RAISECOM

www.raisecom.com

RC959-4FE16E1(-BL) (B)
Product Description
(Rel_02)

Raisecom Technology Co., Ltd. provides customers with comprehensive technical support and services. For any assistance, please contact our local office or company headquarters.

Website: http://www.raisecom.com

Tel: 8610-82883305

Fax: 8610-82883056

Email: export@raisecom.com

Address: Raisecom Building, No. 11, East Area, No. 10 Block, East Xibeiwang Road, Haidian District, Beijing, P.R.China

Postal code: 100094

Notice

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute the warranty of any kind, express or implied.

Preface

Objective

This document describes the RC959-4FE16E1(-BL) Ethernet over PDH in aspects of product overview, product structure, functions and features, management and maintenance, networking and application, technical specifications, and so on. This document helps you quickly understand and know the RC959-4FE16E1(-BL) well.

Version

The following table lists the product versions related to this document.

Product name	Version
RC959-4FE16E1	• Hardware version: RC959-4FE16E1-B Rev.A.0 • System software version: ROS_4.11.1252.RC959-4FE16E1-B

Conventions

Symbol conventions

The symbols that may be found in this document are defined as below.

Symbol	Description
⚠ Warning	Indicate a hazard with a medium or low level of risk which, if not avoided, could result in minor or moderate injury.
⚠ Caution	Indicate a potentially hazardous situation that, if not avoided, could cause equipment damage, data loss, and performance degradation, or unexpected results.
Note	Provide additional information to emphasize or supplement important points of the main text.
Tip	Indicate a tip that may help you solve a problem or save time.

General conventions

Convention	Description
Times New Roman	Normal paragraphs are in Times New Roman.
Arial	Paragraphs in Warning, Caution, Notes, and Tip are in Arial.
Boldface	Buttons and navigation path are in **Boldface**.
Italic	Book titles are in *italics*.
`Lucida Console`	Terminal display is in `Lucida Console`.
Book Antiqua	Heading 1, Heading 2, Heading 3, and Block are in Book Antiqua.

Change history

Updates between document versions are cumulative. Therefore, the latest document version contains all updates made to previous versions.

Issue 02 (2012-12-30)

Second commercial release

- Modified the voltage range of the AC power and DC power.

Issue 01 (2012-03-15)

Initial commercial release

Contents

Figures

Tables

1 Overview

This chapter is an overview of the RC959-4FE16E1(-BL), including the following sections:

- Introduction
- Characteristics

1.1 Introduction

The RC959-4FE16E1 Ethernet over PDH (herein and after referred to as RC959-4FE16E1) is a new-generation and low-capacity EoPDH. It is developed by Raisecom to implement Ethernet service access and aggregation for enterprise leased line by making full use of SDH/PDH cable resources.

Designed to access Ethernet service with bandwidth ranging from 2 Mbit/s to 32 Mbit/s, the RC959-4FE16E1 supports abundant Ethernet features. In addition, the RC959-4FE16E1 provides flexible networking modes to form a network with other Raisecom devices. It provides you with multiple Ethernet access solutions to meet your differentiated requirements.

According to transmission-side E1 interface types, RC959-4FE16E1 is divided into RC959-4FE16E1-BL (balanced) and RC959-4FE16E1 (unbalanced). The appearances for these two devices are shown in the following figures.

Figure 1-1 RC959-4FE16E1-BL appearance

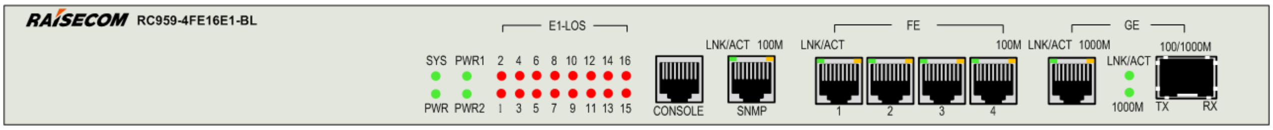
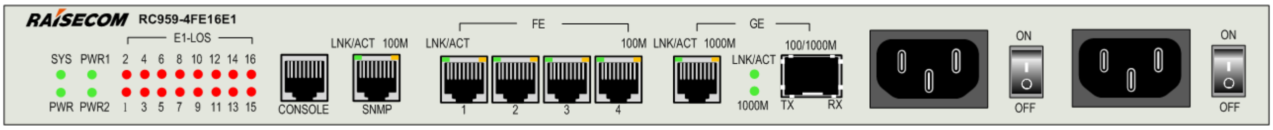


Figure 1-2 RC959-4FE16E1 appearance



Note

If there is no special statement, the RC959-4FE16E1 shown in the following text represents both RC959-4FE16E1-BL and RC959-4FE16E1.

1.2 Characteristics

1.2.1 Powerful compatibility

The RC959-4FE16E1 adopts the EoP chip developed by Raisecom and supports EoPDH international standard (ITU-T G.8040) and GFP encapsulation. Compared with HDLC encapsulation, RC959-4FE16E1 with GFP encapsulation can meet international connectivity standard and network management technology standard, making switching devices from different vendors communicate with each other and be managed centrally.

Not only can RC959-4FE16E1 communicate with other Raisecom GFP switching devices (RC958/RC906G family), the RC959-4FE16E1 can communicate with GFP switching devices from other famous vendors, including ETH-E1 single-way switching devices and ETH-E1 multi-way switching devices.

1.2.2 Flexible topology modes

The RC959-4FE16E1 supports both point-to-point and point-to-multipoint topology modes.

- In point-to-point topology mode, the RC959-4FE16E1 is deployed on both ends of the transmission network to transmit Ethernet service between the head and branches or between branches. The RC959-4FE16E1 can distinguish different services or separate different users by dividing VLAN.
- In point-to-multipoint topology mode, the RC959-4FE16E1 can either be deployed on the local as an aggregator or can be deployed on the remote as a remote demarcation.
  - When deployed on the local, together with the RC958 series on the remote, the RC959-4FE16E1 can make the head aggregate Ethernet services from branches.
  - When deployed on the remote, together with the RC959-GESTM1, the RC959-4FE16E1 can make branches access high-bandwidth Ethernet services.

1.2.3 Abundant management and maintainance functions.

Management functions

The management modes supported by the RC959-4FE16E1 are listed in the following table.

Table 1-1 Management modes

Item	Description
Console interface local management	Manage the device locally by connecting configuration lines.
Telnet remote management	Manage the device remotely with Telnet protocol.
NMS management	Use SNMP to manage the device remotely through NMS. It has friendly GUI and powerful management function.
Remote management	Use extended OAM protocol to manage remote devices.

Maintenance functions

The maintenance modes supported by the RC959-4FE16E1 are shown in the following table.

Table 1-2 Maintenance modes

Item	Description
Ethernet OAM	• EFM: implement point-to-point Layer2 link maintenance and support IEEE 802.3ah standard. • CFM: implement end-to-end Layer2 network maintenance and support IEEE 802.1ag and ITU-T Y.1731 standards. • SLA: implement real-time network performance detection and statistics, including delay, jitter and packet loss ratio.
Loopback	• Support local and remote loopback detection on E1 interface. • Support loopback detection on Ethernet interface.
BERT	Support embedded E1 BERT.
System log	Support recording system information and debugging information in logs and send it to specified destination.
CPU monitor	Monitor task status and CPU utilization in real time.

2 System structure

This chapter describes system structure of the RC959-4FE16E1(-BL), including the following sections:

- Hardware structure
- Software structure

2.1 Hardware structure

2.1.1 Appearance

According to transmission-side E1 interface types, the RC959-4FE16E1 is divided into the RC959-4FE16E1-BL (balanced) and the RC959-4FE16E1 (unbalanced). The RC959-4FE16E1-BL (balanced) is shown in Figure 2-1 and the RC959-4FE16E1 (unbalanced) is shown in Figure 2-2.

Figure 2-1 RC959-4FE16E1-BL front and rear appearances

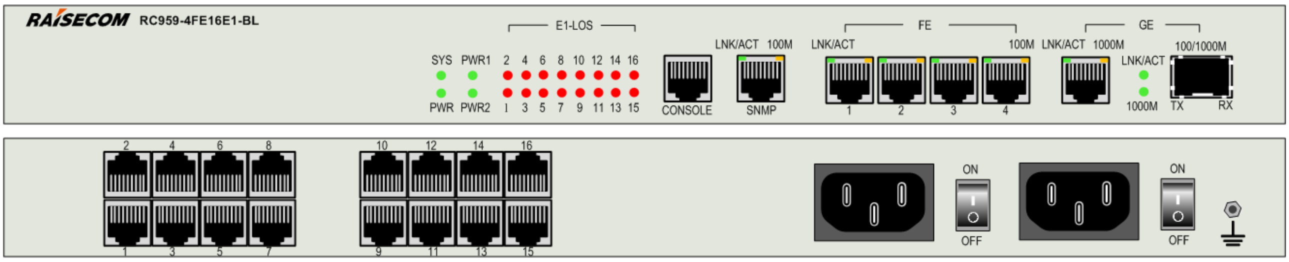
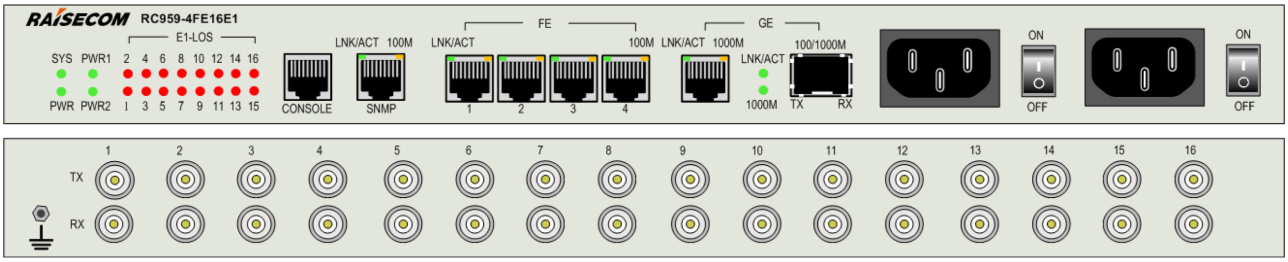


Figure 2-2 RC959-4FE16E1 front and rear appearances



LEDs for the RC959-4FE16E1 balanced and unbalanced devices are same, as listed in Table 2-1.

