www.raisecom.com

RC1108-SHDSL-2W×8 G.SHDSL
Product Description
(P100R002_03)

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: Building 2, No. 28, Shangdi 6th Street, Haidian District, Beijing, P.R.China

Postal code: 100085

Notice

Preface

Objectives

This guide describes main functions of the RC1108-SHDSL-2W×8. To have a quick grasp of the RC1108-SHDSL-2W×8, please read this manual carefully.

Versions

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

Product name	Version	Hardware version
RC1108-SHDSL-2W×8	P100R002	A

Conventions

Symbol conventions

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

Symbol	Description
	Indicates a hazard with a medium or low level of risk which, if not avoided, could result in minor or moderate injury.
	Indicates a potentially hazardous situation that, if not avoided, could cause equipment damage, data loss, and performance degradation, or unexpected results.
	Provides additional information to emphasize or supplement important points of the main text.
	Indicates 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	Names of files, directories, folders, and users are in **boldface**. For example, log in as user **root**.
Italic	Book titles are in *italics*.
Lucida Console	Terminal display is in `Lucida Console`.

Change history

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

Issue 03 (2012-12-05)

The document is updated as follows:

- Modified chapter 7 Cables with Ethernet cables, Configuration cables and power cables related description.
- Optimized chapter 1 and modified some bugs.

Issue 02 (2012-09-15)

The document is updated as follows:

- Modified chapter 7 Cables.

Issue 01 (2012-07-05)

Initial commercial release

Contents

Figures

Tables

1 Overview

This chapter contains the following sections:

- Product positioning
- Functions and features
- Ordering information

1.1 Product positioning

The RC1108-SHDSL-2W×8 is a multi-service aggregation G.Single-pair High Speed Digital Subscriber Line (G.SHDSL) card with independent research and development by Raisecom, which is applied to OPCOM3500E (B) or iTN2100 chassis and can support at most 8 wires of E1 service and 9 lines of Ethernet service aggregation, is the core product of the second-generation G.SHDSL product series.

RC1108-SHDSL-2W×8 adopts dual-channel for service transmission and can take full advantage of cable resources. At the same time it has a flexible networking mode, such as point-to-point, point-to-multipoint, can couple with the other Raisecom devices to form a variety of Ethernet access solutions so as to meet the differentiated user demands.

Figure 1-1 shows the front panel of the RC1108-SHDSL-2W×8.

Figure 1-1 Front panel of the RC1108-SHDSL-2W×8

1.2 Functions and features

1.2.1 Multichannel service aggregation

The RC1108-SHDSL-2W×8 can provide users with E1 service and Ethernet service access. One G.SHDSL line can transmit E1 service and Ethernet service simultaneously. The RC1108-SHDSL-2W×8 can support at most 8 wires of E1 service and 9 lines of Ethernet

service aggregation, meet customers multiple services application needs, and fully utilize the bandwidth resources.

E1 service is transmitted to aggregation card through backplane TDM bus, and Ethernet service is transmitted to front panel GE port, or transmitted to backplane through backplane to provide to switch single card and implement Ethernet service aggregation. GE port speed can be set to FE (Fast Ethernet) or GE (Gigabit Ethernet).

As shown in Figure 1-2, the RC1108-SHDSL-2W×8 connects the RC1103-SHDSL-4W to implement dual-channel Ethernet service and E1 service aggregation. RC1108-SHDSL-2W×8 4-wire G.SHDSL interface EFM signal implements high-speed Ethernet service transmission through EFM Bonding, 2-wire G.SHDSL interface E1 signal decomposes through E1 module, uplink aggregation card to take E1 signal timeslot crossing and implement high-speed E1 service transmission through E1-16E1 card.

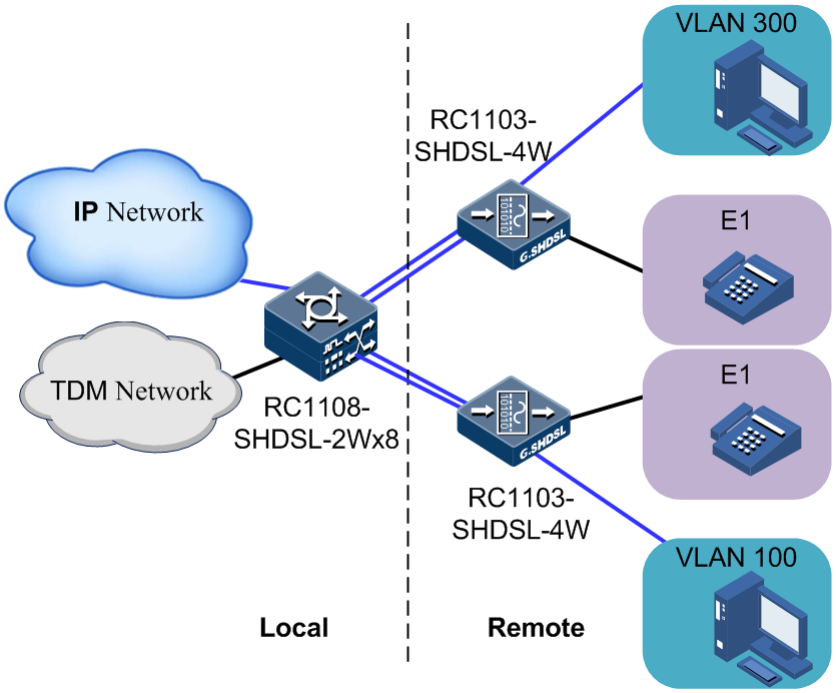


Figure 1-2 Dual-channel service transmission networking

1.2.2 Service bandwidth smooth upgrade

The RC1108-SHDSL-2W×8 supports 2-wire or 4-wire EFM Bonding or M-Pair Bonding, single G.SHDSL interface speed can be up to 15 Mbit/s; uplink EFM bandwidth can be up to 120 Mbit/s. In the situation not to change network structure, user can take reasonable allocation of bandwidth according to the operational requirements. In the subsequent operation and maintenance, user can take smooth upgrade to the service bandwidth according to the increasing demand of service bandwidth.

As shown in Figure 1-3, take EFM Bonding to any two of 4-wire G.SHDSL interfaces as two virtual channels to transmit EFM Ethernet services. The RC1108-SHDSL-2W×8 connects the RC1103-SHDSL-4W and can simultaneously provide VLAN 100, VLAN 200, VLAN 300 and VLAN 400 four user lines and increase service bandwidth.

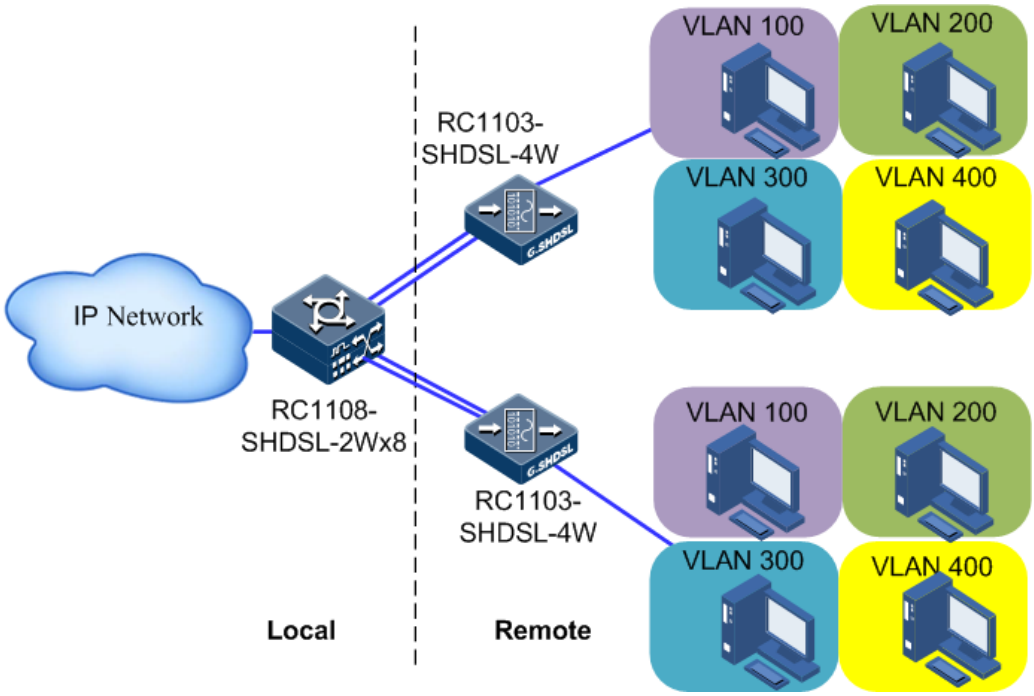


Figure 1-3 Networking with binding virtual channels

As shown in Figure 1-4, take M-Pair Bonding to any two interfaces of 4-wire G.SHDSL interfaces as two virtual channels to transmit EFM Ethernet services. The RC1108-SHDSL-2W×8 connects the RC1103-SHDSL-4W and can simultaneously provide two E1 user lines and increase service bandwidth.

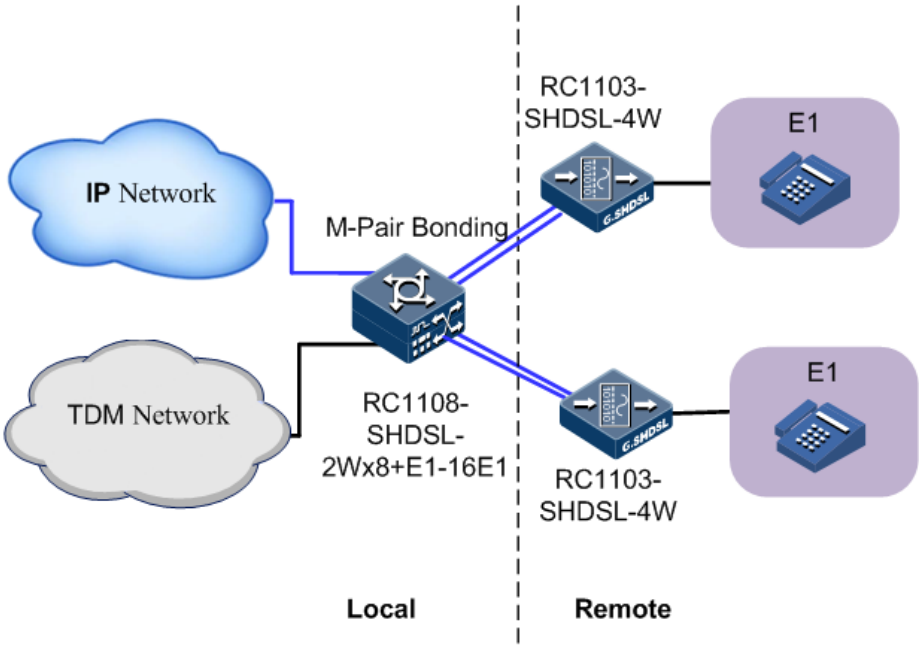


Figure 1-4 Virtual channel M-Pair Bonding networking

1.2.3 Strong anti-noise performance and long transmission distance

G.SHDSL is a technology defined by ITU-T G.991.2 standard to provide bidirectional symmetrical bandwidth data service transmission on ordinary twisted pair. As a result of the superior performance of the TC-PAM (Trellis Coded Pulse Amplitude Modulation) technique, compare with the traditional technique, G.SHDSL compresses the transmission spectrum, improves the anti-noise performance and increases the transmission distance.

The RC1108-SHDSL-2W×8 can probe lines automatically and select the best line speed according to the configured signal-to-Noise Ratio (SNR) threshold, current or worst signal-to-noise ratio tolerance and current line status so as to improve the anti-noise performance.

The RC1108-SHDSL-2W×8 has strong transmission performance; the maximum transmission distance can be up to 6.5km, which can make the maximum use of the current cable resources and increase transmission distance.

1.2.4 Strong compatibility

- The RC1108-SHDSL-2W×8 is compatible with OPCOM3500E (B) and iTN2100 chassis.
- The RC1108-SHDSL-2W×8 is 4W (4 twisted pair) device which can be compatible with 2W (4 twisted pair)/4W (4 twisted pair).
- In the case of the same bunch of cables or narrow frequency band, SHDSL coding mode TC-PAM can be compatible with other coding modes (HDSL or ADSL) to save copper and reduce the crosstalk of the line to the minimum, thereby widely used by carriers.
- G.SHDSL line transmission mode is in accordance with ITU-T G.991.2 standard. As long as different vendors' devices follow the standard, these devices can interconnect with each other.

1.2.5 Layer 2 Ethernet service scheduling

The RC1108-SHDSL-2W×8 supports Layer 2 Ethernet service scheduling, VLAN, QinQ, MAC address forwarding, loopback detection, Layer 2 protocol transparent transmission, link aggregation, QoS, storm control, OAM, Y.1731 and SLA Ethernet switching function so as to meet the carrier-class service management requirements.

1.3 Ordering information

Table 1-1 Product ordering information

Model	Description
RC1108-SHDSL-2W×8	• Single card device, used to OPCOM3500E (B) or iTN2100 chassis. • There are 8 G.SHDSL interfaces downlink, supporting 2-wire, 4-wire EFM Bonding and M-Pair Bonding. • The speed of each line pair is N×64 Kbit/s; the value range of N is 1-178. • When the unicast interface speed is 5.69 Mbit/s, transmission distance is 2.6km. • Ethernet service is transmitted to the IP network through 10/100/1000M auto-negotiation electrical interface or 100M backplane interface, E1 service is transmitted to SDH network through VC12 time slot. • The device can support at most 8 E1 service interfaces and 9 Ethernet service interfaces (including 8 front panel GE interfaces and 1 backplane interface) transmission simultaneously. • Remotely manage the RC1104-FE-4W (A), RC1102-E1-BL (B), RC1102-V35 (B), MSG2110-SHDSL-4W-WP, MSG2110-SHDSL-8W-WP and RC1103-SHDSL-4W device.

Table 1-2 Ordering information about matching chassis

Model	Description
OPCOM3500E-NMS(B)	Network management board
OPCOM3500E-12(B)	6-U chassis, dual power, AC/DC power supply
iTN2100-NMS(C)	Network management board
iTN2100-12(C)	6-U chassis and backplane, dual power, AC/DC power supply

2 Device structure

This chapter contains the following sections:

- Hardware structure
- Software structure

2.1 Hardware structure

2.1.1 Appearance

The RC1108-SHDSL-2W×8 is aggregation card. The appearance of the card is shown as below.

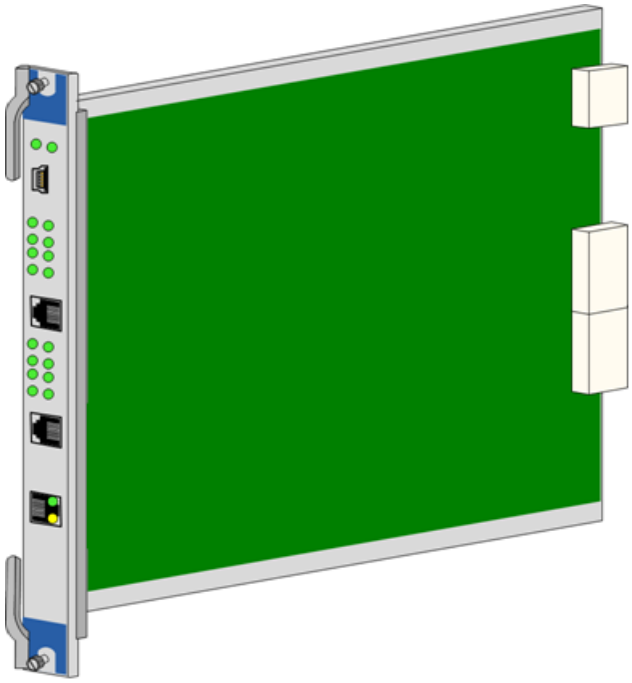


Figure 2-1 Appearance of the RC1108-SHDSL-2W×8

2.1.2 Indicator

The LED description of the RC1108-SHDSL-2W×8 is shown as below.

Table 2-1 LED description of the RC1108-SHDSL-2W×8

LED	Status
SYS	• Blinking Green: CPU works normally. • OFF: CPU works abnormally.
PWR	• Green: power supply is normal. • OFF: power supply is abnormal.
LNK(1–8)	• Green: G.SHDSL line Link status • Blinking Green: the G.SHDSL line is transmitting data. • OFF: G.SHDSL line Down status
GE LNK/ACT	Ethernet interface LINK indicator • Green: Ethernet line Link status • Blinking Green: the G.SHDSL line is transmitting data. • OFF: Ethernet line Down status
GE 1000M	Ethernet interface indicator • Yellow: the interface speed is 1000 Mbit/s • OFF: the interface speed is 10/100 Mbit/s
STU-C(1–8)	• Green: the current device is local device. • OFF: the current device is remote device.

2.1.3 Interface

Table 2-2 Description of the RC1108-SHDSL-2W×8 interface

Interface	Type	Description
G.SHDSL interface	RJ45	Used to access client side Ethernet and E1 service
GE electrical interface	RJ45	Used to transmit uplink Ethernet service to IP network
–	Mini USB	Debugging cards

2.2 Software structure

The software structure of the RC1108-SHDSL-2W×8 is shown as below. The card mainly includes the switching module, G.SHDSL module and E1 module.

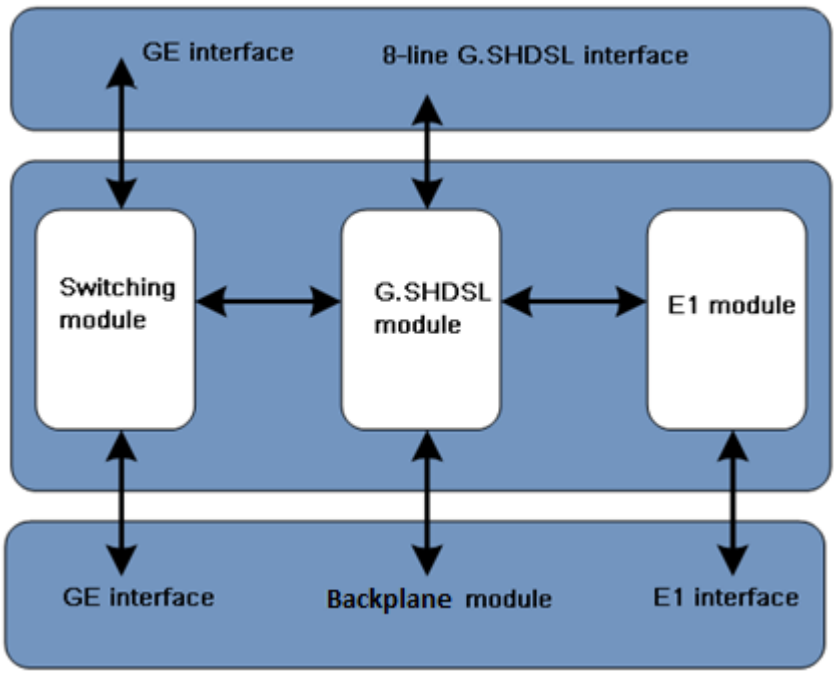


Figure 2-2 Software structure

Table 2-3 describes the RC1108-SHDSL-2W×8 software structure.

