RayView Network Management for RS1010

User Guide

V3.02

2014. 7

Revision History

Version	Date	Description
V3.00	2013-12-24	Primarily Released
V3.01	2014-6-20	
V3.02	2014-7-1	

Contents

Overview

1.1 Introduction

RayView network management system is developed to manage the RS1010 equipments; it adopts Client/Server structure, supports SNMP protocol; it performs excellent management to the network such as resource management, configuration management, alarm management, performance management and security management, which is compliant to ITU-T Recommendation. With its intuitively clear Graphical User Interface (GUI), the network operator can master RayView system easily in a short time.

This document is intended to instruct in the basics of RayView software installation, operation and maintenance. It is proper to Network Maintenance Engineer, Network Planning Designer, Equipment Commissioning Engineer and etc.

1.2 Feature

- Intuitively clear Graphical User Interface (GUI)
- Intelligible DXC configuration interface
- Client/Server structure
- Simple Network Management Protocol (SNMP)
- Ethernet management interface for network management
- Performs resource, configuration, alarm, performance and security management specified in ITU-T recommendation
- Overall management for local and remote equipment
- Real-time monitoring device interface status and quality of traffic transmission
- Remote Power Down detection (RPD) for fault location
- Perfect alarm and performance statistic

1.3 Client/Server Structure

RayView software is of 3 layers Client/ Server structure, see Figure 1-3-1:

According to Figure 1-3-1, RayView software is divided into 3 parts:

- Object application layer(Client terminal GUI object);
- Service object layer (Object module);
- Object resource layer (Device and Database);

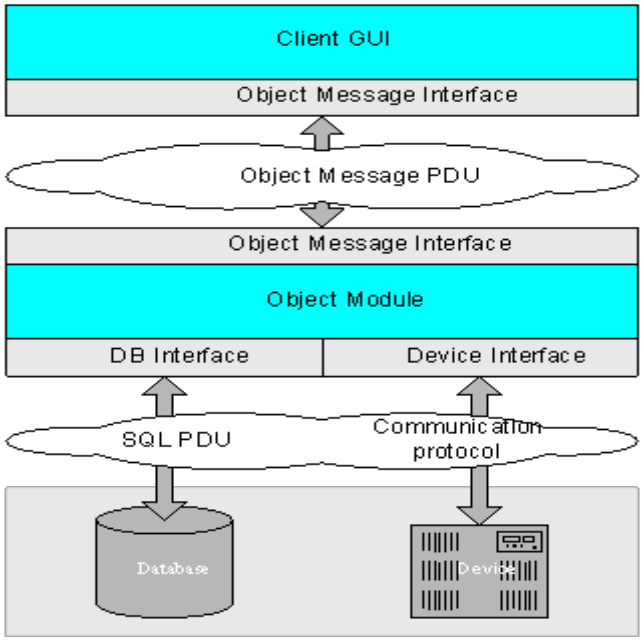


Figure 1-3-1 C/S Structure

The functional description of the three layers is as follows:

- ✧ Object application layer

  The object application layer provides user operation interface window, which is the typical "thin client", to deal with the window display, window alternation operation and the display logic related closely to the window operation, etc.; the client terminal adopts Java interface.

- ✧ Service object layer

  The service object layer equals to "middleware" service layer, consists of middleware service management process and managed object (MO). This layer aim to complete the information transmission between network/NE resource and client terminal.

- ✧ Object resource layer

  This layer is composed of 3 parts:

  a.NE real resource

  in the system, the NE real resource is provided by Proxy of NE gateway. The Proxy can implement the information transmission between the associated NEs by internal addressing protocol.

  b. NE resource mapping

  store a copy of data that is the same as the NE configuration data by database, called NE resource mapping; the database also stores the network resource data and NE history alarm for querying.

  c. Network resource

  Network resource refers to the relationship attribute between NEs, such as network topology relationship, link channel of end-to end, and etc. Generally, the information of this part is stored in network management database.