Table 2-1 LEDs

LED	Description	
SYS	• Blinking green: CPU is operating properly. • Off: CPU is operating abnormally.	
PWR/PWR1/PWR2	• Green: the power supply is normal • Off: the power supply is abnormal.	
E1-LOS(1~16)	• Red: E1 interface loses signals. • Off: E1 interface receives signals normally.	
SNMP	LNK/ACT	• Green: the link is successfully connected. • Blinking green: data are transmitted on the interface. • Off: the link is unsuccessfully connected.
	100M	• Green: the interface rate is 100Mbit/s. • Off: he interface rate is 10Mbit/s.
FE	LNK/ACT	• Green: the link is successfully connected. • Blinking green: data are transmitted on the interface. • Off: the link is unsuccessfully connected.
	100M	• Green: the interface rate is 100Mbit/s. • Off: he interface rate is 10Mbit/s.
GE	LNK/ACT	• Green: the link is successfully connected. • Blinking green: data are transmitted on the interface. • Off: the link is unsuccessfully connected.
	1000M	• Green: the interface rate is 1000Mbit/s. • Off: he interface rate is 100Mbit/s.

2.1.2 Power supply

The RC959-4FE16E1 supports dual power supply backup and 3 power supply combination modes, as listed in Table 2-2.

Table 2-2 Power supply connection modes

Power	Description
Dual AC power	Provide two AC power interfaces. The rated voltage for all interfaces is 100–240V.
Dual DC power	Provide two direct current (DC) power supply interfaces. The rated voltage for all interfaces is -48 V, and the voltage range is -36 to -60 V.
AC+DC	Provide an AC power interface and a DC power interface. • The rated voltage for AC power interface is 100–240V. • The rated voltage for DC power interface is -48 V, and the voltage range is -36 to -60V.

2.1.3 Interfaces

Except the transmission-side E1 interface, the RC959-4FE16E1-BL and the RC959-4FE16E1 support same interfaces, as listed in Table 2-3.

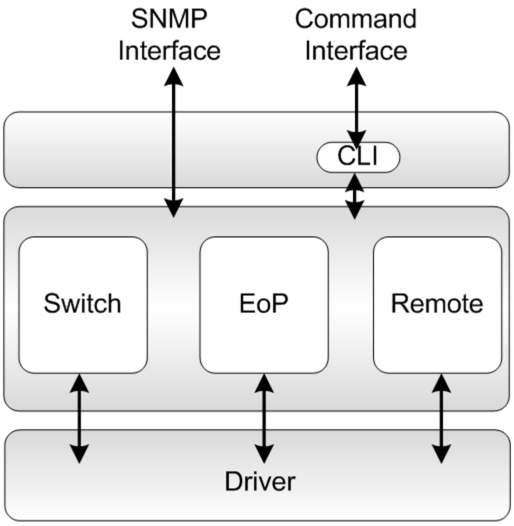
Table 2-3 Interfaces

Item	Interface	Type	Description
User-side interface	FE electrical interface	RJ45	Be used to access user-side Ethernet services.
	GE electrical interface	RJ45	Be used to access user-side Ethernet services.
	GE optical interface	SFP	Be used to access user-side Ethernet services.
Transmission -side interface	E1 balanced interface	RJ45	Be used to connect transmission-side E1 lines to transmit services to SDH network.
	E1 unbalanced interface	BNC	
Assistant interface	Console interface	RJ45	Be used to configure or debug locally.
	SNMP interface	RJ45	Be used to transmit NMS information.

2.2 Software structure

The software structure of the RC959-4FE16E1 is divided into three parts. The lower level is the driver module. The middle is the function module, including switch, EoP and remote management modules. The upper is the user interface module.

Figure 2-3 Software structure



Description of the RC959-4FE16E1 software structure is listed in Table 2-4.

Table 2-4 Software structure

Module	Description
Driver	A functional module used to drive hardware to work.
Switch	• Configure Ethernet interface attributes, and make a performance statistics on Ethernet interface. • Support switching function and Ethernet features, such as VLAN, QinQ, transparent transmission of Layer2 protocol, ACL, QoS, link aggregation, loopback detection, storm control, interface protection, port mirror and so on.
EoP	• PDH interface module: configure frame modes, timeslots, loopback detection, error code detection and clocks on E1 interface; make a performance statistics on E1 interface; check LOS, AIS, LOF, LOMF and CRC alarms. • VCG management module: add/delete VCG members; enable/disable the LCAS function; check LOM, SQM alarms and alarms for failing to receive SQ and CRC.
Remote management	Configure and manage the remote with extended OAM.
SNMP interface	Provide you with an interface to manage the RC959-4FE16E1. In this mode, the RC959-4FE16E1is managed by the NMS.
Command line interface (CLI)	Provide you with an interface to manage the RC959-4FE16E1. In this mode, the RC959-4FE16E1 is managed by the Console interface.

3 Features

This chapter describes features of the RC959-4FE16E1(-BL), including the following sections:

- EoP features
- Ethernet features

3.1 EoP features

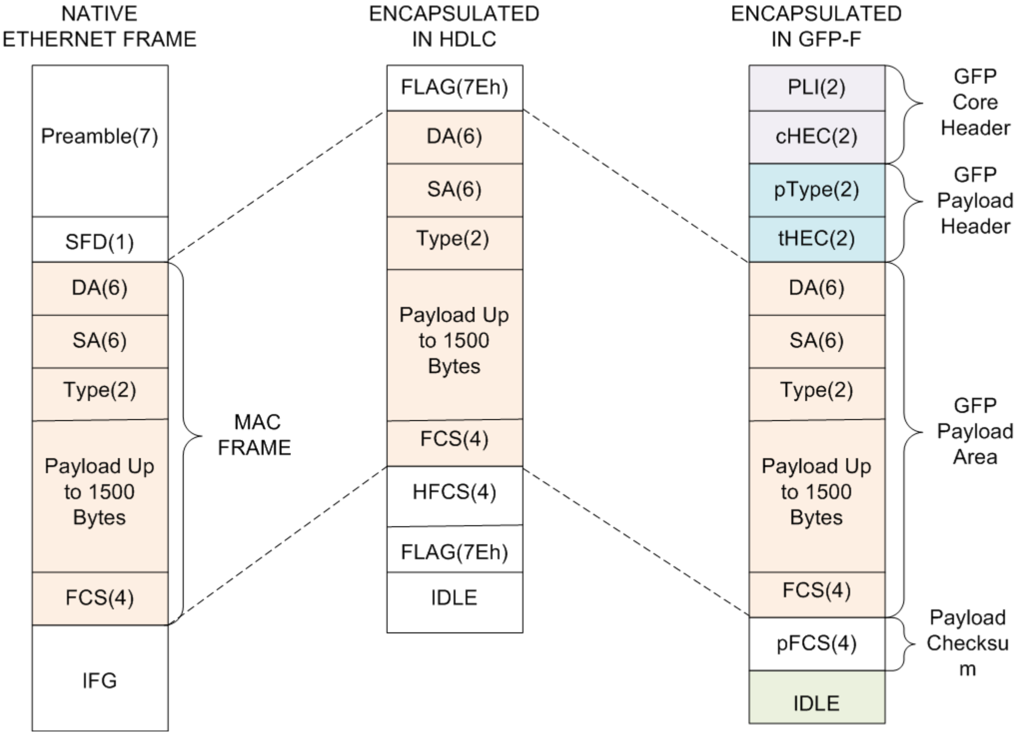
The RC959-4FE16E1 adopts an EoP chip developed by Raisecom. It strictly complies with ITU-T G.7041, G.7042, G.7043, and G.8040 standards. By adopts GFP encapsulation, it implements ETH-one-way E1 mapping and ETH-multiway E1 mapping, and supports LCAS.

3.1.1 GFP encapsulation

Ethernet encapsulation refers to putting Ethernet frames as payload in non-Ethernet frames for transmission. There are multiple encapsulation technologies, such as HDLC, LAPS, and GFP, which can be theoretically used in EoP; however, GFP encapsulation has the following advantages over HDLC/LAPS encapsulation:

- Figure 3-1 describes the format comparison among native Ethernet frame, HDLC frame and GFP frame. HDLC frame has a flag (Flag, 0x7E) to denote the start and end of a frame. Usually, this flag will extend the bandwidth, because HDLC must substitute the escape sequence with a longer escape sequence. Therefore, in GFP encapsulation, you can realize stable and predictable payload throughput and guarantee the throughput committed to customers.
- The number of bytes in the GFP frame is in accordance with the one in the Ethernet frame. And the place where the Ethernet MAC frame stays in the GFP frame is same to that in the native Ethernet frame. However, HDLC frame has a different place for the Ethernet MAC frame. Therefore, GFP encapsulation is much simpler to be re-synchronized.

Figure 3-1 Comparing GFP and HDLC encapsulation formats



The GFP encapsulation process is shown as below:

Step 1 Discard the Preamble (7) and SFD (1) in the native Ethernet MAC frame.

Step 2 Take the rest contents as the payload and add them to GFP payload area.

Step 3 Add overhead byte such as PLI and cHEC (PLI and cHEC are used for frame alignment, and make up completed GFP frame.

3.1.2 Mapping processes

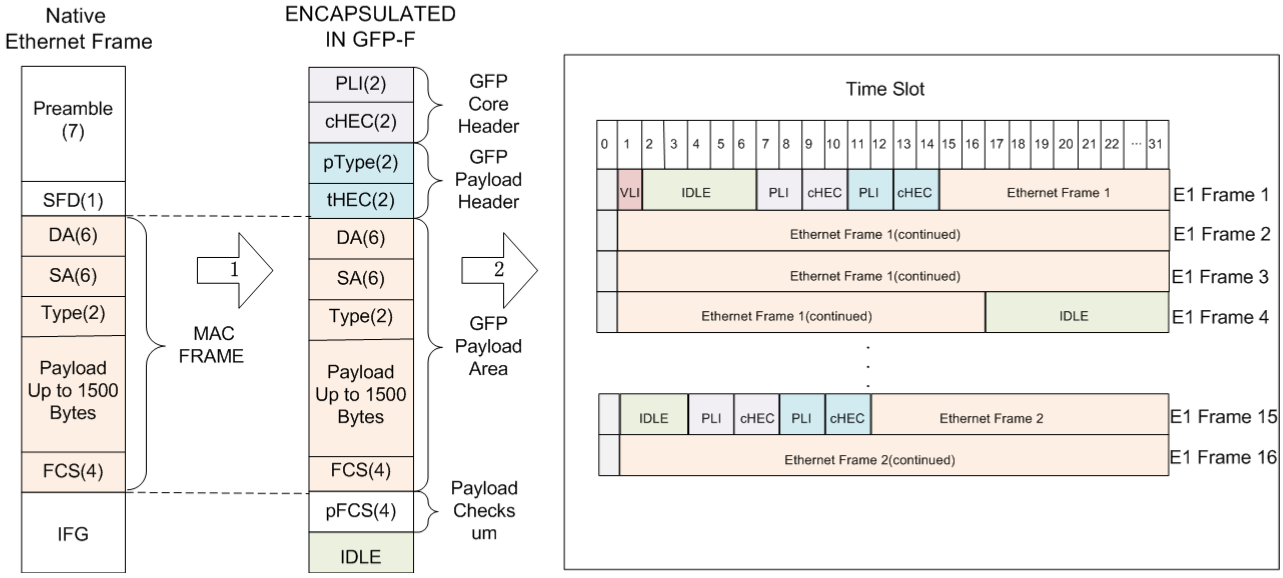
Mapping processes from GFP frames to E1 frames is divided into Eth-E1 one-way mapping and Eth-E1 multiway mapping.

