



ZXR10 ZSR V2

Intelligent Integrated Multi-Service Router

Product Description

Version: 2.00.20

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

LEGAL INFORMATION

Copyright © 2014 ZTE CORPORATION.

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

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

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

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

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

Users may visit the ZTE technical support website <http://support.zte.com.cn> to inquire for related information.

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

Revision History

Revision No.	Revision Date	Revision Reason
R1.0	2015-03-30	First edition

Serial Number: SJ-20150204153047-003

Publishing Date: 2015-03-30 (R1.0)

Contents

About This Manual	I
Chapter 1 Product Location and Features	1-1
1.1 Product Location	1-1
1.2 Product Features.....	1-2
Chapter 2 Product Structure	2-1
2.1 Product Appearance.....	2-1
2.2 Hardware Structure	2-5
2.3 Software Structure.....	2-7
Chapter 3 Functions and Features	3-1
3.1 IPv4 Routing Protocols and IP Basic Services	3-1
3.1.1 Unicast Routing Protocols.....	3-1
3.1.2 Multicast Routing Protocol	3-3
3.1.3 Policy Route and Routing Policy.....	3-5
3.1.4 DHCP and DNS	3-6
3.2 WAN Access.....	3-6
3.3 Routing and Switching Integration	3-8
3.4 MPLS	3-9
3.5 VPN	3-10
3.5.1 IPsec and GRE.....	3-10
3.5.2 MPLS VPN	3-14
3.5.3 Smart Dial Control.....	3-15
3.6 QoS	3-16
3.7 Security Features	3-18
3.7.1 ACL.....	3-18
3.7.2 Anti-Attack.....	3-19
3.7.3 Firewall.....	3-19
3.7.4 Multiple Security Authentication Modes.....	3-23
3.7.5 uRPF.....	3-24
3.8 Network Reliability.....	3-24
3.9 IPv6 Features	3-26
3.9.1 IPv6 Basic Functions.....	3-26
3.9.2 IPv6 Unicast Routing Protocols	3-26
3.9.3 IPv6 Multicast Routing Protocols	3-27

3.9.4 IPv6 Tunnel Functions	3-28
3.9.5 6PE and 6VPE	3-30
3.9.6 NAT64	3-30
3.10 NAT	3-31
3.11 Network Management Features	3-31
3.12 System Operation and Maintenance	3-33
Chapter 4 Network Applications	4-1
4.1 Application Scenario of Access Networks of Enterprise Headquarters and Branches	4-1
4.2 Application Scenario of Egress Gateways in Enterprise Networks.....	4-2
4.3 Application Scenario of Convergence and Access Networks of Industry Networks.....	4-4
4.4 Application Scenario of Telecom Operators' DCN Networks	4-5
Chapter 5 Technical Indexes	5-1
Figures.....	I
Tables	III
Glossary	V

About This Manual

Purpose

This manual describes the product location and features, product structure, functions and applications, technical parameters of the ZXR10 ZSR V2 series routers.

Intended Audience

This manual is intended for:

- Network planning engineers
- Network maintenance engineers

What Is in This Manual

This manual contains the following chapters:

Chapter 1, Product Location and Features	Describes the location and highlights of the ZXR10 ZSR V2.
Chapter 2, Product Structure	Describes the appearance, hardware structure, and software structure of the ZXR10 ZSR V2.
Chapter 3, Functions and Features	Describes software features and major functions of the ZXR10 ZSR V2.
Chapter 4, Network Applications	Describes applications of the ZXR10 ZSR V2 in actual network architectures.
Chapter 5, Technical Indexes	Describes technical indexes of the ZXR10 ZSR V2.

Conventions

This manual uses the following conventions.

Italics	Variables in commands. It may also refer to other related manuals and documents.
Bold	Menus, menu options, function names, input fields, option button names, check boxes, drop-down lists, dialog box names, window names, parameters, and commands.
Constant width	Text that you type, program codes, filenames, directory names, and function names.
[]	Optional parameters.
{ }	Mandatory parameters.
	Separates individual parameters in a series of parameters.

	Warning: indicates a potentially hazardous situation. Failure to comply can result in serious injury, equipment damage, or interruption of major services.
	Caution: indicates a potentially hazardous situation. Failure to comply can result in moderate injury, equipment damage, or interruption of minor services.
	Note: provides additional information about a certain topic.

Chapter 1

Product Location and Features

Table of Contents

Product Location	1-1
Product Features	1-2

1.1 Product Location

The ZXR10 ZSR V2 series is an intelligent multi-service router integrating routing, switching, wireless, security, VPN, and broadband user access management functions. The ZXR10 ZSR V2 uses the modular and extensible system architecture, and can be used to establish intelligent, efficient, reliable, flexible, and networks with ease of maintenance. The ZXR10 ZSR V2 can be widely used in the following scenarios:

- Egress gateways of campus networks, government networks, and enterprise networks
- Access networks of enterprise headquarters and branches
- Mobile office networks
- Convergence network and access network of industry networks

The ZXR10 ZSR V2 series includes five types of products:

- ZXR10 3800-8
- ZXR10 2800-4
- ZXR10 1800-2S

Mounting a wireless function module to the ZXR10 1800-2S results in two sub-models: ZXR10 1800-2S(G) and ZXR10 1800-2S(W).

- ZXR10 1800-2E

Mounting a wireless function module to the ZXR10 1800-2E results in sub-model ZXR10 1800-2E(G).

- ZXR10 2800-3E

Mounting a wireless function module to the ZXR10 2800-3E results in sub-model ZXR10 2800-3E(G).

Figure 1-1 shows an external view of each product.

Figure 1-1 External Views of the ZXR10 ZSR V2 Series Products

1.2 Product Features

High Performance, Ensuring No Network Access Bottleneck

With increase of enterprise applications, network traffic increases. New applications such as video conferencing, distance learning, and remote disaster recovery have higher and higher requirements for performance on nodes processing network data.

The ZXR10 ZSR V2 provides high performance and ensures no network access bottleneck.

- The high-performance multi-core processor and intelligent switching engine guarantee high-performance protocol processing and management control processing, and implement high-speed L2 and L3 packet forwarding. This improves the overall performance of the system. Multi-layer distributed forwarding and processing ensures that the system resources can be allocated properly for multiple simultaneous services, which guarantees the high forwarding performance of the system. Each slot supports a maximum of 10 Gbps bus bandwidth, ensuring smooth service packet forwarding.
- The ZXR10 ZSR V2 supports various types of interfaces, including wired interfaces such as the GE interface, FE interface, POS interface, CPOS interface, E1 interface, xDSL interface, synchronous serial interface and asynchronous interface, and wireless interfaces such as the 3G/LTE interface and Wi-Fi interface. FE interfaces are integrated on the MPUs, and these interfaces can be used as WAN interfaces or LAN interfaces. This provides the flexible access capability and improves the price/performance ratio.
- The ZXR10 ZSR V2 uses a high-availability design. The AC power and DC power are used for redundancy. The power supply modules, fan modules, and service boards support hot swapping. The system software uses the modular design and new functions can be added, which improves stability and flexibility of the system. The ZXR10 ZSR V2 supports availability technologies such as OAM detection, BFD for everything, FRR, VRRP, and link aggregation.

- The ZXR10 ZSR V2 provides the control-plane security function. The ZXR10 ZSR V2 classifies control-plane packets, and performs multi-level rate limit and scheduling. The traffic suppression, protocol white list, protocol authentication functions can be set. The ZXR10 ZSR V2 supports anti-DDOS attacks, anti-ARP attacks, and attack-source tracing, which guarantees equipment security to the maximum extent.
- The ZXR10 ZSR V2 provides the ACL function and supports a L2 and L3 hybrid ACL processing algorithm. The efficient ACL processing capability and user-friendly ACL log statistics management function help to perform elaborate service management.
- The ZXR10 ZSR V2 uses a refined design. The ZXR10 1800-2S uses a desktop design, so it is small and flexible. The ZXR10 2800-4 and 3800-8 use a front-outlet design, so that maintenance and operations can be performed at one side of each device. The ZXR10 2800-4 and 3800-8 can be installed in cabinets whose depth is 300 mm to save space of equipment rooms. The ZXR10 2800-4 and 3800-8 also can be installed in narrow space such as outdoor cabinets, vehicle-mounted cabinets, base stations, and office cabinets to reduce operation and maintenance costs. The ZXR10 2800-2E and ZXR10 3800-3E can be installed in a cabinet 600 mm deep. They can also be installed in outdoor cabinets, vehicles, base stations, and device cabinets in offices, so the O&M cost is relatively low.

Wired and Wireless Access, Anytime and Anywhere

Compared with a conventional network, a wireless network has larger coverage. It extends the network access range, and can provide supplementary for a wired network. Mobile office work can be performed through wireless networks, which removes the time-space bottleneck. Operating as a 4G router, the ZXR10 ZSR V2 guarantees network reliability, and improves the network bandwidth value. The ZXR10 ZSR V2 provides the following functions:

- Supports 3G (including WCDMA, and TD-SCDMA) and LTE (including TDD and FDD) formats.
- Provides built-in wireless modules, plug and play USB cards and special interface cards to meet requirements of different network structures.
- Provides an extension feeder to solve the signal coverage problem when the device is located in a equipment room corner or office corner where the wireless signal is weak.
- Aware of 3G/LTE signal strength and detects link quality in real time to guarantee the customer SLA.
- Provides the Smart Dial-up Control and 24-hour backup functions. The xDSL or 3G/LTE standby link can be connected based on policies to protect services or perform load sharing. This improves viability of networks and reliability of services.
- Uses the multi-link load sharing technology, monitors interconnected links of different carriers, and performs intelligent routing for data flows sent to the Internet. This ensures that users can access the Internet through optimal links.
- Supports establishing VPN channels in 3G/LTE networks, which improves security of wireless links.
- Supports Wi-Fi access and 802.11b/g/n radio frequency mode adjustment, so that the access rate can be dynamically adjusted in accordance with the environment.

- Supports the guard interval to avoid data interference.
- Supports Wi-Fi multimedia and provides wireless QoS, which guarantees quality of applications such as the voice and video services.
- Supports different authentication modes, including none, WEP, WPA, WPA2 (TKIP and AES-CCMP), and WAPI hard encryption.

Multiple Functions, Reducing Costs

The ZXR10 ZSR V2 provides different functions to meet requirements of different network structures.

- Provides the router, switch, firewall, AP, NAT gateway, and VPN gateway functions. The functions can be loaded as needed, which provides a flexible platform to implement optimal service deployment.
- Supports the GRE, IPSec, and MPLS VPN over GRE functions to meet requirements of VPN applications in different network structures.
- Supports MPLS, provides L2 and L3 MPLS VPN solutions, and supports the PWE3 circuit simulation technology to bear TDM traffic.
- Supports stateless firewall and controls incoming and outgoing traffic, which guarantees network security.
- Supports hardware-based QoS and H-QoS, and provides different SLAs for different users and services, which meets requirements of elaborate control.

Flexible Extension and Smooth Upgrade

The ZXR10 ZSR V2 provides different available forwarding engines with different performance, and upgrade can be performed smoothly. This reduces users' costs and meets future network requirements.

- Management and Packet Forwarding Units (MPFUs) with different forwarding performance are provided for the ZXR10 2800 and ZXR10 3800. The cards can be used as needed. This reduces the network construction costs, and solves problems caused by future performance upgrade.
- The ZXR10 1800-2E and ZXR10 2800-3E feature different transferring performance. Users can select products as required to reduce network-construction cost.
- The ZXR10 ZSR V2 supports the IPv4 and IPv6 stacks, so IPv4 and IPv6 access can be provided at the same time.
- The ZXR10 ZSR V2 supports 6in4, 6to4 and 6in4 tunnels to transmit data between the IPv4 network and IPv6 network. The ZXR10 ZSR V2 also supports NAT444, NAT64 and 6RD for smooth evolution from IPv4 to IPv6.

Ease of Commissioning and Maintenance, Supporting Fast Network Deployment

The ZXR10 ZSR V2 provides a visual commissioning and maintenance method that supports convenient and fast operations, remote maintenance, and any-time diagnosis.

- The ZXR10 ZSR V2 supports USB commissioning, automatic configuration, and in-batch version upgrade through NMS. In this way, zero-touch automatic configuration, in-batch deployment, and ease of maintenance can be performed.

- The ZXR10 ZSR V2 supports SQA to perform real-time network quality detection and location through ICMP-echo, UDP, TCP, FTP, DNS, HTTP and SNMP. SQA can be used together with VRRP, static routes, interface backup, link backup, policy routes and the ZXNPA to provide alarms of different levels based on automatic network performance thresholds, and perform graphic detection and management.
- The ZXR10 ZSR V2 supports port mirroring and Netflow 1:1 sampling, so that traffic can be displayed with explicit features. This provides an effective monitoring method for accurate network control and operation.
- The ZXR10 ZSR V2 supports WEB GUI network management and the Netnumen to implement visual service deployment and maintenance. The ZXR10 ZSR V2 provides a tool for one-click service creation and one-click information collection, which helps network administrators to perform quick service provisioning and high-efficiency maintenance.

Green Energy Saving

The ZXR10 ZSR V2 complies with the green and environmental protection idea in design, research and development, manufacturing, logistics, and projects, and helps users to construct low-noise, low-energy, and high-efficiency communication networks.

- The ZXR10 ZSR V2 uses advanced 28 nm chips, so performance is improved and energy consumption is reduced.
- The ZXR10 ZSR V2 uses a excelsior hardware structure design and advanced submarine-level muting technology.
- The intelligent fan system automatically adjusts the fan speed in accordance with system operation, which reduces energy consumption and device noise.
- The boards and cards supports the sleep function, which complies with the EEE standard. Idle and low-speed ports reduce energy consumption by 2/3, and reduce carbon dioxide emissions.
- The ZXR10 ZSR V2 uses nonleaded green materials, and the manufacturing process strictly complies with the RoHS standard.

This page intentionally left blank.

Chapter 2

Product Structure

Table of Contents

Product Appearance.....	2-1
Hardware Structure	2-5
Software Structure.....	2-7

2.1 Product Appearance

Overview

Designed on a modular structure, with hot-pluggable boards and parts, the ZXR10 ZSR V2 provides flexible extensibility. The entire set consists of a subrack, a backplane, a main-control forwarding board, a line interface board, a power module, and a fan subrack.

ZXR10 3800-8 Product Appearance

For the main components of the ZXR10 3800-8 chassis, see [Figure 2-1](#).

Figure 2-1 Main Components on the Front Side of the ZXR10 3800-8 chassis



For the front view of the ZXR10 3800-8 chassis, see [Figure 2-2](#).

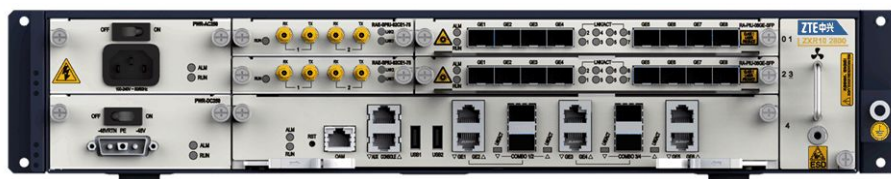
Figure 2-2 Front View of the ZXR10 3800-8 chassis

ZXR10 2800-4 Appearance

For the main components of the ZXR10 2800-4 chassis, see [Figure 2-3](#).

Figure 2-3 Main Components on the Front Side of the ZXR10 2800-4 chassis

For the front view of the ZXR10 2800-4 chassis, see [Figure 2-4](#).