Table 2-3 Software structure description

Module	Description
G.SHDSL module	• G.SHDSL module can take EFM Bonding to G.SHDSL interface accessed EFM service and take M-Pair Bonding to E1 service so as to increase the virtual channel bandwidth and improve the service transmission distance. • G.SHDSL module can encapsulate packets with different types of frames, including EFM, E1 and FEM-E1.
Switching module	User can configure switching module to implement VLAN, QinQ, MAC address forwarding, loopback detection, Layer 2 protocol transparent transmission, link aggregation, QoS, storm control, OAM, Y.1731 and SLA Ethernet switching functions.
E1 module	E1 module can decompose E1 signal from EFM-E1 signal access to G.SHDSL interface or from E1 signal after G.SHDSL encapsulation.
Backplane module	Functional module on the backplane of OPCOM3500E (B) or iTN2100 chassis. The RC1108-SHDSL-2W×8 can be used to iTN2100 chassis to implement backplane channel management function.
8-wire G.SHDSL interface	• 8-wire G.SHDSL interface can access 8 wires of EFM service and 8 wires of E1 service. Each G.SHDSL interface support the transmission rate of 64 Kbit/s to 15 Mbit/s. • Transmit EFM service and E1 service signals to G.SHDSL module for frame type encapsulation. • G.SHDSL interface SHDSL frame format adopts TC-PAM coding mode, including PAM 4, PAM 16, PAM 32, PAM 64 and PAM 128 according to different electrical level of grid. Therein, PAM 16 and PAM 32 are are defined by ITU-T G.991.2, PAM 4, PAM 16 and PAM 128 are extended TC-PAM. The transmission speeds of PAM 4, PAM 16, PAM 32, PAM 64 and PAM 128 increase progressively. • G.SHDSL line transmission mode is in accordance with ITU-T G.991.2 standard.
GE interface	• The front panel GE interface is uplink Ethernet port, which is used to complete Ethernet service aggregation. • The backplane interface connects to the switching board on OPCOM3500E (B) or iTN2100 chassis to transmit Ethernet service.
E1 interface	The backplane E1 interface will upload the E1 signals abstracted from E1 module to aggregation card and then transmit E1 services through E1 service card.

3 Functions and features

This chapter contains the following sections:

- G.SHDSL functions and features
- Ethernet functions and features

3.1 G.SHDSL functions and features

The aggregation card RC1108-SHDSL-2W×8 with independent research and development by Raisecom can be inserted into OPCOM3500E (B) or iTN2100 chassis to provide users with both E1 service and Ethernet service access simultaneously so as to complete point-to-multipoint service transmission and aggregation and access to TDM network and IP network through uplink interface.

3.1.1 G.SHDSL card functions and features

With the rapid development of Internet, the demand to distance learning, telemedicine, video conference and other multimedia applications has a substantial increase, which comes up with a higher demand on network bandwidth and high-speed transmission. In order to adapt to the new situation and needs, there are a variety of broadband access technologies, especially the development of twisted pair copper cable broadband access technology.

ADSL (Asymmetric Digital Subscriber Line) systems refers to a kind of wider used twisted pair copper cable broadband access technology, which is a digital subscriber line system with discrete multi-tone (DMT) line code. However, with the continuous expansion of ADSL application and the continuous change of broadband service demand, ADSL technology has gradually revealed many insurmountable weaknesses in service development and operation and maintenance, such as short transmission distance, low downlink speed, weaker line diagnostic capabilities and weak anti-interference ability.

G.SHDSL is defined by ITU-T G.991.2 standard, which refers to a technology to provide a bidirectional symmetrical bandwidth data service transmission on ordinary twisted pair. The TC-PAM (Trellis Coded Pulse Amplitude Modulation) technology with superior performance has compressed the transmission spectrum, improved the anti-noise performance, increased the transmission distance, and therefore, has significant technical advantage compared with ADSL technology.

G.SHDSL mainly applies to commercial high-speed broadband service, its superior performance mainly reflected in the following aspects:

- Symmetric DSL technology: different from traditional ADSL technology, G.SHDSL provides symmetrical service.
- Good compatibility: G.SHDSL is compatible with other transmission technologies including DSL technology in access network.
- High transmission speed and bandwidth: G.SHDSL can be adaptive to various transmission speeds to meet the diversified user requirements; each pair of twisted-pair can provide 64 Kbit/s–15 Mbit/s symmetrical speeds and can provide greater bandwidth through the interface binding.
- Long-distance transmission, small interference: compared with the traditional ADSL technology, due to the advantages of G.SHDSL coding mode, the same speed can obtain longer transmission distance; the same transmission distance can obtain higher transmission speed; the same speed and transmission distance can improve the signal-to-noise ratio tolerance.

Frame type

G.SHDSL card supports packet encapsulation of different frame types. User can use the RC1108-SHDSL-2W×8 for different types of service transmission.

The RC1108-SHDSL-2W×8 supports the following frame types:

- EFM: transmitting pure Ethernet service
- E1: transmitting pure E1 service
- EFM-E1: dual-channel frame type, concurrently transmitting Ethernet service and E1 service

Virtual channel binding

To take PAF (PME Aggregation Function) bonding transmission to virtual channel, by definition, refers to bind multiple lines (virtual channels) to form a new channel for service transmission. The bonding here does not mean physically bind multiple pairs of lines together, but bind multiple G.SHDSL interfaces with the virtual channels formed from internal chip corresponding interface mapping for service transmission; user can configure the virtual channel PAF bonding to increase the transmission bandwidth.

The virtual channel EFM Bonding can be dynamically adjusted based on the status of the line bandwidth; when PAF binds two equal bandwidth lines, if one of the lines is interrupted, the virtual channel bandwidth will reduce to half of the original; when the interrupted line is recovered, the virtual channel bandwidth will recover to the original value.

The RC1108-SHDSL-2W×8 provides 8 G.SHDSL interfaces; each interface as a single line takes service transmission to high-speed digital subscriber line, also it can bind up to 4 G.SHDSL interfaces as a virtual channel to take service transmission.

As shown in Figure 3-1, when the RC1108-SHDSL-2W×8 as the central office device receives signals, G.SHDSL 4 interfaces will access to 5.7M bandwidth EFM service respectively. Through EFM Bonding transmission service of virtual channel 1, only when virtual channel 1 takes service transmission, it increases the transmission bandwidth of virtual channel 1, GE interface EFM service can reach 22.8M bandwidth. The GE interface in backplane module can connect to the switching board of chassis to transmit Ethernet service. Accordingly, when the RC1108-SHDSL-2W×8 as the central office device sends signals, the virtual channel 1 can assign different service bandwidth to each G.SHDSL interfaces to increase the service transmission distance.

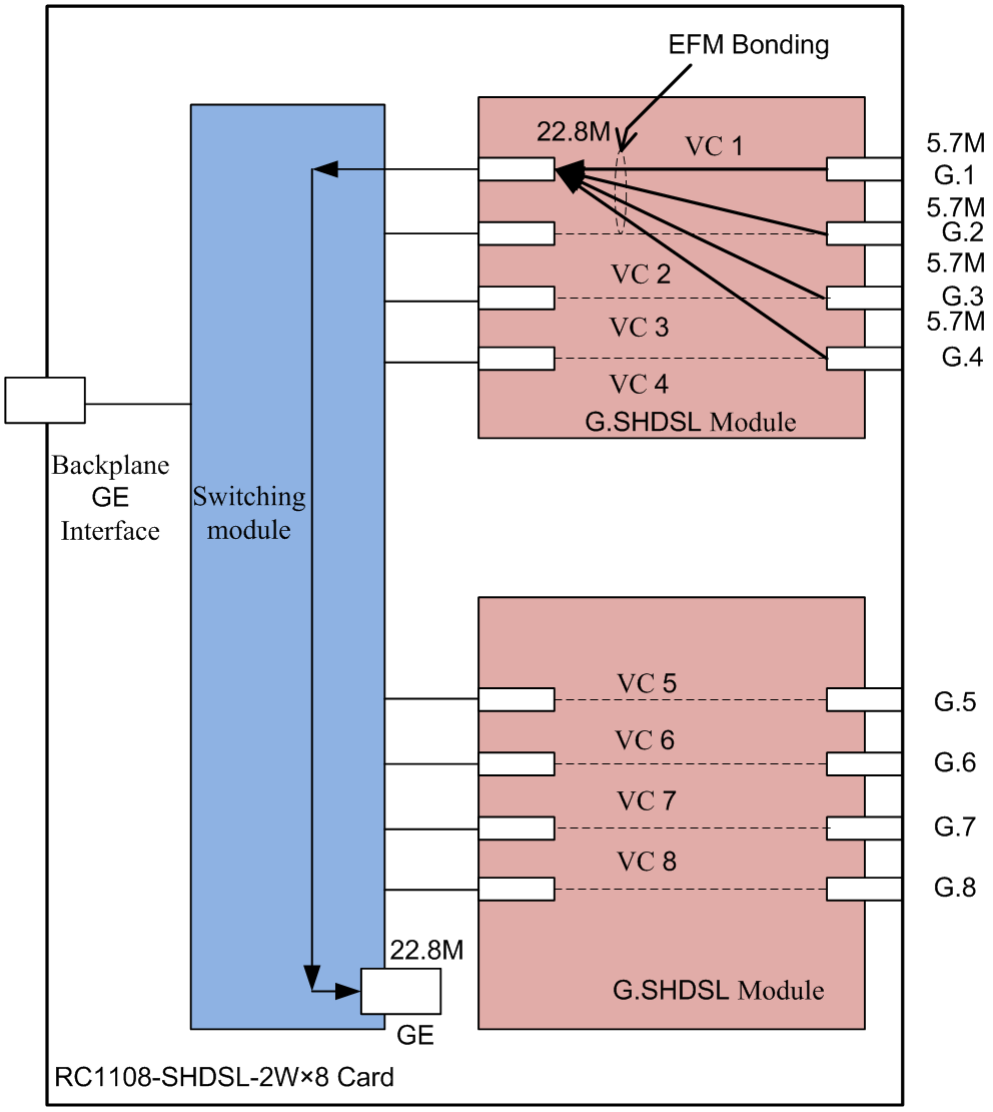


Figure 3-1 EFM Bonding principle

Virtual channel M-Pair Bonding refers to take multi-line pairs bonding to G.SHDSL interfaces transmitting E1 signal to improve service bandwidth. Configure to virtual channel M-Pair Bonding, the service will be shunted in a multi-line, when one of them fails, the whole service will be interrupted.

The RC1108-SHDSL-2W×8 provides 8 G.SHDSL interfaces; each interface as a single line takes service transmission to high-speed digital subscriber line. To take M-Pair Bonding, it can access 4 E1 services at most, two-two bonding to make 2M service be assigned to each lime equally. When the transmission speed is reduced, the service transmission distance will increase.

As shown in Figure 3-2, the RC1108-SHDSL-2W×8 as the central office device receives signal, G.SHDSL 4 interfaces will access to 2M bandwidth E1 service respectively. Through M-Pair Bonding, implement line 1 and line 2 bonding to form virtual channel 1 and transfer line 1 service. Similarly, it can implement virtual channel 3, virtual channel 5 and virtual channel 7 after bonding to transfer E1 service. The 4-wire 2M E1 signals of 4 G.SHDSL interfaces decapsulating from E1 module can take E1 signals time slot cross through upper aggregation card SDH bus and take E1 service landing.

Accordingly, the RC1108-SHDSL-2W×8 as the central office device sends signals; E1 module can encapsulate the E1 frame signal, assign different service bandwidth to G.SHDSL interfaces through virtual channel, which increase the service transmission distance.

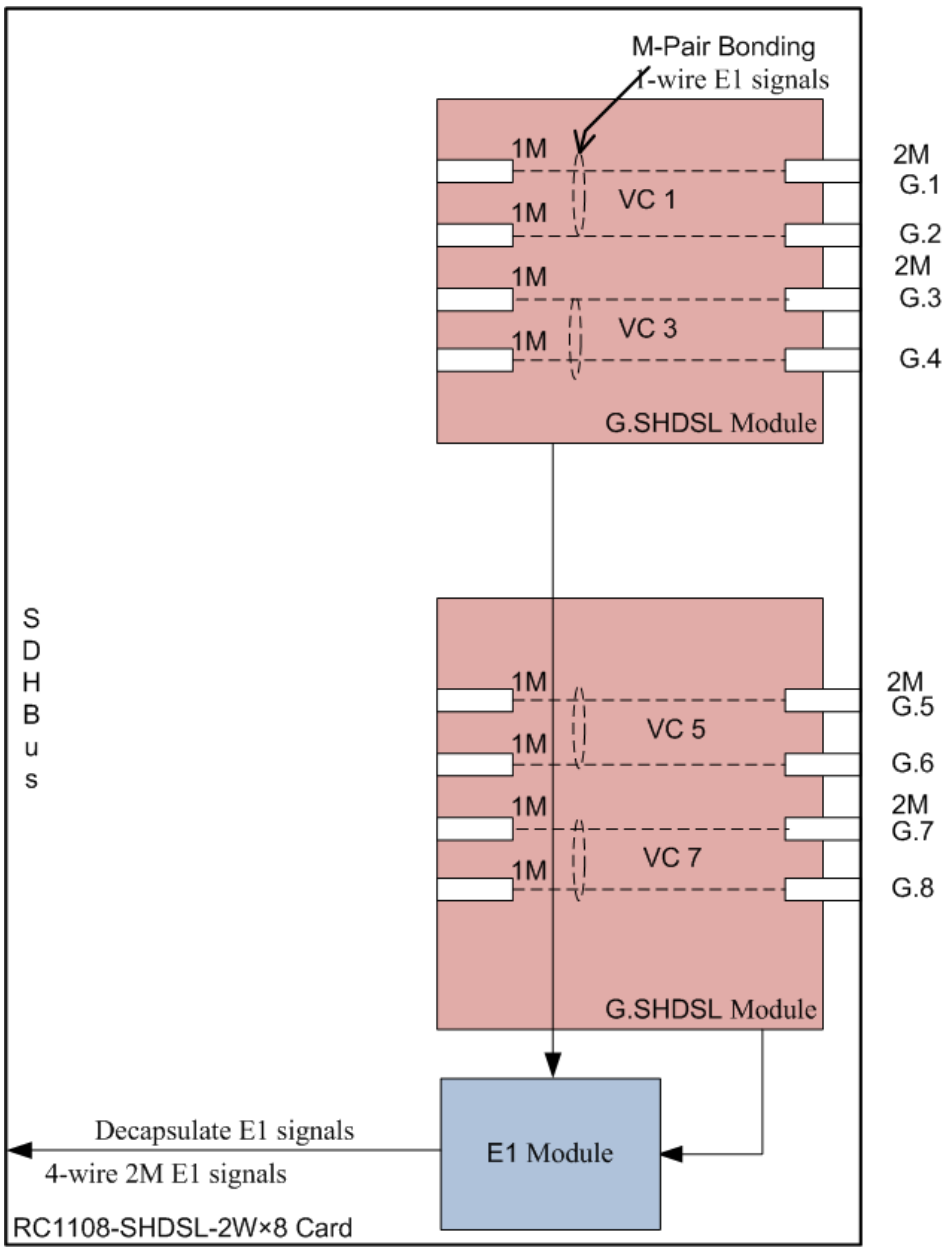


Figure 3-2 M-Pair Bonding principle

Dual-channel service transmission

When the RC1108-SHDSL-2W×8 takes variety of service aggregation, the dual-channel service transmission model can be used.

The dual-channel service transmission principle is shown in Figure 3-3. The RC1108-SHDSL-2W×8 as the central office device receives signal, each G.SHDSL interface will receive 5.7M bandwidth signal, including 3.7M EFM signal and 2M E1 signal. The virtual channel 1 will take EFM Bonding to 4-wire 3.7M EFM signal, only when the virtual channel 1 transmits service, it can increase the transmission bandwidth of virtual channel 1, and GE

interface EFM service can reach 14.8M bandwidth. The GE interface in backplane module can connect to the switching board of chassis to transmit Ethernet service. The 4-wire 2M E1 signals of 4 G.SHDSL interfaces decapsulating from E1 module can take E1 signals time slot cross through upper aggregation card SDH bus and take E1 service landing, which implements dual-channel service transmission.

Accordingly, when the RC1108-SHDSL-2W×8 as the central office device sends signals, the virtual channel 1 can assign different service bandwidth to each G.SHDSL interfaces to increase the service transmission distance. E1 module can encapsulate E1 frame signal, the EFM frame signal and E1 frame signal can simultaneously transmit EFM service and E1 service when they are encapsulated again through G.SHDSL interface.

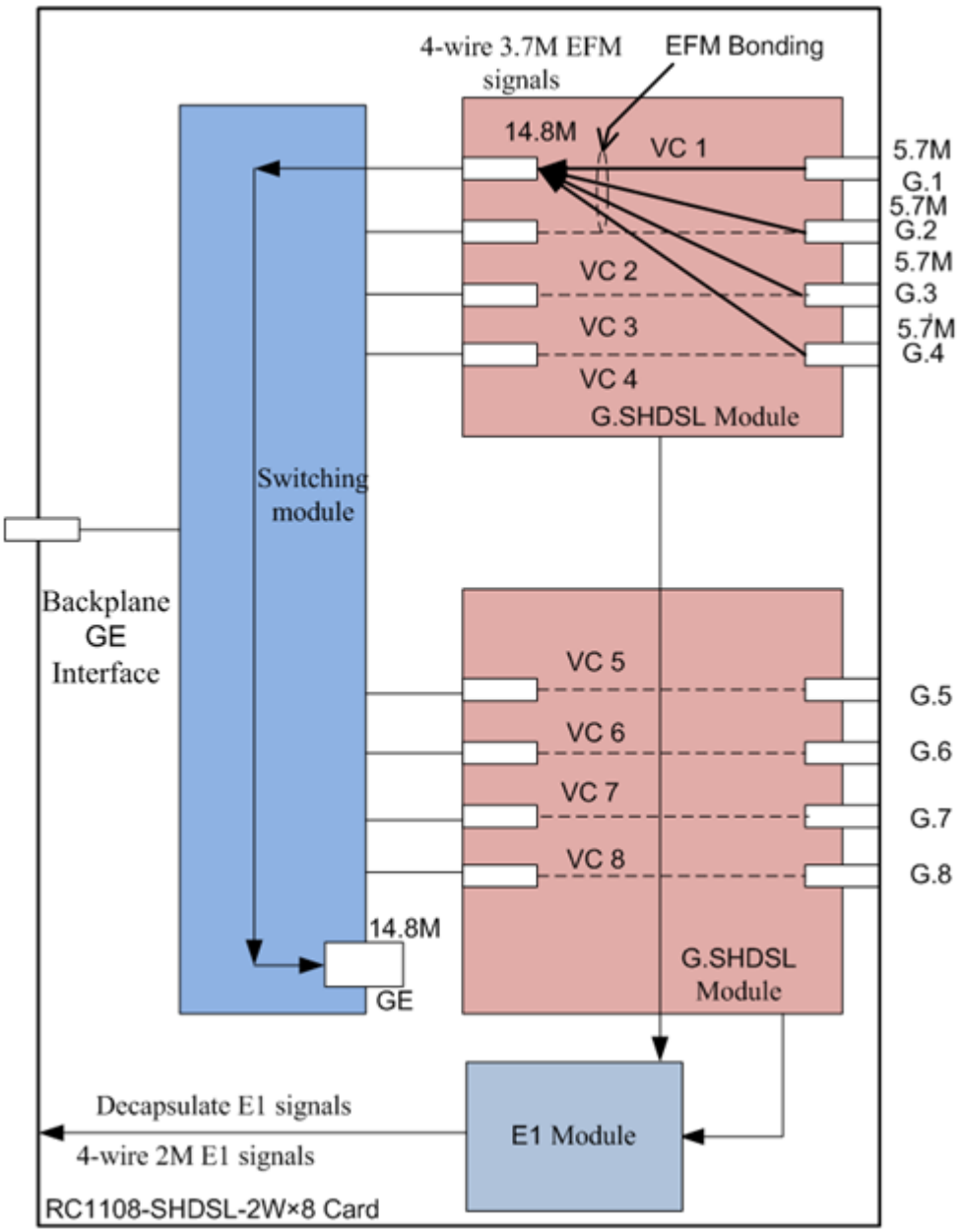


Figure 3-3 Dual-channel service transmission principle

Clock mode

The RC1108-SHDSL-2W×8 clock mode is divided into: local clock, system clock and E1 line clock.

Under normal circumstances, the RC1108-SHDSL-2W×8 as CO device needs to provide clock and transmit the clock signal accurately so that the CPE device can restore the service in accordance with the extracted clock signal. Here the device clock source needs to be configured as local clock mode. The local clock is mainly used for research and development testing, but not be used in the actual network.

When the timing source configuration is successful, if one line or some lines E1 are configured to enable retiming function, then the E1 line clock of these lines is the retiming

source for the user to select. E1 line clock source is mainly used for E1 landing or SDH network online, through E1 line extracted clock to implement E1 service clock synchronization.