Installation and Login

1.4 Installation

Steps

System installation should be followed as the step below:

Step1 Start the setup program

Step2 Load installation wizard

Step3 Select installation directory

Step4 Copy file

Step5 Confirm installation completed

Step6 Start server automatically

Step7 Star client terminal manually

Note

1. Make sure that all the firewall , anti-virus software and WiFi are closed before the installation

2. Mase sure that the firewall and WiFi are closed during using this management software.

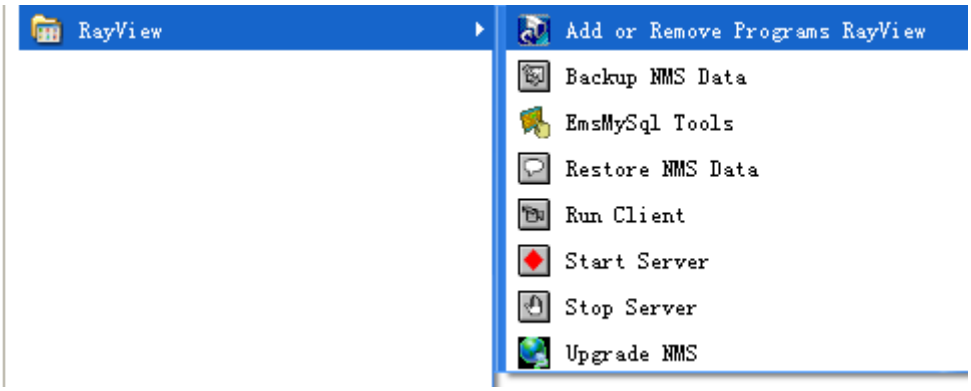
1.5 Uninstallation

Steps

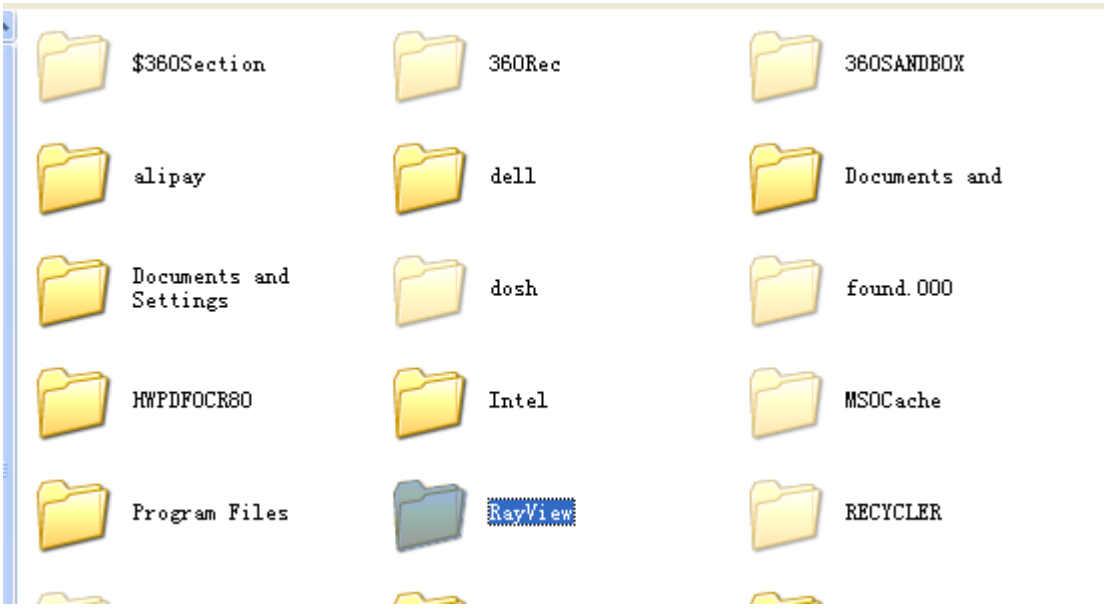
Step1 Click [Start-Programs-RayView-Add or Remove programs RayView]

Step2 Load uninstallation wizard

Step3 Do the uninstallation step by step



Step4 Under the installation directory, delete the RayView folder.