Figure 2-4 Front View of the ZXR10 2800-4 chassis

ZXR10 1800-2S Appearance

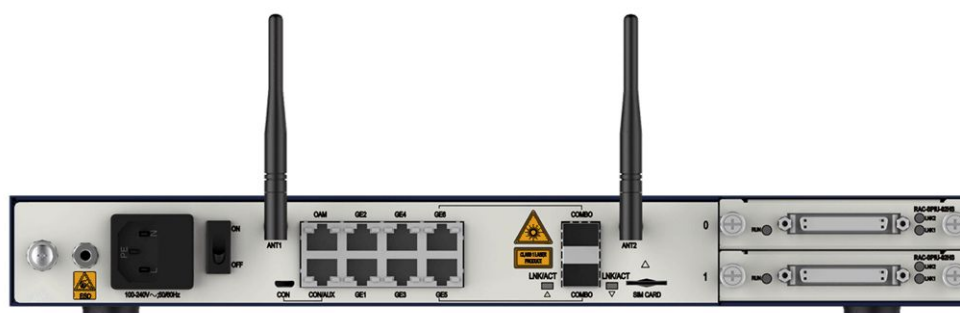
For the main components of the ZXR10 1800-2S chassis, see [Figure 2-5](#).

Figure 2-5 Main Components on the Front Side of the ZXR10 1800-2S chassis

For the front view of the ZXR10 1800-2S chassis, see [Figure 2-6](#).

Figure 2-6 Main Components on the Front Side of the ZXR10 1800-2S chassis

For the back view of the ZXR10 1800-2S chassis, see [Figure 2-7](#).

Figure 2-7 Main Components on the Back Side of the ZXR10 1800-2S chassis**Note:**

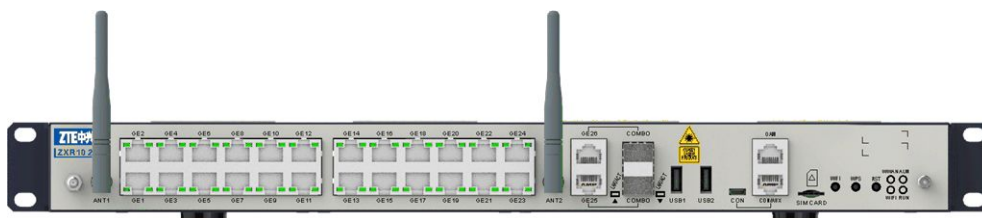
Both the ZXR10 1800-2S(G) and the ZXR10 1800-2S(W) support the wireless function. Each of them is configured with a wireless module and a pair of antennas. If no wireless module is configured, the chassis has no antenna.

ZXR10 2800-3E Appearance

For the appearance of the ZXR10 2800-3E chassis, see [Figure 2-8](#).

Figure 2-8 ZXR10 2800-3E Appearance

For the front view of the ZXR10 2800-3E chassis, see [Figure 2-9](#).

Figure 2-9 ZXR10 2800-3E Front View**NOTE****Note:**

The sub-model ZXR10 2800-3E(G) is embedded with a wireless module and supports the wireless communication function. Two antennas are installed. When the wireless module is removed, there is no antenna on the chassis.

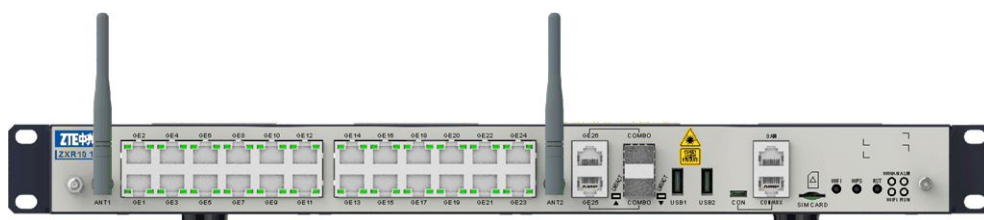
For the back view of the ZXR10 2800-3E chassis, see [Figure 2-10](#).

Figure 2-10 ZXR10 2800-3E Back View**ZXR10 1800-2E Appearance**

For the appearance of the ZXR10 1800-2E chassis, see [Figure 2-11](#).

Figure 2-11 ZXR10 1800-2E Appearance

For the front view of the ZXR10 1800-2E chassis, see [Figure 2-12](#).

Figure 2-12 ZXR10 1800-2E Front View**Note:**

The sub-model ZXR10 1800-2E(G) is embedded with a wireless module and supports the wireless communication function. Two antennas are installed. When the wireless module is removed, there is no antenna on the chassis.

For the back view of the ZXR10 1800-2E chassis, see [Figure 2-13](#).

Figure 2-13 ZXR10 1800-2E Back View

2.2 Hardware Structure

Overview

The hardware system of the ZXR10 ZSR V2 consists of functional units such as the MPFU, line interface card, high-speed backplane, power supply module, and fan module. These functional units are interconnected through high-speed serial buses and Ethernet buses.

Overall Hardware System Structure

In the hardware system structure of the ZXR10 ZSR V2, the forwarding plane and control plane are separated.

- The MPFU is the system core, and it communicates with other units through the backplane.
- The engine of the MPFU is a multi-core CPU. The cores are divided into forwarding cores and control cores. The forwarding cores and other system units form a forwarding logical plane that forwards packets and processes services. The control cores and other system units form a control logical plane that performs routing protocol interaction, routing calculation, system management, and control message synchronization.
- The forwarding plane and control plane are separated, so the impacts to each other caused by extension of the functions and performance in the two planes are reduced to the minimum extent. This guarantees high flexibility of the system.

The power supply and fan systems of the ZXR10 ZSR V2 uses the modular design. Power supply modules and fan modules are installed to sub-racks and connected to the high-speed backplane, which achieves the non-cable design. The ZXR10 2800-4 and ZXR10 3800-8 supports AC and DC power supply modules for redundancy. The ZXR10 1800-2S supports only one AC power supply module or one DC power supply module.

Operational Principle of the Hardware System

The forwarding plane and control plane of the ZXR10 ZSR V2 are separated. After packets are processed by the physical-layer chip of a line interface card and frame resolution is performed,

- For a common service flow, the packets are forwarded to the MPFU. The traffic management module and data forwarding module in the MPFU send the packets to the interface on the destination line interface card.
- For protocol packets or control packets, the packets are converged in the gigabit Ethernet switching module. The management and control module in the MPFU interacts with the processing unit on a line interface card to process the packets.

MPFUs and Line Interface Cards

The MPFU is the control node of the ZXR10 ZSR V2. The MPFU forwards packets, and manages and maintains the entire device. The MPFU consists of the packet forwarding module, management and control module, clock processing module, and alarm monitoring module. It forwards packets, and manages the system clock source, control plane, system maintenance plane and environmental monitoring plane.

ZXR10 2800-4 and ZXR10 3800-8 provide three types of MPFUs: MPFU-A, MPFU-B, and MPFU-C that provide different forwarding performance respectively. The MPFUs use the modular design, support hot swapping, and support forwarding plane and control plane separation.

The MPFUs of the ZXR10 1800-2S, ZXR10 1800-2E, and ZXR10 2800-3E are fixed in the chassis, so it does not support hot swapping, but it supports forwarding plane and control plane separation.

The ZXR10 ZSR V2 provides different line interface cards and supports different interface rates and different numbers of ports, which meets requirements of different networks and services.

For a description of MPFUs and line interface cards, refer to the “Hardware Description” of the ZXR10 ZSR V2.

Power Supply Modules

The ZXR10 ZSR V2 supports AC power supply (100 V to 240 V, and 50 Hz to 60Hz) and DC power supply (-72 V to -38 V). The ZXR10 1800-2S supports only one AC power supply module or one DC power supply module. The power supply module is fixed in the device box and cannot be removed or installed. The ZXR10 2800-4, ZXR10 3800-8, ZXR10 1800-2E and ZXR10 2800-3E support DC and AC power supply modules for redundancy, and the power supply modules can be removed and installed.

Fan Modules

There is a vertical fan module on the ZXR10 ZSR V2. The ZXR10 ZSR V2 can automatically adjust the fan speed in accordance with the system operation, and supports the fan state monitoring and alarm functions. The ZXR10 ZSR V2 uses down draught heat dissipation. Cold air enters the device from one side, passes by the boards and power supply modules, and leaves the device from the other side.

2.3 Software Structure

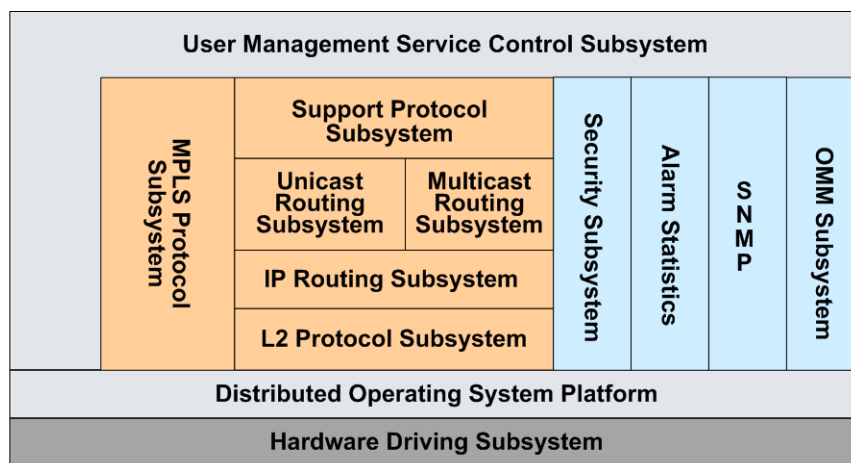
Overview

The software system of the ZXR10 ZSR V2 is based on the software platform with proprietary intellectual property rights, which can satisfy various network requirements in high-performance and complex commercial service environments. The software platform owns a wide set of network features established on international standards.

Overall Structure

For the overall software structure, see [Figure 2-14](#).

Figure 2-14 ZXR10 ZSR V2 Overall Software Structure



The major functions of each subsystem in the ZXR10 ZSR V2 software structure are described as follows:

- **Hardware driving subsystem:** provides software driving for the main-control forwarding board, the line interface board, the backplane, the fan, and the power module.
- **The distributed operating system platform:** provides the real-time operating platform. As the kernel of the ZXR10 ZSR V2 software system structure, it manages the hardware system structure of the entire system and provides a unified operating platform for application programs on the entire software system. It features high reliability, real-time, self-recovery, maintainability, and encapsulation features.
- **L2 protocol subsystem:** provides the driving program of the switching chip, L2 link control, and management protocols. It also provides support for L3 protocols.
- **IP route subsystem:** As the kernel of the router software system structure, it runs IPv4 and IPv6 routing protocols such as Routing Information Protocol (RIP), OSPF, BGP, and the multicast routing protocol. This system is in charge of receiving and storing routing information in the router, establishing the global routing table, selecting, forwarding, and exchanging routes, and maintaining the route table.
- **Unicast routing protocol subsystem:** collects the network topology information by exchanging information with other routers in the network, forms an IP unicast routing table, and notifies the routing table to the IP forwarding plane to forward unicast IP packets.
- **Multicast routing protocol subsystem:** forms a multicast forwarding routing table for the bottom layer to forward multicast data packets.
- **Support protocol subsystem:** completes IP data processing, ICMP protocol processing, Address Resolution Protocol (ARP) processing, Transfer Control Protocol (TCP) processing, User Datagram Protocol (UDP) processing, Telnet guarding process and client program processing, File Transfer Protocol (FTP) and Trivial File Transfer Protocol (TFTP) processing in the router. The support subsystem provides services for the routing subsystem and the management subsystem.

- MPLS protocol subsystem: provides LDP, RSVP with Traffic Engineering extensions (RSVP-TE), L2/L3 VPN, and provides basic MPLS functions and label forwarding services.
- Security subsystem: provides multiple security protection functions on the equipment. It provides functions such as packet filtering, encryption password, authentication, modification of configuration request licenses, several VPN technologies, Network Address Translation (NAT), Message Digest 5 Algorithm (MD5), user authentication, and statistics to completely satisfy equipment guaranty and user requirements for secure applications.
- Alarm statistical subsystem: maintains the configuration for various statistical alarms, saves various statistics, and provides a query interface.
- SNMP subsystem: provides functions of the SNMP Agent, and supports all protocol operations for the SNMP Agent specified in SNMP V1/V2/V3.
- Network management subsystem: provides network configuration management, fault management, performance management, and security management functions for the equipment, and completes the management for services, versions, configuration files, and various logs in the file system of the equipment.
- User management service control subsystem: completes user access and management functions, include user service configuration, and Authentication, Authorization and Accounting (AAA) functions, PPP user management, IP user management, VPLS service control, and multicast user management.
- System management: provides file management, equipment management (for the power module and the fan module), monitoring maintenance, and diagnosis debugging functions to ensure the stable operational state of the equipment.

Software Features

The software system of the ZXR10 ZSR V2 uses the software platform, which is a multi-task distributed real-time network operating system that provides unified IP protocol support for all equipment of ZTE. The software system platform provides a mature and stable structure, which is provided based on service requirements. Considering the operation and maintenance cost, service expansibility, and application requirements, the software system platform provides the following features:

- Fine encapsulation
 - Supports several operating systems and supports the smooth upgrade of the operating system.
 - Supports a uniform configuration style for all ZTE products to facilitate user operation and maintenance.
- Powerful monitoring function
 - Monitors exceptions with processes and the memory.
 - Monitors the operational state or abnormal state of the power module, the rotation speed or ineffectiveness of the fan module, the voltage, the current, and the environment temperature.

- Provides rapid troubleshooting functions to ensure high stability of product versions.
- Flexible modular component structure
 - Software functions based on the software platform can be easily extended or removed, and new functions can be quickly developed upon the original structure.
 - Software functions can be flexibly customized as required to rapidly respond to user requirements.
- Extension of new carrier-class Ethernet services based on the uniform platform
 - Supports L2 and L3 VPN mechanism, supports Hierarchy of VPLS ([H-VPLS](#)) to satisfy the requirement of layered service deployment, and supports multicast functions inside the VPN. The ZXROSng platform can also provide rapid VPN deployment through the unified network management system, and can rapidly deploy multicast services such as user video and IPTV.
 - Provides a complete QoS mechanism by supporting traffic classification, traffic labeling, traffic speed-limit, traffic shaping, congestion management, and congestion avoidance mechanisms.
 - Supports IPv4/IPv6 dual protocol stacks. The ZXROSng platform supports the IPv4/IPv6 transition mechanism in various application scenarios, such as manual general tunnels, automatic 6To4 tunnels, and 6PE.
- Optimal mutual operability, in compliance with mainstream protocols and standards

Chapter 3

Functions and Features

Table of Contents

IPv4 Routing Protocols and IP Basic Services	3-1
WAN Access	3-6
Routing and Switching Integration	3-8
MPLS	3-9
VPN	3-10
QoS	3-16
Security Features	3-18
Network Reliability	3-24
IPv6 Features	3-26
NAT	3-31
Network Management Features	3-31
System Operation and Maintenance	3-33

3.1 IPv4 Routing Protocols and IP Basic Services

3.1.1 Unicast Routing Protocols

Overview

The ZXR10 ZSR V2 series products fully supports various IPv4 unicast routing protocols, including the static route, the RIP, the OSPF, the IS-IS, and the BGP.

Static Route

The static route is manually configured by the administrator to simplify the network configuration and improve the network performance. It is normally used in a scenario with a relatively simple network structure. When a fault occurs in the network or the network topology is changed, the static route is not changed automatically and needs to be manually modified by the administrator.

The ZXR10 ZSR V2 series products supports the configuration of a static route based on the next hop or on the egress. It also supports the association between static routes and VRF instances.

RIP

The RIP is a dynamic routing protocol for the distance vector based on the UDP. It periodically broadcasts the routing table to its neighbors, maintains the relationship

between routers, and calculates its routing table in accordance with received routes. The RIP is simple in operation and is applicable to small-scale networks.

The ZXR10 ZSR V2 series products supports the following RIP functions:

- Basic functions of the RIP v1/v2, such as horizontal splitting, poisonous reversion, interface authentication, route summary, and redistribution of various routing protocols.
- Load sharing of the RIP.
- VPN access function of the RIP.
- The RIP Management Information Base (MIB) function.

OSPF

The OSPF routing protocol is an Interior Gateway Protocol (IGP) based on link state, which exchanges routing information between routes inside the same Autonomous System (AS). The OSPF is one of the widely applied IPv4 IGP routing protocols.