In order to ensure that the device services are at the same clock, user needs to configure the clock mode for system clock. The system clock is mainly used for aggregation applications, taking E1 service clock synchronization with the other boards of the device through OPCOM3500E (B) or iTN2100 device system clock.

3.1.2 G.SHDSL interface functions and features

With the extensive use of multimedia services, the traditional Ethernet and telephone network transmission and access modes has come out the following weaknesses: short transmission distance, weak anti-interference and limited transmission speed.

When access Ethernet signals and E1 signals through the G.SHDSL interface, the RC1108-SHDSL-2W×8 card will encapsulate these two signals to SHDSL frame format. At the same time, compatible with Ethernet signals and E1 signal transmission standard, RC1108-SHDSL-2W×8 can implement the demand for high-speed, long distance and stable service transmission.

Coding mode

The G.SHDSL interface adopts TC-PAM coding mode as its frame format. TC-PAM is of low complexity, low delay, strong anti-interference, good frequency spectrum performance and suitable for long-distance transmission. Thus, with TC-PAM coding mode, user can increase the line deployment distance under the requirement of friendly service to ensure line performance.

In the case of the same bunch of cables or narrow frequency band, SHDSL coding mode TC-PAM can be compatible with other coding modes (HDSL or ADSL) to save copper and reduce the crosstalk of the line to the minimum, thereby obtaining a wide range of applications.

SHDSL frame format adopts TC-PAM coding mode, including PAM 4, PAM 16, PAM 32, PAM 64 and PAM 128 according to different electrical level of grid. Therein, PAM 16 and PAM 32 are ITU-T G.991.2 standard defined system, PAM 4, PAM 16 and PAM 128 are extended TC-PAM. The transmission speeds of PAM 4, PAM 16, PAM 32, PAM 64 and PAM 128 increase progressively.

SHDSL line transmission mode is divided into ANNEX A and ANNEX B in accordance with ITU-T G.991.2 standard. ANNEX A is used in America and Japan, and thus is called the American mode. ANNEX B is used in Europe, and thus is called the European mode. Different standards stand for different transmission mode capabilities. The ITU-T G.991.2 also defines two standards: ANNEX A/F and ANNEX B/G. ANNEX A/F are also called the American mode and ANNEX F is an extension to ANNEX A standard. ANNEX B/G is also called the European mode and ANNEX G is an extension to ANNEX B standard.

Link mode

G.SHDSL link has two modes: fixed speed mode and line probing speed mode.

- Fixed speed mode refers to the fixed link speed set by user. In the process of transmission, this speed will not change with the line status.
- Line probing speed mode refers to the device can probe line automatically and select the best link speed according to the configured signal-to-noise ratio threshold, current or

worst signal-to-noise ratio tolerance and current line status. In the process of transmission, this speed will not change with the line status.

3.2 Ethernet functions and features

3.2.1 MAC address table

MAC address table

Ethernet device implements the fast forwarding of Ethernet packets through MAC address forwarding rule; each device has a MAC address and the interface forwarding table, which is MAC address table. MAC address table refers to a Layer 2 forwarding table including the corresponding relationship between MAC address and forwarding interface. All the ingress interface packets will be forwarded according to the MAC address table, which is the basis for Ethernet device to implement the fast forwarding of Layer 2 packets.

MAC address table contains the following information:

- Destination MAC address
- Destination MAC address corresponding interface ID
- Interface subordinated VLAN ID
- MAC address table entry type

RC1108-SHDSL-2W×8 device can show global-based, interface-based and VLAN-based MAC address table information.

MAC address table classification

MAC address table entry is divided into static address table entry and dynamic address table entry.

- Static MAC address table entry: also called “permanent address”, added and removed by the user manually, not aging with time. For the network with small topology change, to add static address table entry manually can reduce the broadcast traffic in network, improve the security of the interface and prevent table entry from losing after the system reset, interface board hot swapping or interface board reset.
- Dynamic MAC address table entry: the device can add dynamic MAC address table entry through MAC address learning mechanism or manual establishments. The table entry will be aged according to the aging time configuration, and be empty after he system reset, interface board hot swapping or interface board reset. Dynamic MAC address entry is stored in the cache of RC1108-SHDSL-2W×8 and the number is depended on the cache capacity.

MAC address aging time

The aging mechanism of MAC addresses takes effects on dynamic MAC addresses only. The MAC address table has capacity limit. To utilize MAC address table resources to the maximum, the RC1108-SHDSL-2W×8 updates the MAC address table through the aging mechanism. While the system dynamically creates a MAC address entry, it enables the aging timer. If the RC1108-SHDSL-2W×8 does not receive packets from the MAC address again within aging time, it deletes the MAC address entry.

The RC1108-SHDSL-2W×8 supports auto-aging. The aging time ranges from 0s to 3825s.

MAC address learning

In general, most MAC address entries are created and maintained through the MAC address learning mechanism. When a packet is sent to the RC1108-SHDSL-2W×8, the RC1108-SHDSL-2W×8 searches the MAC address table for the port ID that is related to the MAC destination address of the packet. If successful, the RC1108-SHDSL-2W×8 will forward the packet to the receiving port. Meanwhile, the RC1108-SHDSL-2W×8 adds the relevant MAC source address, port ID, and VLAN ID to the MAC address table.

When a packet can be sent to the learned MAC address through other ports, the packet will be directly forwarded to the receiving port according to the MAC address table. If the MAC destination address is not listed in the MAC address, the RC1108-SHDSL-2W×8 floods the packet to all ports except for the port that receives this packet. In addition, the MAC source destination of the packet will be added to the MAC address table on the RC1108-SHDSL-2W×8.

MAC address learning quantity limitation

With the MAC address learning mechanism, the RC1108-SHDSL-2W×8 can obtain MAC addresses for all devices at a network segment where a port is. For packets that are sent to these MAC addresses, the RC1108-SHDSL-2W×8 will directly forward these packets by looking up the MAC address table. Therefore, forwarding efficiency is improved.

If the MAC address table is over great, a longer time is needed to search for related MAC address entries. Therefore forwarding performance of the RC1108-SHDSL-2W×8 is reduced. By limiting the number of the MAC addresses learned on an Ethernet port, the administrator can control the numbers of the entries in the MAC address table of the Ethernet switching card. When the number for learned MAC addresses exceeds the maximum value, the port will not learn any MAC address.

MAC address forwarding mode

When forwarding packets, based on the information about MAC address entries, the RC1108-SHDSL-2W×8 adopts following modes:

- Unicast: when a MAC address entry, related to the destination MAC address of a packet, is listed in the MAC address table, the RC1108-SHDSL-2W×8 will directly forward the packet to the receiving port through the egress port of the MAC address entry. If the entry is not listed, the RC1108-SHDSL-2W×8 broadcasts the packet to other devices, as shown below.

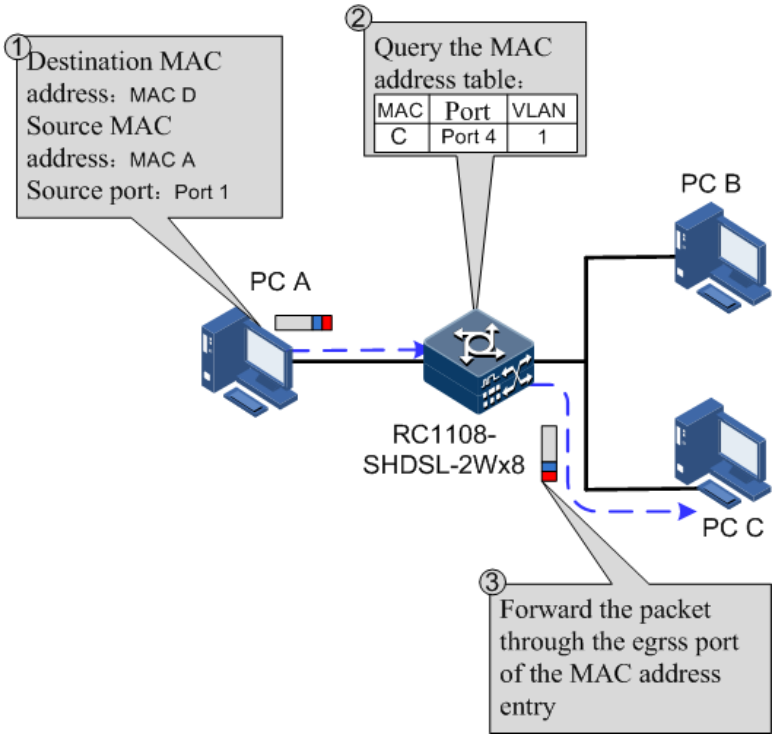


Figure 3-4 Forwarding packets according to the MAC address table

- Multicast: when the RC1108-SHDSL-2W×8 receives a packet of which the destination MAC address is a multicast address, and this MAC address is listed in the MAC address table, the RC1108-SHDSL-2W×8 transmits the packet from the egress port. If the MAC address is not listed, the RC1108-SHDSL-2W×8 broadcasts the packet to other devices, as shown below.

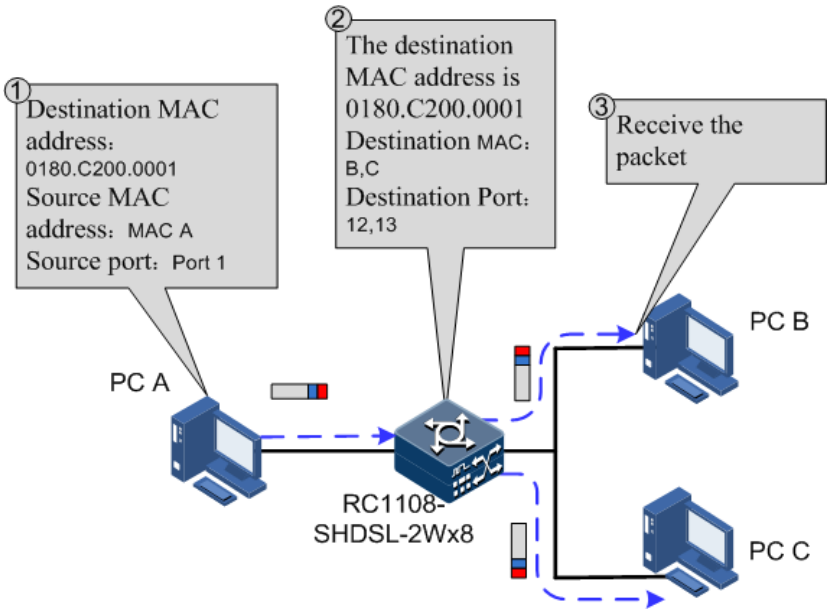


Figure 3-5 Multicasting packets according to the MAC address table

- Broadcast: when the RC1108-SHDSL-2W×8 receives an all-F packet, or this MAC address is not listed in the MAC address table, the RC RC1108-SHDSL-2W×8 forwards

the packet to all ports except the port that receives this packet. Broadcast addresses are special multicast addresses, as shown below.

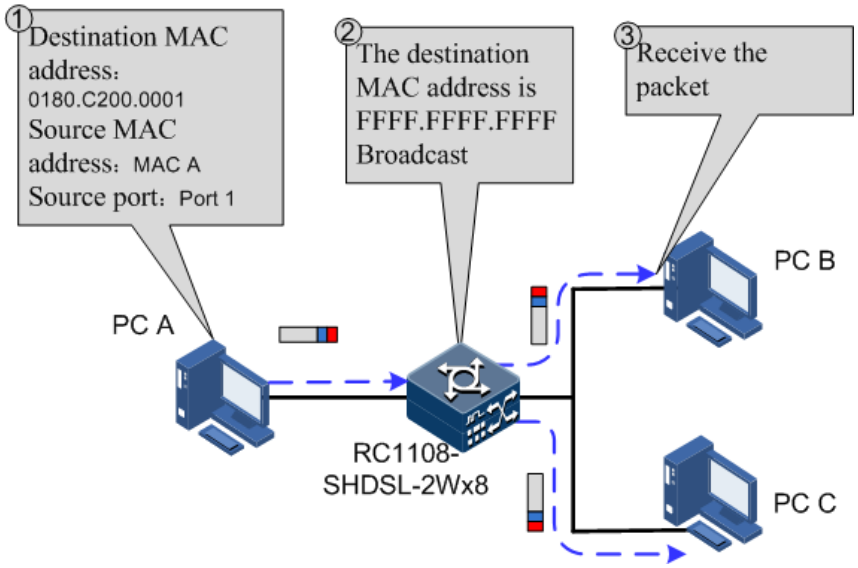


Figure 3-6 Broadcasting packets according to the MAC address table

MAC address forwarding policy

The static MAC address table has three forwarding policies:

- Forwarding
- Discarding
- Mirroring to the mirroring port

According to different service requirements and network traffic, you can configure policies for MAC address forwarding. If a service is not required, you can discard its packets from a source MAC address or destination address. When monitoring flow of a service, you can configure policies to mirror packets of the source MAC address or the destination address to the mirroring port.

MAC address table polling

The MAC address table keeps learning and updating on the network, so it is different at different time. When you need to query the current dynamic MAC address table or the RC1108-SHDSL-2W×8 reports a fault to the Network Management System (NMS), the RC1108-SHDSL-2W×8 must be enabled with MAC address table polling.

The NMS obtains the MAC address tables by polling the MAC address table. Because a MAC address table consists of a limited number of MAC address entries, if you keep polling, a number of resources are occupied. You can stop polling the MAC address table if not needed. Then you can re-poll it as required.

3.2.2 VLAN overview

Layer 2 switch forwards packets by maintaining the MAC address table and according to the destination MAC address table, which effectively utilizes network bandwidth and improves network performance. It effectively isolates collision domains rather than broadcast domains.

When excessive computers are connected to a network, more broadcast traffic is generated, which deteriorates network performance or even blocks the network. To avoid this, broadcast domain must be divided to reduce broadcast traffic, which introduces the VLAN technology.

VLAN is Layer 2 isolation technology. It divides computers in a LAN logically into different parts which are independent of each other and cannot visit each other. In this way, Layer 2 isolation is implemented.

In terms of functions, the VLAN has identical features to the LAN. However, different form the LAN, members in the same VLAN can communicate with each other without any restriction.

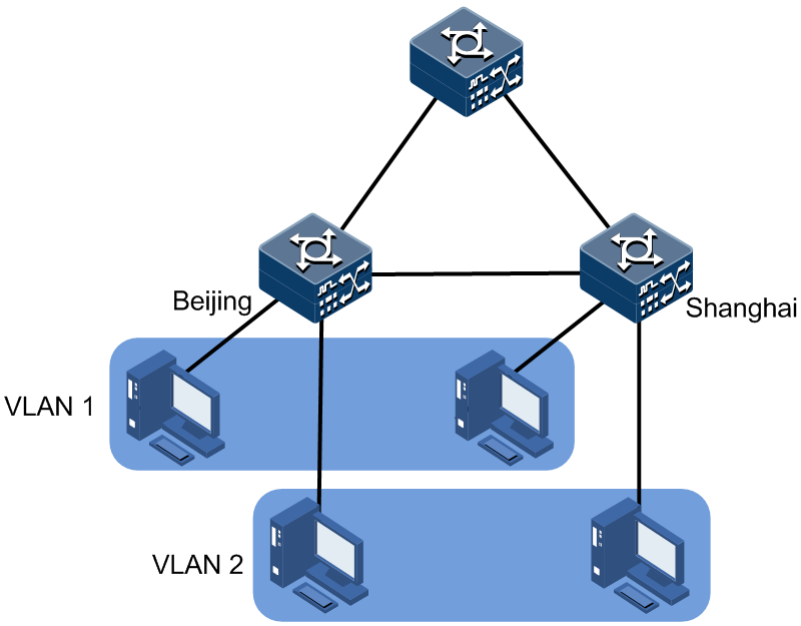


Figure 3-7 VLAN division

As shown in Figure 3-7, computers in Beijing and computers in Shanghai belong to two LANs, but no services are transmitted between computers in the same LAN. When a broadcast storm is generated, all the computers in the same VLAN receive broadcast packets, which occupy and wastes bandwidth. By dividing computers into VLANs, you can isolate computers that do not need to communicate with each other. In this way, network security is enhanced, broadcast traffic is reduced, and broadcast storm is reduced.

The advantage of VLAN

VLAN has the following advantages:

- Divide broadcast domain and reduce broadcast storm. A VLAN is a logical subnet or a broadcast domain.
- Enhance network security. The member in a VLAN can receives data frames sent from other members of this VLAN rather than members of other VLANs. Members of different VLANs can communicate with each other only through routers or Layer 3 device rather than directly.
- Simplify network management. Different from the physical subnet divided by routers, VLAN can enable computers to locate in different spots and have new computer added.

The working principle of VLAN

After devices are divided into different VLANs, they work as logical groups. Then MAC address learning and data switching are based on VLANs. Each VLAN has an independent MAC address table.

When an interface of a RC1108-SHDSL-2W×8 receives a data frame, the RC1108-SHDSL-2W×8 checks the VLAN to which the interface belongs and then searches the MAC address table for the VLAN. If the destination MAC address of the data frame is listed in the MAC address table, the RC1108-SHDSL-2W×8 forwards the data frame; if not, the RC1108-SHDSL-2W×8 discards the data frame.

802.1Q protocol and VLAN label

After a VLAN is configured for the RC1108-SHDSL-2W×8, to identify data frames of different VLANs, you need to add VLAN Tag to data frames, which is implemented through the 802.1Q protocol.

The 802.1Q protocol defines a new Ethernet frame field. Compared with standard Ethernet frame, 802.1Q frame has a 4-byte label after the source MAC address, as shown below.

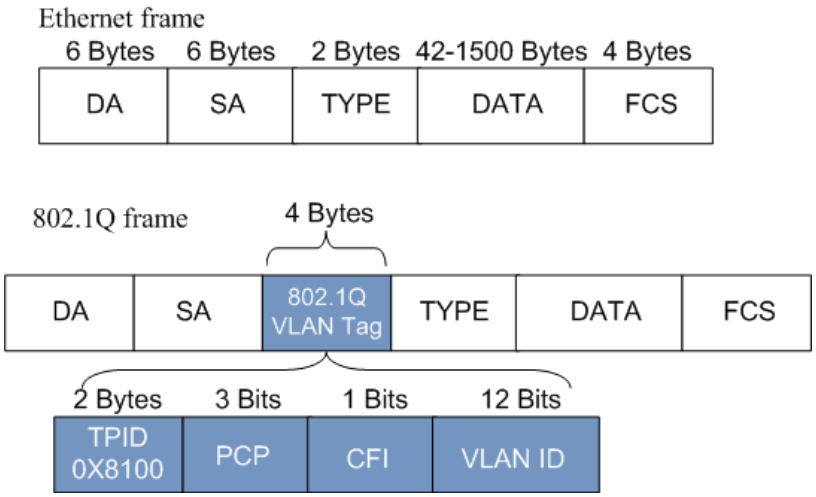


Figure 3-8 Standard Ethernet frame format and 802.1Q frame format

- Tag Protocol Identifier (TPID): a new type defined by IEEE. It indicates that the packet is added with 802.1Q tag. The 802.1Q TIPD is 0x8100.
- VLAN ID: 12 bits, the ID of a VLAN, ranging from 1 to 4094. Port VLAN ID (PVID) is also called default interface VLAN ID. In an interface-based VLAN, each interface has a PVID. When an untagged packet enters the interface, the RC1108-SHDSL-2W×8 forwards data frames according to PVID. The RC1108-SHDSL-2W×8 complies with VLAN standards defined in IEEE 802.1Q, and supports 4094 concurrent VLANs.
- Canonical Format Indicator (CFI): a frame used in data switching between the BUS Ethernet and FDDI and token ring network.
- Priority: 3 bits, priority of a frame. Its value ranges from 0 to 7. The greater the value is, the higher the priority is. It is used when the RC1108-SHDSL-2W×8 sends high priority data frames upon network congestion.

Interface mode and packet forwarding

The RC1108-SHDSL-2W×8 supports three interface modes, as listed in Table 3-1.

