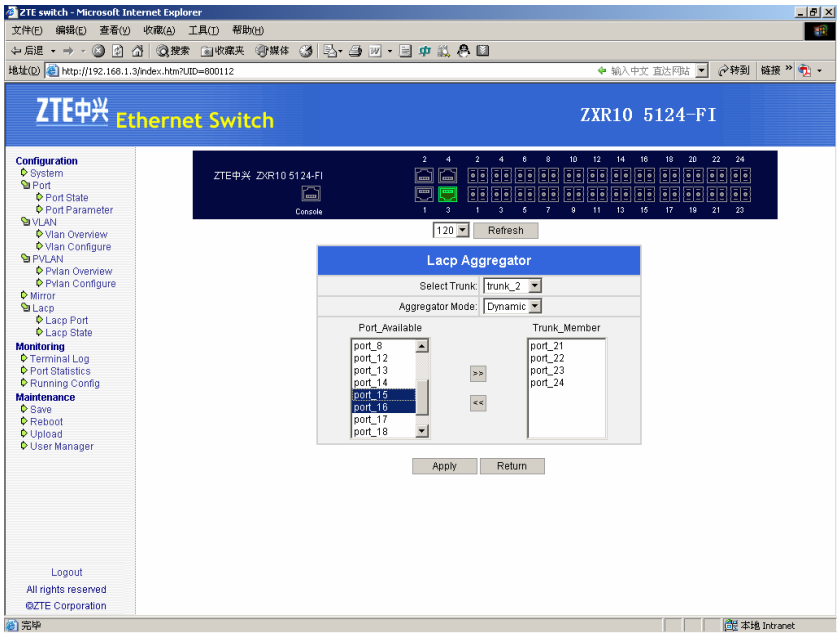
- This page shows information of assembling group, as shown in Table 435.

TABLE 435 ASSEMBLING GROUP DETAIL

Parameters	Description
Attached Ports	Attached ports in the assembling group
Active Ports	Active ports in the assembling group
GroupMode	Assembling mode of the assembling group

7. Click on **Config** button on the right to open the corresponding assembling group configuration page, as shown in Figure 64.

FIGURE 64 ASSEMBLING GROUP INFORMATION



8. To configure the attribute "Aggretator Mode" of selected assembling group in the page, and to bind port to assembling group. Select port in the optional port column and click >> button or free port from assembling group, select port in the port column and click <<button).

END OF STEPS

Result LACP management has been configured.

Note Only ports with same attributes can be binded to same assembling group. Number of ports binded to assembling group is up to 8.

Important! Avoid binding port connected to network management host to assembling group. Otherwise the network management will be interrupted.

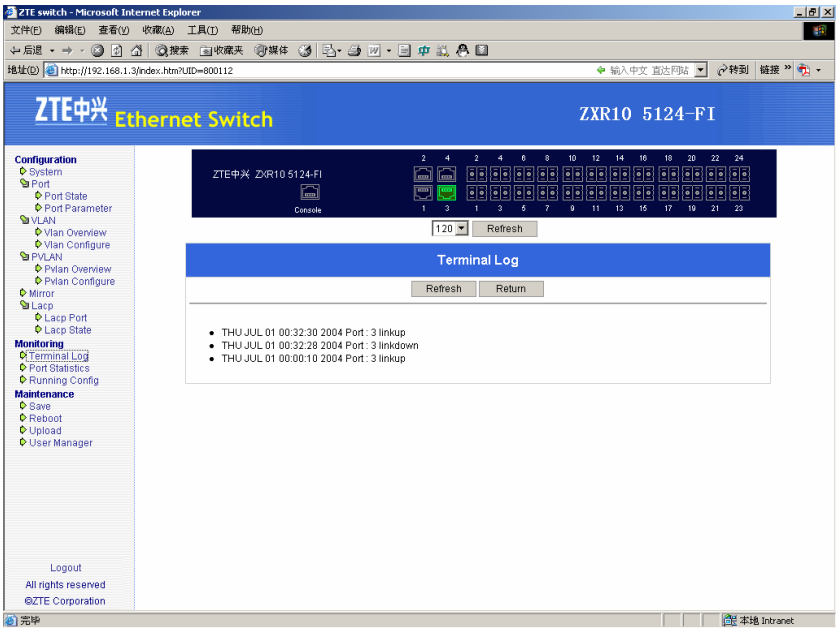
Configuring Terminal Record

Purpose This topic describes the configuration of terminal record.

Steps For the configuration of terminal record, perform the following steps.

1. Click the catalog tree in the left of the system main page **Monitoring** > **Terminal Log** to open the terminal log information page, as shown in Figure 65.

FIGURE 65 TERMINAL LOG INFORMATION



2. Click **Refresh** button in the page to update the terminal log information.

END OF STEPS

Result Terminal log information is accessible.