The ZXR10 ZSR V2 series products supports the following OSPF functions:

- Basic OSPF functions, including basic protocol functions, neighbor authentication, virtual link, STUB, Not-So-Stubby Area (NSSA), type-3 Link State Advertisement (LSA) aggregation, type-5 LSA aggregation, and redistribution of other routing protocols
- Load sharing of OSPF routes
- VPN access and advanced functions, including sham-link
- OSPF-TE
- OSPF BFD
- OSPF FRR
- OSPF MIB

IS-IS

The IS-IS routing protocol is made by the International Organization for Standardization (ISO) to support the ConnectionLess Network Service (CLNS). As an extension of the IS-IS, the IETF supports to bear the IP routing information. The IS-IS is also an IGP based on the link state. The IS-IS is one of the most widely applied IPv4 IGP routing protocols.

The ZXR10 ZSR V2 series products supports the following IS-IS functions:

- Basic functions of the IS-IS protocol
- Extended functions of the IS-IS protocol, such as Hostname, Overload-bit
- Load sharing of IS-IS routes
- VPN access of the IS-IS
- IS-IS-TE
- IS-IS BFD
- IS-IS FRR
- IS-IS MIB

BGP

The BGP is an inter-domain routing protocol between ASs, used to exchange the network availability information between ASs running the BGP protocol.

The ZXR10 ZSR V2 series products supports the following BGP functions:

- Basic functions of the BGP protocol, and enhanced functions such as session authentication, route oscillation suppression, route reflector, alliance, extended community attribute, route aggregation, and route filtering
- Load sharing of BGP routes
- MP-BGP function, supporting AFI types such as IPv4 unicast, IPv4 multicast, IPv4 labeled-unicast, IPv4 mdt, IPv6 unicast, IPv6 multicast, IPv6 labeled-unicast, and VPNv4
- BGP BFD
- BGP FRR
- BGP MIB

3.1.2 Multicast Routing Protocol

Overview

Multicast is a point-to-multipoint or multipoint-to-multipoint communication mode, in which several receivers receive the same information from one source at the same time. Multicast-based applications include video conference, remote learning, and software distribution.

IGMP

Through the Internet Group Management Protocol (IGMP), the host notifies the multicast router on its network of the group that it joins or leaves. This means that, the multicast router knows whether is any multicast group member on the network and determines whether to forward multicast data packets to this network. When a multicast router receives a multicast data packet, it checks the multicast destination address in this data packet and forwards data packets to interfaces or downstream routers of members in this group.

The ZXR10 ZSR V2 supports IGMPv1, IGMPv2, and IGMPv3 protocols.

PIM-SM

The PIM-SM is applicable to the following situations:

- Group members are scattered in a wide range.
- Network bandwidth resources are limited.

The PIM-SM does not depend on a specific unicast routing protocol.

PIM-SM assumes that all routers on a sharing network section do not need to send broadcast packets and a router can send or receive multicast packets only after it initially requests to join a multicast group.

Through setting the Rendezvous Point (RP), the PIM-SM notifies the multicast information to all routers supporting the PIM-SM. In the PIM-SM, the router explicitly joins or quits a multicast group, so the network width occupied by data packets and control packets is reduced.

PIM-DM

The PIM-DM is a multicast routing protocol in dense mode, which transmits multicast data in the "push" mode. It is applicable to small-scale networks where broadcast group members are relatively dense.

PIM-SSM

The Protocol Independent Multicast-Source-Specific Multicast (PIM-SSM) features all advantages of the PIM-SM protocol, except that it does not create the sharing tree but creates the shortest-path tree based on sources. The PIM-SSM directly creates the shortest-path tree when it receives a membership report message from a specific source to the group.

As a subset of the PIM-SM, the PIM-SSM is applicable to the well known source. The PIM-SSM is valid both inside a domain and between domains. The PIM-SM needs to use the MSDP protocol for inter-domain multicast routing, while the PIM-SSM does not need to.

Static Multicast

The multicast static route is used in the scenario that multicast packets need to be forwarded in accordance with the specified path instead of the optimal path of the unicast route.

The static multicast provides the egress and ingress of users to configure the multicast routing table directly, and forms a multicast forwarding table in accordance with this configuration. If both the static multicast route and the dynamic multicast route exist, the static multicast route is preferential. The logical position of the static multicast is equivalent in the PIM-SM and the PIM-DM, so it can be understood as a special multicast routing protocol. In accordance with the specific application environments, the multicast static route performs the following functions:

- Modifies the Reverse Path Forwarding (RPF) route. In general, the network topology structure and the transmission of the multicast are the same as those of the unicast. The user can configure the multicast static route to change the RPF route, and create a transmission path different from the unicast for the multicast data.
- Connects the RPF route: When the unicast route in the network is changed, the multicast data cannot be forwarded because there is no RPF route. The user can configure the multicast static route to create an RPF route, and create multicast routing entries to guide the forwarding of multicast data.

MSDP

The MSDP is a mechanism connecting several PIM domains. It operates above the TCP protocol to provide the PIM-SM with the information of multicast sources outside the PIM domain.

The MSDP speaker inside a PIM-SM domain uses the TCP connection to create the MSDP neighbor session relationship with MSDP neighbors in other domains. When the MSDP speaker knows about a new multicast source inside the local domain (through the PIM registration mechanism), the MSDP creates a Source Active (SA) message and sends this message to all MSDP neighbors.

3.1.3 Policy Route and Routing Policy

Policy Route

The ZXR10 ZSR V2 supports policy routes to forward data packets in accordance with specified policies.

The policy route provides a packet forwarding policy, in which the packets should be matched and matching items are filtered in accordance with feature fields in these packets. Operations are set for these objects, including two types:

- Route options, used to modify the forwarding path
- Packet modification option, used to modify features of filtered packets

The policy route provides traffic engineering to some extent, so that traffic with different QoS or data with different natures (such as voice and FTP) run on different paths.

Routing Policy

The routing policy is a policy used to release and receive routes. Based on the routing protocol, the routing policy changes route generation, release, or selection results by changing some parameters or setting a particular control mode in accordance with a particular rule.

The ZXR10 ZSR V2 supports the routing policy on the following routes: RIP, OSPF, IS-IS, BGP, and VRF.

- During the release of control routes, the routing policy only releases routes satisfying the set conditions.
- During the receiving of control routes, the routing policy only receives necessary and valid routes, which controls the capacity of the routing table and improves the network security.
- The routing policy filters and controls introduced routes.
- When a routing policy introduces the routing information discovered by other routing protocols, the routing policy only introduces the routing information that satisfies the set conditions, and it also sets attributes of the introduced routing information to make it satisfy this protocol.
- The routing policy sets the corresponding attributes of routes used to filter traffic.

3.1.4 DHCP and DNS

DHCP

The Dynamic Host Configuration Protocol (DHCP) technology performs centralized dynamic management and configuration for users. Based on the client/server communication mode, the client proposes a configuration request (parameters such as IP address, subnet mask, and default gateway) to the server and the server returns the corresponding configuration information in accordance with the policy.

DHCP uses UDP as the transport protocol. A host sends messages to Port 67 of a DHCP server, and the server returns a message to Port 68 of the host.

The ZXR10 ZSR V2 supports DHCP client, DHCP relay, and DHCP server functions to support DHCP requirements under different scenarios.

DNS

The DNS is a distributed database for TCP/IP application programs, which is used to make conversion between domain names and IP addresses. With the DNS, the user can directly use the meaningful domain names that are easy to remember, and the DNS server in the network resolves them into the correct IP addresses.

As a DNS client, the ZXR10 ZSR V2 sends DNS resolution request to the DNS server, receives response packets from the DNS server, and sends them to users.

3.2 WAN Access

PPP

The PPP is a widely used Wide Area Network (WAN) protocol that provides the router-to-router and host-to-network point-to-point connection across synchronous and asynchronous circuits. The PPP provides an entire set of plans to solve problems during link establishment, maintenance, disconnection, upper-layer protocol negotiation, and authentication.

The PPP includes the Link Control Protocol (LCP) and the Network Control Protocol (NCP). It negotiates link negotiation and link maintenance on the point-to-point interface (such as E1/T1/POS), and provides the upper layer with a packet encapsulation format different from the Ethernet protocol.

For upper-layer protocol packets (such as IP packets and MPLS packets), the PPP only encapsulates a 2-byte protocol field before the packet and adds a PPP header with two fixed values, meaning 0xFF03. This PPP header can be compressed in accordance with the negotiation as needed.

The PPP negotiation is divided into the LCP, authentication (optional), and NCP phases. For the last two phases,

1. The authentication phase is selected as needed. It is normally used to authenticate access users on a router equipment.
2. NCP control protocols include the IP Control Protocol (IPCP), IPv6CP, MPLSCP, OSINLCP, and the BCP. The IPCP (supporting the IPv4) must be negotiated, while other NCP protocols can be selected as needed. After successful IPCP negotiation, the protocol is up on the PPP port.

Compared with Ethernet encapsulation, the PPP has the following features:

- The bandwidth usage of the PPP is higher, which is more apparent for short packets. Additionally, the encapsulation of PPP packet headers is simpler, and the packet transceiving mechanism also removes the complicated MAC header encapsulation and de-capsulation of Ethernet encapsulation.
- However, the protocol status machine of the PPP is more complicated than that of Ethernet encapsulation. The PPP interface sets the protocol to up only after successful negotiation, and then the upper layer can send and receive service packets.

For the PPP interface, the protocol status is down by default when it is created. The port is up only after the PPP link is negotiated successfully. Both parties periodically send LCP keep-alive packets. If no ECHO response is received for N ($N \geq 1$) keep-alive requests continuously, both the link and the protocol status are set to down, which trigger recalculation and route update operations.

ML-PPP

The ML-PPP is a technology that binds several PPP links to increase the bandwidth. It can be applied on interfaces supporting the PPP.

HDLC

The High-level Data Link Control (HDLC) is a bit-orientated link-layer protocol. Parallel to layer-2 protocols such as the PPP and frame relay, the HDLC provides services with different requirements for upper-layer protocols.

The prominent feature of the HDLC is that the data does not need to be a character set. The HDLC can provide apparent transmission for any bit stream.

FR

The Frame Relay (FR) is a high-performance WAN protocol that runs on the physical layer and the data link layer in the Open System Interconnection (OSI) reference model. The FR is a data packet exchange technology. As a simplified form of the X.25, it saves some complicated functions of the X.25 (such as the window technology and the data retransmission technology) and provides the error-correction function with higher-layer protocols. Compared with the X.25, the FR operates on better X.25 equipment, which provides higher reliability. The FR strictly corresponds to the bottom two layers in the OSI reference model, and provides better performance and higher transmission efficiency than the X.25.

The FR WAN equipment normally includes the Data Terminal Equipment (DTE) and the Data Circuit Terminal Equipment (DCE), which are located on both ends of the FR. The router is normally used as the DTE.

The FR provides connection-orientated communication on the data link layer. A defined communication link exists between each pair of equipment, which has a Data Link Connection Identifier (DLCI). Services are provided through the FR Permanent Virtual Circuit (PVC) that is identified by the DLCI. The value of the DLCI is normally specified by the FR service provider. The DLCI range that is available to users is 16 to 1007, while other DLCIs are reserved for the protocol.

The FR supports both the PVC and the Switching Virtual Circuit (SVC). At present, the PVC mode is mostly used in the FR. The PVC is a manual mode of configuring virtual circuits, it is simple, highly efficient, and multiplexed.

3.3 Routing and Switching Integration

Overview

To meet intranet requirements, the ZXR10 ZSR V2 provides high-density Ethernet switching modules, which achieves seamless integration of routers and switches.

The ZXR10 ZSR V2 supports the VLAN, SuperVLAN, QinQ, SmartGroup functions. It supports L2/L3 mode switching on Ethernet ports to achieve inter-board L2 switching. L2 and L3 configuration can be completed on the same interface. The ZXR10 ZSR V2 supports L2 functions such as STP and broadcast storm suppression.

Broadcast Storm Suppression

If broadcast frames are endlessly forwarded in a network and the number of broadcast frames increases rapidly, communication in the network is affected. This means that a broadcast storm is generated, which degrades network performance. Through the broadcast storm suppression function, a threshold for broadcast frames received on a port can be set. When the number of broadcast frames exceeds the threshold, the extra frames are dropped. This prevents a broadcast storm, and guarantees network operation.

The ZXR10 ZSR V2 supports the following storm suppression:

- Broadcast packet suppression
- Multicast packet suppression
- Unknown-packet suppression
- Rate limit in two modes: bps and pps

STP

In a L2 switching network, once there is a loop, packets are cycled in the loop and the number of packets increases. This causes a broadcast storm, and all available bandwidth is occupied. As a result, the network is unavailable. STP is a L2 management protocol.

It selectively blocks a redundant link to remove a loop in a network and provides the link backup function.

The same as other protocols, STP is updated based on network development. At first, IEEE 802.1D-1998 STP is widely used. Based on STP, IEEE 802.1w RSTP and IEEE 802.1s MSTP are developed.

The ZXR10 ZSR V2 supports STP, RSTP, MSTP, and transparent transmission over these protocols.

3.4 MPLS

LDP

The MPLS is a multi-layer switching technology that combines layer-2 switching technologies and layer-3 switching technologies. Using labels as the mode of aggregating the forwarding information, the MPLS runs under the routing hierarchy, supports several upper-layer protocols, and can be provided on several physical platforms.

The ZXR10 ZSR V2 supports the MPLS technology, including the following features:

- Supports basic functions and the label forwarding service of the MPLS, implements the LDP signaling protocol. The MPLS signaling protocol is in charge of distributing labels, establishing the LSP, and transmitting parameters during the LSP establishment process.
- Supports the Graceful Restart function on the MPLS signaling protocol layer, and continuously forwards label data when the protocol is interrupted.
- Supports the MPLS Ping/Tracert functions, and detects the availability of the LSP through MPLS echo request and MPLS echo reply messages.
- Supports the LDP FRR function. The ZXR10 ZSR V2 can quickly switch data traffic when the LSP is interrupted.
- Supports the load sharing function of the MPLS LSP.
- Supports the processing of multi-layer labels.
- Supports management functions such as the LSP loop detection mechanism.
- Supports the MPLS CoS and supports the mapping between IP packets in the ToS domain and MPLS packets in the EXP domain.

Static Tunnel

The static tunnel is a tunnel manually configured by the administrator. It does not need to be triggered by the MPLS signaling protocol or exchange control packets, so it consumes few resources and is applicable to small-scale stable networks with simple topologies. The tunnel created through label allocation in static mode cannot be dynamically adjusted with the change of network topology, and needs to be manually configured by the administrator.

The static tunnel command needs to be configured on each Label Switch Router (LSR) of the entire tunnel, including the header node, interim nodes, and the tail node. Services can be properly forwarded on the LSP of this tunnel only after the tunnel is correctly configured on all nodes.

MPLS-TE

Network congestion is a major problem affecting the performance of the backbone network. It is normally caused because network resources are insufficient, or the network is partially congested because the load of network resources is not balanced. The Traffic Engineering (TE) solves the congestion caused by unbalance load.

The MPLS TE is a technology that combines the TE technology and the MPLS. Through the MPLS TE, the service provider can accurately control the traffic path to avoid congested nodes, which solves the problem that some paths are overloaded while other paths are idle, and taking existing bandwidth resources into full utilization. Additionally, the MPLS TE can reserve resources during the establishment of the LSP tunnel, which ensures the QoS.

Through the OSPF TE or the IS-IS TE, the MPLS TE establishes a link bandwidth resource database for all nodes in the MPLS network, and uses the CSPF algorithm to calculation the tunnel establishment path in accordance with the link bandwidth resource database and the tunnel constraint conditions. The MPLS TE finally uses the RSVP-TE signaling protocol to establish the TE tunnel on the path calculated by the CSPF algorithm.