Table 3-1 Interfaces modes and packet forwarding

Interface mode	Forwarding modes for ingress packet		Forwarding modes for egress packet
	Untag packet	Tag packet	
Access	Add the Tag of the Access VLAN to packets.	• If the VLAN ID for a packet is identical to the Access VLAN, the packet is received. • If the VLAN ID for a packet is not identical to the Access VLAN, the packet is discarded.	• If the VLAN ID for a packet is identical to the Access VLAN, the packet is sent with the Tag removed. • If the VLAN ID for a packet is in the VLAN ID list on an interface, the packet is sent with the Tag removed. • If the VLAN ID for a packet is not in the VLAN ID list on an interface, the packet is discarded.
Trunk	• If the native VLAN is in the VLAN ID list on an interface, the packet is received and is added with the Tag of the native VLAN. • If the native VLAN is not in the VLAN ID list on an interface, the packet is discarded.	• If the VLAN ID for a packet is in the VLAN ID list on an interface, the packet is received. • If the VLAN ID for a packet is not in the VLAN ID list on an interface, the packet is received.	• If the VLAN ID for a packet is identical to the native VLAN and the packets are allowed to pass through the interface, the packet is sent with the Tag removed. • If the VLAN ID for a packet is not identical to the native VLAN and the packets are allowed to pass through the interface, the packet is sent with its original Tag.
Hybrid	• If the default VLAN is in the VLAN ID list on an interface, the packet is received and is added with the Tag of the default VLAN. • If the default VLAN ID is not in the VLAN ID list allowed by the interface, the packet is discarded.	• If the packet VLAN is in the VLAN ID list allowed by an interface, the packet is received. • If the packet VLAN is not in the VLAN ID list allowed by an interface, the packet is discarded.	• If the VLAN on the Hybrid interface is untagged, the packet is forwarded with the tag removed. • If the VLAN on the Hybrid interface is tagged, the packet is sent with its original Tag.

VLAN division

In general, there are 4 modes to divide VLAN:

- VLAN division based on interface: this method, the most simple and efficient, defines VLAN members by interface. After an interface is added to a specified VLAN, it can forward packets of the specified VLAN.
- VLAN division based on subnet: this method defines VLAN members by network address. When a computer is relocated, you do not need to reconfigure the VLAN. However, the RC1108-SHDSL-2W×8 needs to verify the network address of each packet, which takes a long time and lowers forwarding efficiency of the chip.

- VLAN division based on MAC address: this method configures a VLAN for each MAC address of a computer. When a computer is relocated, you do not need to reconfigure the VLAN. However, when thousands of computers are relocated, you need to conduct too much configuration workload, which greatly lowers forwarding efficiency.
- VLAN division based on protocol: this method divides a network into VLANs by protocol that each computer supports. When a computer is relocated, you do not need to reconfigure the VLAN, nor add VLAN frame tag. This method reduces network communication but the RC1108-SHDSL-2W×8 has to check Ethernet frame head of each packet. Thus, this method takes a long time and lowers forwarding efficiency of a chip.

The RC1108-SHDSL-2W×8 supports VLAN based on interface.

3.2.3 QinQ

QinQ (802.1Q in 802.1Q, also called Stacked VLAN or Double VLAN) technology is an extension of 802.1Q, which is defined in the 802.1ad standard defined by the IEEE.

Basic QinQ

Basic QinQ is a simple Layer 2 VPN tunnel technology. At the ISP's access end, QinQ encapsulates an outer VLAN Tag for a private packet, so that the packet traverses the backbone network of the Internet Service Provider (ISP) carrying double VLAN tags.

In the Internet, the packet is transmitted according to the outer VLAN Tag (public VLAN Tag). And the private VLAN Tag is transmitted as the data in the packet.

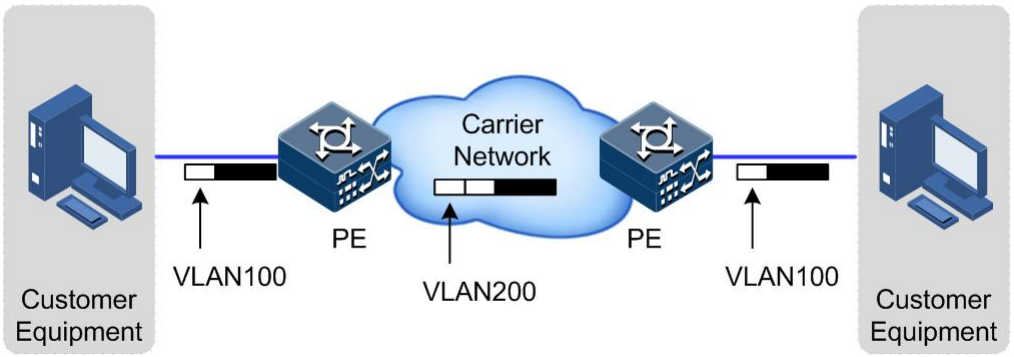


Figure 3-9 Typical networking of basic QinQ

As shown above, the RC1108-SHDSL-2W×8 is the Provider Edge (PE). The uplink port is connected to the ISP's network and the downlink port is connected to the Customer Equipment (CE).

A packet is sent to the PE by the CE, and the packet carries a Tag VLAN 100. When passing through the downlink port of the PE, the packet is added with an outer Tag VLAN 200. And then the packet is sent to the ISP network through the uplink port of the PE.

When the packet with the outer Tag VLAN200 is sent to the other PE, this PE will remove the outer Tag from the packet and then send the packet to the other CE. Now, the packet carries the TAG VLAN 100 only.

3.2.4 Loopback detection

Loopback detection can be classified into two types: port-based loopback detection and VLAN-based loopback detection. Port-based loopback detection is mainly used for edge ports. Port-based loopback detection performs loopback detection on ports. When a loopback is found on a port, the port will be blocked. When the auto-recovery time is reached, the port will be released again. VLAN-based loopback detection performs loopback detection in VLANs.

The loopback detection can address the influence on network caused by a loopback, providing the self-detection, fault-tolerance and robustness.

Loopback detection proceeds as below:

- All ports on the RC1108-SHDSL-2W×8 send the Loopback-Detection packet periodically (the interval can be configured. By default, the interval is 4 seconds).
- The RC1108-SHDSL-2W×8 checks the source MAC field of the received packet. If the MAC address of the RC1108-SHDSL-2W×8 is saved in the source MAC field, it is believed that a loopback is detected on some port of the RC1108-SHDSL-2W×8. Otherwise, the packet is discarded.
- When the receiving port number is not smaller than the sending port number, the receiving port will be blocked. Otherwise, keep the receiving port Up.

3.2.5 Layer 2 protocol transparent transmission

The transparent transmission function is a main function for Ethernet devices. In general, the ISP's edge device charges for transparently transmission of Layer 2 protocol packets. The transparent transmission function is enabled on the port where the ISP's edge device is connected to the user network. A Layer 2 protocol packet is transmitted through the ingress port and is encapsulated on the edge device (the ingress port) of the Internet Service Provider (ISP). And then the Layer 2 protocol packet is transmitted to the ISP network. The Layer 2 protocol packet traverses the ISP to the other edge device (the egress port). Then this edge device decapsulates the Layer 2 protocol packet and transmits it to the user network through the egress port.

The transparent transmission function consists of encapsulation and decapsulation processes. And basic principles are shown as follows:

- Encapsulation: on the ingress port of the ISP, the device adopts a special multicast address (by default, it is 010E.5E00.0003) to modify the MAC destination address of the Layer 2 protocol packet. On the ISP's network, the modified packet is taken as a data to be forwarded in the VLAN where the user belongs.
- Decapsulation: on the egress port of the ISP, the device recognizes the specified multicast address and restores it to original MAC destination address of the Layer 2 protocol packet. And then the Layer 2 protocol packet is transmitted to specified user network.
- Layer 2 protocol transparent transmission work with QinQ. In addition, it can be operated alone. In real, after the MAC address of a Layer 2 protocol packet is modified, the packet also needs to be added with an outer Tag to traverse the ISP.

3.2.6 QoS

Generally, Internet (IPv4), based on the store-and-forward mechanism, only provides Best-Effort service for users. When the network is overloaded or congested, this service mechanism cannot ensure timely and complete transmission of packets.

With the ever-growing of network application, users bring different service quality requirements on network application. Then network should distribute and schedule resources for different network applications according to users' demands.

Quality of Service (QoS) can ensure real-time and integrated service when network is overloaded or congested and guarantee the whole network runs high-efficiently.

QoS consists of a number of traffic management technologies:

- Priority trust
- Priority mapping
- Traffic classification
- Queue scheduling
- Traffic speed limit based on ports and VLANs

Figure 3-10 shows networking with QoS.

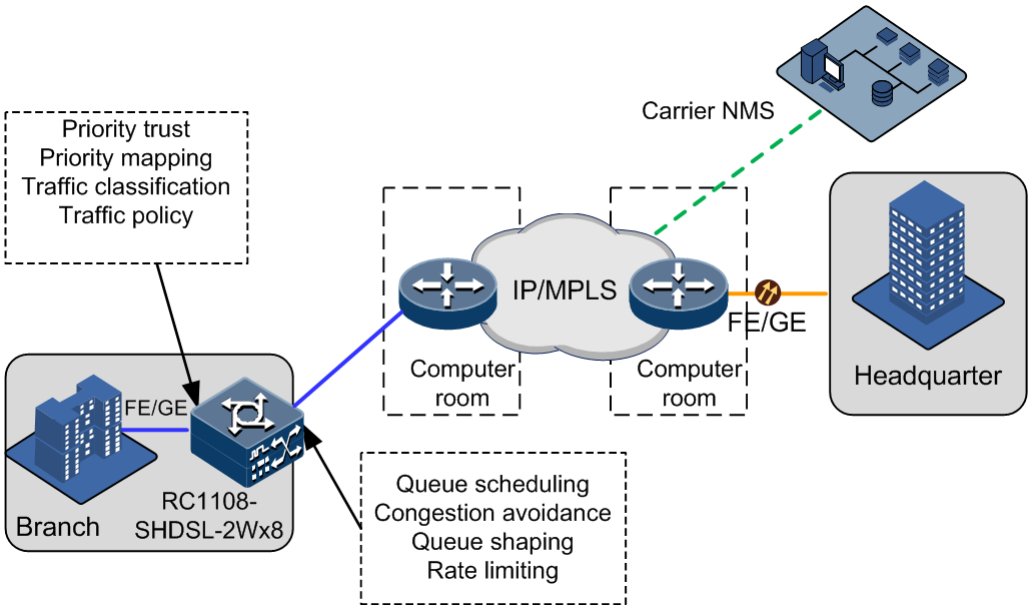


Figure 3-10 Networking with QoS

Priority trust

Priority trust refers that a packet adopts its own priority as the classification standard to perform follow-up QoS management on the packet. In general, the greater the value is, the higher the priority is.

The RC1108-SHDSL-2W×8 card supports port-based priority trust. The priorities are divided into priority based on Differentiated Services Code Point (DSCP) of IP packets and priority based on Class of Service (CoS) of VLAN packets.

Priority mapping

When the RC1108-SHDSL-2W×8 receives a packet on an interface, it sends the packet to packet queues of different local priorities according to the preset mapping between external priority and local priority so that the interface can schedule these packet queues in the egress direction.

The prerequisite for queue scheduling is specifying local priority for the packet. For a packet from an uplink device, the RC1108-SHDSL-2W×8 maps external priority of the packet to different local priorities or directly configures local priority for the packet based on interface, and then schedule queues according to local priorities:

- For IP packets, configure the mapping between ToS priority or DSCP priority and local priority.
- For VLAN packets, configure the mapping between CoS priority and local priority

You can manage mapping by configuring:

- Mapping between CoS priority and local priority
- Mapping between DSCP priority and local priority
- Default priority for an interface
- Priority overriding

Note

The local priority refers to an internal priority that is assigned to packets. It is related to the queue number on the egress port. The greater the value is, the more quickly the packet is processed.

The RC1108-SHDSL-2W×8 supports DSCP priority based on IP packets and CoS priority based on VLAN packets.

Table 3-2 and Table 3-3 list mapping between local priority and DSCP or CoS priority.

Table 3-2 Mapping between local priority and DSCP priority

Local	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
DSCP	0–7	8–15	16–23	24–31	32–39	40–47	48–55	56–63

Table 3-3 Mapping between local priority and CoS priority

Local	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
CoS	0	1	2	3	4	5	6	7

Traffic classification

Traffic classification is a process that recognizes specified packets according to certain rules. All resulting packets can be treated differently to differentiate the service implied to users.

The RC1108-SHDSL-2W×8 configures port trust based on traffics. The RC1108-SHDSL-2W×8 classifies traffics by CoS and DSCP. In addition, it supports classifies traffics based on Access Control List (ACL) rules, class mapping mechanism, and VLAN ID. Figure 3-11 displays the traffic classification process.

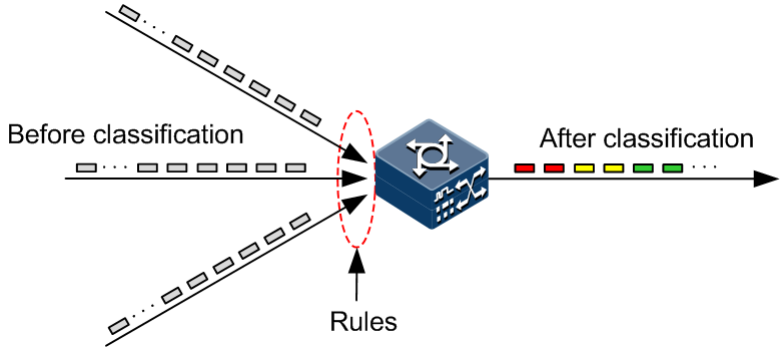


Figure 3-11 Traffic classification process

Structure for IP packet header is displayed in Figure 3-12. An 8-bit ToS field is contained in this packet. For the RFC1349, the first 3 bits of the ToS field representing the ToS priority. For the RFC247, the ToS field is re-defined. The first 6 bits (0–5 bits) represents the priority of IP packets, which is called DSCP priority, ranging from 0 to 63, where the last 2 bits (6 and 7 bits) are reserved bits. Structures for ToS and DSCP priorities are displayed in Figure 3-13.

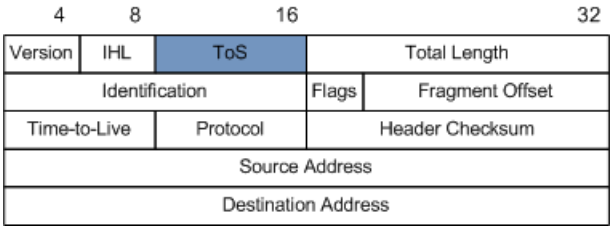


Figure 3-12 IP packet header structure

Figure 3-13 Structures for ToS priority and DSCP priority

IEEE 802.1Q-based VLAN packets are a modification of Ethernet packets. A 4-bit 802.1Q header is added between the source address and protocol type, as shown in Figure 3-14. The 802.1Q header consists a 2-bit Tag Protocol Identifier (TPID, valuing 0x8100) filed and a 2-bit Tag Control Information (TCI) field.

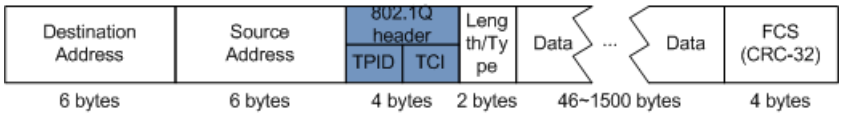


Figure 3-14 VLAN packet structure

The first 3 bits of TCI field represent the CoS priority, which ranges from 0 to 7. CoS priority only applies to the Layer 2 network so as to ensure the service quality.

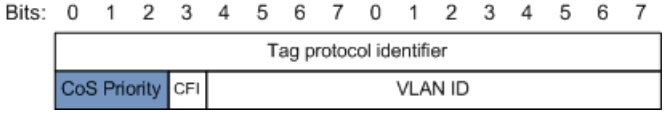


Figure 3-15 CoS priority packet structure

The value for local priority is based on the DSCP value or CoS value of a packet. It can be configured according to port trust status and packet types.

Note

- Configurations for QoS trust status and policy trust status are exclusive. The later configured one takes effect.
- Global QoS trust status and port QoS trust status are designed for different devices. You cannot configure them concurrently for the same device.

Queue scheduling

Users need to perform the queue scheduling when delay-sensitive services need better QoS services than non-delay sensitive services and when the network is congested once in a while.

Queue scheduling adopts different scheduling algorithms to send packets in a queue. Scheduling algorithms supported by the RC1108-SHDSL-2W×8 include Strict-Priority (SP), Weight Round Robin (WRR). All scheduling algorithms are designed for addressing specified traffic problems. And they have different effects on bandwidth distribution, delay, and jitter.

- SP: the device strictly schedules packets in a descending order of priority. Packets with lower priority cannot be scheduled until packets with higher priority are scheduled, as shown in Figure 3-16.

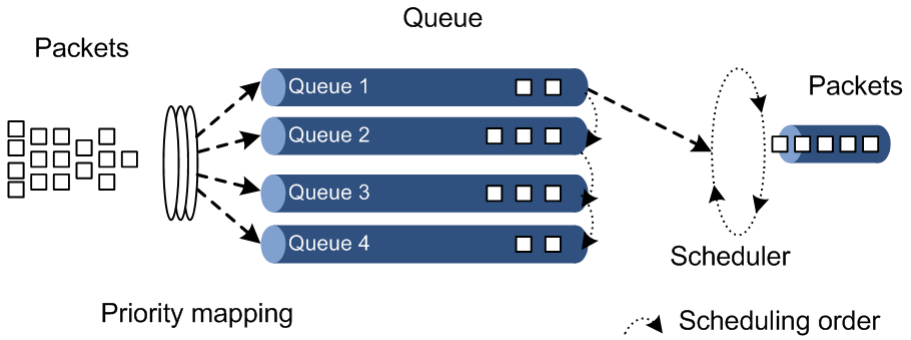


Figure 3-16 SP scheduling

- WRR: on the basis of scheduling packets in a polling manner according to the priority, the device schedules packets according to the weight of the queue, as shown in Figure 3-17.

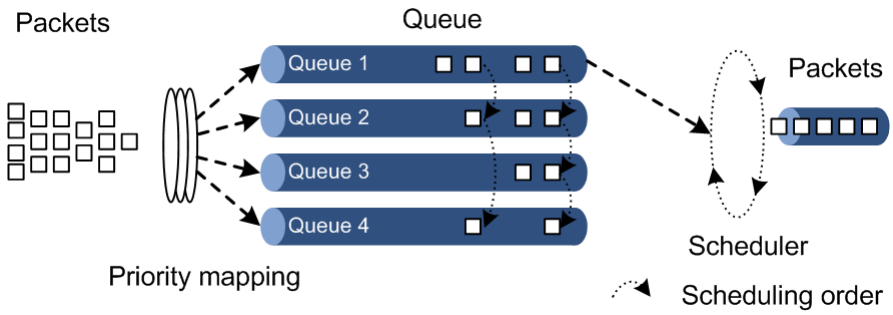


Figure 3-17 WRR scheduling

Interface based traffic speed limit

Traffic speed limit refers to limiting rate on traffics received and sent by a device. The traffic speed limit adopts a token bucket to limit traffics. If the traffic speed limit function is configured on a port, all packets sent and received by this port need to be processed by the token bucket in advance. If there are no enough tokens in the token bucket, a packet can be sent or received. Otherwise, the packet must be discarded.

The traffic speed limit function is displayed in Figure 3-19.

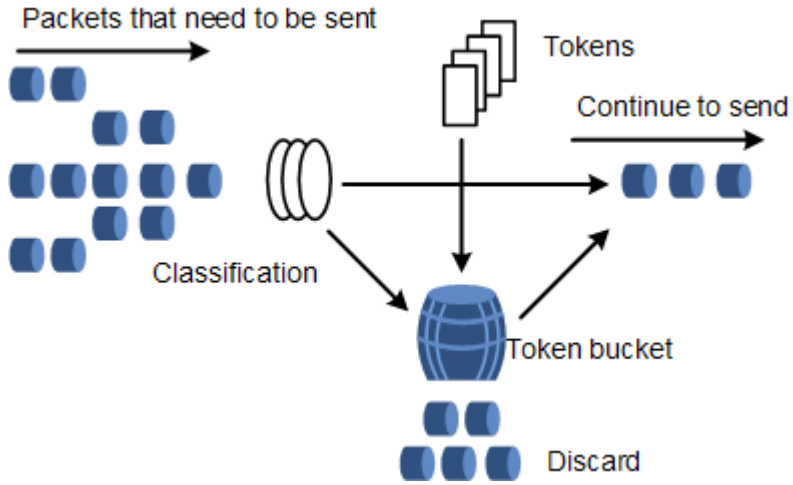


Figure 3-18 Traffic speed limit

In addition to supporting traffic policy-based traffic speed limit, the RC1108-SHDSL-2W×8 supports port-based and VLAN ID-based traffic speed limit.