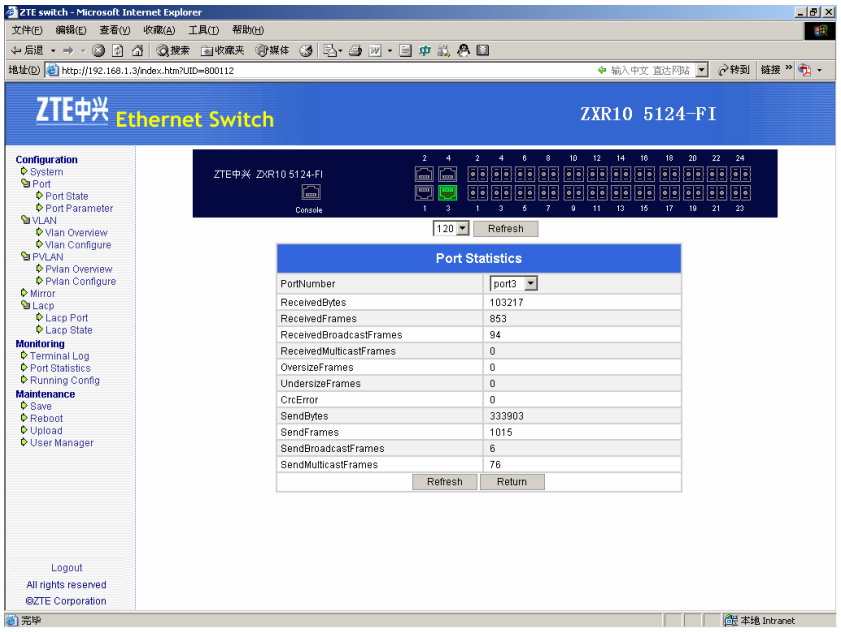
Configuring Port Statistics

Purpose This topic describes the configuration of port statistics.

Steps For the configuration of port statistics, perform the following steps.

1. Click the catalog tree in the left of the system main page **Monitoring** > **Port Statistics** to open the port statistics information page, as shown in Figure 66.

FIGURE 66 STATISTICAL INFORMATION



2. Click **Refresh** button in the page to update the port statistics information.
3. Select the items in the **PortNumber** column to get the statistics data on the port.

END OF STEPS

Result This shows statistics data on the port.

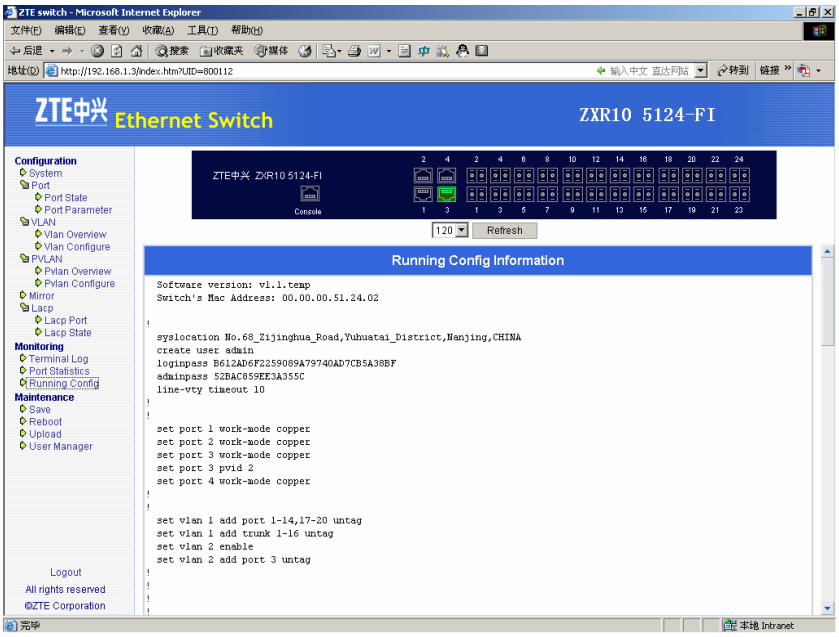
Configuring Information

Purpose This topic describes to open the configuration of information.

Steps For the opening of configuration of information, perform the following step.

1. Click the catalog tree in the left of the system main page **Monitoring** > **Running config** to open the configuration information page, as shown in Figure 67.

FIGURE 67 CONFIGURATION INFORMATION



END OF STEPS

Result The page shows the configuration information of the switch.

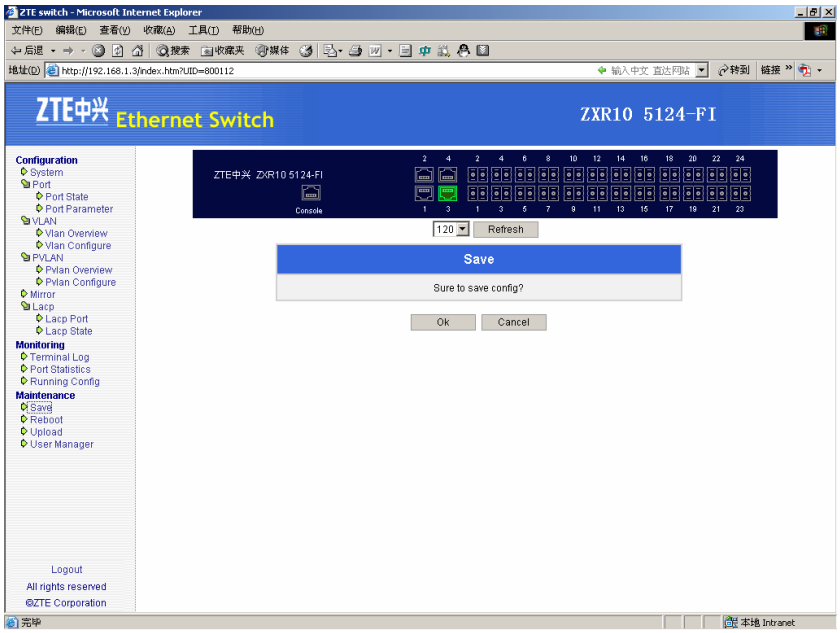
Saving Configuration

Purpose This topic describes the configuration saving reminder page.