ETH-one-way E1 mapping process

The process that GFP frame is mapped to one-way E1 container is shown as below:

- As shown in Figure 3-2, the E1 container adopts framed mode, uses TS0 as the frame header, and transmits service by using the multiframe that consists of 16 single frames. The TS1 of the first frame in every E1 multiframe is used as VLI, so the payload area of the first frame should start from TS2. The payload area of the rest 15 single frames starts from TS1. VLI is used to transmit VCAT and LCAS information, which is not involved in the ETH-one-way E1 mapping process. However, it takes actual effect in the ETH-multiway E1 mapping process. Therefore, in one-way E1 mapping process, the value of VLI is 0x00.
- "Transmit" encapsulated GFP frames to the payload area of E1 container byte by byte. Every frame in the E1 container consists of 32 bytes. The Ethernet inter-frame gaps (GFP inter-frame gaps) are padded with IDLE.

Figure 3-2 ETH-one-way E1 mapping process

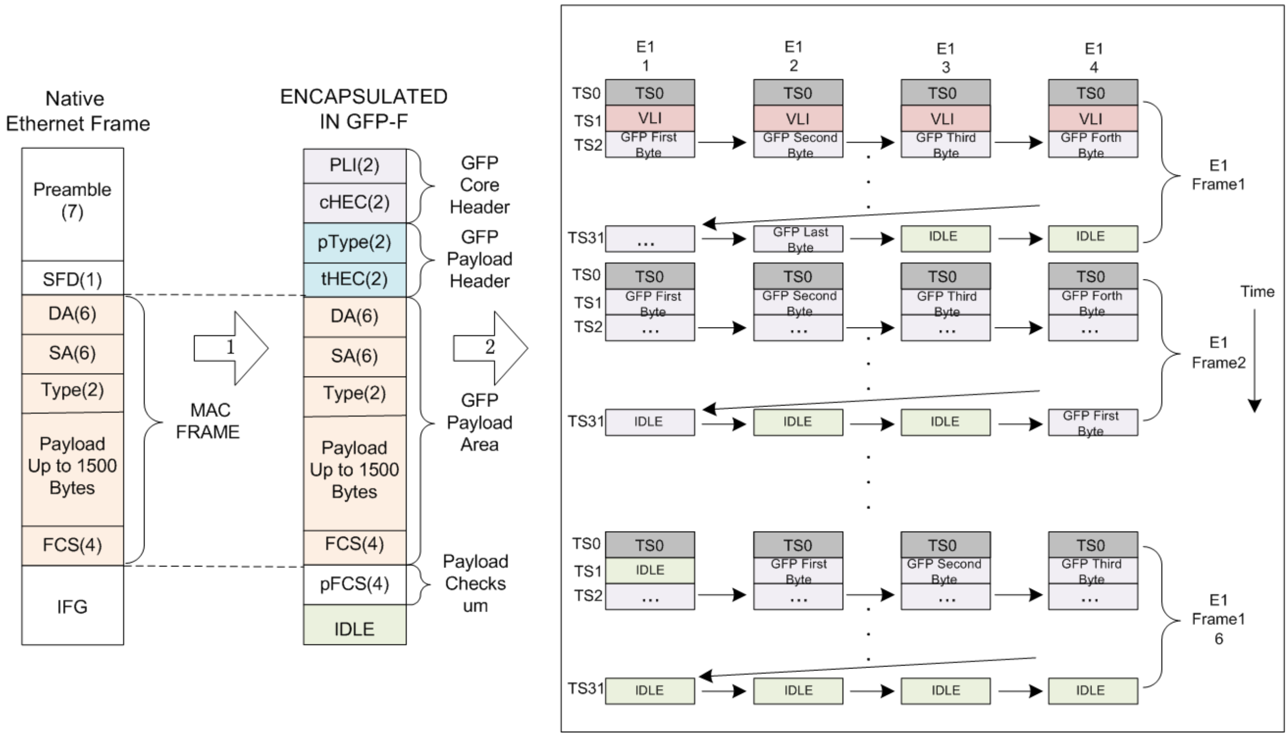


ETH-multiway E1 mapping process

ETH-multiway E1 mapping refers to mapping one-way ETH signals to N-way E1 container. The N-way E1 container will bind and transmit these signals to enlarge transmission bandwidth.

ETH-multiway E1 mapping is called VCAT. N-way E1 is called VCG.

Figure 3-3 ETH-multiway E1 mapping process



The process that GFP frame is mapped to multiway E1 container is shown as below:

Step 1 As shown in Figure 3-3, the E1 container adopts framed mode, uses TS0 as the frame header, and transmits service by using the multiframe that consists of 16 single frames. The TS1 of the first frame in every E1 multiframe is used as VLI, so the payload area of the first frame should start from TS2. The payload area of the rest 15 single frames starts from TS1.

Step 2 Sequently map the encapsulated GFP frames to payload area of all members in a VCG in a way of interleaving bytes. For example, the first byte of GFP frame PLI (1) is mapped to TS2 of the first frame in E1-1. The second byte PL (2) is mapped to TS2 of the first frame in E1-2, and so on. The GFP inter-frame gaps are padded with IDLE.

3.1.3 LCAS

Multiway E1 protocol converters use VCAT technology to increase bandwidth, but VCAT technology has some problems:

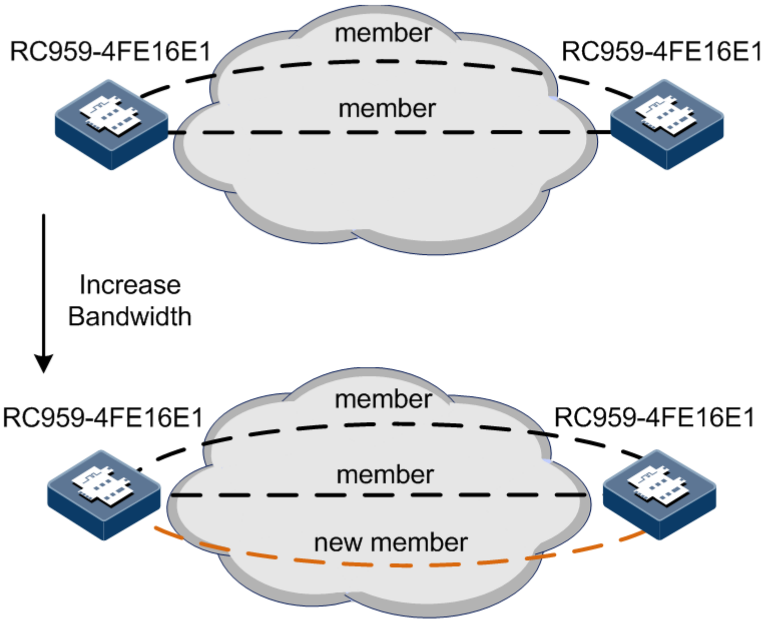
- Upon establishing service, if the bandwidth is adjusted, the service will be influenced.
- If any physical channel in the VCG fails, the whole VCG will be invalid. And the service will be interrupted.

Link Capacity Adjustment Scheme (LCAS) can address these problems by dynamically adjusting bandwidth and protecting VCAT service.

Dynamically adjusting bandwidth

As shown in Figure 3-4, you can increase link bandwidth by adding members to a VCG. Conversely, you can decrease link bandwidth by deleting members from a VCG. Meanwhile, the service will be interrupted when LCAS dynamically adjusts bandwidth.

Figure 3-4 LCAS dynamically adjusting bandwidth



Protecting VCAT services

As shown in Figure 3-5, when the link of the member in a VCG is invalid, LCAS will delete the member. When the link is restored, LCAS will automatically add this member again.

Because LCAS deletes invalid members, the bandwidth will be decreased. But it must ensure services cannot be interrupted when the channel fails.

Figure 3-5 Protecting LCAS VCAT services

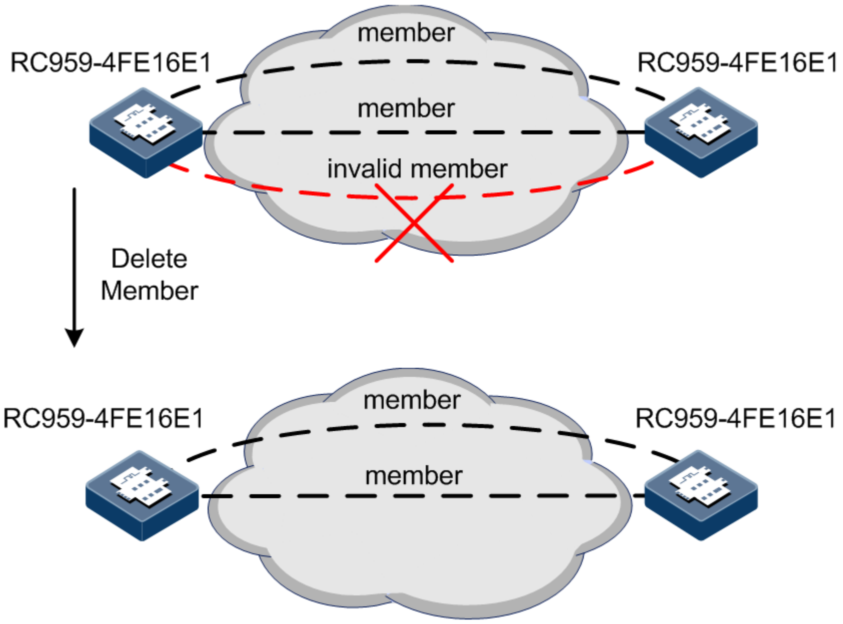


Table 3-1 lists virtual cascading features supported by the RC959-4FE16E1.