The ZXR10 ZSR V2 supports the following MPLS TE features:

- Supports OSPF TE and IS-IS TE.
- Supports Constrained Shortest Path First (CSPF) algorithm.
- Provides basic functions of the RSVP-TE protocol in accordance with the RFC, and establishes and maintenances the TE tunnel by exchanging Path/Resv messages.
- Provides link protection and node protection functions of the RSVP-TE FRR protocol in accordance with the Facility mode defined by the RFC, so that the LSP possesses the location protection capability of the RSVP-TE.
- Provides the Graceful Restart function defined by the RFC, the Extensions to GMPLS RSVP Graceful Restart, and the recovery processing mechanism when several adjacent nodes are restarted simultaneously.
- Supports RSVP-TE MIB function.
- Provides extended functions, including the Make Before Break (MBB), re-optimization, priority preemption, abstract refreshing, automatic routing, FA, hot-standby, and authentication functions.

3.5 VPN

3.5.1 IPsec and GRE

IPsec VPN

The IPsec is an IP-layer security framework protocol drafted by the Internet Engineering Task Force (IETF), which provides protection for the transmission of sensitive data in an unprotected network environment (such as the Internet). The IPsec defines the format and related basic structure of IP data packets, which provides confidentiality, data integrity,

anti-replay, and enhanced identity authentication functions for the transmission of IP data packets during network communication.

- Confidentiality indicates that user data is encrypted for protection and is transmitted as encrypted texts.
- Data integrity indicates that the data is not modified during the transmission process. The IPSec authenticates the received data to determine whether the packet is falsified.
- Anti-replay indicates that the IPSec determines whether a data packet is duplicated by comparing the sliding window on the target host with the sequence number in the received data packet. In this way, it prevents malicious users from intercepting an IPSec data packet and inserting it into the session again.
- Source authentication indicates that the IPSec identifies the identity of the data sender through the pre-shared encryption key or the RSA signature.

The IPSec uses the following two major framework protocols:

- Authentication Header (AH): The AH is a packet header authentication protocol, providing data source authentication, data integrity check, and packet anti-replay functions. The AH protocol does not encrypt protected data packets.
- Encapsulation Security Payload (ESP): The ESP protocol provides both authentication functions and the encryption function. The ESP provides the same authentication functions as the AH protocol (except that the data integrity check of the ESP does not include IP packet headers), and also provides the encryption function to improve the security of IP data packets.

The IPSec transmits IP data packets under the following two modes:

- Tunnel mode: In tunnel mode, the AH or ESP is inserted before the original IP header and a new IP header is formed before the AH or ESP. The tunnel mode is used to connect two security gateways (such as routers).
- Transmission mode: In transmission mode, the AH or the ESP is inserted after the IP header but before the transmission-layer protocol. The transmission mode is mainly used for end-to-end connection between hosts. It uses the address in the original IP packet header for addressing.

The ZXR10 ZSR V2 has the following IPSec features:

- Supports to create the security association manually or in the IKE dynamic association mode (isakmp).
- Supports the IKEv1 encryption key negotiation and exchange. The IKE supports the following security mechanisms:
 - Diffie-Hellman (DH) exchange and encryption key distribution: The DH algorithm is a public encryption key algorithm, with which both communication parties calculate the shared encryption key by exchanging data but not transmitting the encryption key. The encryption prerequisite is that both parties exchanging the encryption data must have a shared encryption key.
 - Perfect Forward Secrecy (PFS): The PFS is a security feature indicating that the security of other encryption keys is not affected after one encryption key is

decrypted, because these encryption keys are not derived from each other. The encryption key for the second phase of the IPsec is exported from that of the first phase. If the IKE encryption key of the first phase is stolen, the attacker may collect enough information to export the IPsec SA encryption key of the second phase. The PFS ensures the security of the encryption key in the second phase by executing an additional DH exchange.

- Identity authentication: It means that the identities of both parties are confirmed. The ZXR10 ZSR V2 supports the pre-shared key verification mode, in which the validation word is used to create the encryption key. If the validation word is different, the same encryption key cannot be created on both parties.
- Identity protection: The identity data is encrypted and transmitted after the encryption key is generated to protect the identity data.
- Supports the AH protocol and the ESP protocol. Both protocols can be used together.
- Supports the transmission of data packets in tunnel mode and in transmission mode.
- Supports the following two general hash algorithms to ensure that the data is not modified during the transmission:
 - HMAC-MD5: uses the 128-digit encryption key to calculate the hash.
 - HMAC-SHA-1: uses the 160-digit encryption key to calculate the hash.
- Supports encryption algorithms such as the DES-CBC, 3DES-CBC, AES-128-CBC, AES-192-CBC, and AES-256-CBC.
- Supports the DPD detection of the IPsec.
- Supports the NAT traversing of the IPsec.
- Supports the IPsec+GRE network architecture.
- Supports the IPsec to be associated with the VRF.

GRE VPN

The GRE protocol encapsulates particular data packets of the network-layer protocol, so that these encapsulated data packets can be transmitted in the IPv4 network.

When the router receives an original data packet (Payload) that needs to be encrypted and routed, the GRE first encapsulates this packet into a GRE packet and then encapsulates it in the IP protocol. The IP layer will then be fully responsible for forwarding this packet. The protocol of the original packet is called the passenger protocol, the GRE is called the encryption protocol, and the IP packet in charge of packet forwarding is called the delivery packet or the transport protocol. The GRE does not care for the specific format or contents of the passenger protocol during the above processes.

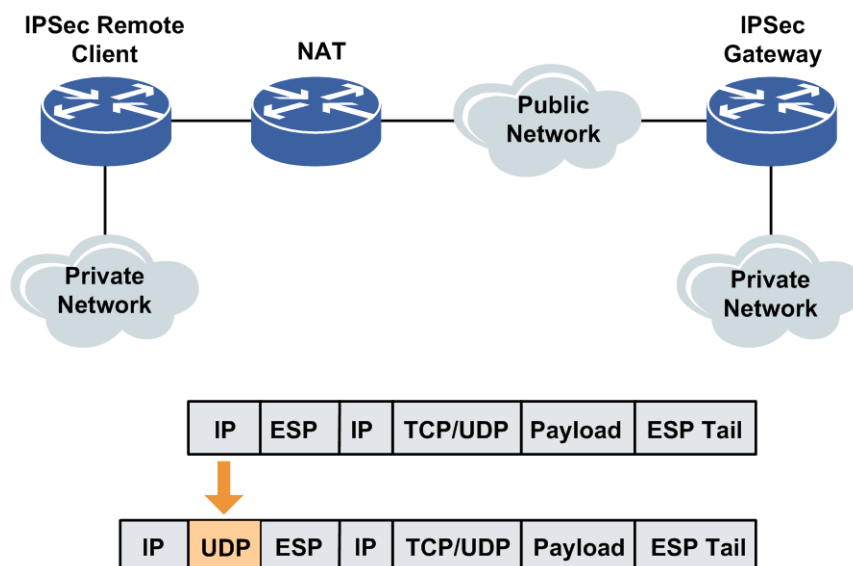
The GRE has the following advantages:

- The multi-protocol local network can transmit packets over the backbone network of a single protocol.
- Discontinuous subnets are connected to establish a VPN.
- The work scope of the network is extended to include protocols restricted by the routing gateway.

IPSec NAT

In a network, if there are routers between two IPSec routers, the IPSec routers must support IPSec NAT, so that NAT-T negotiation is performed through IKE and ESP packets can be encapsulated and decapsulated through UDP. Figure 3-1 shows an IPSec NAT application.

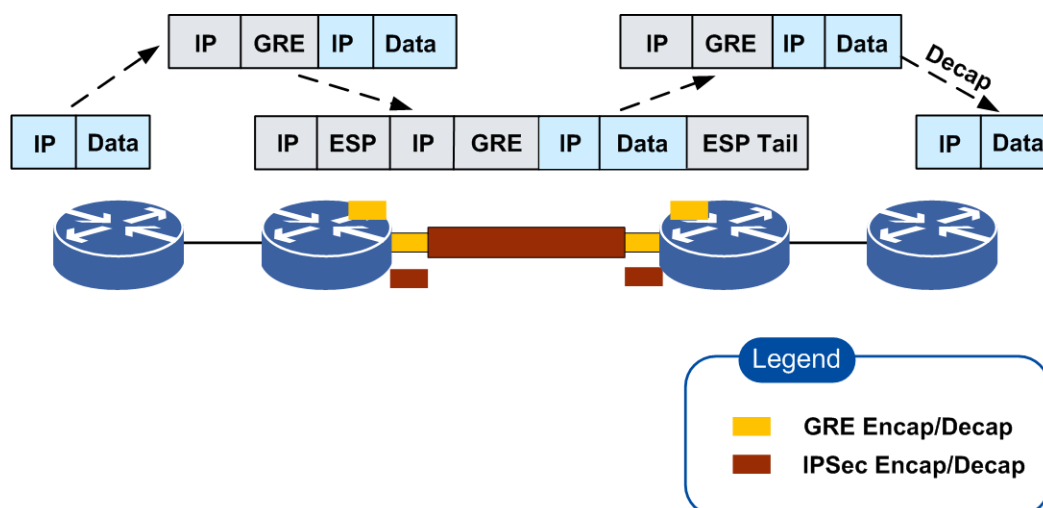
Figure 3-1 IPSec NAT



GRE Over IPSec

An IPSec tunnel supports unicast only, and cannot protect broadcast data. GRE supports encapsulation for non-IP packets, IP multicast packets, and IP broadcast packets. Therefore, GRE Over IPSec can be used to protect broadcast data in a GRE tunnel. GRE Over IPSec is used in application scenario where routing protocols need protection, see Figure 3-2.

Figure 3-2 GRE Over IPSec VPN



3.5.2 MPLS VPN

Overview

The MPLS VPN provides data secrecy of the ISP and supports to use a non-unique dedicated IP address in the VPN. The VPN forwarding table includes the corresponding label for VPN-IP address, through which the data is transmitted to the corresponding location.

The MPLS VPN has the following advantages:

- The configuration of VPN connection is simple, so it imposes no pressure upon the existing backbone network.
- It does not impose any requirement upon existing users, so users do not need to make any modification. The configuration for adding a user into the VPN is also simple.
- It provides powerful network extensibility.
- VPN users can continue using original dedicated addresses without making any modification. The VPN-ID is used on the backbone network to maintain uniqueness in the entire network.
- It is easier to provide value-added services, such as different COSs.

MPLS L2VPN

The ZXR10 ZSR V2 supports the MPLS L2VPN in Martini mode. It uses the VC-Type and the VC-ID to identify a Virtual Circuit (VC). The ZXR10 ZSR V2 supports the following functions:

- Uses the LDP protocol as the basic signaling.
- Supports both the VPWS and the VPLS L2 VPN services.
- Supports the L2VPN MIB.
- Supports 129-type FEC encoding.
- Supports the Pseudo Wire (PW) class configuration, heterogeneous structure, status Tag, Length, Value (TLV), Virtual Circuit Connectivity Verification (VCCV), and control field configuration for the VPWS service.
- Supports the L2VPN reflector for the VPLS service.
- Supports the L2VPN Graceful Restart function.
- Supports the MAC address filtering and restriction functions.
- Supports PWE3.
- Supports CESoPSN.
- Supports SAToP.
- Supports L2VPN and L3VPN Bridge Function.

MPLS L3VPN

The ZXR10 ZSR V2 supports the L3 VPN based on the MPLS/BGP. It uses existing public network resources to provide users with services of the virtual and dedicated network,

satisfying users' service requirements and security requests for transmitting private data on the public network.

The ZXR10 ZSR V2 supports the following MPLS L3VPN functions:

- Supports dynamic (BGP, RIP, OSPF, IS-IS) and static (static route) VPN accesses.
- Supports policy controls such as RT rewriting and SOO.
- Supports several cross-domain VPN modes.
- Supports the VPN routing restriction function.
- Supports the VPN FRR.

3.5.3 Smart Dial Control

Smart Dial Control (SDC) is a dial-on-demand backup technology used to interconnect routers through the PSTN, ISDN, or a 3G wireless network.

Dial on demand: No connection is pre-established between two routers. When data needs to be transmitted between the routers, the SDC flow is started to establish a connection, and then messages can be transmitted. When the connection is idle, SDC automatically disconnects the connection.

The dial-on-demand function provided by SDC is flexible, economical, and efficient. In actual applications, SDC is used as backup to provide guarantee for main line communication. It provides an alternative auxiliary channel when communication fails on a main line due to a line failure or another fault, which ensures that services can be provided properly.

The SDC module provides the following functions:

- Dialing backup function
 - Dialing backup triggered by a failed active link (or interface): After the active link (or interface) is invalid for a period, the standby interface dials, and the standby link is activated. When the active link (or interface) is recovered for a period, the standby link is disconnected.
 - Dialing backup triggered by an overloaded active link (or interface): When the load on the active link (or interface) exceeds the specified percentage of the link capacity, the standby interface dials, and the standby link is activated. The standby link operates together with the active link. When the load on the active link (or interface) is reduced to the specified percentage of the link capacity, the standby link is disconnected.
 - Link backup through route detection: When the SDC module detects that some routes that need backup are lost, dialing is triggered and backup routes to the specified destination are generated.
- Dial-on-demand function
 - Permanent dialing: After permanent dialing is configured on a dialing interface, dialing is immediately triggered until dialing is succeeded.

- Automatic dialing: When a device is started up and the physical dialing interface is up, automatic dialing is triggered.
- Manual dialing: Manual dialing can be performed or disabled through command configuration.
- Triggered dialing: Flows received on a router can be divided into triggering flows and non-triggering flows. For a triggering flow, if no connection is established, the router establishes a dialing connection with the remote router. For a non-triggering flow, the router does not call the remote router.

3.6 QoS

Overview

With the popularization of diverse services (voices, data, and video) and the continuous progress of the Fixed Mobile Convergence (FMC) process, the multiservice bearer network is required to provide differential services for different services and different users, so that it can distinguish services and guarantee the QoS of user services in accordance with the Service Level Agreement (SLA). The QoS guaranty is provided under various application models to provide end-to-end QoS, so that the network can sense and manage services, provide delicate operation of services, and finally improve users' service experiences.

Stream Classification and Labeling

In accordance with service classification policies, including the destination MAC, source MAC, VLAN ID, 802.1P, Type Of Service (ToS)/DSCP, and the IP quintuple (protocol type, destination IP, source IP, destination port number, and source port number), service packets are divided into several priorities or types. Additionally, the CoS of Ethernet packets, the ToS of IP packets, and the EXP field of DSCP or MPLS packets are labeled to provide class-based scheduling, congestion management, and traffic reshaping.

Traffic Supervision

Through the token bucket algorithm, the traffic entering the network is restricted within a correct range. The ZXR10 ZSR V2 supervises and punishes the exceeding traffic, such as discarding packets, coloring packets, or resetting packet priorities, to protect network resources and carrier's profits.

The ZXR10 ZSR V2 supports the Single-rate Three Color Marker (SrTCM) and Two-rate Three Color Marker (TrTCM) coloring algorithms, and supports the Color-Blind and Color-Aware coloring modes. The ZXR10 ZSR V2 supports port-based and stream-based coloring modes, and can apply them in either the ingress or the egress.

Traffic Reshaping

The traffic reshaping function caches and sends egress traffic out at a relatively even speed, so that the traffic rate satisfies the processing capability of downstream equipment.

The ZXR10 ZSR V2 supports port-based and queue-based traffic reshaping.

Queuing

The queuing technology solves the congestion of network nodes through a series of scheduling algorithms. High-priority packets are forwarded preferentially, while low-priority packets also get the corresponding scheduling chances fairly.

The ZXR10 ZSR V2 supports the PQ, the Weighted Fair Queuing (WFQ), and the CBWFQ modes.

Congestion Avoidance

Because the processing capability and caching capability of the network equipment are limited, packets above equipment capabilities may cause network congestion. If these packets are discarded simply, the global synchronization symptom occurs.

The ZXR10 ZSR V2 avoids congestion in RED/WRED mode to improve the network quality. The WRED can sense services, including the IP priority, DSCP, and MPLS EXP, and sets different earlier-phase discarding policies for packets with different priorities. This means that, it provides differential discarding features for different services.