Steps For the configuration of saving, perform the following steps.

1. Click the catalog tree in the left of the system main page **Maintenance** > **Save** to open the configuration saving reminder page, as shown in Figure 68.

FIGURE 68 CONFIGURATION SAVING REMINDER



2. Click **OK** to save the configuration, or click **Cancel** to give up the saving.

END OF STEPS

Result This saves the configuration.

Important! Saving the configuration will cover the primary configuration files, please be sure to cover the files before clicking **OK**.

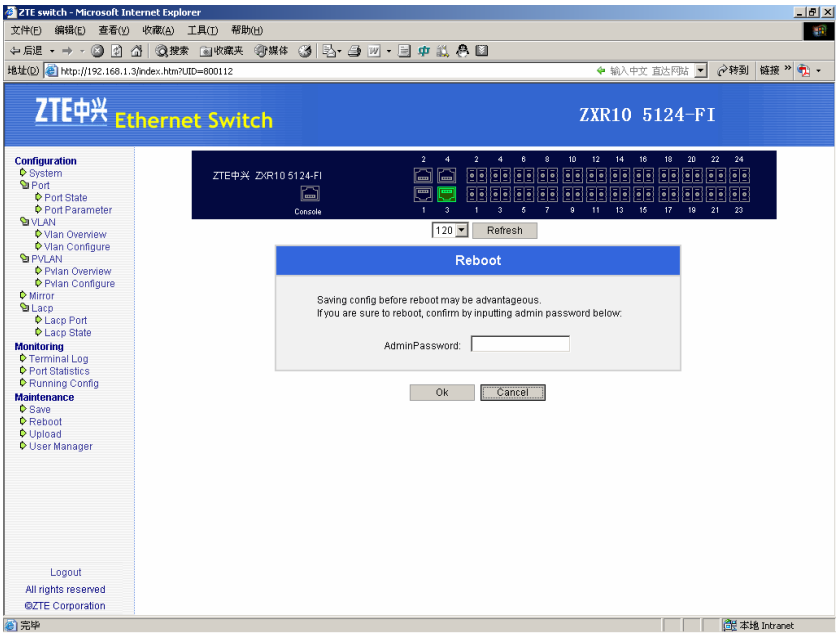
Rebooting an Equipment

Purpose This topic describes the rebooting of equipment.

Steps For the configuration of rebooting equipment, perform the following steps.

1. Click the catalog tree in the left of the system main page **Maintenance** > **Reboot** to open the reboot page, as shown in Figure 69.

FIGURE 69 REBOOT



2. Input the password of admin in the text column, then click **OK** to reboot the switch, or click **Cancel** to give up rebooting.

END OF STEPS

Result This reboots the switch.

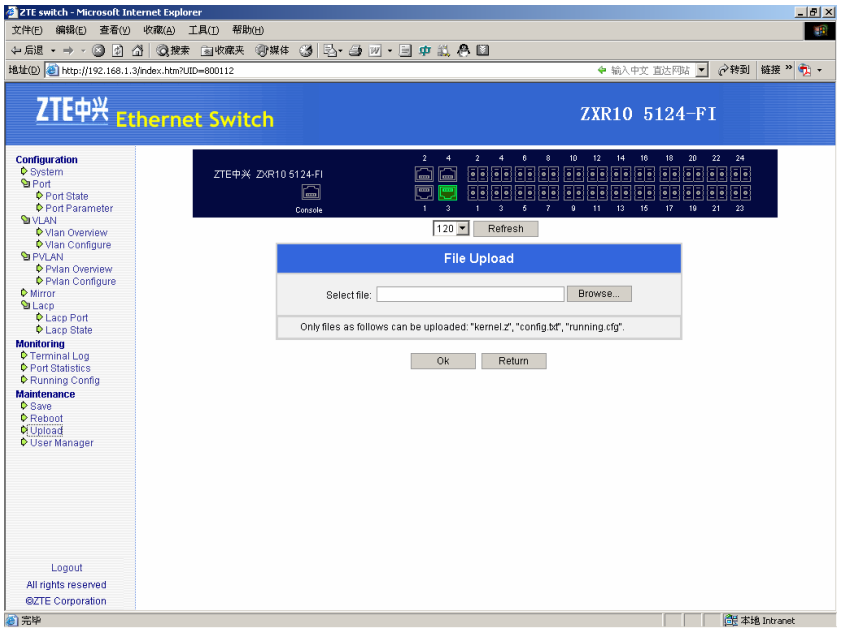
Uploading a File

Purpose This topic describes the uploading of file.

Steps For the configuration of file uploading, perform the following steps.