Table 3-1 Virtual cascading features

Feature	Description
VCG	Support up to 16 VCGs.
Virtual cascading member	A VCG supports up to 16 members.
LCAS	Supported
VCG alarma and statistics	Supported

3.2 Ethernet features

The RC959-4FE16E1 supports abundant Ethernet features.

3.2.1 VLAN

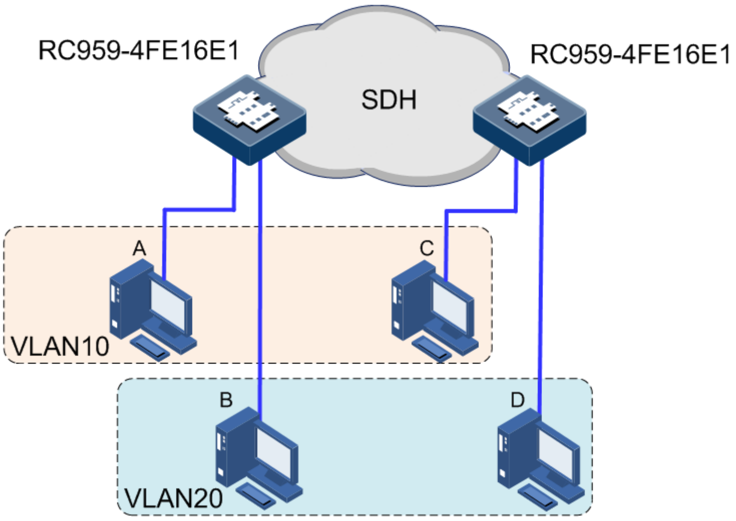
In the Local Area Network (LAN), all hosts are in the same broadcast domain. So the broadcast packets in the LAN will be continuously forwarded by Layer2 devices, forming a broadcast storm and influencing the network performance.

The VLAN technology can partition a physical LAN into different broadcast domains (VLAN) in logic. Hosts in the same VLAN can directly access to each other, while hosts in different

VLANs cannot directly communicate with each other. Therefore, broadcast packets can only be forwarded in a VLAN, avoiding broadcast storms.

Not only can VLAN be used to divide broadcast domains and to avoid broadcast storms, it can also be used to logically partition a large LAN into multiple small independent LANs (VLAN). These VLANs are allowed by geographic location. All small LANs (VLAN) are isolated from each other. As shown in Figure 3-6, A, B, C, D are connected to a large LAN by the RC959-4FE16E1. A and B are in the same place while B and D are in another place. By VLAN, A and C can be grouped into VLAN 10 while B and D are grouped into VLAN 20. These two VLANs are isolated from each other and cannot communicate directly.

Figure 3-6 VLAN application



As shown in Figure 3-7, the VLAN frame is based on native Ethernet. Besides, a VLAN Tag (4) is added before Type (2). A VLAN ID (12) is included in the VLAN Tag to identify and distinguish VLANs. Therefore, there are 4096 (2^{12}) VLANs in total. According to the protocol, 0 and 1095 are reserved VLANs. Therefore, there are 4094 VLANs available.

Figure 3-7 VLAN frame

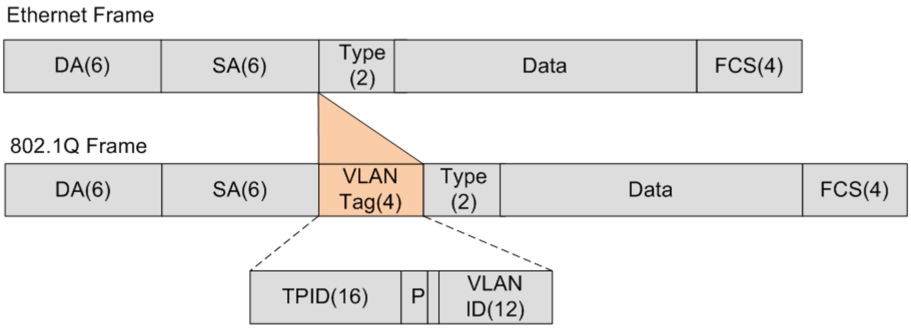
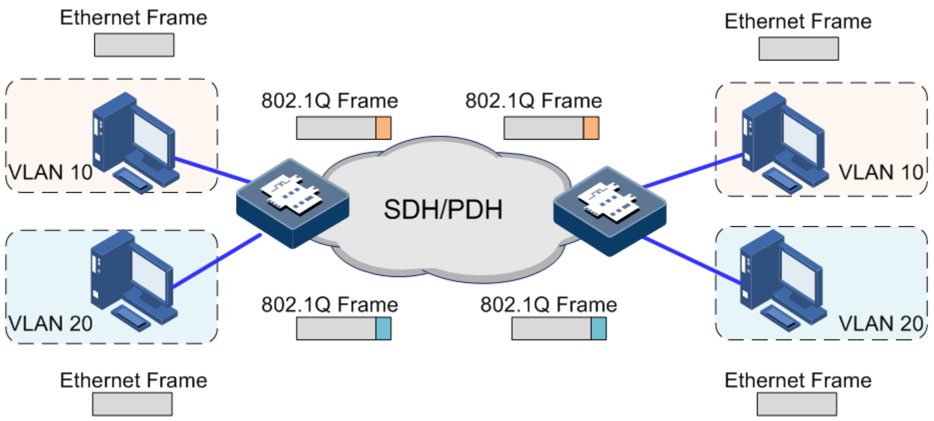


Figure 3-8 describes the VLAN principle. The native Ethernet frame is added with VLAN ID when it accesses to the network through the RC959-4FE16E1. Then the native Ethernet frame becomes 802.1Q frame and is transmitted across the network. The destination removes the VLAN ID and sends the native Ethernet frame to destination users.

Figure 3-8 VLAN principle



3.2.2 QinQ

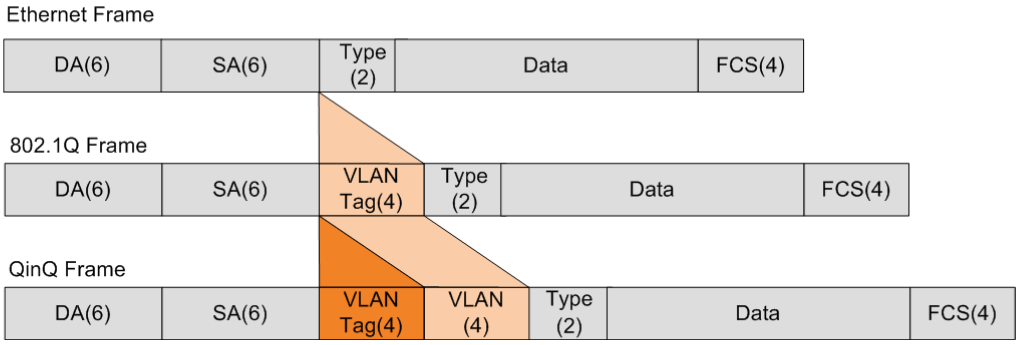
QinQ is the abbreviation of 802.1Q in 802.1Q. QinQ is a Layer 2 tunneling protocol based on the IEEE 802.1Q technology. QinQ encapsulates a private VLAN tag in a public VLAN tag; therefore, a packet traverses the backbone network of the Internet service provider (ISP) carrying double VLAN tags.

Features of QinQ are shown as below:

- QinQ makes the whole network provide a maximum of 4094 ×4094 VLANs, which address low resources of public VLAN ID.
- You can plan your own private VLAN ID, which will not conflict with the public VLAN ID.
- QinQ provides a simple and flexible Layer 2 VPN solution.

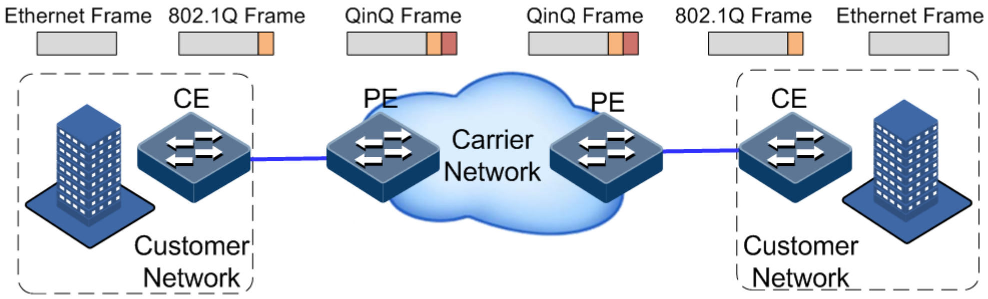
A QinQ frame refers to a frame that is added with another VLAN Tag domain before the VLAN Tag domain of the 802.1Q frame, as shown in Figure 3-9.

Figure 3-9 QinQ frame



QinQ principle is shown in Figure 3-10. The native Ethernet frame is added with a private VLAN ID by Customer Equipment (CE) and is added with a public VLAN ID by Provider Equipment (PE) when accessing to ISP. Then the native Ethernet frame is formed as a QinQ frame. This packet traverses the public network carrying double VLAN tags.

Figure 3-10 QinQ principle



3.2.3 Layer 2 transparent transmission

The Layer 2 transparent transmission function is used to make the Layer 2 protocol packets of the user network traverse ISP network and thus make the Layer 2 protocol run in the user network at different locations.

The transparent transmission function is enabled on the interface that connects edge network device of the carrier and user network. Layer 2 protocol packets of user network enter from transparent transmission interface, are encapsulated by the edge network devices (ingress ends of packets) and then enters carrier network. Packets are transmitted through carrier network to arrive edge devices (egress ends of packets) at the other end or carrier network. Edge devices decapsulate outer Layer 2 protocol packets and transparently transmits them to the customer network.