MPLS QoS

The ZXR10 ZSR V2 supports the following MPLS QoS features:

- Supports the MPLS QoS based on the Diff-Serv model. The MPLS QoS completes the priority mapping between MPLS, IP, and Ethernet packets, and distinguishes data streams of different services in accordance with the EXP in the label. This means that, it provides differential services and ensures the QoS for voice and video services.
- Supports three standard carrier MPLS QoS tunnels: Uniform Tunnel, Pipe Tunnel and Short Pipe Tunnel.
- Combines the MPLS-TE and the Diff-Serv, so that the IP/MPLS core network owns service identification capabilities. The tunnel is also established to ensure the bandwidth for high-priority services.
- Supports QoS scheduling inside the MPLS VPN, and ensures that key VPN services are forwarded preferentially by achieving Diff-Serv inside the VPN.
- Distinguishes PWs in accordance with user services and maps the service PW to the corresponding MPLS tunnel. By achieving service-based end-to-end QoS that is easier to be deployed and plans the bandwidth, the ZXR10 ZSR V2 provides operation guaranty for the differential management and services of multiple services.

H-QoS

Through hierarchal scheduling and unified centralized configuration, the H-QoS provides delicate QoS for high-quality services and users, reduces the construction cost of the equipment accessed into the network, and simplifies the maintenance cost of the entire network. Additionally, the H-QoS improves the QoS of the entire network.

The H-QoS provides delicate scheduling in hierarchal mode and provides reliable service support for users to deploy multiple services.

The ZXR10 ZSR V2 supports the following hierarchal QoS features:

- Supports multi-hierarchy traffic management through setting multi-hierarchy scheduler, meeting network deployment requirements.
- Supports multi-user, multi-service, and multi-traffic classification requirements to perform congestion avoidance and traffic shaping.
- Supports packet marking in H-QoS queue scheduling.
- Supports traffic statistics for service scheduling in the hierarchal QoS and provides visualized management of the traffic service model. This means that, the maintenance and management personnel have better understanding of the network.

3.7 Security Features

3.7.1 ACL

An ACL is used to permit or deny packet flows based on configured rules. Packet filtering rules determine the ACL type. ACL rules can be defined based on the following conditions:

- MAC address
- VLAN
- Source IP address
- Destination IP address
- Source port number
- Destination port number
- Transport-layer protocol number
- ToS
- Time range

After an ACL is created, it must be applied on an interface. Data flows on an interface are bidirectional, so the direction (input or output) must be specified when an ACL is applied on an interface.

To configure an ACL on an interface, an ACL, the interface on which the ACL is applied, and the direction in which the ACL is applied on the interface must be defined. The ACL operation procedure is as follows:

1. The ACL type is identified through the ACL serial number. Packets are checked based on the ACL to determine whether the packets can pass the interface.
2. ACL rules are used for checking packets in accordance with the configuration order of the rules. Rules configured first are used for checking packets first.
3. Once the packets match a rule, the router stops checking the packets.
4. For the matched packets, whether the packets are allowed to pass the interface depends on the corresponding action (permit or deny) configured for the rule.
5. If the packets match no rule, the default rule is used, that is, the packets are disallowed to pass the interface.

The ZXR10 ZSR V2 provides the following ACL features:

- Supports standard ACLs and extended ACLs
- Supports L2 ACLs, L3 ACLs, and L2/L3 hybrid ACLs
- Supports ACL time range
- Supports ACL log statistics
- Supports collecting statistics on the hit rate
- Supports ACL binding in batches

3.7.2 Anti-Attack

IP Source Attack Defense

The ZXR10 ZSR V2 supports the following IP source attack defense mechanisms:

- IP and MAC binding: In accordance with configuration, a binding relationship can be established between the specified IP address and MAC address. For packets with the specified IP address (source), if the MAC address is different from the bound MAC address, the packets are dropped. This prevents attacks by packets with false IP addresses.
- ARP scanning: Static IP and MAC association table can be generated in batches through the ARP scanning function.
- IP source guard: When the ZXR10 ZSR V2 is used as a L2 device, a binding table can be used to guard IP source cheat.

ARP Attack Defense

The ZXR10 ZSR V2 supports the following ARP attack defense mechanisms:

- Uses periodic gratuitous ARP packets, so that users' packet can be properly forwarded to gateways without being attacked or intercepted.
- Uses strict ARP learning to prevent ARP cheat.
- Uses ARP protection to prevent ARP cheat.
- Uses dynamic ARP inspection to prevent ARP cheat.
- Uses ARP packet suppression to prevent ARP flooding.
- Uses ARP Miss message suppression to prevent ARP flooding.

3.7.3 Firewall

Security Zone

The ZXR10 ZSR V2 supports security zones, including the [DMZ](#). All security policies are implemented based on security zones. After security zones are configured, the firewall function can be configured in the security zones. Security zone configuration includes the security zone name, priority, interface added to the security zone, and the DMZ. In general, a DMZ is a filtering subnet that provides a security zone between an internal network and external network.

Packet-Filtering Firewall and Fragmented-Message Filtering

Packets can be filtered through ACL configuration. Packets are filtered based on information such as the protocol number of the upper-layer protocol operating over IP, source IP address, destination IP address, source port number and destination port number in a packet and the packet transmission direction.

Packet filtering is used in the firewall function. To forward a packet, the ZXR10 ZSR V2 retrieves information in the header of the packet and checks the packet based on the ACL rules. The ZXR10 ZSR V2 determines whether to forward or drop the packet based on the comparison result.

Packet filtering supports fragmented-message filtering. The packet filtering firewall identifies packet types, such as non-fragmented message, first fragmented message, and non-first fragmented message. All types of packets are filtered.

Stateful Firewall

Stateful firewall is an extension of the packet-filtering firewall. It takes each packet as an independent unit to perform ACL check and filtering, and also considers application-layer associativity between packets.

- The stateful firewall uses different state tables to monitor TCP sessions or UDP sessions. The ACL determines the sessions that are allowed to be established. Only the packets related to the allowed sessions are forwarded.
- For a TCP session or UDP session, the stateful firewall analyzes the application-layer state information about packets, and filters packets that do not match the current application-layer state.
- The stateful firewall has the advantages of the packet-filtering firewall and proxy firewall, providing the high speed and security.

The stateful firewall performs filtering for application-layer packets, meaning state-based packet filtering. The stateful firewall can detect the information about the application-layer protocol session that wants to pass the firewall. The stateful firewall maintains the session state and checks the protocol number and port number of session packets. If the packets do not match rules, the packets are disallowed to pass the firewall. The stateful firewall maintains the state information about each connection to dynamically determine whether to allow passing the packets or drop the packets. The stateful firewall also can monitor various application-layer protocol traffic.

Blacklist

The blacklist is used to filter packets based on source VPN and source IP address. The packet fields checked by the blacklist are simpler than those checked by ACLs, so packets can be filtered at high speeds. In this way, packets sent from the specified IP addresses are shielded. The blacklist can be statically configured or dynamically generated by the firewall.

Besides the IP addresses statically configured in the blacklist, when the ZXR10 ZSR V2 detects that there are IP-scanning attacks or port-scanning attacks from the specific IP

address, this IP address is added to the blacklist. If the blacklist function is enabled, any packets from the IP address are filtered. The aging period of the static blacklist and dynamic blacklist can be configured. When packets match the blacklist, even if the packets are permitted in accordance with the ACL rules, the firewall drops the packets.

Blacklist configuration can be exported to a file, and blacklist configuration can be imported through a file.

White List

If the IP address and VPN of a host are added to the white list, the firewall does not perform IP-scanning attack check or port-scanning attack check for packets sent from the host. The firewall does not add the IP address to dynamic blacklist, and the IP address cannot be added to the static blacklist.

After receiving a packet, the ZXR10 ZSR V2 checks whether the source IP address of the packet is in the white list. If yes, the ZXR10 ZSR V2 does not perform IP-scanning attack check or port-scanning attack check for the packet, and does not add the IP address to the dynamic blacklist. Other security filtering procedures are performed, such as ACL packet filtering, stateful firewall, and traffic statistics and monitoring, which achieves the optimal security filtering effects.

The aging period can be configured for the white list. White list configuration can be exported to a file, and white list configuration can be imported through a file.

Anti-DDOS Attack

As the network environment becomes more and more complicated, as the core part processing various complicated protocol data packets, the control-layer processor of the router equipment is easier to be attacked by network broadcast storms, PING flooding, and TCP syn flooding. To prevent these attacks from affecting the CPU and even leading to service error, pause, or interruption, the ZXR10 ZSR V2 provides a flexible and complete stream-control mechanism for the traffic entering the control layer.

- The ZXR10 ZSR V2 divides received CPU traffic into several queues with different priorities to ensure that important protocol packets, such as the BGP and the OSPF, and customized data packets are processed preferentially. Each queue sets different thresholds for different packet types.
- The ZXR10 ZSR V2 supports CAR speed limit for the traffic sent from the physical ingress ports.
- The ZXR10 ZSR V2 supports the CAR speed limit for customized packets in accordance with the source address, protocol type, TCP/UDP port number, and the physical ingress port number.
- The ZXR10 ZSR V2 supports the configuration of the number of packets sent per second and their priorities in a specific rule.
- The ZXR10 ZSR V2 supports the function of detecting exceptions for packets sent from logical ports. The ZXR10 ZSR V2 checks the speed of all received packets on logical ports, stops the packet-receiving operation on the port when it finds that

the traffic sent on the port reaches the specified threshold, extends the operation appropriately, and then continues receiving packets.

Through dividing and treating data packets with different priorities, the multi-queue sending technology, the configuration of the port sending policy, and the speed limit for sent streams, the ZXR10 ZSR V2 effectively ensures that important data packets with higher priorities are sent preferentially, and shields attacks from error packets.

Anti-DOS Attack

The ZXR10 ZSR V2 supports the following anti-DOS attack mechanisms:

- LAND attack defense
- Smurf attack defense
- WinNuke attack defense
- SYN flood attack defense
- ICMP flood attack defense
- UDP flood attack defense

Anti-Scanning Attack

The ZXR10 ZSR V2 supports the following anti-scanning attack mechanisms:

- Ping-death attack defense
- Large-ICMP attack defense
- ICMP-unreachable attack defense
- ICMP-redirect attack defense
- ICMP fragment attack defense
- IP fragment attack defense
- Teardrop attack defense
- Fraggle attack defense
- Tracert attack defense

Anti-Abnormal-Packet Attack

The ZXR10 ZSR V2 supports the following anti-abnormal-packet attack mechanisms:

- Abnormal TCP packet attack defense
- IP incorrect option attack defense
- Syn fragment attack defense
- Unknown protocol attack defense
- IP spoofing attack defense
- IP option packet attack defense
- TCP No-Flag packet attack defense
- TCP Syn Fin packet attack defense
- TCP Fin-No-Ack packet attack defense

3.7.4 Multiple Security Authentication Modes

AAA

The ZXR10 ZSR V2 support multiple security authentication modes.

With different authentication policies for user access, the ZXR10 ZSR V2 provides complete AAA authentication and authorization functions. Different access authentication policies can be configured to perform different authentication and authorization for users selectively as needed.

The AAA supports the following three authentication modes:

- Local authentication
- RADIUS authentication
- TACACS+ authentication

The AAA supports the following four authorization modes:

- Direct trusting authorization: The AAA performs authorization without the user account.
- Local account authorization: The AAA performs authorization in accordance with user accounts configured locally.
- TACACS+ authorization: The TACACS+ is divided into authentication and authorization. The TACACS+ server authorizes users.
- Authorization after successful RADIUS authentication: The authorization and authentication of the RADIUS protocol cannot be split.

Protocol Security Validation

In accordance with the security validation requirements of different protocols, the ZXR10 ZSR V2 provides complete protocol security validation functions for the Secure Shell (SSH), PPP, routing protocol, and SNMP protocol.

Security validation for the SSH protocol:

- Supports encryption authentication based on the MD5
- Supports encryption authentication based on the SHA1

Security validation for PPP access:

- Supports the Password Authentication Protocol (PAP)-based validation mode.
- Supports the Challenge Handshake Authentication Protocol (CHAP)-based validation mode.

Security validation for the routing protocol:

- Supports the explicit packet authentication for the RIP v2, OSPF, and IS-IS.
- Supports the MD5-based encryption authentication for the RIP v2, OSPF, IS-IS, and the BGP.
- Supports the MD5-based encryption IPsec AH authentication for the RIPng, OSPFv3, and the BGP-4+.

- Supports the SHA1-based encryption IPsec AH authentication for the RIPng, OSPFv3, and the BGP-4+.

SNMP security validation:

Supports the encryption and authentication for the SNMP v3.

3.7.5 uRPF

The ZXR10 ZSR V2 supports the URPF function to avoid network attacks based on source address cheats.

The source address cheating method is common among DoS attacks. The attacker fakes a source address (which is normally a valid network address) to access the equipment to prevent it from providing services properly. The URPF can effectively avoid this type of attacks.

The ZXR10 ZSR V2 supports the following URPF features:

- Supports the Strict RPF checking function.
- Supports the Loose RPF checking function.
- Supports the Loose RPF checking function that ignores the default route.
- Supports the ACL checking function.

3.8 Network Reliability

Ping Detect

The Ping Detect automatic detection function, which uses request/response packets of the ICMP to detect whether the destination is reachable, and feeds back the detection result to the associated standby function module to trigger active/standby switchover. This means that, it provides the backup function based on the availability of applications on the network layer.

BFD

An important function of any network equipment is to quickly detect communication faults with adjacent systems and rapidly create other paths. The BFD protocol greatly supports this purpose. The BFD is used to provide a low-load and fast fault detection mechanism between adjacent forwarding engines. The BFD, together with the FRR, can provide millisecond-level link detection and route switchover functions on the forwarding layer.

The ZXR10 ZSR V2 supports the following BFD features:

- Supports the BFD detection function of version 0 and version 1.
- Supports the BFD for BGP detection.
- Supports the BFD for OSPF detection.
- Supports the BFD for IS-IS detection.
- Supports the BFD for LDP LSP detection.
- Supports the BFD for TE tunnel detection.

- Supports the BFD for static route next-hop detection.
- Supports the BFD for policy route detection.
- Supports the BFD for VRRP detection.

FRR

When particular links or nodes in the network become ineffective, the packets reaching the destination through these ineffective nodes may be discarded or form a loop. Traffic interruption or traffic loop inevitably occurs in the network until the network re-converges to calculate out a new topology and route. The interruption normally continues for several seconds. To reduce the traffic interruption period in the network, a mechanism must be provided to provide the following functions:

- Rapidly discovers ineffective links.
- Rapidly provides another recovery path when the first link fails.
- Avoids the forwarding loop "micro-loop" in the follow-up network recovery process.

The ZXR10 ZSR V2 provides IP FRR and MPLS FRR function.

- With the IP FRR function provided by the ZXR10 ZSR V2, the routing protocol module avoids no-loop active/standby routes in accordance with the loop configured by the user. During the forwarding process, the forwarding module forwards traffic according to the active route and detects the port status of the active route. When an exception occurs on the active port, the ZXR10 ZSR V2 rapidly switches the traffic over to the standby route, which reduces the traffic switchover period and the number of discarded packets.

The IP FRR is normally used together with the routing protocol. The ZXR10 ZSR V2 supports the following IP FRR: static route FRR, OSPF FRR, IS-IS FRR, and BGP FRR.

- MPLS FRR is a localised protection technology for MPLS-TE networks. After the FRR function is configured for an LSP, when a link or node in the protected LSP fails, traffic is rerouted to the standby link. FRR is a measure for temporary protection. When the protected link is recovered or a new LSP is established, traffic is rerouted to the protected LSP or the new LSP.

VRRP

By providing a set of detection and competition mechanism, the VRRP protocol provides the gateway backup functions in the multi-address access LAN (such as the Ethernet). The VRRP protocol backs up gateway equipment in the LAN to maintain the interrupted operation of host equipment accessed into the network system. That is, the VRRP backs up the route next-hop equipment for the accessed host equipment.