Note

1. Make sure that all the firewall , anti-virus software and WiFi are closed before the uninstallation

2. After uninstallation, you should delete the RayView folder under the installation directory, otherwise, the next installation of RayView may be unsuccessfull, or the rayview can not work normally.

1.6 Login

Steps

Step1: Select Language

Step2: Double click "Run Client" icon;

Step3: Type User name and password in the login dialog box;

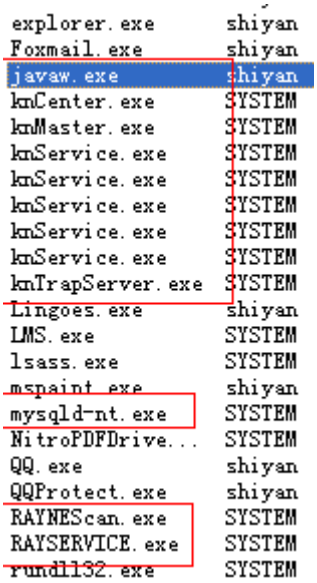
Step4: click 'OK' to enter

User name: 0001 Password: 0001

Note

1. There is only one default administrator ID "0001" and the default password is "0001" after RayView installation, which should be modified to guarantee the system security. When using the system, the administrator should create new user and assign them into the corresponding restriction group.

2. You can open task manager, make sure the following processes are exist.



Basic Operation

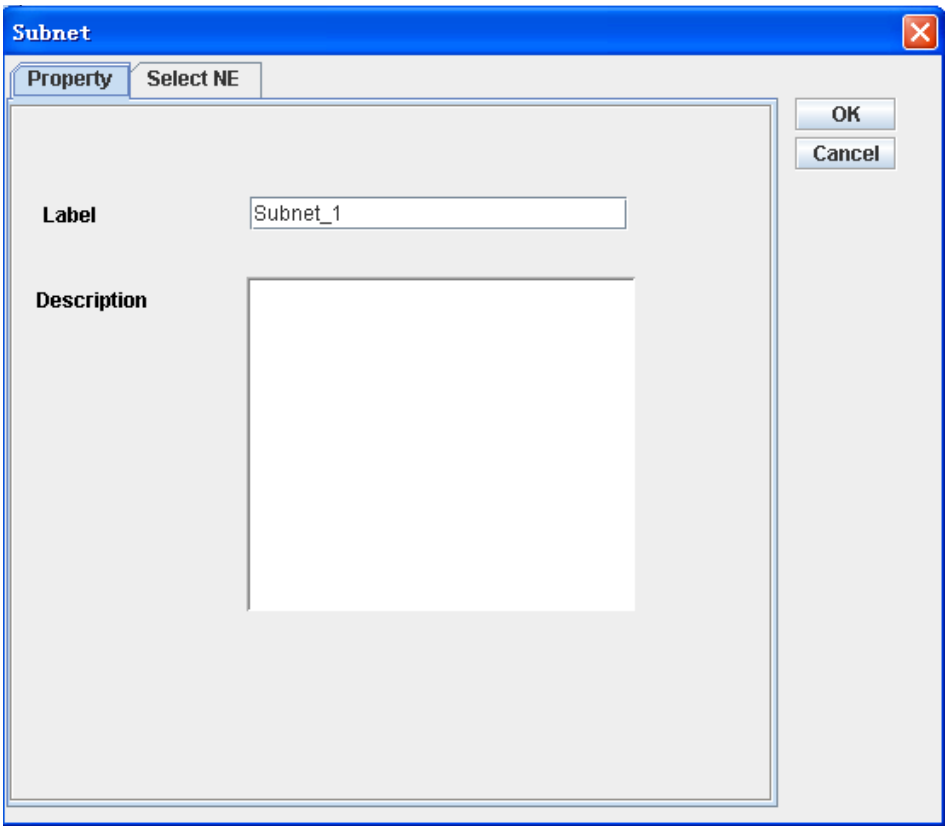
1.7 Create subnet

Steps

Click root node in the left side navigation bar, and then right-click to select [new subnet] in the right interface, the "new subnet" dialog box is shown:

Step1: input subnet label and description;