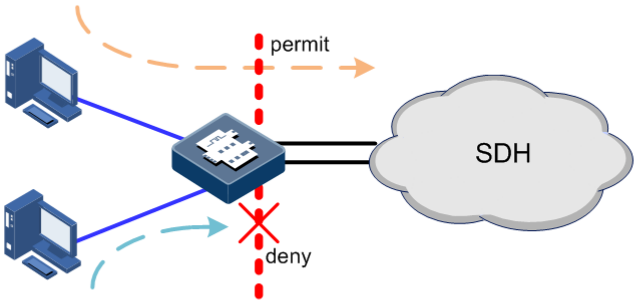
The encapsulation and decapsulation processes are shown as below:

- Packet encapsulation: on the ingress of a packet, the destination MAC address of a Layer 2 protocol packet is replaced with a specified multicast MAC address (the default value is 010E.5E00.0003.). In the carrier network, the modified packet is forwarded as data in a VLAN to which the user belongs.
- Packet decapsulation: on the egress of a packet, the RC959-4FE16E1 sends the packet with specified multicast MAC address (The default value is 010E.5E00.0003.), reverts the destination MAC address to the original address of Layer 2 protocol packet, and then sends the packet to assigned user network.

3.2.4 ACL

ACL refers to a series of rules configured for the RC959-4FE16E1 to filter packets. The rules can decide which packets to be transmitted or discarded as shown in Figure 3-11.

Figure 3-11 ACL



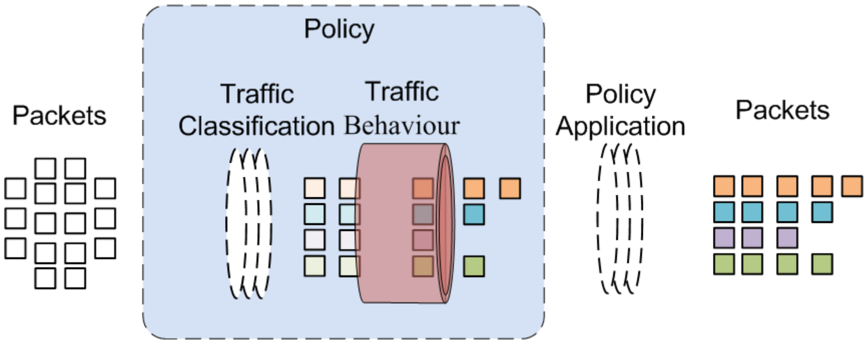
According to the source IP/MAC address, destination IP/MAC address, source port number, destination port number, protocol type and the physical interface number, ACL classifies packets that enter the RC959-4FE16E1. After classification, according to these rules, the RC959-4FE16E1 will decide which packets to be received or rejected.

3.2.5 QoS

Network services are abundant while the network resources are limited. Therefore, network resources may be grabbed. To meet service quality, network manager can use Quality of Service (QoS) to reasonably plan and distribute network resources to use network resources efficiently.

Traffic classification and traffic policy

Figure 3-12 Traffic classification and traffic policy



- Traffic classification refers that the RC959-4FE16E1 categorizes packets according to a series of rules.
- Traffic behavior refers that the RC959-4FE16E1 conducts the QoS process for a certain packet.
- Traffic policy refers that the RC959-4FE16E1 binds the traffic classification and traffic behavior together to conduct the corresponding QoS process for a certain packet.
- Policy application refers that the RC959-4FE16E1 applies defined traffic policy to specified interfaces.

Common traffic behaviours are listed in the following table.

Traffic behavior	Description
Remarking	A certain priority field in the packet is re-marked by the RC959-4FE16E1.
Redirection	The packet is forwarded not according to the corresponding relationship between the destination address and the interface. The packet is redirected to other interfaces for being forwarded.
Policing and shaping	Monitor the rate of the traffic and discard the traffic that exceeds the threshold, limiting the traffic within a proper range.

Priority trust and priority mapping

Priority trust refers that the RC959-4FE16E1 uses the priority of a packet as a classification basis to conduct subsequent QoS management on the packet.

The priorities of trust are shown as below:

- CoS-based priority: fits for 802.1Q packets.
- DSCP-based priority: fits for IP packets.

Modes for priority mapping are shown as below:

- CoS-LocalPriority mapping: the CoS priority is mapped to the local priority.
- DSCP-LocalPriority mapping: the DSCP priority is mapped to the local priority.
- LocalPriority-Queue mapping: the local priority is mapped to an interface queue.

Queue scheduling

Queue scheduling refers that the interface uses different scheduling algorithms to send packets in a queue. According to algorithms, scheduling modes can be divided into SP and WRR.

- In SP mode, packets are strictly scheduled in a descending order of priority. Only when packets with high priority are scheduled, will packets with low priority can get a chance to be scheduled, as shown in Figure 3-13.
- In WRR mode, packets are scheduled in a polling manner according to the weight of the queue. The queue with heavier weight will get more chances to schedule packets, vice versa, as shown in Figure 3-14.

Figure 3-13 SP scheduling

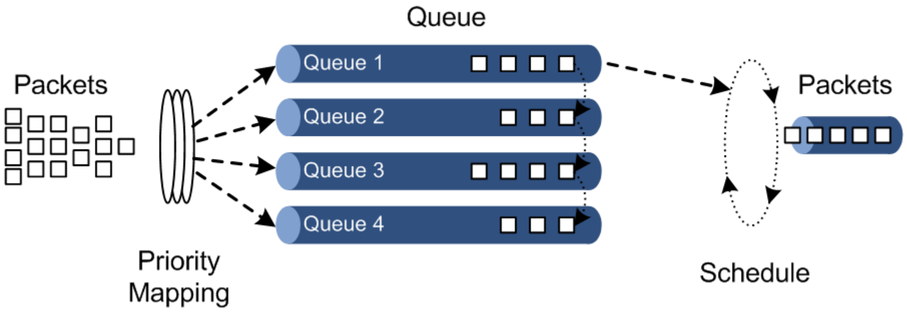
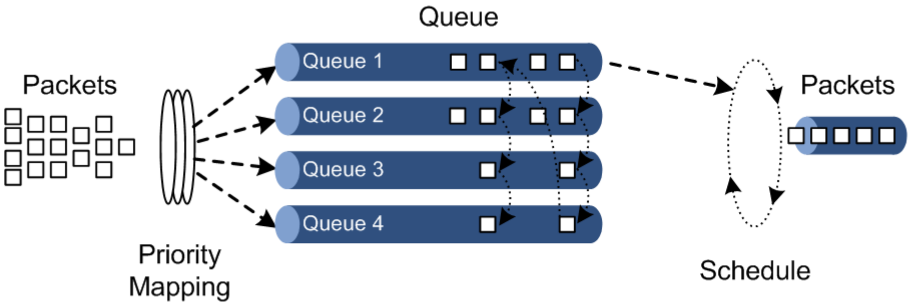


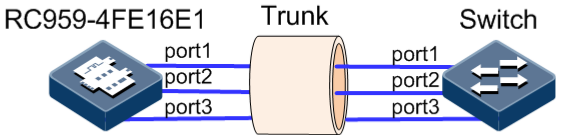
Figure 3-14 WRR scheduling



3.2.6 Link aggregation

Link aggregation is a method of bundling multiple physical links into a logical link, as shown in Figure 3-15. Three Ethernet ports of the RC959-4FE16E1 are connected to three peer Ethernet ports. Three physical links are bundled together to form a Trunk group, where the three ports are member ports of the group.

Figure 3-15 Link aggregation



With the link aggregation function, you can:

- Increase the link bandwidth: because the link aggregation function bundles multiple physical links together, the bandwidth becomes the sum of all the physical link bandwidths. Link aggregation provides you a method to increase link transmission efficiency.
- Improve the link reliability: in a link aggregation group, all members dynamically make backup for each other. When one link fails, other links can do its work quickly to ensure transmitting service properly.

3.2.7 Loop detection

The loop detection function on Ethernet interfaces can detect whether a loopback is generated on the interface regularly. If detecting a loopback, the interface will report Trap alarm and decide whether to close the interface where the loopback is generated. This function can make you quickly discover the existence of an interface loopback to avoid broadcast storms caused by the loopback.

3.2.8 Storm control

When a great amount of broadcast, multicast and unicast packets pass through an Ethernet interfaces, a traffic storm can be formed on the interface, which could lead to network congestion. The storm control function can control the size of the broadcast, multicast and unicast traffics that are allowed to pass through the Ethernet interface, avoiding traffic storms.

3.2.9 Interface protection

Interface protection refers that upon an interface is added to an interface protection group, the Layer 2 and Layer 3 packets between interfaces are isolated and cannot access to each other. However, the interface in an interface protection group can access to the one that is not in the group. Or interfaces that are not added to the interface group can also access to each other. Interface protection function enhances the network security and provides a flexible networking mode.

3.2.10 Port mirroring

Port mirror refers to mirroring packets of the source port to the monitor port without affecting packets forwarding. You can use this function to monitor the receiving and sending status of some port to analyze the network situation.

Figure 3-16 Port mirroring

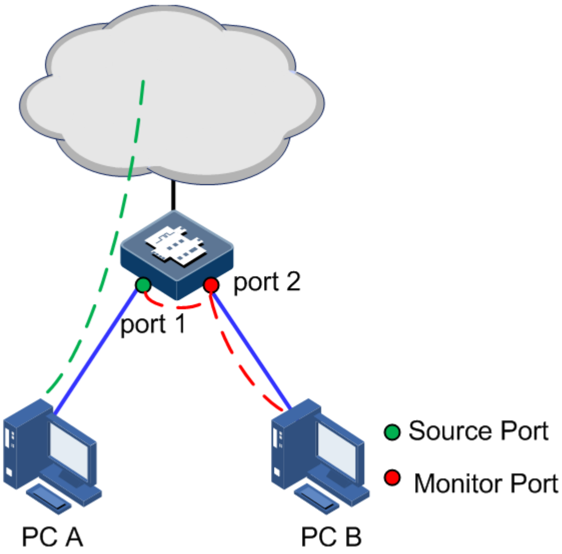


Figure 3-16 describes the principle of the port mirroring function. PC A sends and receives packets through Port 1. To monitor PC A, PC B is connected to Port 2. After enabling the port mirroring function of the RC959-4FE16E1, packets on Port 1 will be copied and mirrored to Port 2. Therefore, PC B can obtain the packets sent or received by PC A.