The ZXR10 ZSR V2 supports the following VRRP features:

- Supports basic functions of the VRRP.
- Supports the heartbeat line function of the VRRP.
- Supports the binding of the VRRP and the BFD detection.
- Supports the binding of the VRRP and the PING detection.

- Supports detecting the status of specified ports through the VRRP.
- Supports detecting key route information through the VRRP.
- Supports VRRP group management functions to uniformly receive or send protocol packets in several VRRP groups.
- Supports the VRRP MIB function.

3.9 IPv6 Features

3.9.1 IPv6 Basic Functions

The ZXR10 ZSR V2 supports IPv4/IPv6 dual-protocol stacks.

- Supports the IPv6 basic protocol, IPv6 protocol, and the Neighbor Discovery protocol.
- Supports the TELNET6 and the SSHv6 for remote user login and connection.
- Supports the TCP6, UDP6 and the Socket IPv6.
- Supports the IPv6 DHCP Relay/Server and the DNS6 Client.
- Supports the PMTU discovery function.
- Supports IPv6 link detection functions such as the Ping6 and the Trace6.
- Supports the IPv6 ACL function.
- Supports the IPv6 QoS function.
- Supports security function such as the IPv6 VRRP and the IPv6 uRPF.

3.9.2 IPv6 Unicast Routing Protocols

Overview

The ZXR10 ZSR V2 supports unicast routing protocols such as the IPv6 static route, RIPng, OSPFv3, IS-ISv6, BGP4+, and the IPv6 policy route.

IPv6 Static Route

The IPv6 static route indicates that the network administrator specifies the route information in the IPv6 routing table through configuration commands. It does not create the routing table in accordance with the routing algorithm in the same way as the IPv6 dynamic route.

When the dynamic route is configured, routers need to frequently exchange routing tables with each other and will easily become overloaded. The static route can be used to solve this problem. With the static route, the user only needs to make few configurations to avoid using the dynamic route.

The ZXR10 ZSR V2 supports the configuration of the IPv6 static route by specifying the next hop or the egress interface.

RIPng

Based on the UDP, the RIPng uses port 521 to send and receive data packets.

The ZXR10 ZSR V2 supports the RIPng basic protocol, route summary and redistribution, RIPng route load sharing, RIPng protocol MIB function, RIPng VRF access instance, and the function of associating the IPv6 BFD with the RIPng.

OSPFv3

The OSPFv3 is used to provide the routing function in the IPv6 network.

The ZXR10 ZSR V2 supports the OSPFv3 basic protocol, route summary and redistribution, OSPFv3 route load sharing, OSPFv3 authentication, OSPFv3 protocol MIB function, OSPFv3 VRF access instance, and the function of associating the IPv6 BFD with the OSPFv3.

IS-ISv6

The work principle of the IS-ISv6 is similar to that of the IS-ISv4.

The ZXR10 ZSR V2 supports the IS-ISv6 basic protocol, route summary and redistribution, IS-ISv6 route load sharing, IS-ISv6 route filtering, IS-ISv6 authentication, IS-ISv6 protocol MIB function, IS-ISv6 VRF access instance, and the function of associating the IPv6 BFD with the IS-ISv6.

BGP4+

The BGP4+ is an extension of the BGP protocol. It inherits the basic message format of the BGP4 and adds extended attributes for transmitting the IPv6 routing information.

The ZXR10 ZSR V2 supports the basic protocol, route attributes, route summary, route distribution, reflector, and alliance functions of the BGP4+, policy filtering of BGP4+ routes, BGP4+ route load sharing, BGP4+ authentication, BGP4+ protocol MIB function, BGP4+ VRF access instance, and the function of associating the IPv6 BFD with the BGP4+.

IPv6 Policy Route

The concept and principle of the policy route in the IPv6 are the same as those in the IPv4, except that IPv6 addresses and routes are used for the configuration.

3.9.3 IPv6 Multicast Routing Protocols

Overview

IPv6 multicast is different from IPv4 multicast in that the IPv6 multicast address mechanism is greatly enhanced. But group member management, multicast packet forwarding, and multicast route establishment functions are basically the same as those in IPv4 multicast.

MLD

The MLD protocol originates from the IGMP protocol. The MLDv1 corresponds to the IGMPv2, and the MLDv2 corresponds to the IGMPv3.

Different from the IGMP protocol that uses the packet type with the IP protocol number of 2, the MLD protocol uses the ICMPv6 (with the IP protocol number of 58) packet type, including the MLD query packet (type 130), MLDv1 report packet (type 131), MLDv1 leaving packet (type 132), and MLDv2 report packet (type 143). The MLD protocol and the IGMP protocol have different packet format, but their protocol behaviors are completely the same.

The ZXR10 ZSR V2 supports the MLDv1/v2 protocol.

IPv6 PIM

The IPv6 PIM protocol is different from the IPv4 PIM in the IP address structure in the packet, but other protocol behaviors in them are basically the same. The IPv6 PIM also supports the SM, DM, and SSM modes.

The ZXR10 ZSR V2 supports the IPv6 PIM-DM, IPv6 PIM-SM, and IPv6 Protocol Independent Multicast-Source Specific Multicast ([PIM-SSM](#)) protocols.

3.9.4 IPv6 Tunnel Functions

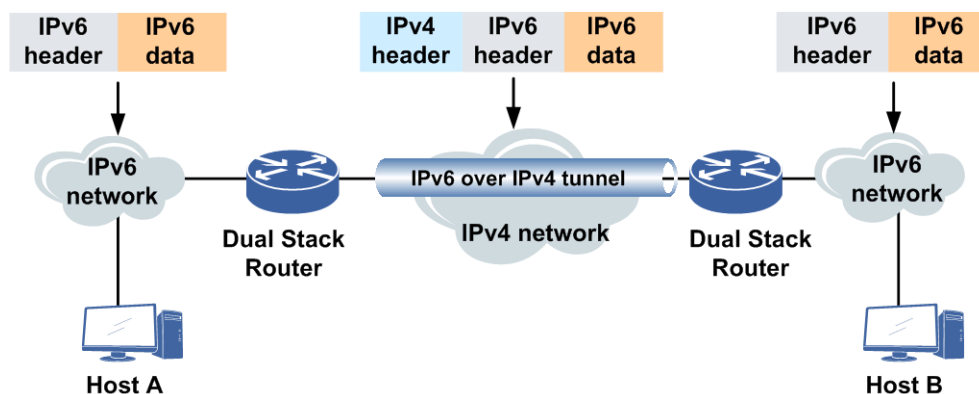
Overview

The ZXR10 ZSR V2 supports IPv6 tunnel protocols, including IPv6 over IPv4 configuration tunnel and automatic tunnel, IPv4 over IPv6 tunnel, and ISATAP tunnel.

IPv6 over IPv4

The IPv6 over IPv4 tunnel mechanism encapsulates IPv4 packet headers before an IPv6 data packet and passes the IPv6 packet over the IPv4 network through tunnels to provide the interconnection of separated IPv6 networks, see [Figure 3-3](#).

Figure 3-3 IPv6 over IPv4 Tunnel Principle



The IPv6 over IPv4 tunnel can be established between hosts, from a host to an equipment, from an equipment to a host, or between equipments. The destination of a tunnel may be the final destination of the IPv6 packet, or the IPv6 packet can be further forwarded. In

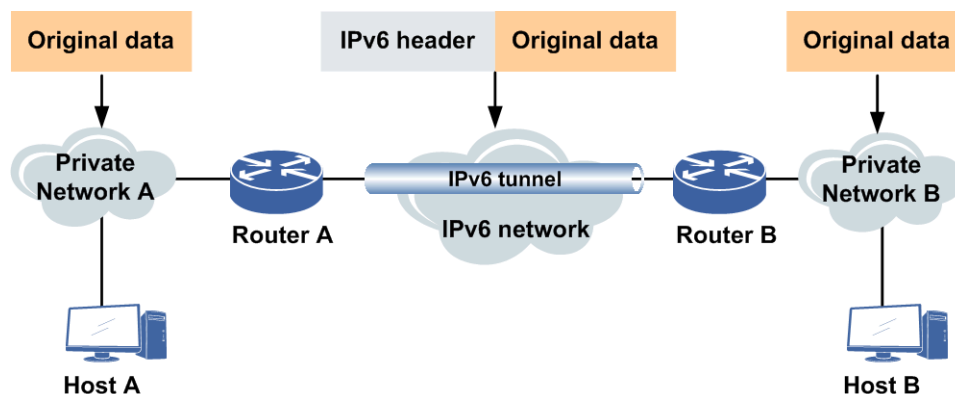
accordance with the different ways of acquiring IPv4 addresses on the tunnel destination, tunnels can be divided into configuration tunnels and automatic tunnels.

- If the destination address of an IPv6 over IPv4 tunnel cannot be automatically got from the destination address of the IPv6 packet, it needs to be manually configured. This type of tunnel is called the configuration tunnel, such as the 6in4 tunnel and the GRE tunnel.
- If the interface address of an IPv6 over IPv4 tunnel uses the special IPv6 address format with an IPv4 address, the IPv4 address of the tunnel destination can be automatically got from the destination address of the IPv6 packet. This type of tunnel is called the automatic tunnel, such as the 6to4 tunnel and the ISATAP tunnel.

IPv4 over IPv6

The IPv4 or IPv6 over IPv6 tunnel protocol encapsulates IPv4 or IPv6 data packets, so that the data packets can be transmitted in another IPv6 network. The encapsulated data packet is the IPv6 tunnel packet, see [Figure 3-4](#).

Figure 3-4 IPv4 over IPv6 Tunnel Principle



ISATAP

The ISATAP can access the dual-stack node inside the IPv4 site into the IPv6 router through the automatic tunnel, so that the dual-stack node that does not share the same physical node with the IPv6 router can send data packets to the IPv6 next hop through the IPv4 automatic tunnel.

The ISATAP transition mechanism uses the IPv6 address with an IPv4 address, so the IPv6-in-IPv4 automatic tunnel technology is used in the site with either a global IPv4 address or a private IPv4 address. Because the ISATAP address format uses both the site unicast IPv6 address prefix and the global unicast IPv6 address prefix, the ISATAP supports both site and global IPv6 routes.

3.9.5 6PE and 6VPE

6PE

In an IPv4 MPLS network, 6PE uses an existing MPLS to interconnect islanding IPv6 networks. 6PE uses the BGP/MPLS VPN principle to establish MP-BGP peers between PEs. IPv6 routes in IPv6 sites are distributed between the PEs, and packets are forwarded through IPv4 MPLS labels in the IPv4 network. In this way, islanding IPv6 networks can communicate with each other.

6VPE

The 6VPE is a technology used to provide BGP MPLS VPN services in the IPv6 user network. The work principle of the 6VPE originates from the BGP MPLS VPN in the IPv4, and the 6VPE is an extension of the IPv4 BGP MPLS VPN.

The 6VPE is not restricted to IP protocol versions used on the backbone network. This means that, the IPv6 VPN traffic is transmitted through IPv6 tunnels or IPv4 tunnels.

The ZXR10 ZSR V2 supports the 6VPE and supports to run the IPv6 static route, RIPng, OSPFv3, IS-ISv6, and EBGp protocols between Customer Edges (CEs) and Provider Edges (PEs).

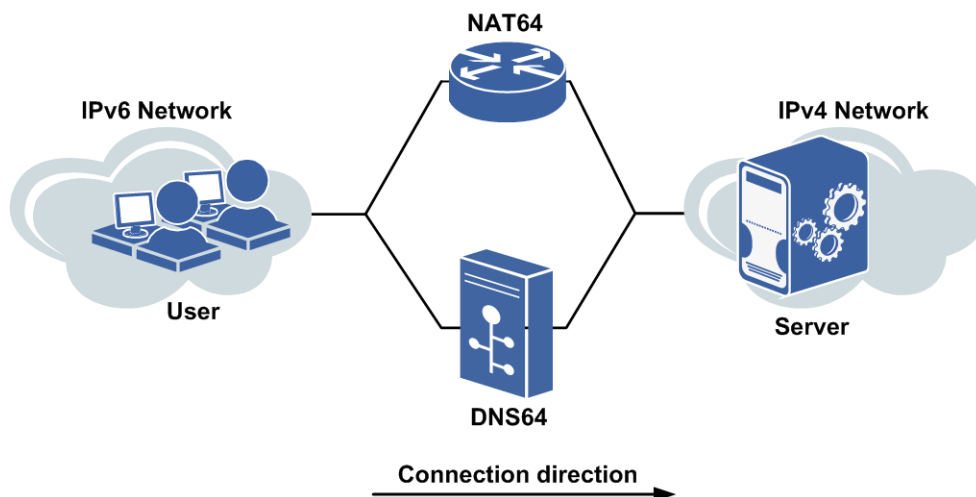
3.9.6 NAT64

NAT64 is an IPv4-IPv6 transition technology through which IPv6 hosts can use IPv4 services. The key of IPv6 network transition is users' IPv6 transition. NAT64 allows IPv6 users to use IPv4 application services.

NAT64 is defined to be widely used in scenarios where IPv6 clients initiate IPv4 service sessions. It simplifies NAT-PT scenarios, and facilitates deployment, operation and maintenance.

Figure 3-5 shows a NAT64 application scenario.

Figure 3-5 NAT64 Application Scenario



NAT has the following features:

- An IPv6 host actively sends a connection request to an IPv4 service.
- The NAT64 unit is separated from the DNS unit.

NAT64 only supports session initiated by IPv6 hosts for IPv4 services, and address mapping to IPv4 server addresses is simple in IPv6 networks, so it is unnecessary to perform complicated management for associations between domain names and addresses. This avoids the DNS security problem and DNSSEC compatibility problem.

- The DNS needs to support the DNS64 function.

The DNS used in NAT64 must support the DNS64 function, so that A records can be translated into AAAA records. When there is no AAAA record in the system, A records can be queried through DNS proxy.

The ZXR10 ZSR V2 supports the NAT64 function.

3.10 NAT

NAT can translate an IP address in one network to another IP address in another network. In general, NAT is used to map one address used in a private network or intranet to one or multiple addresses used in a public network or Internet.

NAT has the following advantages:

- Limits the number of IP addresses used in private networks that need [IANA](#) registration.
- Saves the number of global IP addresses needed in private networks. (For example, one entity can use one IP address for communication in the Internet.)
- Maintains privacy of LANs, because internal IP addresses are not public.

The ZXR10 ZSR V2 has the following NAT features:

- Supports in/out side NAT
- Supports NAT44 and NAT64
- Supports multi-egress NAT
- Supports static NAT and dynamic NAT
- Supports mapping mode, filtering mode, and hybrid mode
- Supports PAT
- Supports ALG applications, including TCP ALG (FTP, RSTP, H323, and PPTP) , UDP ALG (DNS, SIP, and H323) , and ICMP ALG

3.11 Network Management Features

Overview

The ZTE NetNumen™ is a network management system constructed on the data communication network, which performs centralized maintenance and management

upon various types of network equipment in a wide area and complicated application environment.

Network Management Network Architecture

The following two network architectures can be used between the NetNumen™ network management system and the ZXR10 ZSR V2:

- In-band management: The network management information and the service data is transmitted in the same channel without extra DCN network.
- Out-of-band management: The network management information is transmitted in the network management network independent of the service data. So an extra DCN network is required. The NetNumen™ network management system is connected to the out-of-band management port of the ZXR10 ZSR V2, so the network information and the service information can be transmitted separately.

NetNumen™ Network Management System

The NetNumen™ U31 (BN) network management system is a unified network management system developed by ZTE to manage Synchronous Digital Hierarchy (SDH), Multi-Service Transport Platform (MSTP), Wavelength Division Multiplexing (WDM), Packet Transport Network (PTN), Optical Transport Network (OTN), and IP equipment (routers and switches). It covers management layers including NE management, network management, and service management.

The NetNumen™ U31 (BN) network management system provides the following functions:

- Fault management: ensures the stable operation of the network.
- Performance management: enables the user to have a complete understanding of service situations in the network.
- Resource management: ensures that network resources are utilized properly.
- View management: ensures that the user have a clear view of the network operational status.
- Configuration management: provides fast service deployment.
- Security management: guarantees network security.
- Northbound interface: supports third-party system integration.