The Traffic Shaping (TS) function is used to control the rate of packets so that packets are sent at an even rate. Traffic shaping is used to adapt the transmission rate of packets to the downstream devices to prevent unnecessary packet loss and congestion.

Traffic shaping is a traffic control action used to limit traffic and resources by monitoring the specification of the traffic. In traffic shaping, token buckets are also used to measure the traffic.

The main difference between traffic shaping and traffic speed limit is that the RC1108-SHDSL-2W×8 caches the packets discarded in traffic speed limit. These packets are stored in a buffer.

The traffic shaping function is displayed in Figure 3-19.

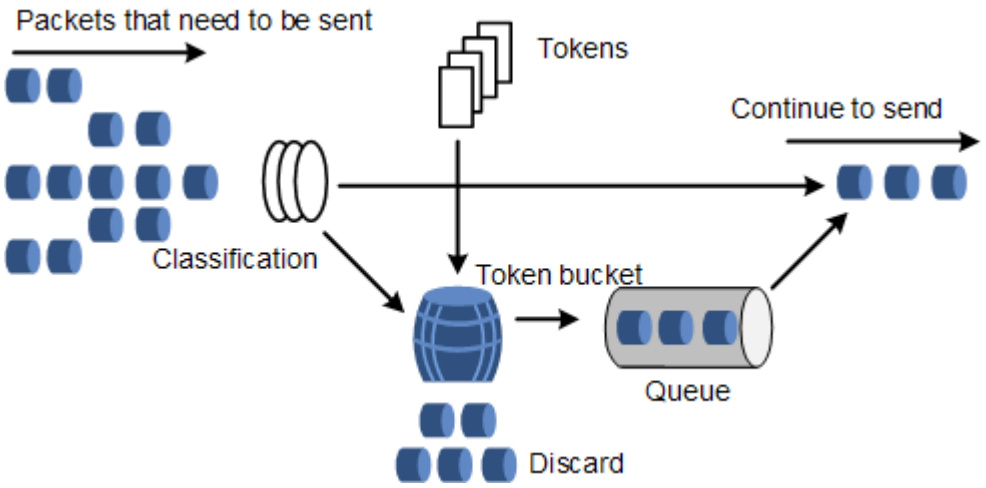


Figure 3-19 Traffic shaping

The delay may be increased just because the traffic shaping technology puts the packets into a buffer or a queue.

By default, rates for all ports or VLANs are negotiated. No restriction is put on the bandwidth.

Traffic speed limit function is performed on ARP, TCP Data, TCP Ctrl, UDP, and Non-TCPUDP packets. When the packet transmission rate exceeds the threshold, the packet will be discarded or delayed to transmit.

3.2.7 Link aggregation

With link aggregation, multiple physical Ethernet ports are combined to form a logical aggregation group. Multiple physical links in one aggregation group are taken as a logical link. Link aggregation helps share traffic among members in an aggregation group. In addition to effectively improve the reliability on links between devices, link aggregation can help gain higher bandwidth without upgrading hardware.

The RC1108-SHDSL-2W×8 support manual link aggregation. The process of aggregating multiple physical ports to a logical interface does not require any protocol. The consistency of interface parameters is ensured manually.

3.2.8 Storm control

On most Layer 2 network, unicast traffic is much heavier than broadcast traffic. If rate for broadcast traffic is not limited, when a broadcast storm is generated, total bandwidth will be occupied. Therefore, network performance is reduced and unicast packet cannot be forwarded. In addition, communication between devices may be interrupted.

Configuring storm control on RC1108-SHDSL-2W×8 prevents broadcast storm occurring when broadcast packets increase sharply in the network. Thus, ensure that the unicast packets can be properly forwarded.

Broadcast traffic may exist in following forms, so you need to limit the bandwidth for them on the RC1108-SHDSL-2W×8.

- Unknown unicast traffic: the unicast traffic whose MAC destination address is not in MAC address table. It is broadcasted by the RC1108-SHDSL-2W×8.
- Unknown multicast traffic: the multicast traffic whose MAC destination address is not in MAC address table. Generally, it is broadcasted by the RC1108-SHDSL-2W×8.

- Broadcast traffic: the traffic whose MAC destination address is a broadcast MAC address. It is broadcasted by the RC1108-SHDSL-2W×8.

4 Operation, management and maintenance

This chapter includes the following sections:

- Basic operation and maintenance tools
- Ethernet OAM
- Backup and upgrade system software

4.1 Basic operation and maintenance tools

RC1108-SHDSL-2W×8 card needs to insert to OPCOM3500E (B) or iTN2100 chassis to cooperate with NMS so as to implement the device operation and maintenance management.

4.1.1 Login

Login through Console interface

Console interface is a common port which connects a network device with a PC running terminal simulation program. Users can configure and manage the local device by Console port.

Login device through the Console interface under the following two situations:

- First power-up
- Fail to login device in Telnet mode

If users want to login a device through PC connecting with console port, firstly, users should connect console port of cable device with RS-232 of PC as shown in Figure 4-1; secondly, users should run terminal simulation program, such as “Hyper Terminal” program of windows XP operation system, and configure communication parameters as shown in Figure 4-2; finally, users can login the device.

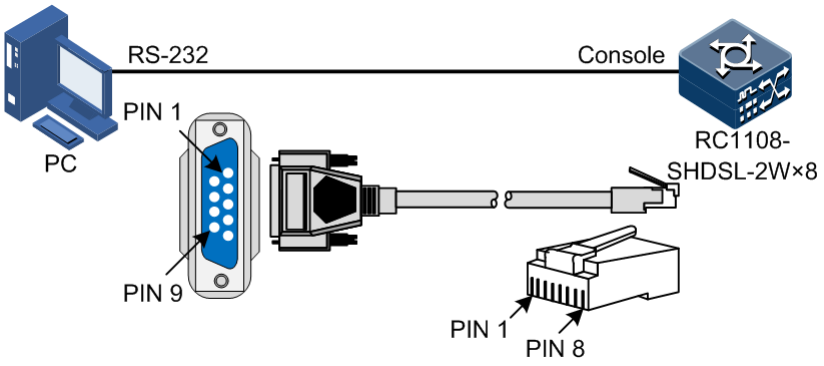


Figure 4-1 Login device through Console interface

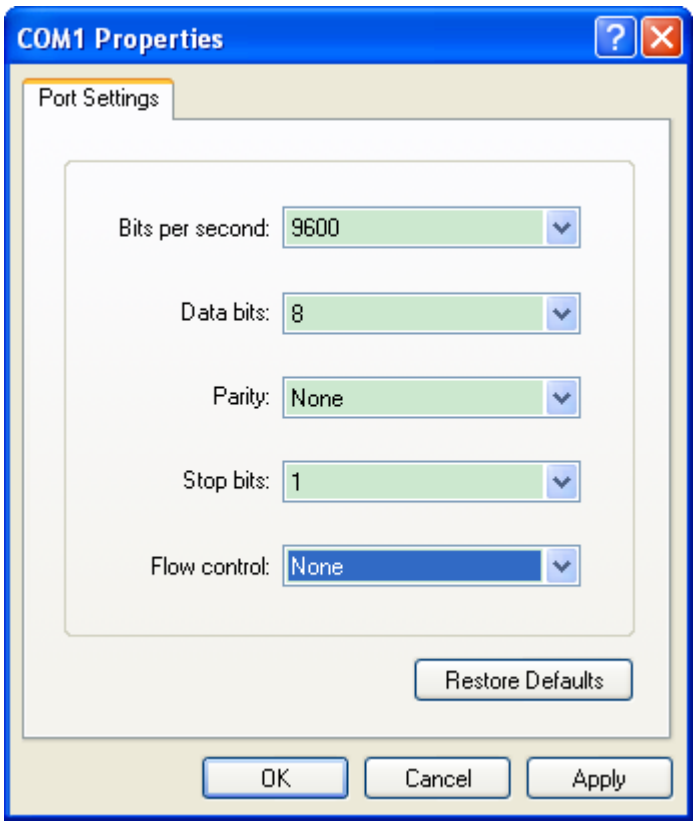


Figure 4-2 Communication parameters configuration in "HyperTerminal"

Note

Microsoft Company is not in support of hyper-terminal since Windows Vista system, users operate Windows Vista or Windows 7 system please download HyperTerminal program from internet. It is free to download HyperTerminal program.

Login through Telnet

Through Telnet, you can remotely log in to the RC1108-SHDSL-2W×8 through a computer. In this way, it is not necessary to prepare a computer for each RC1108-SHDSL-2W×8.

The RC1108-SHDSL-2W×8 supports the following two Telnet services:

- Telnet Server: you can log in to the RC1108-SHDSL-2W×8 through Telnet program that runs on a computer, and then configure it, as shown in Figure 4-3. Now the RC1108-SHDSL-2W×8 provides Telnet server service.

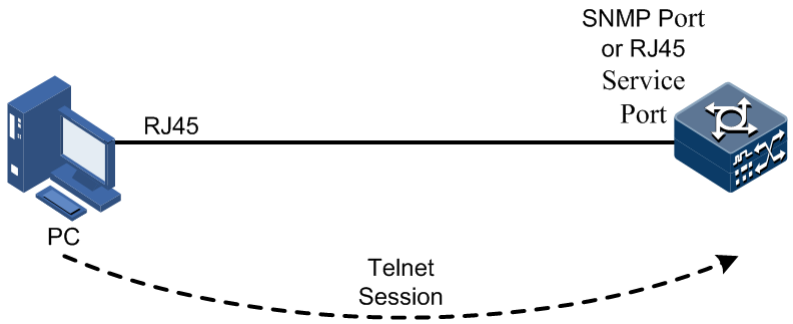


Figure 4-3 Networking with the RC1108-SHDSL-2W×8 as Telnet server

- Telnet Client: after you connect to the RC1108-SHDSL-2W×8 through a terminal emulation program or Telnet through PC, you can log in to another RC1108-SHDSL-2W×8 through Telnet and then manage and configure this RC1108-SHDSL-2W×8. As shown in Figure 4-4, Device A provides both Telnet server service and Telnet client service.

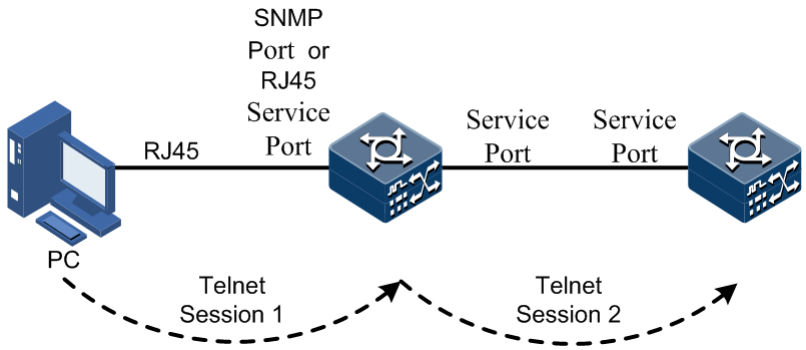


Figure 4-4 Networking with the RC1108-SHDSL-2W×8 as Telnet client

4.1.2 Maintenance and test tools

The RC1108-SHDSL-2W×8 supports diagnosing and debugging system hardware, software and link bugs with the following tools.

PING

Packet Internet Grope (PING), a most widely used command for diagnosing and debugging, is to test whether two devices are connected. The PING function is implemented through Internet Control Message Protocol (ICMP) Echo packets. If the connection is normal, response packets will be replied with.

Traceroute

The Traceroute command is to show the path along which a packet traverse to the destination. The PING command can detect the path, but it cannot record all network devices that the packet passes through because of the limit on the IP header.

BERT

When conducting E1 service access and transmission, the RC1108-SHDSL-2W×8 must be enabled with Bit Error Rate Tester (BERT) to test errored bits online. Conduct link test or connectivity test on the condition that loopback forms on the peer E1 interface; if no loopback forms, enabling BERT will fail.

Port mirroring

Port mirroring refers to mirroring packets of the source port to the monitor port without affecting packets forwarding (mirroring port is a special port which cannot transmit services like common service interfaces). User can use this function to monitor the receiving and sending status of some port and analyse the network situation.

4.2 Ethernet OAM

Initially, Ethernet is designed for LAN. Operation, Administration and Maintenance (OAM) is weak for its small size and a NE-level administrative system. With continuous development of Ethernet technology, the application scale of Ethernet in telecom network becomes wider and wider. Compared with LAN, the link length and network size for telecom network is bigger and bigger. The lack of effective management and maintenance mechanism has seriously obstructed Ethernet technology applying to the telecom network.

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

Combined with G.SHDSL technology and Ethernet technology, EFM G.SHDSL is fit for the first mile access between a telecommunications company and a customer's premise. Compared with other G.SHDSL access services, EFM G.SHDSL is applied to a wider range of applications.

4.2.1 EFM

OAM mode and OAM discovery

The OAM link process for Ethernet is the discovery phase, in which an OAM entity discovers a remote OAM entity and establishes a session with it.

In the discovery phase, a connected Ethernet OAM entity (OAM enabled on ports) informs others of its Ethernet OAM configurations and supported Ethernet OAM capabilities by the local node by exchanging information OAMPDU. After another OAM entity receives parameter configurations of the peer, it decides whether to establish OAM link. If both parties agree on establishment of an OAM link, Ethernet OAM protocols will work on the data link layer.

The RC1108-SHDSL-2W×8 can choose one of the following two modes to establish an Ethernet OAM link:

- Active mode
- Passive mode

Only the OAM entity in active mode can initiate an OAM link while the OAM entity in passive mode can wait for connection request of the active OAM entity.

After the OAM link is established, both parties keep connected by exchanging information OAMPDU. If an OAM entity does not receive information OAMPDU within 5s, it judges that connection expires and connection re-establishment is required.

OAM loopback

OAM loopback occurs only after an Ethernet OAM link is established. When connected, the active OAM entity initiates OAM loopback command, and the peer OAM entity responds to the command.

When the remote OAM entity is in loopback mode, all packets except OAMPDU packets are sent back. By observing this, the network administrator can judge the link performance (packet loss ratio, delay, and jitter).

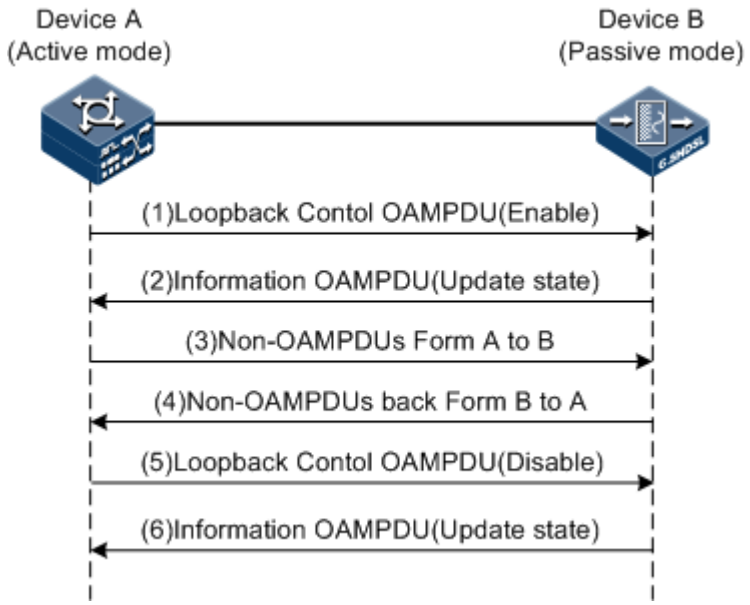


Figure 4-5 OAM loopback

As shown in Figure 4-5, port 1 on Device A works in active mode. After the 802.3ah OAM link between Device A and Device B is established, enable remote loopback on port 1.

The process for OAM loopback is as below:

Step 1 Device A sends a Loopback Control OAM PDU packet with the Enable information to Device B, and waits for response.

Step 2 After receiving the Loopback Control OAM PDU packet with the Enable information, Device B replies the Information OAM PDU (Update state) packet to Device A, and enters the loopback state (in this state, the Device B sends back the non-OAM PDU packet.

Step 3 After receiving the response, Device A sends Device B a non-OAM PDU test packet.

Step 4 After receiving a non-OAM PDU test packet, Device B sends back it to Device A.

Step 5 If Device A needs to stop remote loopback, it sends Device B a Loopback Control OAM PDU packet with the Disable information.

Step 6 After receiving the Loopback Control OAM PDU packet with the Disable information, Device B exits loopback state, and sends Device A an Information OAM PDU (Update state) packet.

User can locate the specific fault area through subsection loopback detection so as to help user solve the fault.

OAM event

It is difficult to detect a failure on the Ethernet, especially when the physical communication works properly while the network performance deteriorates slowly. A flag is defined in OAMPDU packet to allow an OAM entity to transmit faulty information to the peer. The flag may stand for the following threshold events:

- Link fault: signals from the peer are lost.
- Dying gasp: an unpredictable event occurs, such as power failure.
- Critical event: an uncertain critical event occurs.

In an OAM link, an OAM entity keeps sending an Information OAM PDU packet with a threshold event to the peer. In this way, the network administrator can learn state of a link and take actions accordingly.

The network administrator monitors Ethernet OAM through the Event Notification OAMPDU packet. When a link fails, an OAM entity detects the failure, and sends the peer OAM entity an Event Notification OAMPDU packet with the following threshold events:

- Error frame event: the number of error frames exceeds the threshold in a time unit.
- Error frame period event: the number of error frames unit exceeds the threshold in a period (specified N frames).
- Error frame second event: the number of error frames in M seconds exceeds the threshold.

Note

If an error frame is generated in a second, the second is called the error frame second.

Acquiring OAM MIB

The RC1108-SHDSL-2W×8 can acquire the link configuration/statistics of peer device through OAM so as to learn the link status and parameters.

4.2.2 CFM

To expand application of Ethernet technologies on a Carrier network, the Ethernet must be ensured with the same Quality of Service (QoS) as the Carrier transport network. Connectivity Fault Management (CFM) solves this problem by providing overall OAM tools for the Carrier Ethernet.

CFM is a network-level Ethernet OAM technology, providing end-to-end connectivity fault detection, fault notification, judgement and location functions. It is used to diagnose fault actively for Ethernet Virtual Connection (EVC), provide cost-effective network maintenance solution and improve network maintenance via the fault management function.

The RC1108-SHDSL-2W×8 provides CFM function that supports both ITU-Y.1731 and IEEE802.1ag standards.

CFM consists of the following components:

- MD

Maintenance Domain (MD, also called Maintenance Entity Group (MEG)) is a network that runs the CFM function. It defines network range for OAM management. MD has a level property, with 8 different levels (level 0 to level 7). The bigger the number is, the higher the level is and the larger the MD range is. Protocol packets in a lower-level MD will be discarded after entering a higher-level MD. If no Maintenance association End Point (MEP) but a Maintenance association Intermediate Point (MIP) is in a MD, the protocol can traverse the higher-level MD. However, packets in a higher-level MD can traverse lower-level MDs. In the same VLAN range, different MDs can be adjacent, embedded, but not crossed.

As shown in Figure 4-6, MD 2 is in MD 1. Packets in MD 1 need to traverse MD2. Configure MD 1 at level 6, and MD 2 at level 3. Then packets in MD 1 can traverse MD 2 and implement connectivity fault management of the whole MD 1. However, packets in MD 2 cannot diffuse into MD 1. MD 2 is a server layer while MD 1 is a client layer.