4 Management and maintenance

This chapter describes management and maintenance of the RC959-4FE16E1(-BL), including the following sections:

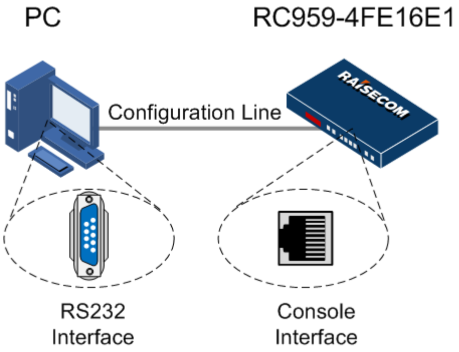
- Product management
- Product maintenance

4.1 Product management

4.1.1 Console interface local management

Console interface local management refers that you can connect the serial port of a PC and the The console interface of the RC959-4FE16E1 with a configuration line, and then use the terminal emulation program of the PC to configure and manage the RC959-4FE16E1, as shown in Figure 4-1. When the RC959-4FE16E1 is powered on for the first time or is maintained locally, you can operate and manage the RC959-4FE16E1 without depending on the network in this mode.

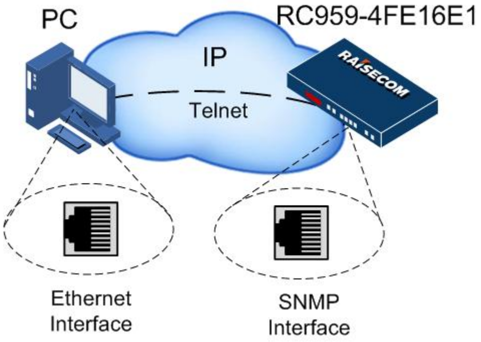
Figure 4-1 Console interface local management



4.1.2 Telnet remote management

Telnet remote management refers that you can connect a port of a PC and the SNMP interface of the RC959-4FE16E1with the network, and then use the Telnet client program of the PC to configure and manage the RC959-4FE16E1, as shown in Figure 4-2. It is a remote management mode, and depends on network to transmit management information. Therefore, in this mode, you must ensure the network is reachable.

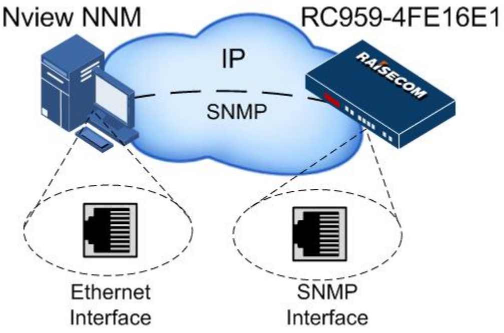
Figure 4-2 Telnet remote management



4.1.3 NMS management

NMS management refers to that you can connect a port of a PC and the SNMP interface of the RC959-4FE16E1 with the network, as shown in Figure 4-3. Differentiated from Telnet remote management, NMS management uses SNMP and you can use professional network management software on the PC to configure and manage the RC959-4FE16E1. This management mode has a friendly graphic user interface (GUI) for convenient and visualized operation. Meanwhile, in this mode, you can collect performance and alarm information in real time, facilitating device management and maintenance.

Figure 4-3 NMS management



SNMP

Simple Network Management Protocol (SNMP) is a widely-used network management protocol. It is used to transmit management information between any two points.

SNMP is divided into Network Management Station (NMS) and Agent. The NMS runs network management software and Agent is the software running on the RC959-4FE16E1. The NMS can send configuration or query packets to Agent and the Agent will reply to these packets. When the RC959-4FE16E1 works improperly or the status is changed, the Agent will actively send Trap to the NMS for reporting alarms or events.

NView NNM

Network Node Management (NView NNM) is a new-generation and comprehensive network node management system developed by Raisecom. NView NNM is based on SNMP and is designed for access network. It is used to address problems such as integrated configuration, fault detection and so on.

NView NNM program adopts Client/Server (C/S) architecture and modular system design. The NView NNM modular system includes the following programmes:

- Server: it is the core of NView NNM network management system. Usually, it is installed on a server which has a high hardware configuration level.
- Database: the database adopts MySQL database management system. Usually, it is installed on a server, which has a high hardware configuration level and can provide a better storage device. Network management topology, alarms, capacity, performance, clients, engineering information and various log messages are saved in the database.

Note

For a larger scale network, the database and the server can be installed on different hosts. In this way, the system efficiency and stability can be improved. At present, NView NNM system only supports MySQL (V5.1.43) database. You can install the MySQL (V5.1.43) database program when installing NView NNM system.

- Performance component: performance component programs include performance server program (PM Server) and performance probe program (PM Probe). These two programs can perform a modular installation according to numbers of devices supporting performance collection. Performance component programs help network administrator to learn the operation status at present or in a past period, such as the load and the traffic. So that it provides evidence for alerting, and troubleshooting network faults and for optimizing network.
- Client: the client is a UGI of NView NNM network management system. Usually, it is installed on the supervisory control computer, charging for reporting service requests and displaying information.

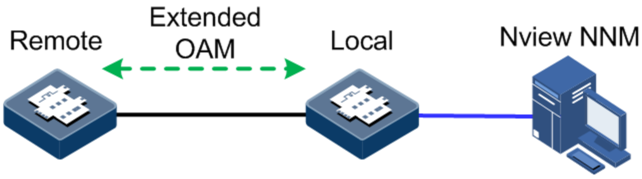
The deploy modes for NView NNM is divided into t standalone deploy mode and distributed deploy mode.

- Standalone deploy mode: in this mode, the NView NNM network system is deployed on a server. It fits for small-scale network. In this mode, costs are reduced. However, because all systems are operated on a server, it provides a higher requirement on hardware configuration of the host.
- Distributed deploy mode: in this mode, modular NView NNM systems are installed on different servers. It fits for large-scale network. In this mode, the database, PM Server and PM Probe are separated from NView NNM server and are installed on different servers. In this way, it shares the hardware process ability of NView NNM server and improves the performance and efficiency.

4.1.4 Extended OAM management

Extended OAM is based on IEEE802.3ah OAM link. It further enhances OAM management function by using standard OAM extendibility. As shown in Figure 4-4, with extended OAM protocol, the local can configure and manage the connected remote device.

Figure 4-4 Extended OAM



Extended OAM supports the following functions:

- Acquire remote attributes: the local can acquire remote attributes, configuration and statistics through extended OAM.
- Configure basic remote functions: the local can configure partial remote functions through extended OAM, including hostname, interface Up/Down, rate, duplex mode, and bandwidth and so on.
- Configure remote NMS: configure related NMS parameters for a remote that supports SNMP NMS, such as IP addresses, default gateway, management IP addresses and read-write community and so on. And then the local can manage the remote through SNMP.
- Remote Trap: when the remote is in Link Up/Down mode, the remote sends extended OAM notification frames to the local, and the local sends remote Trap alarms to NMS.
- Reboot the remote: the local can send commands to reboot the remote.

4.2 Product maintenance

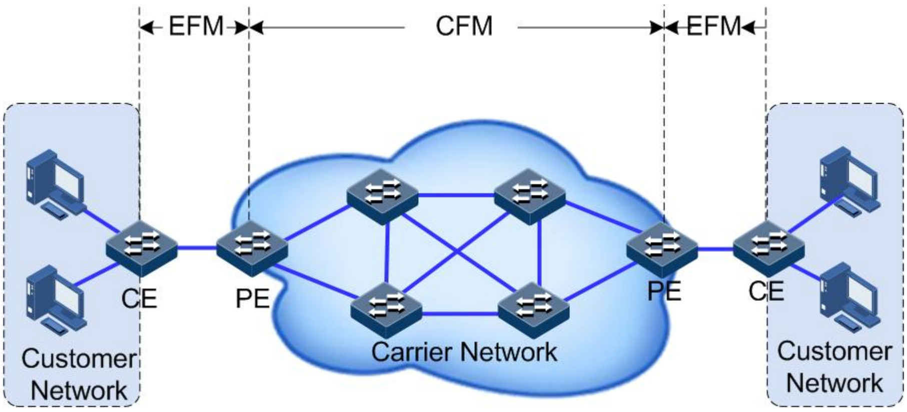
4.2.1 Ethernet OAM

Ethernet operation, administration and maintenance (Ethernet OAM) is a layer2 protocol, used for maintaining Ethernet layer2, detecting service connectivity and locating network faults. In a network, the RC959-4FE16E1 sends OAM packets on MAC level to detect Ethernet links. This method cannot influence other layers and consumes less bandwidth, without influencing services on links.

EFM and CFM

As shown in Figure 4-5, EFM is used to maintain point-to-point Ethernet links between directly connected devices. CFM is used to maintain end-to-end Ethernet links.

Figure 4-5 OAM



Maintenance functions of EFM and CFM are respectively listed in Table 4-1.

Table 4-1 EFM and CFM maintenance functions

Item	Function	Description
EFM	Link performance monitor	The local monitors error code performance on links. When the threshold is exceeded, the error code events will be reported to the peer.
	Fault detection	When finding faults (link faults, dying gasp faults, emergency events), the local will report them to the peer.
	Remote loopback	The local can ask the peer to response to the loopback, and start loopback detection to locate faults.
CFM	Connectivity detection	Detect network link status periodically.
	Loopback detection	Detect any node link status between source end and maintenance domain (MD) to locate faults.
	Layer2 Ping	Based on connectivity detection, test service packet loss ratio and delay.
	Layer2 Traceroute	Based on loopback detection, identify protocol packet route and locate network segments where a fault is generated.
	Performance detection	Calculate packet loss ratio, delay and jitter on a link between two source ends.

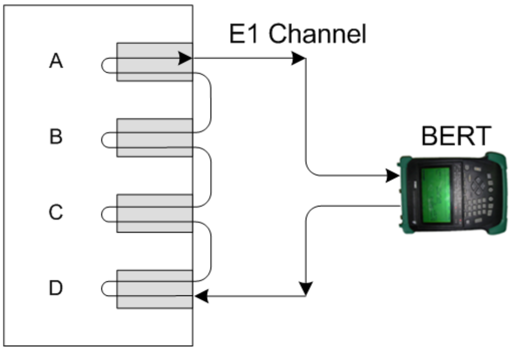
SLA

SLA is an agreement between a customer and a service provider. It is a telecommunication service evaluation standard. Typically, SLA is a real-time network performance detection and statistics technology. It can make a statistics on network performance such as response time, jitter, delay and packet loss ratio, helping you to analyze whether the current performance can meet the signed service agreement.