Netflow

The Netflow technology can quickly distinguish different types of service flows transmitted in the network by analyzing attributes of IP data packets. The Netflow separately traces and accurately measures each data flow that is distinguished out, records its flow attributes such as the transmission direction and destination, counts its starting time, ending time, service type, and traffic information such as the number of data packets and bytes included in this flow. The Netflow outputs the original records of the collected data flow traffic and flow direction information at regular intervals, automatically summarizes original records, and outputs the statistical results.

The ZXR10 ZSR V2 supports the following Netflow features:

- Complies with the mainstream v5, v8, and v9 packet formats in the industry.
- Supports sending packets to the server in IPv4/UDP mode.
- Supports the mode of initially reporting packets.
- Supports the configuration of active and inactive aging periods in the cache.
- Supports multiple servers.
- supports random sampling by flow.
- Supports the configuration of interface traffic sampling rates.
- Supports the Netflow sampling function on physical interfaces and sub-interfaces.
- Supports separate sampling in the ingress and egress directions of an interface.
- Supports independent sampling of multiple services in one direction, such as unicast, multicast, and MPLS.
- Supports sampling rates ranging from 65535:1 to 1:1.

Network Layer Detection

The ZXR10 ZSR V2 provides several network-layer detection functions based on Ping and Trace functions, such as IP Ping, IP Trace, LSP Ping, LSP Trace, multicast Ping, and multicast Trace.

3.12 System Operation and Maintenance

Multiple Configuration Modes

The ZXR10 ZSR V2 provides multiple equipment login and configuration modes for the user to select the appropriate connection configuration mode as needed.

- Configuration through the serial port connection
- Configuration through the Telnet connection
- Configuration through the SSH protocol connection
- Configuration through the SNMP connection
- Version upgrade through USB
- DHCP automatic configuration
- In-batch version upgrade through NMS

System Monitoring, Management and Maintenance

The ZXR10 ZSR V2 supports equipment monitoring, management, and maintenance in several modes, so the equipment can perform the corresponding troubleshooting under each abnormal situation and provide users with parameters during the equipment operation process.

Equipment monitoring functions include:

- There are indicators on the power module, the fan module, the main control module, and each interface board, to indicate the operational state of parts.
- The fan module performs fan monitoring to detect the fan existence status information and adjust the fan speed intelligently.

- The power module function provides the existence information, status information, power information, and the AC/DC information of the power module.
- When the fan module, the power module, or the temperature becomes abnormal, the system raises sound alarms and alarm prompts on the software.
- The network management system collects temperature in distributed mode to monitor the temperature of each board.
- Hot-plugging events and switchover events on the main control board are recorded for users to query.
- The network management system automatically checks version compatibility during the system operating process.
- The network management system monitors the operational state of the software. If the proper operation of the equipment is affected due to abnormal situations, the system restarts the line interface board or switches over the active/standby main control boards.

Equipment management and maintenance functions include:

- The system provides flexible online help in CLI mode.
- The system supports operations by several users simultaneously. The operator can specify whether to allow this function through the corresponding command.
- The system provides multilevel user permission management functions and automatically records user operation logs.
- The system provides the unified management of log, alarm and debugging information in the information center.
- The system provides the CLI mode for users to query the basic information of each main control board, interface board, and optical module.
- The system enables the user to log in through the console port with or without specifying the user name and password.
- The system provides the query of several information items, including the software version information, parts status, environment temperature, CPU occupancy, and memory occupancy.
- The passwords of normal users can be displayed in explicit texts or in encrypted mode.
- The system provides layered management of equipment alarms, supports alarm classification and alarm filtering functions, and can output alarms to the remote server.

Diagnosis and Debugging

The ZXR10 ZSR V2 provides several diagnosis and debugging methods for users to get more debugging information through more methods during equipment debugging. The ZXR10 ZSR V2 supports the dedicated diagnosis and debugging command mode, and supports complete equipment diagnosis and testing functions. The user can detect the equipment at any time and remotely identify the cause when a fault occurs on the equipment.

The ZXR10 ZSR V2 supports the following diagnosis and debugging modes:

- Detecting the operational status of the equipment

- Performing the Ping and Trace Route functions
- Debugging

This page intentionally left blank.

Chapter 4

Network Applications

The ZXR10 ZSR V2 can be used as an egress gateway in enterprise networks, and used in enterprise headquarters and branch access networks, convergence and access networks of vertical industrial networks, and telecom operators' CPE and DCN networks.

Table of Contents

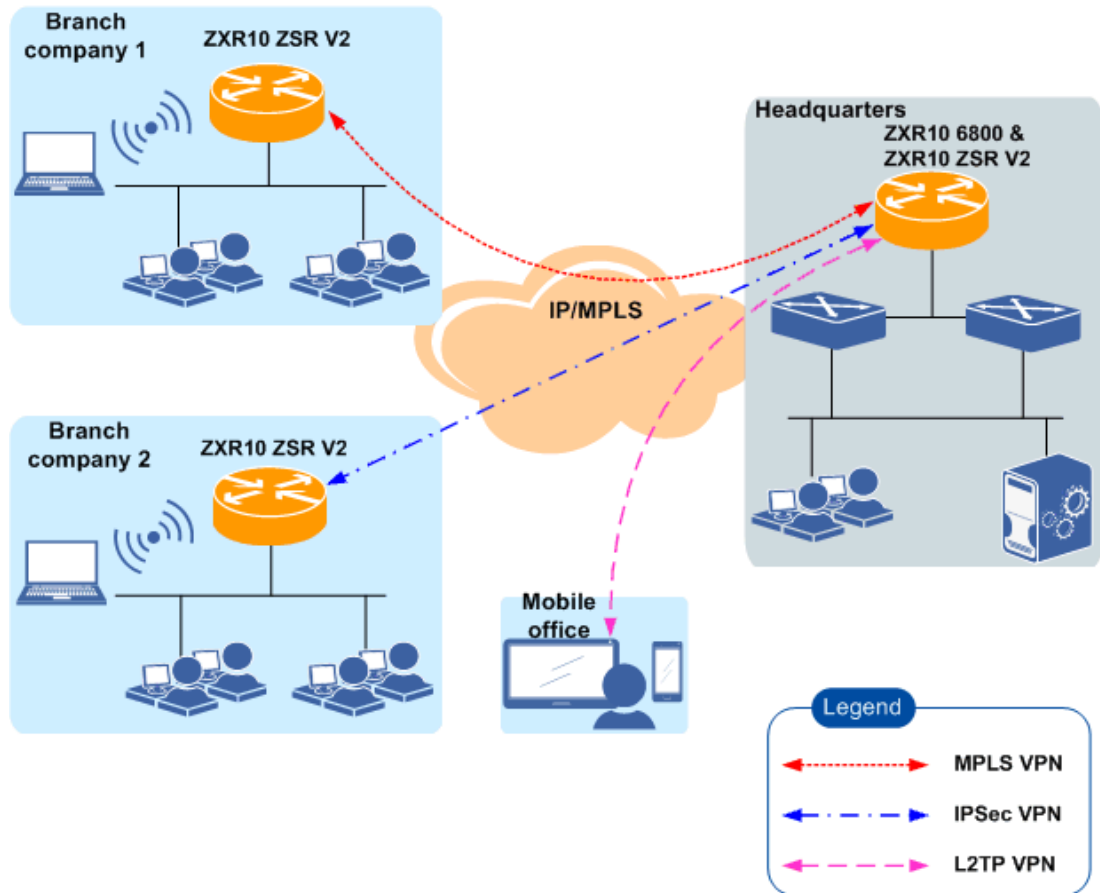
Application Scenario of Access Networks of Enterprise Headquarters and Branches	4-1
Application Scenario of Egress Gateways in Enterprise Networks	4-2
Application Scenario of Convergence and Access Networks of Industry Networks	4-4
Application Scenario of Telecom Operators' DCN Networks	4-5

4.1 Application Scenario of Access Networks of Enterprise Headquarters and Branches

As a router in access networks of headquarters and branches in small/medium-size enterprises, the ZXR10 ZSR V2 provides both network connections for NEs inside enterprises, and access to external WANs and enterprise VPNs, thus ensuring that enterprise users can access both the Internet and enterprise networks rapidly, securely and reliably.

Figure 4-1 shows a typical access network of enterprise headquarters and branches.

Figure 4-1 Access Network of Headquarters and Branches of a Small/Medium-Size Enterprise



As shown in Figure 4-1, the ZXR10 ZSR V2 provides the following functions:

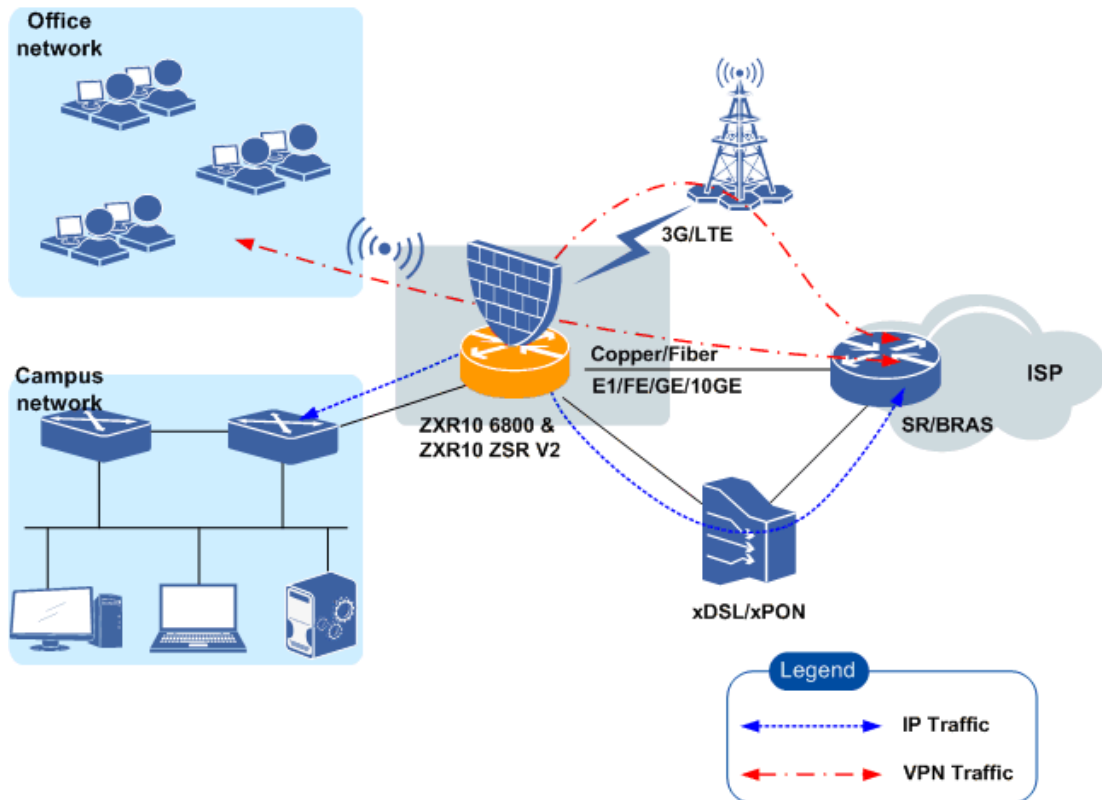
- Through Wi-Fi connections, high-density L2/L3 Ethernet boards, or connected switches, the ZXR10 ZSR V2 can connect to IP network devices inside enterprises, such as PCs, printers, and servers.
- Through multiple wired/wireless links, the ZXR10 ZSR V2 can perform active/standby switchover or load balancing, thus improving both network availability and network bandwidth usage through the intelligent routing technology.
- By using VPN technologies, such as IPSec, GRE, and MPLSVPN, the ZXR10 ZSR V2 ensures secure access between branches and the headquarters of an enterprise.

4.2 Application Scenario of Egress Gateways in Enterprise Networks

As an egress gateway in small/medium-size enterprise networks, small/medium-size campus networks, and other specialized networks, the ZXR10 ZSR V2 provides both network connections for internal NEs and high-speed Internet access.

Figure 4-2 shows the typical network architecture of an egress gateway in an enterprise network.

Figure 4-2 Network Architecture of an Egress Gateway in an Enterprise Network



Abbreviations in the above figure are described below:

3G/LTE	3rd generation mobile communications / Long Term Evolution (4G, 4th generation mobile communications)
Copper/Fiber	Copper cable / Optical fiber
SR/BRAS	Service Router / Broadband Remote Access Server
ISP	Internet Service Provider
xDSL/xPON	Digital Subscriber Line of all types / new-generation Passive Optical Network

As shown in Figure 4-2, the ZXR10 ZSR V2 provides the following functions:

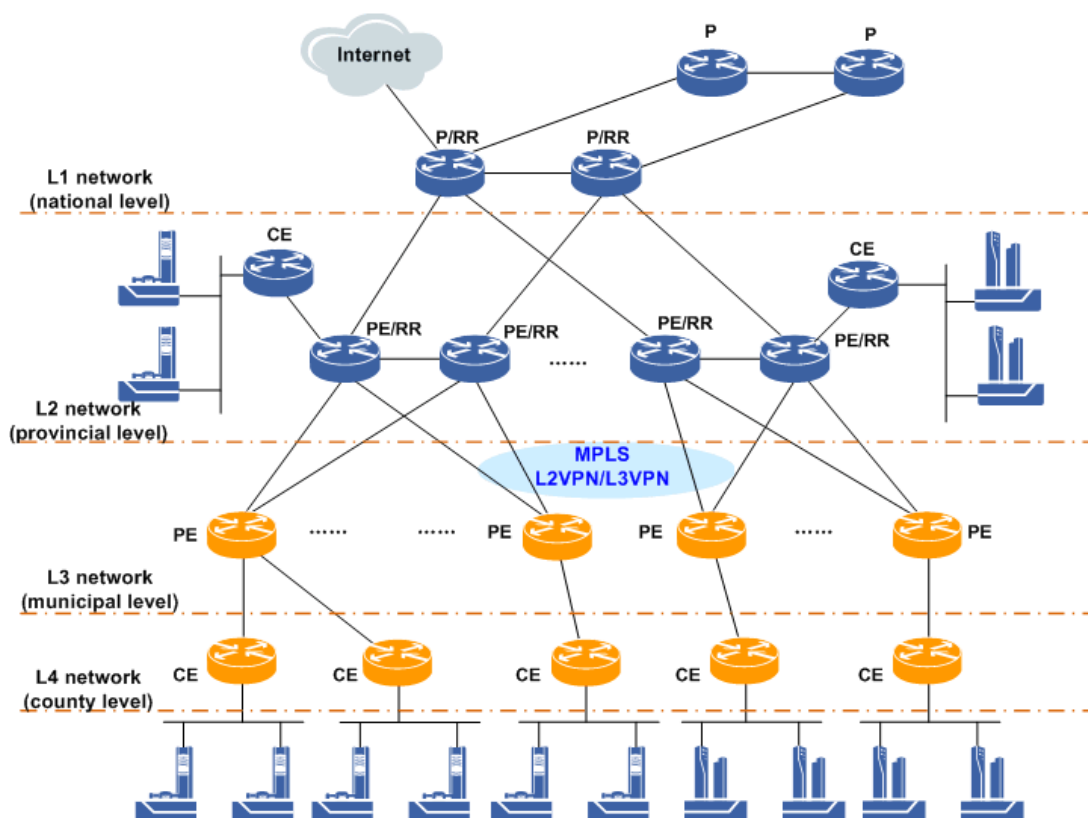
- Through Wi-Fi connections, high-density L2/L3 Ethernet boards, or connected switches, the ZXR10 ZSR V2, as egress gateways in small/medium-size enterprise networks, can connect to IP network devices inside enterprises, such as PCs, printers, and servers.
- The ZXR10 ZSR V2 provides abundant wired/wireless interfaces, including E1 port, serial port, Ethernet port, and POS, xDSL, and 3G/4G interfaces, thus ensuring that the access of branch networks is not restricted by geographical environments.
- Through multiple links, the ZXR10 ZSR V2 can perform active/standby switchover or load balancing, thus improving both network availability and network bandwidth usage.