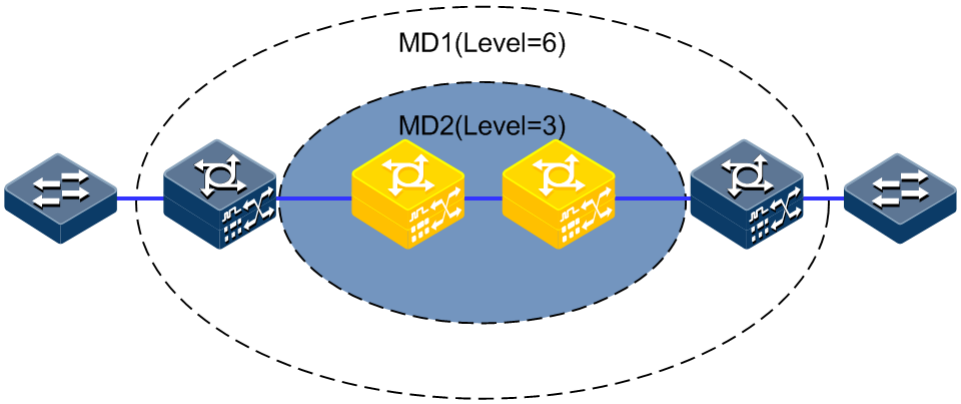


Figure 4-6 MDs at different levels

- Service instance

The service instance is also called a Maintenance Association (MA). It is a part of a MD. One MD can be divided into one or multiple service instances. One service instance corresponds to one service and is mapped to a VLAN group. VLANs of different service instances cannot cross. Though service instance can be mapped to multiple VLANs, one instance can only use a VLAN for sending or receiving OAM packets. This VLAN is the master VLAN for the service instance.

- MEP

As shown in Figure 4-7, MEP is an edge node of a service instance. MEPs can be used to send and process CFM packets. The service instance and the MD where MEP locates decide the VLAN and the level for packets received and sent by MEP.

For any device that runs CFM in the network, the MEP is called local MEP. For MEPs on other devices of the same service instance, they are called Remote Maintenance association End Points (RMEP).

Multiple MEPs can be configured in a service instance. Packets sent by MEPs in one instance take identical S-VLAN TAG, priority and C-VLAN TAG. A MEP can receive OAM packets sent by other MEPs in the instance, intercept packets which at the same or lower level and forward packets of higher level.

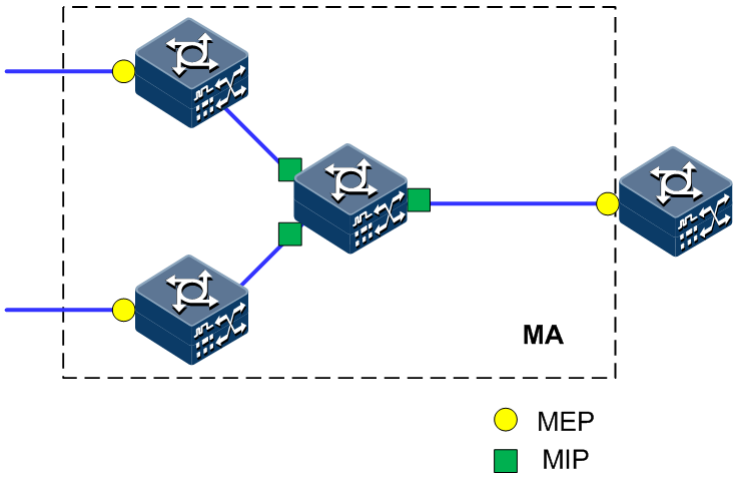


Figure 4-7 MEP and MIP network

- MIP

MIP is the internal node of a service instance, which is automatically created by the device. MIP cannot actively send CFM packets but can process and response to LinkTrace Message (LTM) and LoopBack Message (LBM) packets.

- MP

MEP and MIP are called Maintenance Point (MP).

CFM can provide following OAM functions:

- Fault detection (Continuity Check, CC)

By periodically sending Continuity Check Message (CCM) packets, this function can be realized. One MEP sends CCM and other MEPs in the same service instance can verify the RMEP status when receiving this packet. If the RC1108 fails or a link is incorrectly configured, MEPs cannot properly receive or process CCMs sent by RMEPs. If no CCM is received by a MEP during 3.5 CCM intervals, it is believed the link fails. Then a fault alarm will be sent according to configured alarm priority.

- Fault acknowledgement (LoopBack, LB)

This function is used to verify the connectivity between two MEPs through the source MEP sending LoopBack Message (LBM) and the destination MP sending LoopBack Reply (LBR). The source MEP sends a LBM to a MP who needs to acknowledge a fault. When receiving the LBM, the MP sends a LBR to the source MEP. If the source MEP receives this LBR, it is believed the route is reachable. Otherwise, a connectivity fault occurs.

- Fault location (LinkTrace, LT)

The source MEP sends LinkTrace Message (LTM) to the destination MP and all MPs on the LTM transmission route will send a LinkTrace Reply (LTR) to the source MEP. By recording valid LTR and LTM, this function can be used to locate faults.

In general, CFM is an end-to-end OAM technology on server layer. It helps reduce operation and maintenance cost. In addition, it improves the competitiveness of service providers.

4.2.3 SLA

Service Level Agreement (SLA) is an agreement between users and a service provider about the service quality, priority and responsibility. It is a telecommunication service evaluating standard negotiated by the service provider and users.

In technology, SLA is a real-time network performance detection and statistic technology, which can collect statistics on responding time, network jitter, delay, packet loss ratio, etc. SLA can be used to monitor related metrics by selecting different tasks for different applications.

Basic concepts involved in SLA are shown as follows:

- Operation

It is a static concept. It is a point-to-point SLA network performance testing task, including Layer 2 network delay/jitter test (y1731-echo/y1731-jitter).

- Test

It is a dynamic concept. It is used to describe an execution of one operation.

- Detection

It is a dynamic concept. It is used to describe a procedure for sending-receiving detection packets in a test. According to the definition of operation, one test can contain multiple detections (For an Echo operation, one test contains only one detection.).

- Schedule

It is a dynamic concept. It is used to describe a schedule of one operation. One schedule contains multiple periodical tests.

4.3 Backup and upgrade system software

4.3.1 System software

System software refers to all files required when the RC1108-SHDSL-2W×8 is running, such as the BootROM file, system startup software, the configuration file, and the FPGA file. System software is saved in memory of the RC1108-SHDSL-2W×8 and is managed in file system to facilitate you to manage the memory. The file system function includes backup, upgrade, and deletion of system files.

BootROM file

The BootROM file is used to boot and initialize the RC1108-SHDSL-2W×8. You can upgrade the BootROM file though serial port with xmodem protocol or File Transfer Protocol (FTP). By default, the BootROM is named bootrom or bootromfull.

You can upgrade the BootROM file upon new release in the following two methods:

- Trivial File Transfer Protocol (TFTP) or FTP in command mode
- TFTP or serial transmission in BootROM mode

Configuration file

The configuration file contains the configured items to be loaded upon system power-on. Its suffix is .conf. You can open it through Notepad on Windows OSs. Its features are as below:

- Parameters are saved in mode+command line format.
- Only non-default parameters are saved. For the default value of each parameter, see *RC1108-SHDSL-2W×8 Command Reference*.
- Command lines are organized with mode as basic framework. Command lines of the same mode are organized together as a section. Sections are separated by the exclamation mark (!).

After being powered on, the RC1108-SHDSL-2W×8 reads the configuration file from the memory to initialize itself. The configuration in this file is called the default configuration. The configuration being used by the RC1108-SHDSL-2W×8 is called the current configuration.

If no configuration file is saved in the memory, the RC1108-SHDSL-2W×8 will be initialized with default configuration.

You can modify current configuration through command lines. To enable current configuration to be loaded upon next power-on, you must save it to the memory as the configuration file.

The operations on the configuration file include backup, upgrade, and deletion.

4.3.2 Backup and upgrade

Backup

Backup is to save system files in the memory of the RC1108-SHDSL-2W×8 to the memory of a server so as to recover the backup files and ensure the normal running of the device when the device fails. To recover the old system files upon the following failures:

- System file is lost or damaged due to device failure.
- Device operating failure due to upgrade failure.

It is recommended that user periodically backups system files (for example BootROM file, system startup software, configuration file, FPGA file etc.) of the RC1108-SHDSL-2W×8 to the memory of a server.

Upgrade

To add new features, optimize previous functions or solve the current software version Bug, user can upgrade the device system software (BootROM file, system startup software, configuration file, FPGA file etc.).

Three modes to upgrade the RC1108-SHDSL-2W×8:

- Through serial port in RootROM mode
- Through TFTP in BootROM mode
- Through FTP or TFTP in system configuration mode

5 Technical specifications

This chapter contains the following sections:

- Interface parameters
- EMC specifications
- Lightning prevention requirements
- Specifications
- Environment requirements

5.1 Interface parameters

5.1.1 G.SHDSL interface parameters

The RC1108-SHDSL-2W×8 has 8 G.SHDSL interfaces, with parameters listed in Table 5-1.

Table 5-1 G.SHDSL interface parameters

Parameter	Description
Interface type	RJ45. Each RJ45 interface provides 4 G.SHDSL interfaces
Interface speed	Single line pair, each line transmission speed is 64 Kbit/s–15 Mbit/s
Duplex mode	Full/Half duplex/Auto-negotiation
Coding scheme	Comply with ITU-T G.991.2 standard, supporting PAM 4, PAM 16, PAM 32, PAM 64 and PAM128
Link mode	Fixed rate mode and link probe mode
Connection cable	Category-3 twisted pair

5.1.2 GE electrical interface parameters

The RC1108-SHDSL-2W×8 has 1 GE interface, with parameters listed in Table 5-2.

Table 5-2 GE electrical interface parameters

Parameter	Description
GE interface type	RJ45
Interface speed	10/100/1000 Mbit/s
Duplex mode	Full/Half duplex/Auto-negotiation
Flow control	Comply with IEEE 802.3 standard

5.2 EMC index

The RC1108-SHDSL-2W×8 complies with the ETSI EN 300 386 V1.4.1 standard.

5.3 Lightning prevention requirements

Table 5-3 lists the lightning prevention requirements.

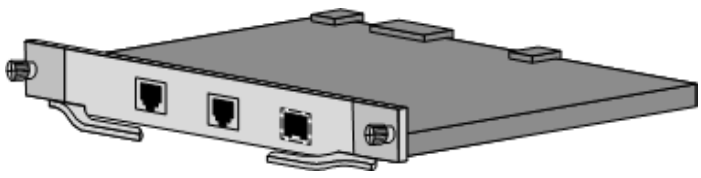
Table 5-3 Power and interface lightning prevention requirements

Item	Type	Lightning prevention requirements
Power	AC	• Common mode 2kV • Differential mode 1kV
	DC	–
Interface	G.SHDSL interface	• Common mode 4kV • Differential mode 4kV
	GE interface	Common mode 4kV

5.4 Specifications

Table 5-4 lists the specifications of the RC1108-SHDSL-2W×8.

Table 5-4 The specifications of RC1108-SHDSL-2W×8

Item	Specifications
Appearance	
Dimension (mm)	240 (Width)×225 (Depth)×25 (Height)

Item	Specifications
	Note The device dimension is shown above, “Height” and “Width” defines the card panel dimension, “Depth” defines the PCB depth.
Weight (kg)	0.4
Power consumption (W)	<20

5.5 Environment requirements

Table 5-5 lists environmental requirements on RC1108-SHDSL-2W×8.

Table 5-5 Environmental requirements on RC1108-SHDSL-2W×8

Item	Requirements
Operating temperature (°C)	-5 to +50
Relative humidity (RH)	≤ 90% (35℃), no condensation
Storage temperature (℃)	-25 to +60
Atmosphere (kPa)	86–106 (70 kPa is equivalent to altitude 3000 m)
Dust free/Water proof requirements	• No special requirements. • IP level is 20.
Noise (dBA)	72–75 in telecom equipment room

6 Device installation

This chapter contains the following sections:

- Device unpacking
- Electrostatic safety
- Card installation
- Installation check
- Software installation

6.1 Device unpacking

Caution

- Electronic components are vulnerable to ESD (Electro Static Discharge) damage. To open the packing box, user needs to wear a properly grounded anti-static wrist, and only get in touch with the edge of the component.
- Stop opening the box immediately if the component is found to be rusted or flooded in unpacking process. Give feedback to the local RAISECOM office after finding out reasons by customers and RAISECOM engineers.

Please pay attention to the following items in the process of opening the packing box:

- Take anti-static protection measures to avoid component damage.
- Pay attention to the impact of environmental temperature and humidity.
- Take the edge of the circuit board to avoid touching the device and printed circuits with hands.

The steps to open packing box:

Step 1 Check each component packing box to make sure whether there is obvious damage.

Step 2 Wear an anti-static wrist and make it grounded properly.

Step 3 Open each box and take out component, as shown in Figure 6-1.

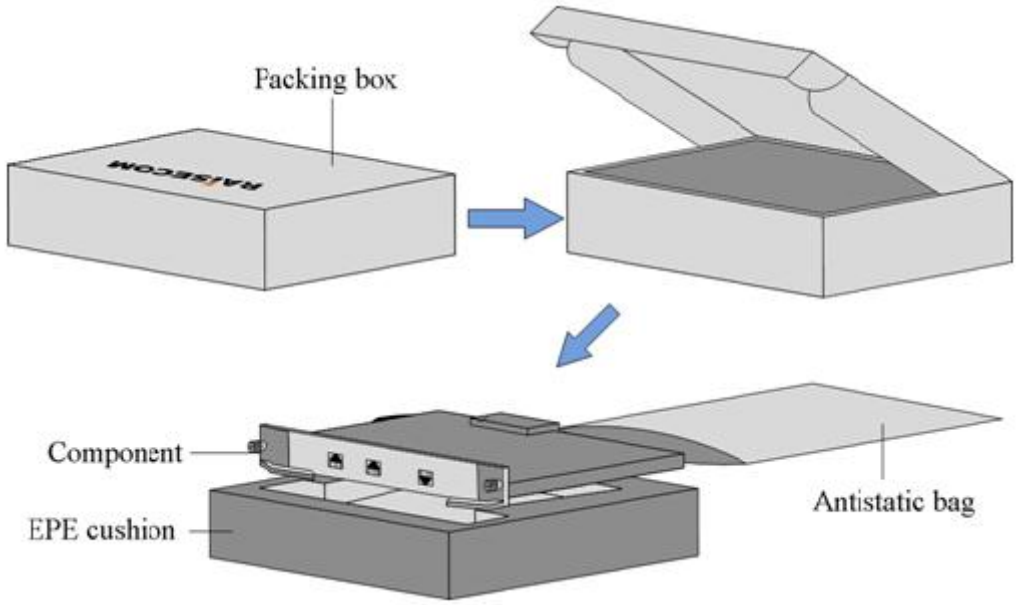


Figure 6-1 Device unpacking

Step 4 Check whether the component is damaged and choose processing method. Execute step 5 if the component need to be installed immediately; if not, execute step 6.

Step 5 Put component on the surface of antistatic materials for electro discharge treatment, and then install them.

Step 6 Package the component again with original packing materials, and store it in a dry and cool environment to avoid sunlight and strong electromagnetic radiation source interference.

6.2 Electrostatic safety

6.2.1 Electrostatic safety

Caution

- Any time contacting equipment or component, working staff must wear ESD wrist. ESD wrist should contact with the skin, and insert the plug to ESD socket on the equipment.
- Avoid any contact between component and clothes because the ESD wrist can't prevent the component from producing electrostatic when contacting with clothes.

In equipment installation, take the anti-static measure to avoid device damage.

Antistatic rules are as below:

- The equipment should be grounded properly in accordance with requirements.
- To prevent body electrostatic from damaging the equipment, working staff must wear ESD wrist before contacting equipment or component and make sure the other side of ESD wrist connects the ground correctly.

- To guarantee anti-static wrist in working condition, the system resistance should be at the range of 0.75 MΩ–10 MΩ. If the resistance is not enough, change a new anti-static wrist in time.

6.2.2 Anti-static preparation

Please wear anti-static wrist before device installation. The anti-static wrist is shown below.

Figure 6-2 Anti-static wrist

Please wear the anti-static wrist according to the following steps:

Step 1 Put hand into anti-static wrist, as shown in Figure 6-3.

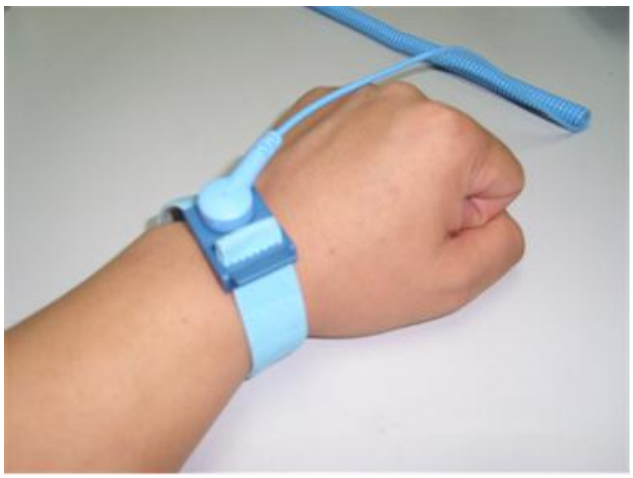


Figure 6-3 Wear anti-static wrist

Step 2 Tighten the lock catch, and confirm the anti-static wrist gets well with skin.

Step 3 Insert the anti-static plug into anti-static jack in the front panel of chassis, as shown in Figure 6-4.

Figure 6-4 Connect anti-static jack

6.3 Card installation

6.3.1 Confirm installation slot

The RC1108-SHDSL-2W×8 needs to be installed on OPCOM3500E (B) chassis or iTN2100 chassis.

The slot distribution of OPCOM3500E (B) is shown in Figure 6-5. User can select the proper installation slot according to the card type.

- Install NMS card, select slot0
- Install the RC1108-SHDSL-2W×8, select slot1-slot5, slot8, slot10–slot12
- Install aggregation card, select slot6 or slot7
- Switching card can only be installed in slot9
- Install power card, select POWER1 and POWER2

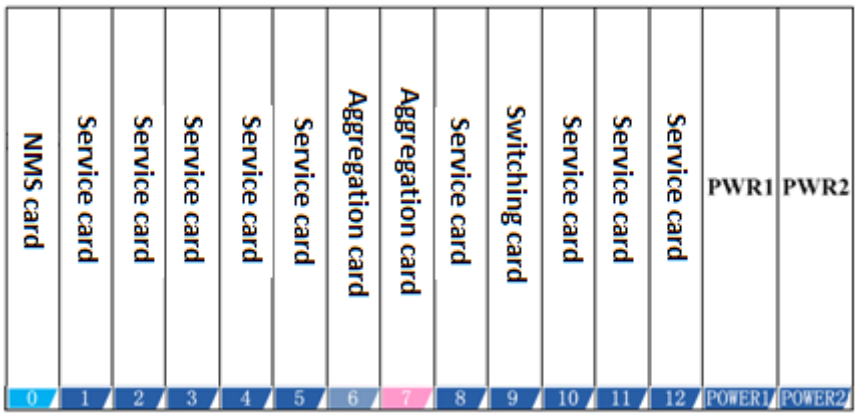


Figure 6-5 OPCOM3500E (B) slot distribution

The slot distribution of iTN2100 is shown in Figure 6-6. User can select the proper installation slot according to the card type.