4.2.2 Loopbacks

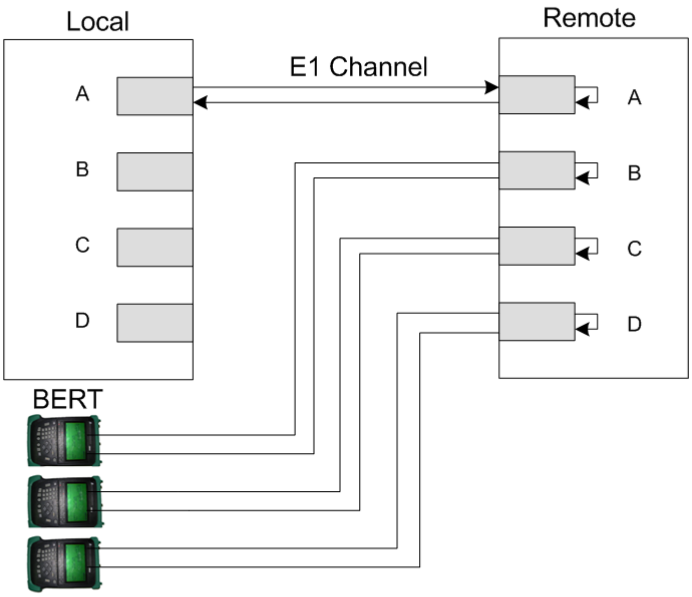
The RC959-4FE16E1 supports local and remote loopbacks on E1 interface.

Figure 4-6 Local loopback



As shown in Figure 4-6, E1 interface local loopback will enable all E1 interfaces to advertise a loopback. Together with connected E1 BERT, it can detect whether there is a fault on E1 interfaces.

Figure 4-7 Remote loopback



As shown in Figure 4-7, when enabling remote loopback on E1 interfaces, ensure at least one E1 link is connected between the local and the remote. E1 interface remote loopback will enable all E1 interfaces to advertise a loopback on the remote. Together with local BERT, it can detect whether there is a fault on E1 interface. In this mode, the maintenance personnel can perform the remote loopback on local.

4.2.3 BERT

The RC959-4FE16E1 supports embedded BERT function to perform error code test on links.

4.2.4 System logs

The system log refers to that the RC959-4FE16E1 records the system information and debugging information in a log and sends the log to the specified destination. When the RC959-4FE16E1 fails, you can check and locate the fault easily.

Destinations for receiving system logs are listed in the following table.

Table 4-2 Destinations for system logs

Destination	Description
Console	Output log messages to the local Console through Console interface.
Host	Output log messages in log files to the host.
Monitor	Output log messages to the monitor, such as Telnet terminal.
File	Output log messages in log files to the Flash.
Buffer	Output log messages to the buffer.

4.2.5 CPU monitor

The CPU monitor function refers that the RC959-4FE16E1can monitor the CUP utilization in real time, helping maintenance personnel locate faults quickly.

Table 4-3 CPU monitor function

Function	Description
Check CPU utilization	● Check dynamic and real-time CPU utilization. ● Check historical CPU utilization within all periods (5 sec, 1 min, 10 min and 2 hour).
CPU utilization threshold alarm	Within a specified sampling period, the system will generate an alarm and send Trap if CPU utilization is over the configured rising threshold or below the declining threshold.

5 Networking applications

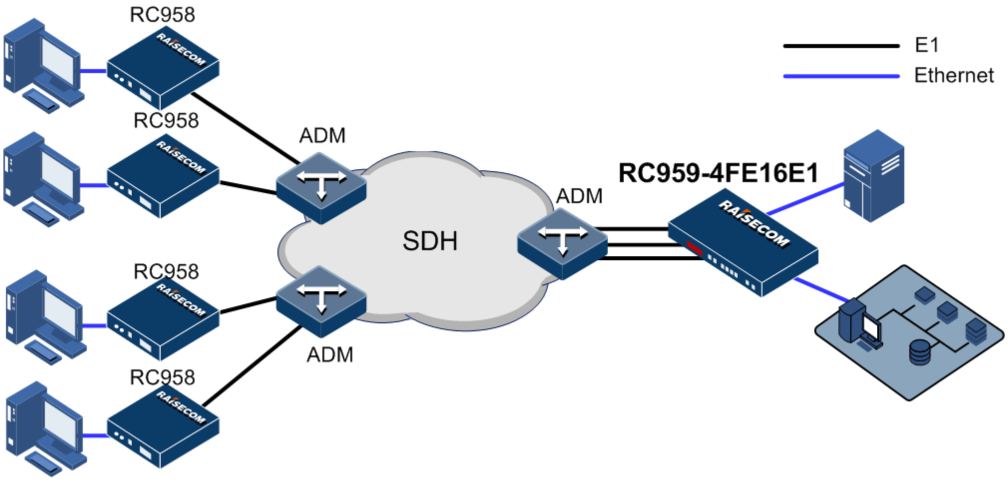
This chapter describes networking applications of the RC959-4FE16E1(-BL), including the following sections:

- Aggregation application
- Point-to-point application
- Remote application

5.1 Aggregation application

The RC959-4FE16E1 can be used as an aggregated interface convertor on local. Its networking topology is shown in Figure 5-1.

Figure 5-1 Aggregation application networking

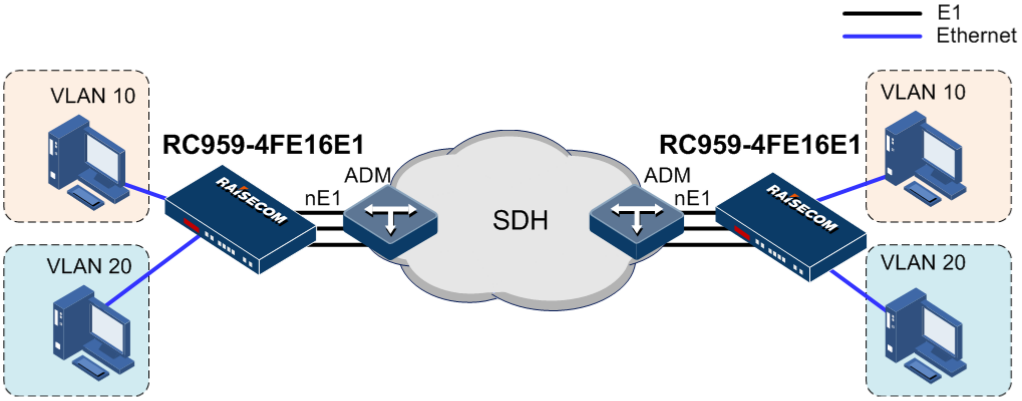


In this networking mode, the local uses the RC959-4FE16E1 as an aggregated device and the remote use RC958 as an Ethernet service access device for branches. The RC959-4FE16E1 supports 16 VCGs at most. In this topology, Ethernet services from four users are transmitted through different VCGs. The bandwidth supported by each VCG ranges from 2M to 32M. However, the total bandwidth of 16 VCGs cannot exceed 32M.

5.2 Point-to-point application

The RC959-4FE16E1 point-to-point application networking is shown in Figure 5-2.

Figure 5-2 Point-to-point application networking

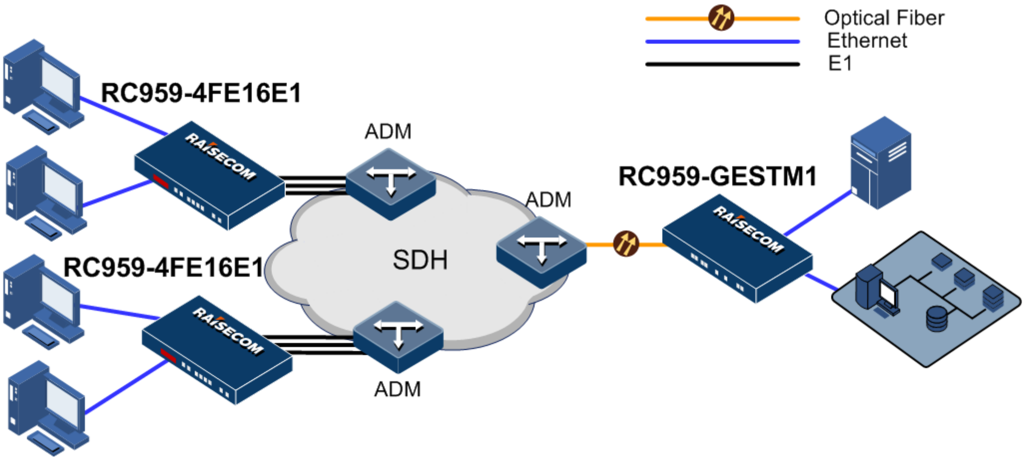


In this networking topology, the RC959-4FE16E1 devices are respectively deployed between head and branches or between branches, making multiple departments connected to each other. In addition, services for different departments are separated by VLAN. All services share a transmission channel with a maximum of 32M bandwidth. In this mode, not only the current transmission resources are protected, costs for networking as well as middle connection nodes are reduced.

5.3 Remote application

The RC959-4FE16E1 can be used as the remote for a network. By working with RC959-GESTM1 on the local, it can meet the high-capacity Ethernet service access requirement, as shown in Figure 5-3.

Figure 5-3 Remote application



In this networking mode, the remote uses the RC959-4FE16E1 to access Ethernet services with a maximum of 32 Mbit/s bandwidth. Besides, it uses VLAN to distinguish different services or users. The local can use RC959-GESTM1 to aggregate more capacity.

6 Technical specifications

This chapter describes technical specifications of the RC959-4FE16E1(-BL), including the following sections:

- Product specifications
- Interface specifications
- Electromagnetic compatibility and lighting protection
- Safety specifications
- Environmental requirements

6.1 Product specifications

Table 6-1 Product specifications

Parameter	Description
Dimension	440 mm (width) × 266 mm (depth) × 1U (height, 1U = 4.45 mm)
Weight	3.55 kg
Power	15W
Power supply	● The rated voltage for AC power interface is 100–240 V. ● The rated voltage for DC power interface is -48 V, and voltage range is -36 to -60 V.