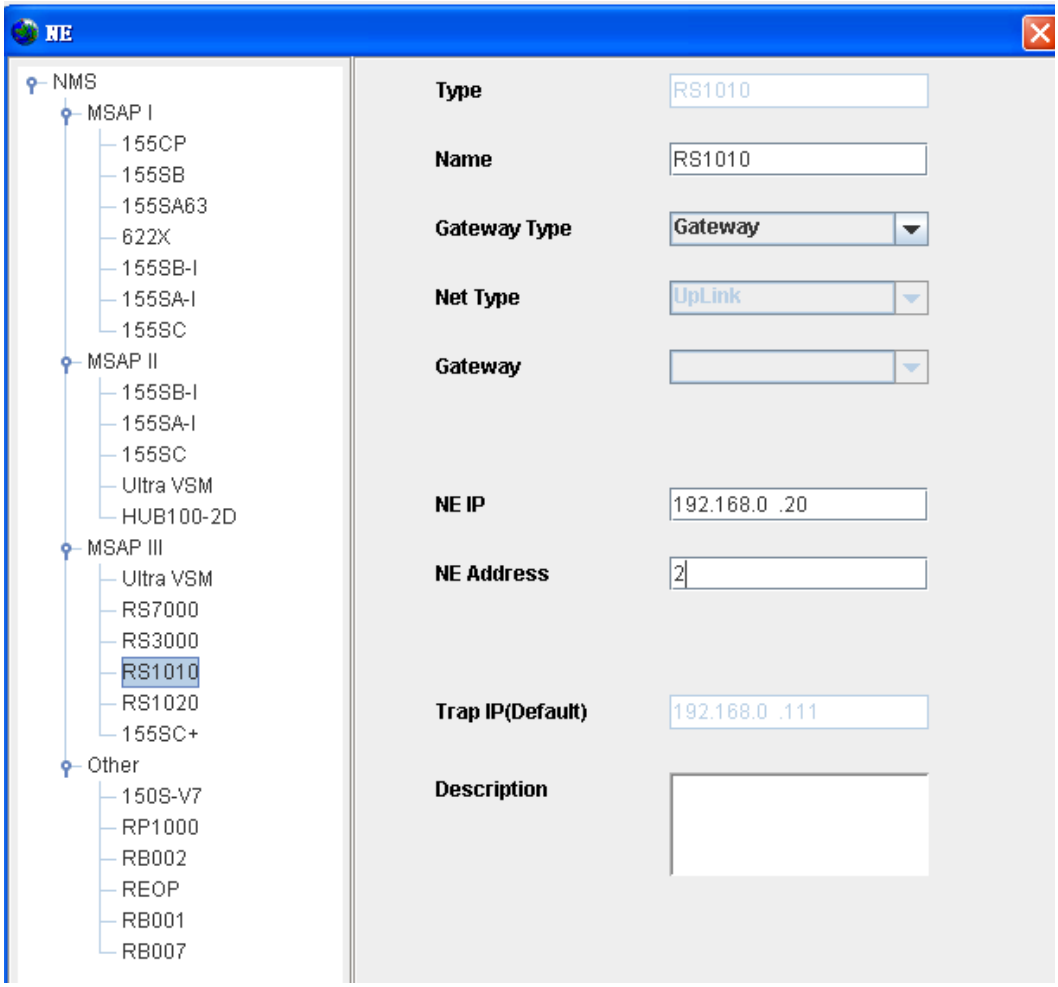
Step2: click <OK>



Note: subnet is just used as a container to carry NE, without any communication parameters.

1.8 Create NE

Steps



Step1: Click root node in the left side navigation bar or enter the subnet node which is already created, and then right-click to select [add NE device] in the right interface, the "NE" dialog box is shown:

Step2: Select the relevant NE device type from the list left side

Step3: input NE name, select gateway type, input IP and NE address;

Step4: Click<OK>

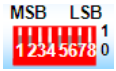
Step5： 

means the device is online, while 

means the device is offline.

Note

The range of the NE address is from 00 to 98, which is set by the address switch on the front panel of RS1010 equipment.