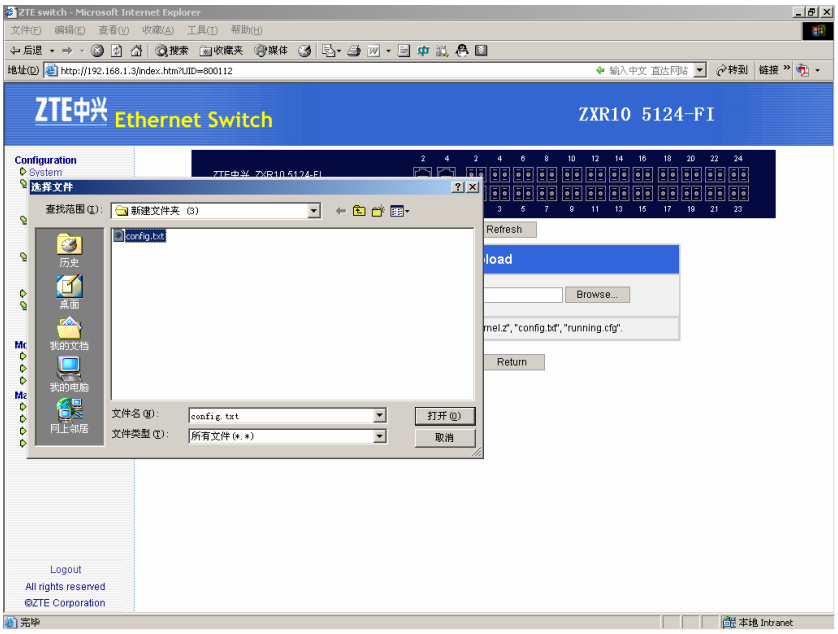
1. Click the catalog tree in the left of the system main page **Maintenance** > **Upload** to open the file upload page, as shown in Figure 70.

FIGURE 70 FILE UPLOAD



2. Click **Browse** to browse and select the file need uploading, as shown in Figure 71; then click **OK** to upload the file.

FIGURE 71 BROWSE AND SELECT FILE



END OF STEPS

Result The file uploaded successfully.

NOTE Considering the safe and application, only three kinds of file are allowed to be uploaded: "running. cfg", "config. txt" and "kernel. z".

Important! Be sure of the validity and usability of the uploaded files, as the uploaded files will cover the primary files. Errors due to improper operations will make the switch unable to work. Curbstone workers should avoid using this function.

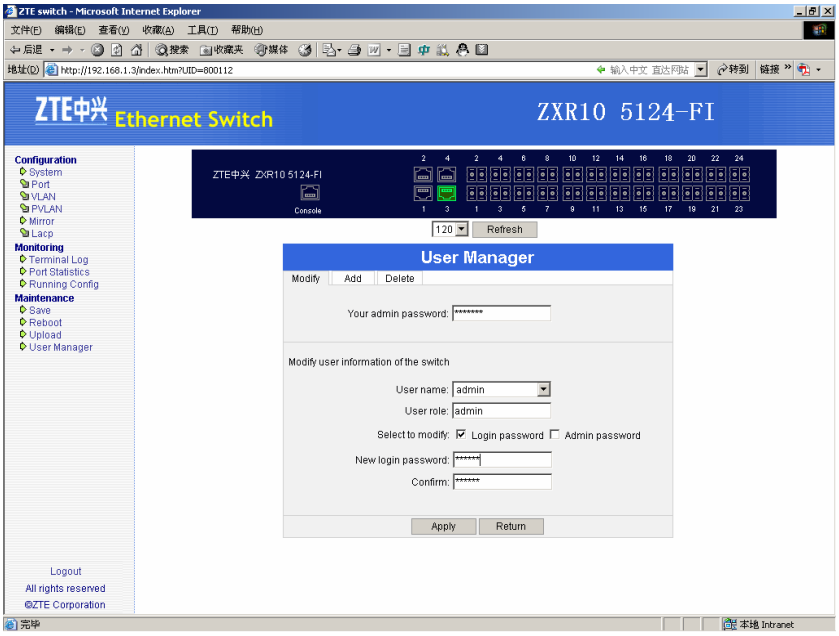
Configuring User Management

Purpose This topic describes the configuration of user management.

Steps For the configuration of user management, perform the following steps.

1. Click the catalog tree in the left of the system main page **Maintenance** > **User Manager** to open the user management page, as shown in Figure 72.