6.2 Interface specifications

6.2.1 FE/GE electrical interface

Table 6-2 FE/GE electrical interface

Parameter	FE electrical interface	GE electrical interface
Interface rate	10/100 Mbit/s	100/1000 Mbit/s
Interface type	RJ45	RJ45
Maximum frame length	9000 bytes	9000 bytes
Duplex mode	Auto	Auto
Flow control	802.3X	802.3X
Auto-MDI	Supported	Supported

6.2.2 GE optical interface

Table 6-3 GE optical interface

Parameter	Description
Interface rate	100/1000 Mbit/s
Interface type	100/1000BASE-FX
Flow control	Supported
ALS	Supported
Performance statistics	Supported

Table 6-4 Detailed Optical interface specifications

Model	Optical interface	Laser type	Receiver type	Wavelength (nm)	Tx power (dBm)	Minimal overload point (dBm)	Rx sensitivity (dBm)	Transmission distance (km)
S1	DSC/PC	FP	PIN	1310	-15 to -8	>-8	<-34	0–25
S2	DSC/PC	FP	PIN	1310	-5 to 0	>-8	<-34	10–60
S3	DSC/PC	DFB	PIN	1550	-5 to 0	>-10	<-36	15–120
SS13	SC/PC	FP	PIN	1310	-12to -3	>-8	<-30	0–25
SS15	SC/PC	FP/DFB	PIN	1550	-12 to -3	>-8	<-30	0–25

Model	Optical interface	Laser type	Receiver type	Wavelength (nm)	Tx power (dBm)	Minimal overload point (dBm)	Rx sensitivity (dBm)	Transmission distance (km)
SS23	SC/PC	FP	PIN	1310	-5 to 0	>-8	<-32	10–50
SS25	SC/PC	DFB	PIN	1550	-5 to 0	>-8	<-32	10–50

Note

Optical interface specifications are defined as below:

- S1 indicates short distance, single-mode and double fiber.
- S2 indicates mid distance, single-mode and double fiber.
- S3 indicates long distance, single-mode and double fiber.
- SS13 indicates short distance, single-mode and double fiber with a 1310nm wavelength.
- SS15 indicates short distance, single-mode and double fiber with a 1550nm
- SS23 indicates mid distance, single-mode and double fiber with a 1310nm wavelength.
- SS25 indicates mid distance, single-mode and double fiber with a 1550nm wavelength.

6.2.3 E1 interface specifications

Table 6-5 E1 interface specifications

Parameter	Description
E1 interface mode	• 120 Ω balanced RJ45 interface • 75 Ω unbalanced BNC interface
Bit rate	2048kbit/s ±50ppm
Code	HDB3
Input resistance	120 Ω (balanced) or 75 Ω (unbalanced)
Electricity feature	Fit for ITU-T G.703 recommendation
Frame structure	Fit for ITU-T G.704 recommendation
Jitter	Fit for ITU-T G.823 recommendation
E1 linear auto-reorganization	Supported

6.3 Electromagnetic compatibility and lighting protection

Electromagnetic compatibility and lighting protection should meet the following requirements:

- EMC

- ESD
- Power supply and interfaces support lighting protection

Lighting protection requirements are listed as below:

Table 6-6 Power supply and interface lighting protection requirements

Item	Type	Lighting protection requirement
Power supply	AC	• Common mode 2 kV • Differential mode 1 kV
	DC	–
Interface	Console interface	1 kV
	SNMP interface	1 kV
	FE/GE electrical interface	6 kV
	GE optical interface	–
	E1 interface	1 kV

6.4 Safety specifications

Safety specification should meet the following conditions:

- CE authentication
- UL authentication
- All interfaces pass the dielectric strength test.

6.5 Environmental requirements

Table 6-7 Environmental requirements

Parameter	Requirement
Temperature (℃)	-5 to +50
Relative humidity (RH)	≤90%
Condensation requirement	No condensation
Storage temperature (℃)	-25 to +60
Atmospherical pressure requirement (kPa)	86–106 (70 Pa equals to 3000-m altitude)
Dustproof/ waterproof requirement	• No special protection requirement • IP level is 20
Environment authentication	Meet EURoHS
Noise requirement (dB (A))	Telecom equipment room: 72–75

7 Appendixes

This chapter lists terms, acronyms, abbreviations, standards, protocols, and cables, including the following sections:

- Terms
- Acronyms and abbreviations
- Standards and protocols compliance
- Cables

7.1 Terms

A

Add/Drop Multiplexer (ADM)

Network element that provides access to all, or some subset of the constituent signals contained within an STM-N signal. The constituent signals are added to (inserted), and/or dropped from (extracted) the STM-N signal as it passes through the ADM.

Automatic Laser Shutdown (ALS)

The technology that is used for automatically shutting down the laser to avoid the maintenance and operation risks when the fiber is pulled out or the output power is over great.

E

Ethernet in the First Mile (EFM)

Complying with IEEE 802.3ah protocol, EFM is a link-level Ethernet OAM technology. It provides the link connectivity detection, link fault monitoring, and remote fault notification for a link between two directly-connected devices. EFM is mainly used for the Ethernet link on edges of the network accessed by users.

Encapsulation

The technique used by layered protocols in which a lower-level protocol accepts messages from a higher-level protocol and places them in the data of the low level frame.

Ethernet

It is founded by Xerox Corporation and defined by DEC,

	Intel, and Xerox. Ethernet is the most widely used LAN. Its rates include 10 Mbit/s, 100 Mbit/s, and 1000 Mbit/s. Ethernet adopts CSMA/CD mechanism and complies with IEEE 802.3 standard.

F

FE	Fast Ethernet
Layer 2 switching	In LAN, the bridge or 802.3 Ethernet switch forwards the grouped data according to the MAC address. Because the MAC address is the second address of an OSI model. So this forwarding way is called layer 2 switching.

G

GE	Gigabit Ethernet
GFP encapsulation	Generic Framing Procedure (GFP) is a generic mapping technology. It can group variable-length or fixed-length data for unified adaption, making data services transmitted through multiple high-speed physical transmission channels.

J

Jitter	A short-term and non-cumulative deviation from the ideal position of an effective instance of date signal at some point.

L

Link Aggregation Group (LAG)	Multiple physical Ethernet interfaces are combined to form a LAG, which increases the bandwidth and realizes load balancing.
Link capacity adjustment scheme	Link Capacity Adjustment Scheme (LCAS) is a mechanism to control the virtual concatenation adaptive functions on ingress and egress. It can add or decrease the link capacity without losing traffic to meet the bandwidth requirement. It also provides a method to adjust the capacity on the invalid link. LCAS can initiate, add, decrease, create and delete the capacity on the point-to-point channels through the operation of network and network element (NE) management system.
Loopback	It is the process that a signal is sent out and then sent back to the sender. It is used to detect and analyze potential faults in a ring network.

O

OAM	Operations, Administration and Maintenance

Q

QinQ	802.1Q in 802.1Q (QinQ), also called Stacked VLAN or Double VLAN, is extended from 802.1Q and defined by IEEE 802.1ad recommendation. This VLAN feature allows the equipment to add a VLAN tag to a tagged packet. The implementation of QinQ is to add a public VLAN tag to a packet with a private VLAN tag, making the packet encapsulated with two layers of VLAN tags. The packet is forwarded over the ISP's backbone network based on the public VLAN tag and the private VLAN tag is transmitted as the data part of the packet. In this way, the QinQ feature enables the transmission of the private VLANs to the peer end transparently. There are two QinQ types: basic QinQ and selective QinQ.
Quality of Service (QoS)	A network security mechanism, used to solve problems of network delay and congestion. When the network is overloaded or congested, QoS can ensure that packets of important services are not delayed or discarded and the network runs high efficiently. Depending on the specific system and service, it may relate to jitter, delay, packet loss ratio, bit error ratio, and signal-to-noise ratio.

7.2 Acronyms and abbreviations

A

ALS	Automatic Laser Shutdown

C

CMF	Client Management Frame

E

EoPDH	Ethernet over PDH

F

FAS	Frame Alignment Signalling

G

GFP	Generic Framing Procedure
GFP-F	Frame-mapped GFP

I	
IEEE	Institute of Electrical and Electronic Engineers
ITU-T	International Telecommunication Union Telecommunication Standardization Sector
L	
LCAS	Link Capacity Adjustment Scheme
LOS	Loss of Signal
M	
MAC	Media Access Control
MDI/MDIX	Media Dependant Interface/Media Dependant Interface Crossover
P	
PDH	Plesiochronous Digital Hierarchy
Q	
QoS	Quality of Service
S	
SFP	Small Form-factor Pluggable
SNMP	Simple Network Management Protocol
V	
VCAT	Virtual Concatenation
VCG	VCAT Group
VLAN	Virtual Local Area Network

7.3 Standards and protocols compliance

ETSI EN 300 386 V1.4.1(2008-04)	Electromagnetic compatibility and Radio spectrum Matters (ERM)

IEEE 802.3	Ethernet interface standard
ITU-T G.703/G.823	E1 interface standard
ITU-T G.703	Electricity feature
ITU-T G.704	Frame structure
ITU-T G.823	Jitter
ITU-T G.8040	EoPDH standard
SG-46	Dial switch define and skill-screen abbreviation specifications
SG-13	Generic network telecommunication interface design specifications
Pollution prevention management methods for Electronic information products	-
Restriction of Hazardous Substances (RoHS) and related exemption orders: 2002/95/EC, 2005/717/EC, 2005/747/EC, 2006/310/EC, 2006/690(691/692) /EC etc.	-

7.4 Cables

Table 7-1 Interface connection cable specifications

Interface	Description
10/100Mbit/s Ethernet electrical interface	100Base-T5 unshielded twisted pair. Used for SNMP interface and Ethernet electrical interface.
LC connector fiber	According to SFP type, select single-mode/multi-mode fiber. Used for Ethernet optical interface.
75Ω unbalanced BNC	Connect unbalanced devices
120Ω balanced RJ45	Connect balanced devices
Power supply interface	• 220V/10A AC power cable • -48V/10A DC power cable

Table 7-2 Wiring of the 120Ω balanced cable connector

RJ45 pin number	Signal	Description
1	TX+	Transmitted+
2	TX-	Transmitted-

RJ45 pin number	Signal	Description
3	NC	Not connected
4	RX+	Received+
5	RX-	Received-
6	NC	Not connected
7	NC	Not connected
8	NC	Not connected

Table 7-3 Wiring of the Console cable connector

RJ45 pin number	Function	DB9 PIN
1	NC	–
2	DSR#	6
3	RxD	3
4	GND	5
5	GND	5
6	TxD	2
7	DTR#	4
8	NC	–

Note

"–" indicates that the corresponding RJ45 and unlisted DB9 pins are not connected.

瑞斯康达科技发展股份有限公司
RAISECOM TECHNOLOGY CO.,LTD.

Address: Raisecom Building, No. 11, East Area, No. 10 Block, East Xibeiwang
Road, Haidian District, Beijing, P.R.China
Postal code: 100094 Tel: +86-10-82883305 Fax: 8610-82883056
http://www.raisecom.com Email: export@raisecom.com