- Install NMS card, select slot0
- Install the RC1108-SHDSL-2W×8, select slot1-slot5, slot8, slot11–slot12
- Install aggregation card, select slot6 or slot7
- Switching card can only be installed in slot9 or slot10
- Install power card, select POWER1 and POWER2

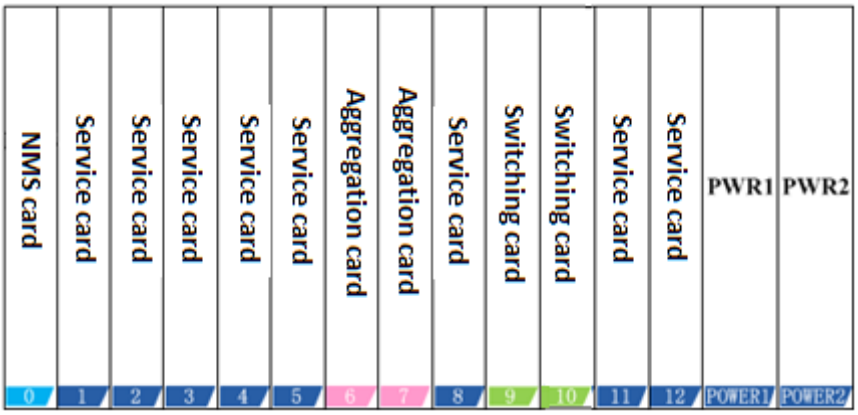


Figure 6-6 iTN2100 slot distribution

Note

There is a terminal jumper cap in the packing box, used in conjunction with J8 jumper on the card to select chassis type. Plug in the jumper cap to install the card on OPCOM3500E (B) chassis; not plug in the jumper cap, install the card on iTN2100 chassis.

6.3.2 Install card

Caution

To install the card, if the card panel connects with the cable, please pull out the cable at first.

Please install the card according to the following steps:

Step 1 Wear anti-static wrist

Step 2 Mark sure the installation slot of card and remove the blank panel on slot, as shown in Figure 6-7.

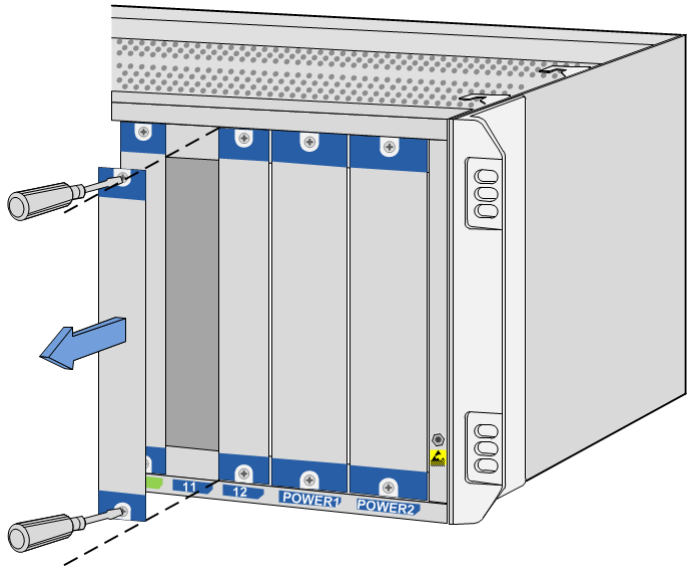


Figure 6-7 Remove the blank panel on chassis slot

Step 3 Insert the card into chassis stably along the slide rail of chassis slot, as shown in Figure 6-8.

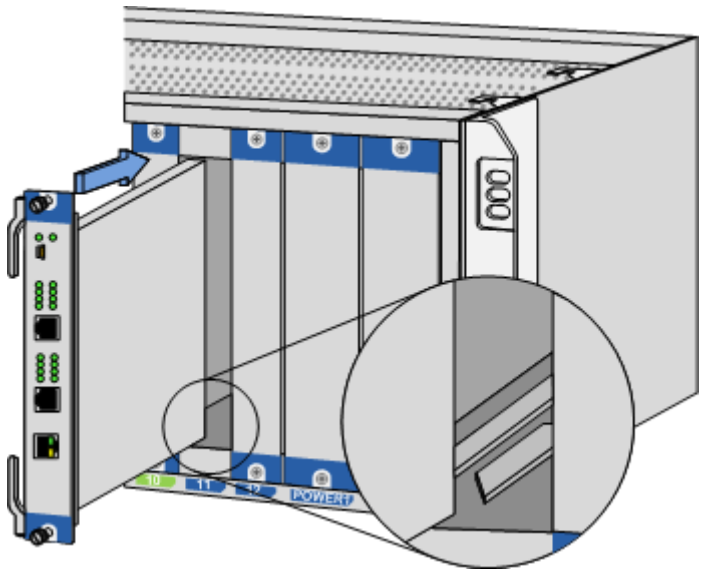


Figure 6-8 Insert the card into chassis

Step 4 Switch the up/down wrench on the card out to make the wrench grip with chassis border.

Step 5 Turn the wrench of card inward with hands to make the card fully insert and fasten, as shown in Figure 6-9.

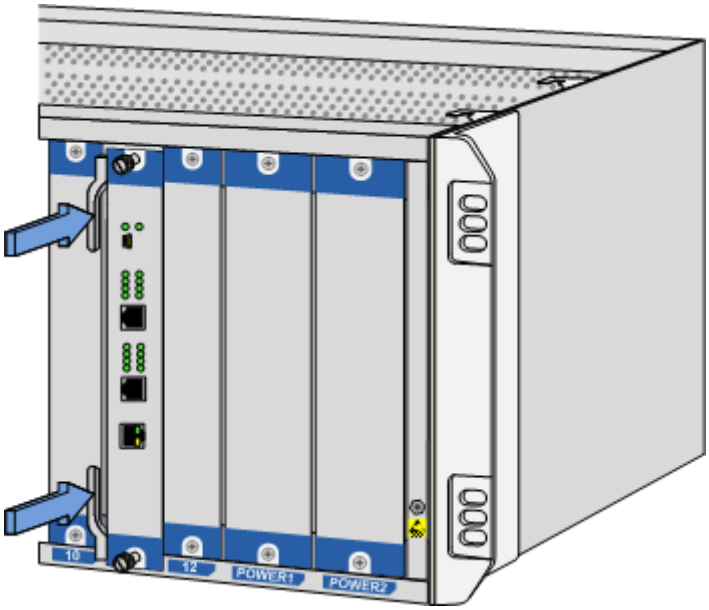


Figure 6-9 Turn the wrench inward

Step 6 Tighten the up/down captive screws tightly with a slotted point screwdriver, as shown in Figure 6-10.

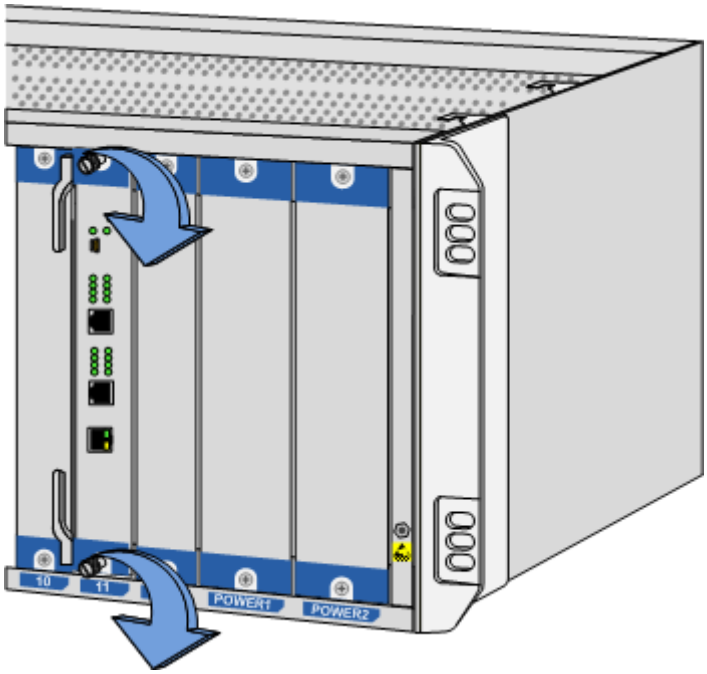


Figure 6-10 Tighten the screws

Note

- Install blank panel to the unused slot.
- During the installation process, if the card cannot be inserted, user can judge whether it is the correct slot inserted according to backplane needle on chassis backplane and the card.

- Please tighten the captive screws at both ends simultaneously after installing the card to the corresponding slot.

6.4 Installation check

6.4.1 Check machine room and the surrounding environment

Please check machine room and the surrounding environment according to Table 6-1 after installation.

Table 6-1 Checking machine room and the surrounding environment

Item	requirement
Cable	Strap or splice the surplus cables to fix them to the reserve place inside the rack to be expanded to facilitate the future expansion maintenance and avoid loss.
Plug	Protect the unused plugs and cover the protection caps.
Machine room environment	Keep clean and tidy, clear the obsolete packing boxes and other sundries. Stack the remaining spares neatly and reasonably. The value of grounding resistance should be less than 1 Ω, and at the same time refer to the relevant national or local standards.

6.4.2 Check rack

Please check the rack according to Table 6-2 after installation.

Table 6-2 Checking rack

Item	Requirement
Rack	• Structure attachments are installed correctly and reliably, switches of doors and locks work normally. • All other connection bolts are installed correctly and reliably, the flat washers and spring washers are installed in a correct order. • The installation location meets the engineering design manual. • The installation is fixed and reliable and consistent with the anti-seismic requirements described in engineering design manual. • The connection of earth wire is correct and reliable. • Anti-static wrist is connected to the ESD jack on the rack.

6.4.3 Check chassis and card

Please check the chassis and card according to Table 6-3 after installation.

Table 6-3 Checking chassis and card

Item	Requirement
Chassis	• Placed firmly and there is enough space for heat dissipation and operation maintenance around the device. The protective earth wire is connected correctly. • Fill with blank panels to slots without installing components for dust and electromagnetic shielding.
Components	• The installation slots of all components are correct. • Install all components firmly without slackening.

6.4.4 Check cables

Please check the cables according to Table 6-4 after installation.

Table 6-4 Checking cables

Item	Requirement
Power cable and ground cable	• The connection is correct and reliable. Power cable inside the rack, ground cable and signal line are laid separately; the distance among power cable outside the rack, ground wire and signal line meet the design requirements, generally greater than 3cm. • Wrap wire nose handle and bare wire required with heat-shrinkable tubing or insulating tape. There is no bare copper wire at wire nose and connection terminal, flat washer and spring washer are installed correctly. • Bind the wire straight and neatly, and all the wire clips should be aligned towards the same direction.
Cable	• The rack alignment is correct. • No damage, breakage, and middle connector. • The plug is clean and no damage; plugs made on site should be proper and plugs connection is correct and reliable. • The line routing is in line with the engineering design manual, easy to maintenance and capacity expansion. • Optical fibres, optical interfaces and flange plates should be connected reliably. • Laying tail fibre outside the cabinet shall take protective measures, such as adding bellows or channels, etc.

6.5 Software installation

The RC1108-SHDSL-2W×8 has already installed all the system required software before leaving factory so that the system can be powered up after hardware installation.

BOOTROM and system software can be installed and upgraded through command line or network management software; in command line mode, they can be upgraded in BOOTROM and system software.

Please refer to *RC1108-SHDSL-2W×8 G.SHDSL Configuration Guide* for the detailed information about BOOTROM and system software installation and operation.

6.5.1 BOOTROM file installation and upgrade

BOOTROM file is the RC1108-SHDSL-2W×8 guide program to initiate RC1108-SHDSL-2W×8. The RC1108-SHDSL-2W×8 has already installed BOOTROM before leaving factory. Power up the RC1108-SHDSL-2W×8 to run BOOTROM file, when it shows “Press space into Bootrom menu...”, please press space to enter BOOTROM menu bar and take operation according to the prompts.

6.5.2 System software installation and upgrade

The required files for the RC1108-SHDSL-2W×8 operation (such as system software, configuration files, etc.) are stored in the storage device. By default, for the commands with possible loss of data (such as the commands to delete and cover files, etc.), the file system will prompt the user for confirmation.

System software and configuration files can be uploaded to the server through TFTP protocol or FTP protocol (**upload** command), or downloaded to the RC1108-SHDSL-2W×8 system (**download** command).

6.6 Remove card

Caution

To remove the card, if the card panel connects with the cable, please pull out the cable at first.

Please remove the card according to the following steps:

Step 1 Wear anti-static wrist

Step 2 Loosen the up/down captive screws, as shown in Figure 6-11.

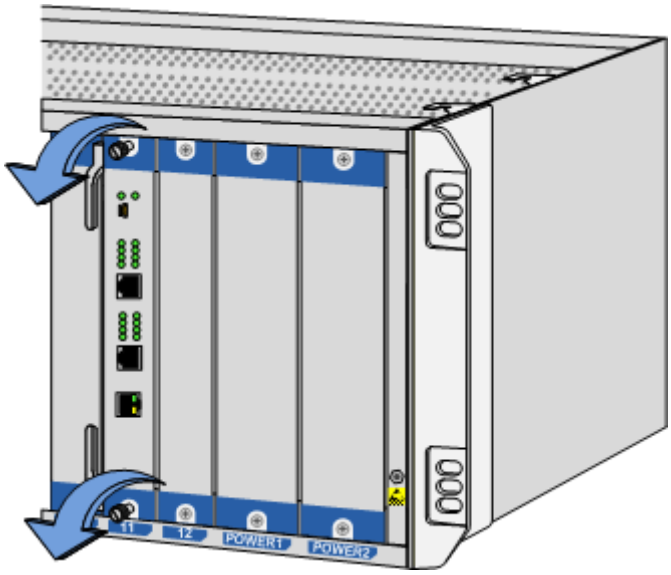


Figure 6-11 Loosen the screws

Step 3 Turn the up/down wrenches of the card outward to make the card break away from motherboard (or pull out it by 1cm), as shown in Figure 6-12.

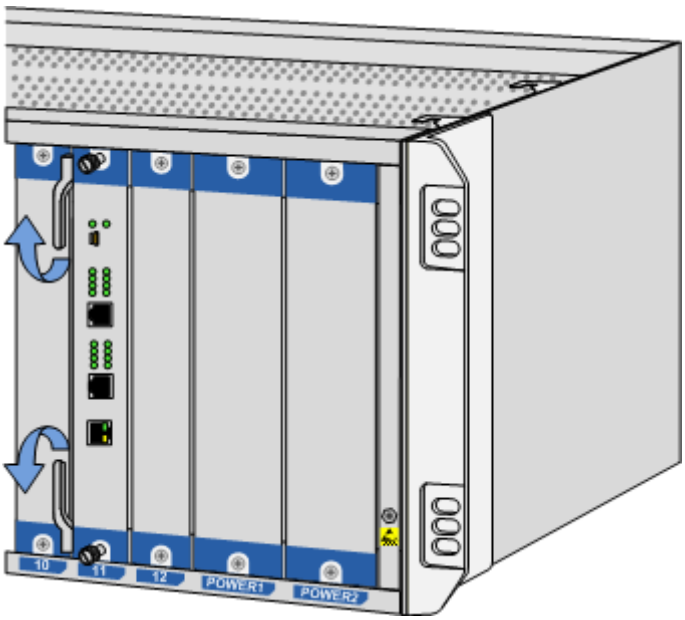


Figure 6-12 Turn the wrench outward

Step 4 Pull the card out gently and parallelly, as shown in Figure 6-13.

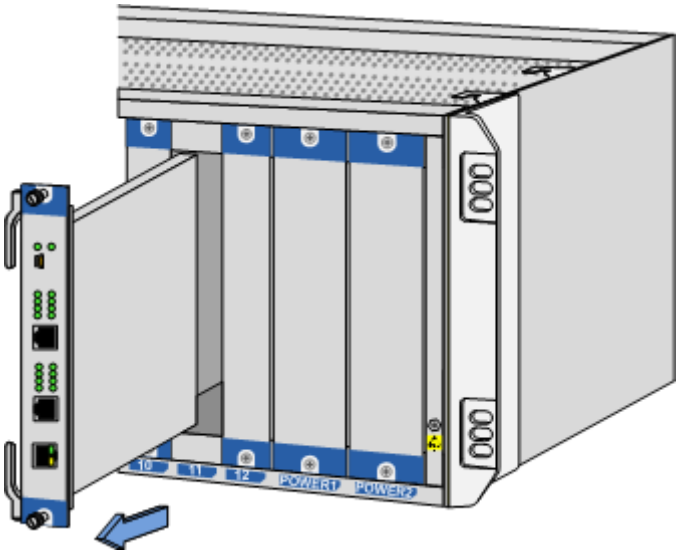


Figure 6-13 Pull the card out

Step 5 Place the removed card into static box or static bag. The vacated slot should be installed blank panel if no longer to install the card.

7 Cables

This chapter includes the following sections:

- Twisted pair
- Ethernet cable
- Configuration cables

7.1 Twisted pair

7.1.1 Introduction

The twisted pair is used to connect the G.SHDSL interface and user. The greater the diameter of the wire is, the longer distance it supports. After aligning line order through distributor frame, bind each user's services to the RC1108-SHDSL-2W×8. Make twisted pair on site.

7.1.2 Appearance

Figure 7-1 shows the appearance of the twist pair.

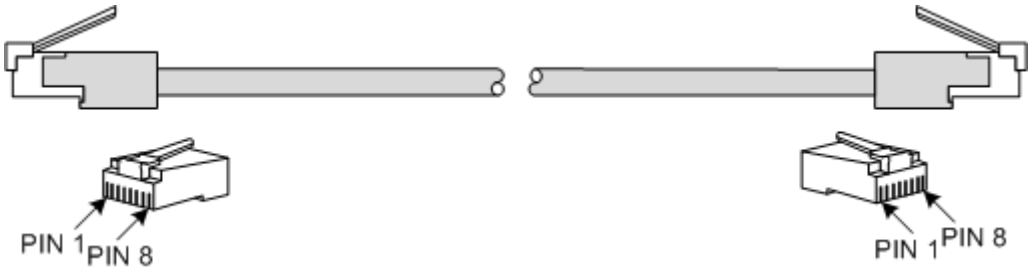


Figure 7-1 Appearance of the twist pair

7.1.3 Technical specifications

Table 7-1 lists technical specifications of the twisted pair.

Table 7-1 Technical specifications of the twisted pair

Item	Description
Connector	RJ45 crystal header
Model	Unshielded twisted pair-Cat3-0.4mm-26AWG-8 pins

7.1.4 Line order

When to use the twisted pair to connect G.SHDSL interface to the distribution frame, the corresponding relation between the line order at the distribution frame side and the G.SHDSL interface side is shown in Table 7-2:

Table 7-2 Corresponding relation between line order at distribution frame side and the G.SHDSL interface side

Wire pair / Interface	(4, 5)	(1, 2)	(7, 8)	(3, 6)
1-4 interfaces	1 interface	2 interface	3 interface	4 interface
5-8 interfaces	5 interface	6 interface	7 interface	8 interface

7.2 Ethernet cable

7.2.1 Introduction

The Ethernet cable is used to connect GE interface to access the user transmitting service.

7.2.2 Apperance

Figure 7-2 shows the appearance of the Ethernet cable.

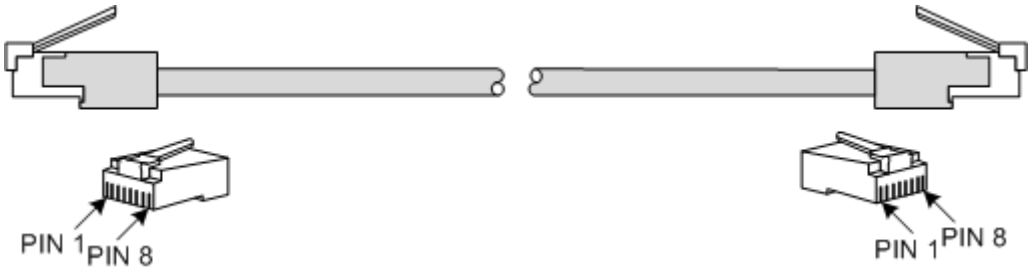


Figure 7-2 Appearance of the Ethernet cable

7.2.3 Technical specifications

Table 7-3 lists EIA/TIA568A standard line order and EIA/TIA568B standard line order description.

Table 7-3 EIA/TIA568A standard line order and EIA/TIA568B standard line order

Connector 1 (RJ45)	EIA/TIA568A standard line order	Connector 2 (RJ45)	EIA/TIA568B standard line order
PIN 1	White/Green	PIN 1	White/Orange
PIN 2	Green	PIN 2	Orange
PIN 3	White/Orange	PIN 3	White/Green
PIN 4	Blue	PIN 4	Blue
PIN 5	White/Blue	PIN 5	White/Blue
PIN 6	Orange	PIN 6	Green
PIN 7	White/Brown	PIN 7	White/Brown
PIN 8	Brown	PIN 8	Brown

Straight-through cable

Straight-through cable requires both ends of RJ45 connector use the same standard line order, generally for EIA/TIA568B standard line order, as shown in Figure 7-3.