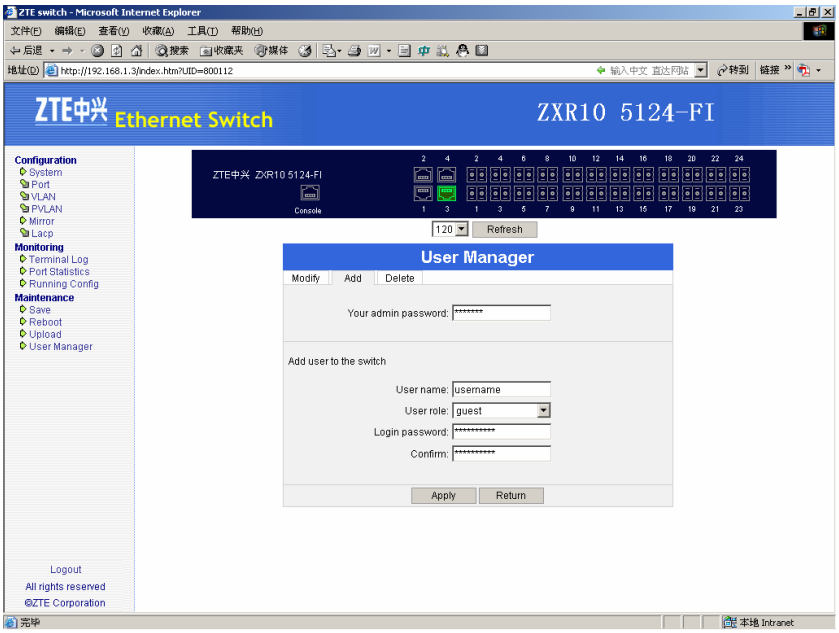
FIGURE 72 USER MANAGEMENT



2. Click **Apply** to submit.

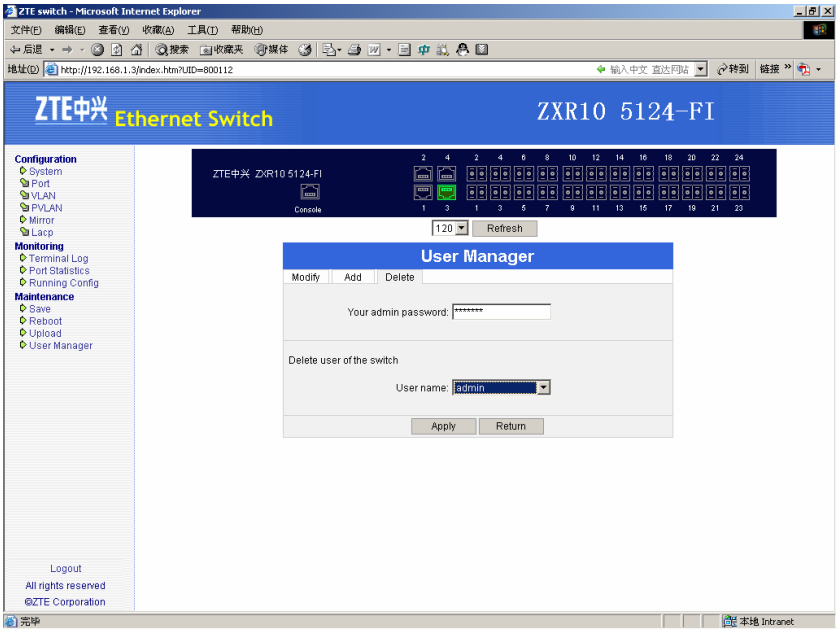
Note: Page is user modification page by default. The login password and management password of users can be modified in this page, but the current management password should be inputted before modification. 3. Click **Add** in the user management page to open the adding user page, as shown in Figure 73.

FIGURE 73 ADDING USER



4. Input the management password of the current user, and add and confirm the information of added user, then click **Apply** to submit.
5. Click **Delete** in the user management page to open **deleting user page**, as shown in Figure 74.

FIGURE 74 DELETING USER



6. Input the management password , and select the user to be deleted, then click **Apply** to submit.

END OF STEPS

Result User management tool has been configured and now it is possible to add and delete a user.

Chapter 10

Maintenance

Overview

Introduction This chapter provides routine maintenance, common test methods and troubleshooting of ZXR10 2920/2928/2952.

Contents This chapter includes the following contents:

Routine Maintenance

Routine maintenance generally refers to daily maintenance and monthly maintenance.

Daily Routine Maintenance

Purpose This topic describes the daily routine maintenance of ZXR10 2920/2928/2952.

Steps For the configuration of routine maintenance, perform the following steps:

1. Query whether the background terminal interface can operate normally.
2. Query whether the status of indicators of the switch is normal.
3. Check whether the fan of the switch runs normally.
4. Check whether the temperature of the switch is normal and whether there is any strange smell in the equipment room.
5. Check system alarm information.
6. Check the communication status between the switch and each connected device by logging into switch through a HyperTerminal or Telnet, and then use the **ping** command to test different network segments and check the connectivity.

   Result: This checks the communication status between switch and the other device connected to.
7. Check whether the switch related services are normal.
8. Record the intraday operations and phenomenon.

   Result: This records the phenomenon status of the switch, includes environment of the equipment room.

   NOTE: Intraday operations refer to the operations performed on that day.

END OF STEPS

Result: This checks the daily routine maintenance.

Monthly Maintenance

Purpose This topic describes the monthly maintenance of ZXR10 2920/2928/2952/5116-FI/5124-FI.

Prerequisites For the monthly maintenance, meet the following requirements.

- Summarize questions encountered in routine operations and please discuss with ZTE maintenance personnel if necessary.
- Summarize and accumulate maintenance experiences in routine maintenance to conduct more efficient maintenance.

Steps

For the configuration of monthly maintenance, perform the following steps:

1. Pay attention to the cleanness of air conditioners and check the performance of the air conditioners at the same time.
2. Clean the cabling trough, check whether the relevant lines are in poor contact and make adjustment in time.
3. Clean the switch.

   Note: Do not over wet the cleaning cloth. Make sure that the interfaces are not affected.
4. Back up the alarm data, statistic data and configuration data.

END OF STEPS

Result

This checks the monthly maintenance of switch.

Maintenance Period

Maintenance and test period of the Ethernet switch system for the reference of the maintenance personnel is shown in Table 436.