- By integrating multiple functions of high-performance NATs, firewalls, APs, and switches, the ZXR10 ZSR V2 ensures both secure access authentication for internal users and secure access to external networks.

4.3 Application Scenario of Convergence and Access Networks of Industry Networks

The ZXR10 ZSR V2 can be applied in the convergence and access layer of a vertical industrial network, such as the power, government, and finance industry networks. As shown in Figure 4-3, L3 and L4 networks form a network architecture together with medium/high-end routers in L1 and L2 networks (such as the ZXR10 M6000 and ZXR10 6800 series routers), thus forming an overall solution from the core layer, convergence layer to the access layer.

Figure 4-3 Convergence and Access Networks of an Industry Network



Abbreviations in the above figure are described below:

P/PE/CE	Provider router / Provider Edge router / Customer Edge router
RR	Router Reflector

As shown in Figure 4-3, the ZXR10 ZSR V2 provides the following functions:

- The ZXR10 ZSR V2, together with medium/high-end routers, builds industry networks. By enabling L2/L3 MPLS VPN, the ZXR10 ZSR V2 achieves secure separation between service systems inside enterprises.
- The ZXR10 ZSR V2 supports high-density E1, CPOS3, and POS3/POS12 interfaces, and thus can satisfy convergence and access requirements of different layers in industry networks.

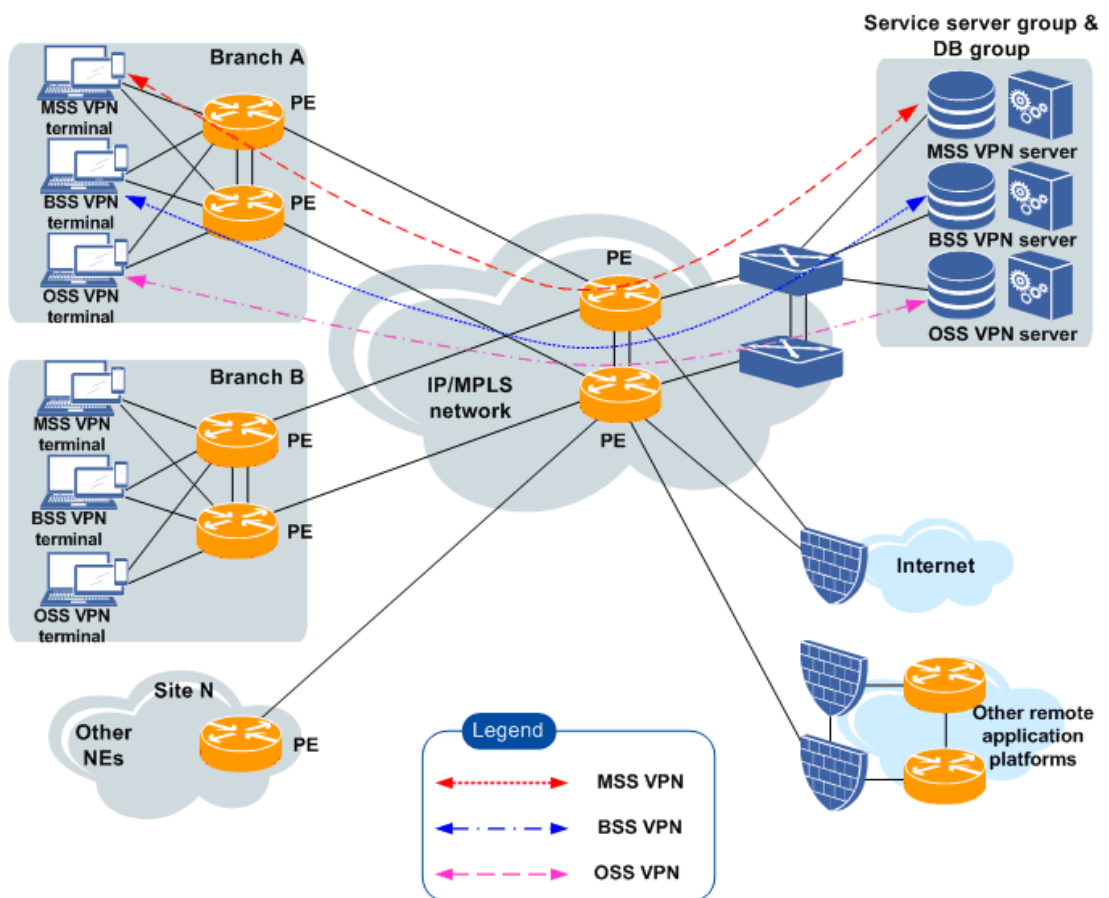
4.4 Application Scenario of Telecom Operators' DCN Networks

As the transmission channels and communication platforms for telecom services, business operations, billing services, NM data transmission, and multimedia communications, telecom operators' DCN networks enable informational and automated supervision, management, maintenance, and decision making upon telecom networks.

The ZXR10 ZSR V2 can be applied in DCN networks, to connect NEs in telecom operators' networks, provide channels or management, maintenance, operation, and internal office of all NEs, and support service deployment.

Figure 4-4 shows a typical DCN network of a telecom operator.

Figure 4-4 Telecom Operator' s DCN Network



Abbreviations in the above figure are described below:

PE	Provider Edge router
MSS	Management Support System
BSS	Business Support System
OSS	Operation Support System

As shown in [Figure 4-4](#), the ZXR10 ZSR V2 provides the following functions:

- As the access router, the ZXR10 ZSR V2, together with other medium/high-end routers, provides the MPLS VPN function, thus achieving secure separation between service systems.
- The ZXR10 ZSR V2 provides reverse Telnet/SSH functions. The ZXR10 ZSR V2 connects to the Console management port of a terminal device through its asynchronous serial port, and provides centralized management upon the terminal device through the reverse Telnet technology.

Chapter 5

Technical Indexes

For the hardware features of the ZXR10 ZSR V2 series products, refer to [Table 5-1](#).

Table 5-1 Hardware Features

Parameter	ZXR10 1800-2S/2S(G)/2S(W)	ZXR10 1800-2E	ZXR10 2800-3E	ZXR10 2800-4	ZXR10 3800-8
Dimension (W × H × D)	380 mm ×43.6 mm ×200 mm	442 mm ×44 mm ×440 mm		442 mm ×80.1 mm ×200 mm	442 mm ×132 mm ×200 mm
Number of SPIU slots	2	2	3	2	4
Number of PIU/DPIU slots	0	0	1/1	2/1	4/2
Fixed interface	2 GE Combo interfaces and 4 GE RJ45 interfaces 2S(W): Wi-Fi interface 2S(G): 3G/LTE interface	WAN: 2×GE Combo ports LAN: 24×GE		MPFUA: 2 GE Combo interfaces and 4 GE RJ45 interfaces MPFUB and MPFUC: 4 GE Combo interfaces and 2 GE RJ45 interfaces	
Memory	2 GB	2 GB	2 GB	2 GB	2 GB
Flash	2 GB	1 GB	4 GB	4 GB	4 GB
USB 2.0	2 USB ports, supporting 3G extension and commissioning through USB	2 USB ports, supporting commissioning through USB	2 USB ports, supporting commissioning through USB	2 USB ports, supporting 3G extension and commissioning through USB	2 USB ports, supporting 3G extension and commissioning through USB
Micro USB	1	1	1	0	0
CONSOLE	1	1	1	1	1
AUX	1	1	1	1	1

Parameter	ZXR10 1800-2S/2S(G)/2S(W)	ZXR10 1800-2E	ZXR10 2800-3E	ZXR10 2800-4	ZXR10 3800-8
Interface type	GE/FE, E1/CE1, V.35/V.24	GE/FE, E1/CE1, V.35/ V.24	GE/FE, E1/CE1, STM-1 POS/CPOS, OC-12/STM-4 POS, ADSL/VDSL, G.SHDSL, V.35/ V.24, 3G/LTE	10GE/GE/FE, E1/CE1, OC-3/STM-1 POS/CPOS, OC-12/STM-4 POS, ADSL/VDSL, G.SHDSL, V.35/ V.24, 3G/LTE	
Power supply	AC: 100 V to 240 V DC: -72 V to -38 V	AC: 100 V to 240 V DC: -72 V to -38 V Supports 1 + 1 redundancy, and supports AC and DC hybrid power supply			
Maximum power	< 55 W	<80 W	<120 W	< 160 W	< 240 W
Operational temperature	-5 °C to 45 °C				
Storage temperature	-40 °C to 70 °C				
Operational humidity	5%–95% (noncondensing)				
Storage humidity	5%–95% (noncondensing)				
MTBF/M-TTR	MTBF: 100000 h MTTR: 0.5 h				

For the software features of the ZXR10 ZSR V2 series products, refer to [Table 5-2](#).

Table 5-2 Software Features

Feature	Description
Supported protocols	L2 protocols: MAC management, VLAN, QinQ, SuperVLAN, Smartgroup, PPP, PPPoE, HDLC, FR, and 802.1x IPv4/IPv6 routing protocols: static routes, RIP/RIPng, OSPF/OSPFv3, IS-IS/IS-ISv6, and BGPv4/BGP4+ Multicast protocols: static multicast, IGMPv1/v2/v3, PIM-DM, PIM-SM, PIM-SSM, MSDP, PIM-SSM mapping, and MLDv1/v2 DHCP: DHCPv4/v6 Relay, DHCPv4/v6 Server, and DHCPv4/v6 Snooping

Feature	Description
MPLS features	Supports LDP, MPLS load sharing, and RSVP-TE Supports MPLS L2/3 VPN, PWE3, Inter-AS Option A/B/C, and 6VPE
VPN features	Supports VPWS, VPLS, HVPLS, 6VPE, GRE, and IPSec
Transition technologies	Supports 6PE, 6VPE, 6in4, 6to4, 4in6, NAT444, NAT64, and 6RD
NAT features	Supports static NAT, dynamic NAT, PAT, multi-egress NAT, NAT ALG, and NAT log
QoS features	Supports H-QoS, QPPB, and time-range QoS Supports flow class, marking, priority inheritance and mapping, traffic shaping, and traffic rate limit Supports PQ, CQ, WFQ, CBWFQ, and physical port based traffic scheduling
3G/LTE features	Supports TD-SCDMA and WCDMA/HSPA+ Supports TDD and FDD LTE
Security features	Supports stateful firewall, control-plane security, CPU security protection, anti-DoS, anti-DDoS, route security, and IPSec encryption Supports MAC and IP binding, anti-ARP attack, MAC address filtering, control of the number of MAC addresses, and control of the number of TCP sessions Supports RADIUS/TACACS+ authentication, uRPF, and SSH
Reliability features	Supports power supply module redundancy, and hot swapping for power supply modules, fan modules, and boards Supports BFD for everything, VRRP, link aggregation FRR, PW redundancy, SDC, and link redundancy
OAM features	Supports Ethernet OAM, MPLS OAM, and SQA Supports commissioning through USB, in-batch management, temperature monitoring, automatic fan speed adjustment, port mirroring, NetFlow V5/V9, and Netflow 1:1 sampling Supports WEB portal, SNMPv1/v2/v3, Telnet, SSHv1/v2, SYSLOG, and RMON

This page intentionally left blank.

Figures

Figure 1-1	External Views of the ZXR10 ZSR V2 Series Products	1-2
Figure 2-1	Main Components on the Front Side of the ZXR10 3800-8 chassis	2-1
Figure 2-2	Front View of the ZXR10 3800-8 chassis	2-2
Figure 2-3	Main Components on the Front Side of the ZXR10 2800-4 chassis	2-2
Figure 2-4	Front View of the ZXR10 2800-4 chassis	2-2
Figure 2-5	Main Components on the Front Side of the ZXR10 1800-2S chassis	2-3
Figure 2-6	Main Components on the Front Side of the ZXR10 1800-2S chassis	2-3
Figure 2-7	Main Components on the Back Side of the ZXR10 1800-2S chassis	2-3
Figure 2-8	ZXR10 2800-3E Appearance	2-4
Figure 2-9	ZXR10 2800-3E Front View	2-4
Figure 2-10	ZXR10 2800-3E Back View	2-4
Figure 2-11	ZXR10 1800-2E Appearance	2-5
Figure 2-12	ZXR10 1800-2E Front View	2-5
Figure 2-13	ZXR10 1800-2E Back View	2-5
Figure 2-14	ZXR10 ZSR V2 Overall Software Structure	2-8
Figure 3-1	IPSec NAT	3-13
Figure 3-2	GRE Over IPSec VPN	3-13
Figure 3-3	IPv6 over IPv4 Tunnel Principle	3-28
Figure 3-4	IPv4 over IPv6 Tunnel Principle	3-29
Figure 3-5	NAT64 Application Scenario	3-30
Figure 4-1	Access Network of Headquarters and Branches of a Small/Medium-Size Enterprise	4-2
Figure 4-2	Network Architecture of an Egress Gateway in an Enterprise Network	4-3
Figure 4-3	Convergence and Access Networks of an Industry Network	4-4
Figure 4-4	Telecom Operator' s DCN Network	4-5

This page intentionally left blank.

Tables

Table 5-1 Hardware Features..... 5-1

Table 5-2 Software Features 5-2

This page intentionally left blank.

Glossary

AAA

- Authentication, Authorization and Accounting

AH

- Authentication Header

ARP

- Address Resolution Protocol

AS

- Autonomous System

CE

- Customer Edge

CHAP

- Challenge Handshake Authentication Protocol

CLNS

- ConnectionLess Network Service

CPE

- Customer Premises Equipment

DCE

- Data Communication Equipment

DCN

- Data Communications Network

DH

- Diffie-Hellman

DHCP

- Dynamic Host Configuration Protocol

DLCI

- Data Link Connection Identifier

DMZ

- Demilitarized Zone

DTE

- Data Terminal Equipment

ESP

- Encapsulation Security Payload

FMC

- Fixed Mobile Convergence

FR

- Frame Relay

FTP

- File Transfer Protocol

H-VPLS

- Hierarchy of VPLS

HDLC

- High-level Data Link Control

IANA

- Internet Assigned Number Authority

IETF

- Internet Engineering Task Force

IGMP

- Internet Group Management Protocol

IGP

- Interior Gateway Protocol

IP

- Internet Protocol

IPCP

- IP Control Protocol

ISO

- International Organization for Standardization

LCP

- Link Control Protocol

LSA

- Link State Advertisement

LSR

- Label Switch Router

MBB

- Make Before Break

MD5

- Message Digest 5 Algorithm

MIB

- Management Information Base

MSTP

- Multi-Service Transport Platform

NAT

- Network Address Translation

NCP

- Network Control Protocol

NSSA

- Not-So-Stubby Area

OSI

- Open System Interconnection

OTN

- Optical Transport Network

PAP

- Password Authentication Protocol

PC

- Personal Computer

PE

- Provider Edge

PFS

- Perfect Forward Secrecy

PIM-SSM

- Protocol Independent Multicast-Source Specific Multicast

PTN

- Packet Transport Network

PVC

- Permanent Virtual Circuit

PW

- Pseudo Wire

RIP

- Routing Information Protocol

RPF

- Reverse Path Forwarding

RSVP-TE

- Resource Reservation Protocol - Traffic Engineering

SDH

- Synchronous Digital Hierarchy

SLA

- Service Level Agreement

SSH

- Secure Shell

SVC

- Switched Virtual Circuit

SrTCM

- Single-rate Three Color Marker

TCP

- Transmission Control Protocol

TFTP

- Trivial File Transfer Protocol

TLV

- Tag, Length, Value

ToS

- Type of Service

TrTCM

- Two-rate Three Color Marker

UDP

- User Datagram Protocol

VC

- Virtual Circuit

VCCV

- Virtual Circuit Connectivity Verification

VPN

- Virtual Private Network

WAN

- Wide Area Network

WDM

- Wavelength Division Multiplexing

WFQ

- Weighted Fair Queuing