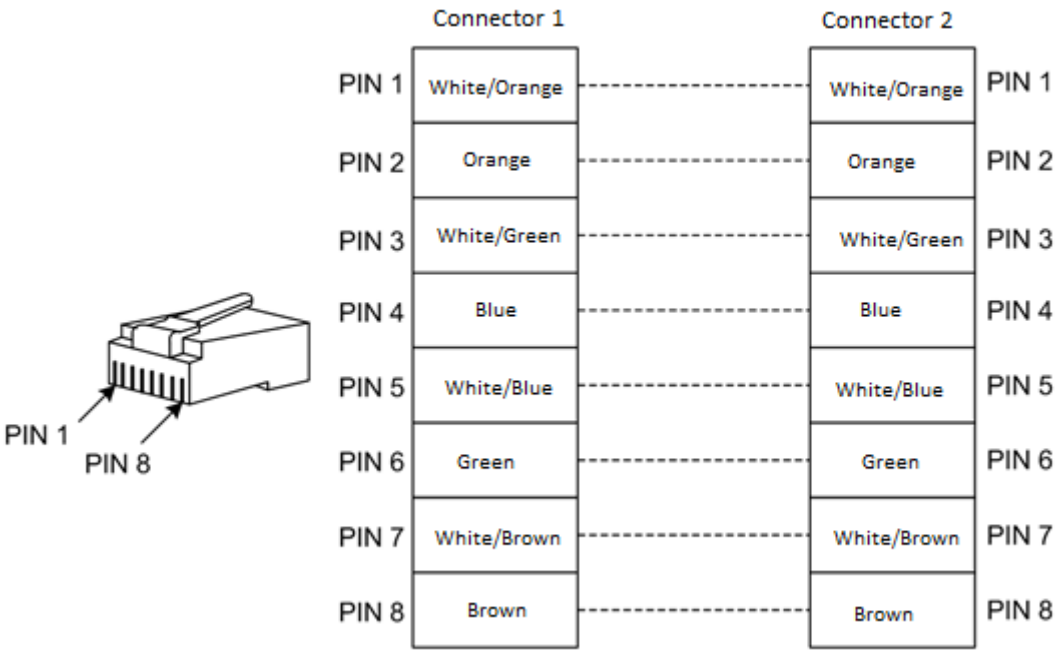


Figure 7-3 Straight-through cable wiring diagram

Cross-over cable

The standard line order of 100 Mbit/s cross-over cable and 1000 Mbit/s cross-over cable are different.

One end of RJ45 connector of 100 Mbit/s cross-over cable is EIA/TIA568A standard line order, the other end is EIA/TIA568B standard line order. The 100 Mbit/s cross-over cable wiring diagram is shown in Figure 7-4.

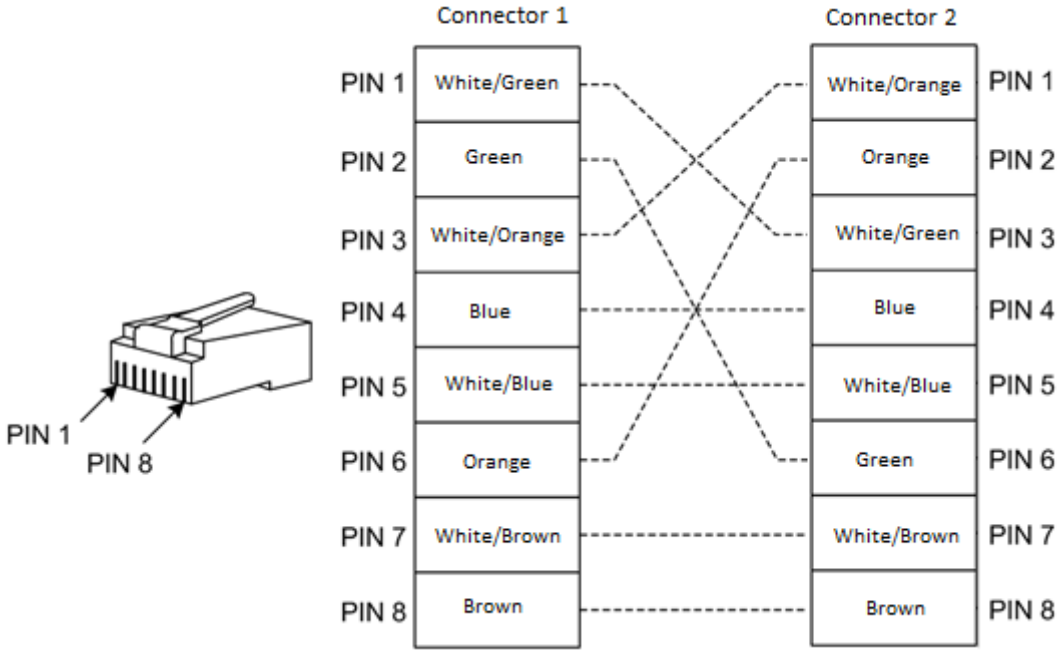


Figure 7-4 100 Mbit/s cross-over cable wiring diagram

1000 Mbit/s cross-over cable uses all the 8 twisted-pairs, the line order of PIN1 and PIN2 is exchanged with PIN3 and PIN 6; the line order of PIN4 and PIN5 also needs to exchange with PIN7 and PIN 8 on both ends of the cable. The 1000 Mbit/s cross-over cable wiring diagram is shown in Figure 7-5.

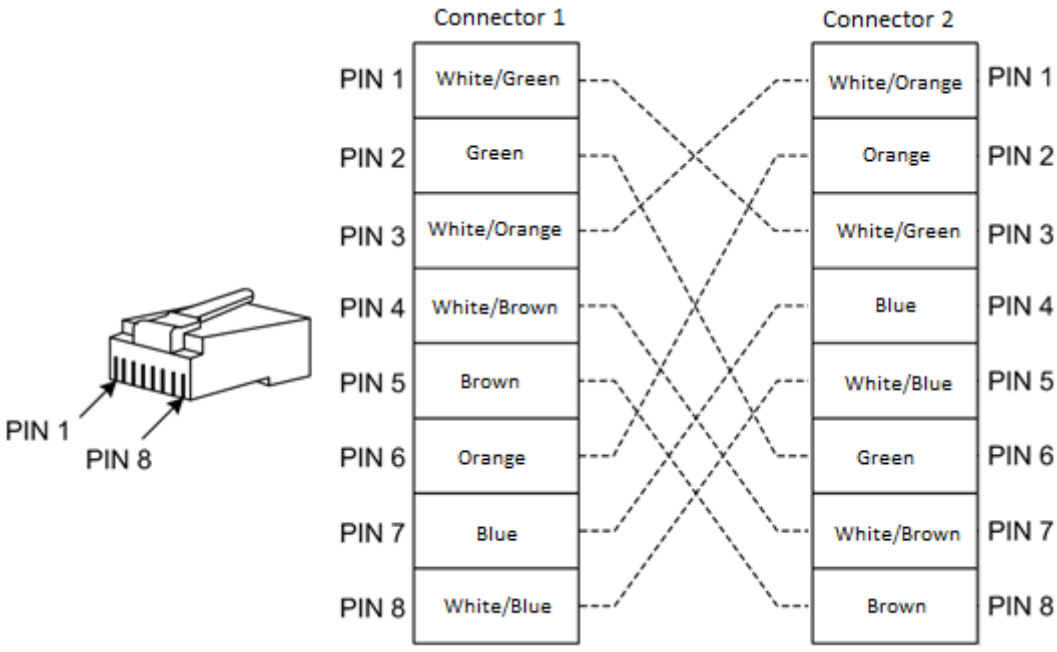


Figure 7-5 1000 Mbit/s cross-over cable wiring diagram

Only the names of two cables are different; straight-through cable is called CBL-ETH-RJ45/RJ45-D, cross-over cable is called CBL-ETH-RJ45/RJ45-X-D. The technical specifications of two network cables are shown in Table 7-4.

Table 7-4 Technical specifications of network cables

Item	Description
Color	Dark grey
Model	UTP-5, UTP-5e or STP
Connector type	RJ45 connector
Pin	8-pin
Length	The cable length D is made based on the customers' requirement. For example: the customer needs 2m cable, and then the cable name is CBL-ETH-RJ45/RJ45-2m.

7.3 Configuration cables

7.3.1 Introduction

The configuration cables are used to connect chassis network management board Console interface to the PC running terminal emulation program and to configure the RC1108-SHDSL-2W×8 through the command line.

7.3.2 Appearance

The configuration cables connector is DB-9 connector and RJ45 connector, as shown in Figure 7-6.

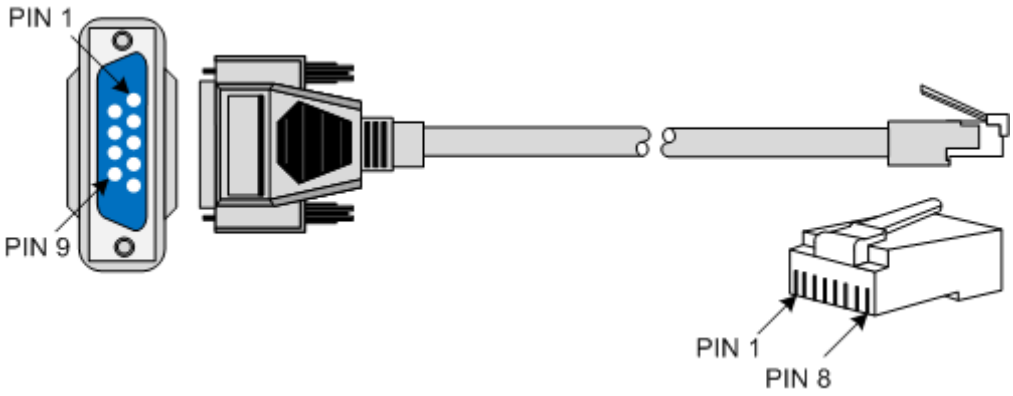


Figure 7-6 Configuration cables

7.3.3 Wiring relation

The PIN No. and wiring relation of RS-232 serial port and RJ45 Ethernet port are shown in Figure 7-7.

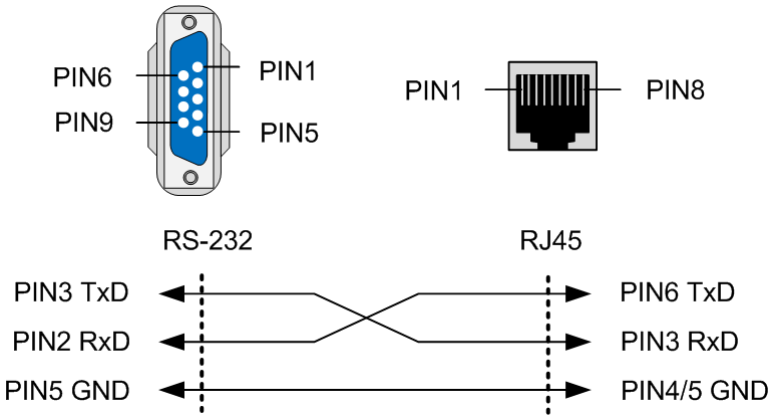


Figure 7-7 PIN No. and wiring relation

The RS-232 serial port PIN definition is shown in Table 7-5.

Table 7-5 RS-232 serial port PIN definition

PIN No.	Function	PIN No.	Function
PIN 1	NC	PIN 5	GND
PIN 2	NC	PIN 6	TxD
PIN 3	RxD	PIN 7	NC
PIN 4	GND	PIN 8	NC

RJ45 Ethernet port PIN definition is shown in Table 7-6.

Table 7-6 RJ45 Ethernet port PIN definition

PIN No.	Function	PIN No.	Function
PIN 1	DCD	PIN 6	DSR
PIN 2	RxD	PIN 7	RTS
PIN 3	TxD	PIN 8	CTS
PIN 4	DTR	PIN 9	RI
PIN 5	GND	-	-

7.3.4 Technical specifications

Table 7-7 shows the technical specifications of configuration cables.

Table 7-7 Technical specifications of configuration cables

Item	Description
Name	CBL-RS232-DB9F/RJ45-2m
Connector	RJ45 connector, DB9 female connector
Model	Unshielded Category-5 flat cable
Length	2m

8 Appendix

This chapter lists standards and protocols to comply with, terms, acronyms and abbreviations.

- Standards and protocols to comply with
- Terms
- Acronyms and abbreviations

8.1 Standards and protocols to comply with

- ITU-T G.991.2 Single-pair high-speed digital subscriber line (SHDSL) transceivers
- MEF Technical Specification MEF 6.1 Ethernet Services Definitions - Phase 2
- MEF Implementation Agreement, MEF 8 Implementation Agreement for the Emulation of PDH Circuits over Metro Ethernet networks
- MEF Technical Specification, MEF 10.1 Ethernet Services Attributes - Phase 2
- IEEE 802.1D-2004 Part 3: Media Access Control (MAC) Bridges
- IEEE 802.1Q-2005 - Standard for Local and Metropolitan Area Networks - Virtual Bridged Local Area Networks
- IEEE 802.1s-2002 - Amendment to 802.1Q Virtual Bridged Local Area Networks: Multiple Spanning Trees
- IEEE 802.3-2005 Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications
- IEEE 802.1ag：Virtual Bridged Local Area Networks Amendment 5: Connectivity Fault Management
- ITU-T Y.1541 Network Performance Objectives For IP-Based Services
- ITU-T Y.1731 OAM Functions and Mechanisms for Ethernet based networks
- RFC3260 New Terminology and Clarifications for Diffserv
- RFC3289 Management Information Base for the Differentiated Services Architecture
- RFC3290 An Informal Management Model for Diffserv Routers
- RFC3317 Differentiated Services Quality of Service Policy Information Base

8.2 Terms

A

ANNEX	According to the ITU-T G.991.2 standard, transmission modes for the SHDSL link are divided into ANNEX A and ANNEX B standards. The ANNEX A standard is used in America and Japan, also termed as an American mode. The ANNEX B standard is used in Europe, also termed as a European mode. Different standards represent different transmission capacities. In addition, the ITU-T G.991.2 standard also defines ANNEX A/F and ANNEX B/G standards. The ANNEX A/F is an American mode and is an extension of the ANNEX A standard. The ANNEX B/G is a European mode and is an extension of the ANNEX B standard.

C

Collision Domain	A section of a network where data packets can collide with one another when being sent on a shared medium or through repeaters. In traditional Ethernet, all devices transmit data packets through the same channel. Before sending data packets, these devices will listen to the network to avoid data collision. A network collision occurs when more than one device attempts to send a packet on a network segment at the same time. Two much data collision will reduce network performance. Therefore, when establishing network, you need to divide collision domain to avoid data collision. Collision domains are found in a hub environment where each host segment connects to a hub that represents only one collision domain. Modern wired networks use a switch to eliminate collisions. By connecting each device directly to a port on the switch, either each port on a switch becomes its own collision domain.

E

Ethernet in the First Mile	Complied with IEEE 802.3ah protocol, Ethernet in the First Mile (EFM) is a link-level Ethernet OAM technology. It provides the link connectivity detection function, link fault monitor function, and remote fault notification function, etc. for a link between two directly connected devices. EFM is mainly used for Ethernet link on edges of the network accessed by users.

G

G.Single-pair High Speed Digital Subscriber Line	G.SHDSL, defined by ITU-T, is a technology that supports bidirectional symmetrical bandwidth data service transmission through common twisted pair. Complying with ITU G.911.2 recommended standards, it uses 16-level grid coding pulse modulation technology of high performance, which compresses transmission frequency spectrum, improves anti-noise capacity, and supports 6 km transmission distance at most. Thus, it has more remarkable technical advantages over Asymmetric Digital Subscriber Line (ADSL).
Broadcast Domain	Broadcast domain describes a group of network stations that receives broadcast packets originating from any device within the group. If too much traffic is transmitted in a large broadcast domain, the network performance will be reduced greatly. What's worse, the network will be congested. Therefore, when establishing network, you need to divide the broadcast domain to improve the network performance. You can divide the broadcast domain with routers or by partitioning VLANs on a device.

L	
Link Aggregation	A computer networking term which describes using multiple networks cables/ports in parallel to increase the link speed beyond the limits of any one single cable or port, and to increase the redundancy for higher availability.
T	
SyncE	A technology adopts Ethernet link codes recover clock, similar to SDH clock synchronization quality, SyncE provides frequency synchronization of high precision. Unlike traditional Ethernet just synchronize data packets at receiving node, SyncE implements real-time synchronization system for inner clock.
Q	
802.1Q in 802.1Q	QinQ (also called Stacked VLAN or Double VLAN) technology is an extension of 802.1Q, which is defined in the 802.1ad standard defined by the IEEE. Basic QinQ is a simple Layer 2 VPN tunnel technology. At the ISP's access end, QinQ encapsulates an outer VLAN Tag for a private packet, so that the packet traverses the backbone network of the Internet Service Provider (ISP) carrying double VLAN tags.
V	
VLAN Mapping	VLAN Mapping is mainly used to replace the private VLAN Tag of Ethernet packets with Carrier's VLAN Tag, making packets transmitted according to Carrier's VLAN forwarding rules. During packets are sent to the peer private network from the Carrier network, the VLAN Tag is restored to the original private VLAN Tag, according to the same VLAN forwarding rules. Therefore packets are correctly sent to the destination.
X	
Virtual Local Area Network	VLAN is a protocol proposed to solve broadcast and security issues for Ethernet. It divides devices in a LAN into different segment logically rather than physically, thus implementing virtual work groups which are based on Layer 2 isolation and do not affect each other.
PAF	PAF refers to perform PME Aggregation Function (PAF) on virtual channels (VC). It bonds multiple lines (VCs) to create a new channel for transmitting services. You can configure PAF to get larger bandwidth.
Line-probe	In this mode, the device automatically probes a line and selects an optimum rate, according to configured SNR threshold, current or the worst SNR tolerance, as well as current line status. During the transmission process, the rate varies on the line status.

8.3 Acronyms and abbreviations

Numerics

A	
ADSL	Asymmetric Digital Subscriber Line
C	
CoS	Class of Service
CFM	Connectivity Fault Management
D	
DSCP	Differentiated Services Code Point
DMT	Discrete Multitone
E	
EFM	Ethernet in the First Mile
ESD	Electro Static Discharge
F	
FE	Fast Ethernet
FTP	File Transfer Protocol
G	
GE	Gigabit Ethernet
G.SHDSL	G.Single-pair High Speed Digital Subscriber Line
I	
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
ITU-T	International Telecommunications Union - Telecommunication Standardization Sector
L	
LACP	Link Aggregation Control Protocol

LBM	LoopBack Message
LBR	LoopBack Reply
LLDP	Link Layer Discovery Protocol
LLDPDU	Link Layer Discovery Protocol Data Unit
LTM	LinkTrace Message
LTR	LinkTrace Reply
M	
MA	Maintenance Association
MAC	Medium Access Control
MD	Maintenance Domain
MEG	Maintenance Entity Group
MEP	Maintenance associations End Point
MIB	Management Information Base
MIP	Maintenance association Intermediate Point
MP	Maintenance Point
MTU	Maximum Transfered Unit
O	
OAM	Operation, Administration and Maintenance
P	
PAF	PME Aggregation Function
PE	Provider Edge
Q	
QoS	Quality of Service
R	
RMON	Remote Network Monitoring

S	
SLA	Service Level Agreement
SP	Strict-Priority
SSHv2	Secure Shell v2
T	
TCI	Tag Control Information
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLV	Type Length Value
ToS	Type of Service
TPID	Tag Protocol Identifier
TC-PAM	Trellis Coded Pulse Amplitude Modulation
V	
VLAN	Virtual Local Area Network
W	
WRR	Weight Round Robin

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

Address: Building 2, No. 28, Shangdi 6th Street, Haidian District, Beijing, P.R.China.
Postal code: 100085 Tel: +86-10-82883305
Fax: 8610-82883056 http://www.raisecom.com Email: export@raisecom.com