TABLE 436 MAINTENANCE AND TEST PERIOD OF ETHERNET SWITCH

No.	Maintenance & Test Item	Test Period
1	Check the running status of the switch.	Daily
2	Check the temperature and humidity in the equipment room and check the power supply.	Daily
3	Check the communication status between the switch and each connected device.	Daily
4	Check whether the relevant services are well developed.	Daily
5	Monthly summarization of routine maintenance problems.	Monthly
6	Monthly summarization of routine maintenance experience.	Monthly
7	Clean the equipment room.	Monthly
8	Clean the switch.	Monthly
9	Yearly summarization.	Yearly
10	Completely maintain and check the equipment in the monitoring room.	Yearly

Single Loop Test Method

Features of Singly Port Loop

Single-port loop test is to check whether a loop exists in the ports of the switch. If such a loop exists, it may result in errors in learning MAC addresses and may easily cause a broadcast storm. In worse cases, switch and network may be down. Starting the single-port loop test and disabling the port with loop can efficiently avoid the influence caused by port loop.

Working principle of single-port loop test, switch sends a test message on a port, if the test message comes back on the port without any changes or just is added a tag, it indicates that a loop exists on this port.

Principle of Single Port Loop Test

The switch sends a test packet through a port. If this test packet is received through the port without any change (or only a tag is attached), it indicates that a loop exists in this port.

The test packet sent by the switch includes the following three parameters:

Source MAC address

It indicates the MAC address of the switch. The MAC address of each switch is unique.

Port Number

Port numbers correspond to the numbers of the ports on the switch one by one.

Discimination Field

For each switch, the digital signature of each port is different.

When three parameters in the test packet sent through port are same as those in the test packet received through the port, a port loop absolutely exists.

Configuring Single-Port Loop Test

Purpose

This topic describes the configuration of single-port loop test.

Steps

For the configuration of single-port loop test, perform the following steps.

1. To enable/disable loop test function of specified port, use command **set loopdetect port** <portlist> **{enable|disable}** in global config mode. This is shown in Table 437.

TABLE 437 SET LOOP DETECT PORT COMMAND

Format	Mode	Function
set loopdetect port <portlist> **{enable|disable**	global config	This enable/disable loop test function of specified port

Result: This enable/disable loop test function of specified port.

Note: By default, port loop test function is disabled.

2. To enable/disable loop test function of specified port in specified vlan, use command **set loopdetect port** <portlist> **vlan** <1-4094> **{enable|disable}** in global config mode. This is shown in

TABLE 438 SET LOOP DETECT PORT VLAN COMMAND

Format	Mode	Function
set loopdetect port <portlist> **vlan** <1-4094> **{enable|disable}**	global config	This enable/disable loop test function of specified port in specified vlan

Result: This enable/disable loop test function of specified port in specified vlan.

Note: By default, port loop test function is disabled.

3. To enable/disable loop test function of a trunk, use command **set loopdetect trunk** <trunklist> **{enable|disable}** in global config mode. This is shown in Table 439.

TABLE 439 SET LOOP DETECT TRUNK COMMAND

Format	Mode	Function
set loopdetect trunk <trunklist> **{enable|disable}**	global config	This enable/disable loop test function of a trunk

Result: This enable/disable loop test function of a trunk.

Note: By default, loop test function of a trunk is disabled.

4. To enable/disable loop test function of a trunk on a designated vlan, use command **set loopdetect trunk** <trunklist> **vlan** <1-4094> **{enable|disable}** in global config mode. This is shown in

TABLE 440 SET LOOP DETECT TRUNK VLAN COMMAND

Format	Mode	Function
set loopdetect trunk <trunklist> **vlan** <1-4094> **{enable|disable}**	global config	This enable/disable loop test function of a trunk on a vlan

Result: This enable/disable loop test function of a trunk on a vlan.

Note: By default, loop test function of a trunk is disabled.

5. To enable/disable loop test protection function of specified port, use command Table 441.

TABLE 441 SET LOOP DETECT PORT PROTECT COMMAND

Format	Mode	Function
set loopdetect port <portlist> **protect {enable|disable}**	global config	This enable/disable loop test protection function of specified port

Result: This enable/disable loop test protection function of specified port

Note: Loop test protection function means that port is automatically blocked when it detects a loop. In this way, influence caused by port loop is avoided.

6. To enable/disable loop test protection function of a trunk, use command **set loopdetect trunk** <trunklist> **protect {enable|disable}** in global config mode. This is shown in Table 442.

TABLE 442 SET LOOP DETECT TRUNK PROTECT COMMAND

Format	Mode	Function
set loopdetect trunk <trunklist> **protect {enable|disable}**	global config	This enable/disable loop test protection function of a trunk

Result: This enable/disable loop test protection function of a trunk.

7. To set time for blocking port with loop, use command **set loopdetect blockdelay** <1-1080> in global config mode. This is shown in Table 443.

TABLE 443 SET LOOP DETECT BLOCK DELAY COMMAND

Format	Mode	Function
set loopdetect blockdelay <1-1080>	global config	This set time for blocking port with loop

Result: This set time for blocking port with loop.

Note: Time for blocking port with loop refers to time for blocking port when a loop is detected, that is, port protection time. Protection takes effect only when loop test protection function of port is enabled.

8. To set interval time of sending loop test packet, use command **set loopdetect sendpktinterval** <5-60> in global config mode. This is shown in Table 444.

TABLE 444 SET LOOP DETECT SEND COMMAND

Format	Mode	Function
set loopdetect sendpktinterval <5-60>	global config	This sets interval time of sending loop test packet

Result: This sets interval time of sending loop test packet.

Note: Loop test function send test packet in an interval time, and judging whether there is a self-loop by judging whether the packet is received in the interval time. Command is used to set the interval time, by second.

9. To display port loop test configuration and port detection status, use command **show loopdetect** in global config mode. This is shown in Table 445.

TABLE 445 SHOW LOOP DETECT COMMAND

Format	Mode	Function
show loopdetect	global config	This displays port loop test configuration and port detection status

Result: This displays port loop test configuration and port detection status.

Note: When the port cannot work normally, configure **show loopdetect** to observe whether a port loop exists. If no loop is detected and the spanning tree of the port is enabled, eliminate fault according to status of spanning status.

END OF STEPS

Result Single-Port loop test has been configured.

Virtual Circuit Test

VCT Function Virtual circuit test (VCT) uses time domain reflectometer (TDR) to diagnose circuit. This test enables to diagnose circuit error status, such as Open, Short, Impedance Mismatch and Good termination, and to obtain the distance of the error circuit with the fitted empirical formula.

Use **show vct port** command on switch to query the VCT result of the specified port.

For interface modules in extended slots, this switch only supports VCT of gigabit electrical interface. For other interface modules, VCT is not supported.

Common Troubleshooting

Hardware and Software Faults

By type, faults include software faults and hardware faults. Hardware faults, if accurately located, usually can be cleared by replacing the hardware. Software and configuration faults can be cleared through proper operations.

In troubleshooting, check whether the device configuration is correct, whether the cables are connected correctly and whether the required environment is satisfied according to the related description in the above sections.

Troubleshooting through Console Port

Purpose

This section describes the troubleshooting through console port.

Prerequisites

To troubleshoot through console port, meet the following requirements.

- Check the configuration cable.
- Check the serial port of the HyperTerminal
- Check console port of the switch.

Steps

For troubleshooting through console port, perform the following steps.

1. Use proper configuration cables. For the connections of configuration cables, see Console Cable.
2. Check the settings of serial port attributes of the HyperTerminal. The correct settings are shown in Table 446.

TABLE 446 SERIAL PORT ATTRIBUTE

Serial Port Attributes	Description
Bit/s (baud rate):	“9600
Date bit	“8”
Parity check	“none”
Stop bit	“1”
Data Stream control	“none”

3. Check whether serial port of HyperTerminal is normal, and replace configuration terminal.
4. Check whether the console port of switch is normal.

END OF STEPS

Result

This checks console port in detail.

Troubleshooting through Telnet

Purpose This section describes the troubleshooting through telnet.

Prerequisites To troubleshoot through telnet, meet the following requirements.

- Check PVID of the port is configured incorrectly.
- Check port is disabled.
- Check VLAN bound with the IP port is disabled.
- Check no valid IP address, subnet mask and default gateway is configured for the switch.
- Check IP address of the switch conflicts with the IP address of another device in the network.

Steps For troubleshooting through telnet, perform the following steps.

1. Modify the PVID of the port to be consistent with the related VLAN ID.
2. Enable the port.
3. Enable the VLAN bound with the IP port.
4. Configure a valid IP address, subnet mask and default gateway for the switch.
5. Modify the IP address of the switch or that of the other device to eliminate the IP address conflict.

END OF STEPS

Result This troubleshoots through Telnet connection.

Troubleshooting a Telnet connection with switch

Purpose This topic describes the remote terminal can access but cannot log in to the switch through Telnet, and system prompts the user that no password is configured.

Prerequisite The login password of the switch is set to null.

Steps For the troubleshooting o logging into switch through Telnet, perform the following steps.

1. Set a non-null login password.

END OF STEPS

Result This sets a non-null password of the switch.

Troubleshooting the browser

Purpose

This topic describes the troubleshooting of web management after opening the web browser.

Prerequisites

To troubleshoot web management, meet the following requirements.

- Browser version is too old to support it.
- Address and port number is written wrong in the browser address fence.
- There is a communication fault between the host and the equipment.
- Switch management port is not set, or the IP address is not set in a correct way.
- Web management function of the switch is not enabled.

Steps

For the troubleshooting of web management, perform the following steps.

1. Update the browser version. The version should be above 4. 0.
2. Examine the configuration of the host to get the right IP address and port number.
3. Examine the connection between the host and the equipment to make sure that the communication is normal.
4. Set the right management port . on the switch and the right IP address.
5. Enable web management function of the switch and set the port number.

END OF STEPS

Result

This troubleshoots web management.

Troubleshooting the Switch through Web

Purpose

This topic describes the troubleshooting of switch through web.

Prerequisite

User name and password set on the switch is different with the one input on the host.

Steps

For the troubleshooting of switch through web, perform the following step.

1. Examine the configuration of the switch, and input the right user name and password.

END OF STEPS

Result This troubleshoots the switch through web.

Troubleshooting the User Name/Password

Purpose This topic describes how to troublshoot the user name/password.

Prerequisite In logging in to the switch, the entered user name or password is incorrect.

Steps For troubleshooting of user name/password, perform the following steps.

1.Confirm whether system administrator can find original user name and password. If the user name and password cannot be found, restart the switch and delete the configuration file.

- Restart the switch, and press any key according to the prompt to enter the boot status in the HyperTerminal.

```
                      Welcome to use ZTE eCarrier!!



Copyright(c) 2004-2006,   ZTE Co.  ,  Ltd.
System Booting.  .  .  .  .  .
CPU: DB-88E6218
Version: VxWorks5.  5.  1
BSP version: 1.  2/6-b
Creation date: Aug  1 2006,  09:40:27



Press any key to stop auto-boot.  .  .
 7

[ZxR10 Boot]:
```

- In the boot status, enter <**zte**> to enter the [BootManager] status of the switch. Enter <?> to get command help.

```
[ZxR10 Boot]: zte

NOTE: Bootline not saved to NVRAM

boot device          : marfec
unit number          : 0
processor number     : 0
host name            : f129750
file name            : vxWorks
inet on ethernet (e) : 10.  40.  89.  206
host inet (h)        : 10.  40.  89.  204
gateway inet (g)     : 10.  40.  89.  204
user (u)             : 5124
ftp password (pw)    : 5124
flags (f)            : 0x0
other (o)            : MAC0-00:32:45:67:89:ab

Attached TCP/IP interface to marfec0.
Warning: no netmask specified.
Attaching network interface lo0.  .  .   done.
Attaching to TFFS.  .  .
test flash passed perfectly!
MarvellDx has been initialized !
Welcome to boot manager!
Type '?' for help

[BootManager]:
```

- Run **del** command to delete the configuration file, and then restart the switch.

```
[BootManager]:ls
KERNEL
RUNNING.  CFG
config.  txt
[BootManager]:del running.  cfg
[BootManager]:del config.  txt
[BootManager]:reboot
```

- After the switch is restarted, use the default user name and password to log in to the switch.

```
Please Press any Key to Start!

Welcome !
ZTE Corporation.
All rights reserved.

login:admin
password:*********
zte>en
password:
zte(cfg)#
```

Troubleshooting Password

Purpose This topic describes how to troubleshoot the enable password.

Steps To troubleshoot the enable password, perform the following step.

1. To trouble shoot to enable password is same as described in Troubleshooting the User Name/Password.

END OF STEPS

Result Password is enabled.

Troubleshooting a Device Connection

Purpose This topic describes how to troubleshoot the interconnection of two devices so that they can be connected to two switch ports in a same VLAN.

Prerequisites To troubleshoot the interconnection of two devices in the same VLAN, meet the following requirements.

- PVID of the port is configured incorrectly.
- Port is disabled.
- VLAN is disabled.
- IP address is not set on the equipment or IP address is not in same network segment.

Steps To troubleshoot the interconnection of two devices in the same VLAN, perform the following steps.

1. Modify the PVID of the port to be consistent with the related VLAN ID.
2. Enable all ports.

3. Enable the VLAN.
4. Add the port to the VLAN and select untag.
5. Set correct IP address on equipment.

END OF STEPS

Result Interconnect of two devices in same VLAN is configured.

Abbreviations

Acronyms and Abbreviations

Note: Acronyms and Abbreviations, used in this particular manual are related to IP product.

Abbreviation	Full Name
ABR	Area Border Router
ACL	Access Control List
AD	Administrative Distance
API	Application Programming Interface
ARP	Address Resolution Protocol
AS	Autonomous System
ASBR	Autonomous System Border Router
ASN	Abstract Syntax Notation
ATM	Asynchronous Transfer Mode
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 Service
COS	Class of Service
CRC	Cyclic Redundancy Check
CRLDP	Constraint based Routing Label Distribution Protocol
CSN	Cryptographic Sequence Number
CSU	Channel Service Unit
DDN	Digit Data Network
DHCP	Dynamic Host Configuration Protocol
DIS	Designate IS

Abbreviation	Full Name
DNS	Domain Name System
DR	Designate Router
DSU	Data Service Unit
EBGP	External Border Gateway Protocol
EGP	External Gateway Protocol
ES	End System
FDDI	Fiber Distributed Data Interface
GER	General Excellent Router
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
LAN	Local Area Network
LAPB	Link Access Procedure Balanced
LCP	Link Control Protocol
LDP	Label Distribution Protocol
LLC	Logical Link Control
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
MTU	Maximum Transmission Unit

Abbreviation	Full Name
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
NSAP	Network Service Access Point
NSP	Network Service Provider
NTP	Network Time Protocol
NVT	Network Virtual Terminal
OAM	Operation And Management
OID	Object ID
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PAP	Password Authentication Protocol
PAT	Port Address Translation
PCB	Process Control Block
PCM	Pulse Code Modulation
PDU	Protocol Data Unit
POS	Packet over SDH
PPP	Point-to-Point Protocol
PSNP	Partial Sequence Num PDU
PRT	Process Registry Table
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
RSVP	Resource Reservation Protocol
SDH	Synchronous Digital Hierarchy
SDLC	Synchronous Data Link Control
SMP	Security Main Processor
SMTP	Simple Mail Transfer Protocol

Abbreviation	Full Name
SNMP	Simple Network Management Protocol
SNP	Sequence Num PDU
SPF	Shortest Path First
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TOS	Type Of Service
TELNET	Telecommunication Network Protocol
TTL	Time To Live
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

This page is intentionally blank.

Tables

This Page is intentionally blank.

Index