As Figure 

shows, the left 4-digit of the switch stands for tens of decimal figures, while the right 4-digit is 0--9. The code mode is 8421 BCD.

For example, the address of ‘10011000’ is ‘98’; the address of "00010101" is "15".

The NE address is unique mark used for network element management, as well as the number for phone. Different devices in a network can't be set to the same address.

1.9 Delete subnet

Steps

1, right-click the subnet icon which is to be deleted, select "delete", pop up the "delete subnet" dialog box.

2, click<OK> .

Note

Delete subnet operation do not delete the NE node, after subnet deleting, the contained NE node will be added under the root node automatically.

1.10 Delete NE

Steps

1, right-click the NE icon which is to be deleted, select "delete", pop up the "delete NE" dialog box.

2, click<OK> .

Note

Delete NE operation will delete all information about the NE, including the remote NE.

1.11 TCP/IP Communication

Purpose

Set IP of NE, gateway IP and subnet mask.

Steps

1. in the navigation tree, select [config-system Manager-TCP/IP communication]

2, click <refresh>, refresh the communication parameters.

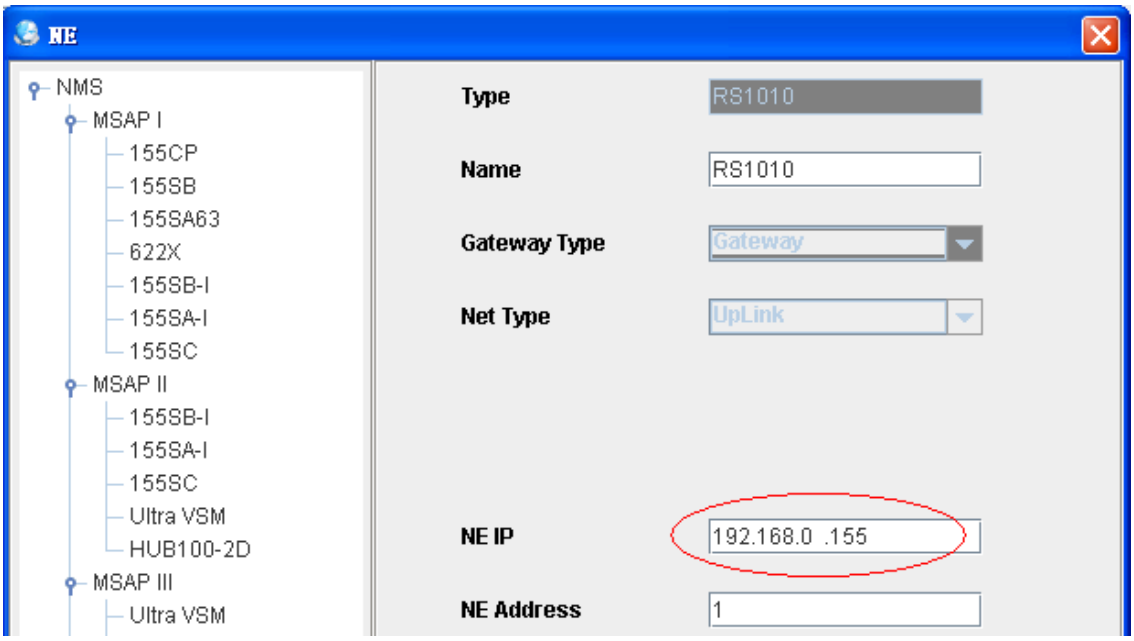
3, set IP of NE, gateway IP and subnet mask.

Note

Name	Description

NE IP	IP address of NE,the default IP address of NE is 192.168.0.155
Gateway	When managing the remote NE across network, TCP/IP communication can be implemented by router, the router IP is the gateway IP
IP mask	Subnet mask of the NE, which is used to determine subnet mask, whether the NE is on the local subnet or on a remote network.

Note 1, if the IP address of NE in "TCP/IP communication" is modified, the IP address of NE in "NE " window should also be modified, the IP address in two location should be the same.



Note 2: The default IP address is 192.168.0.155.

The address of NE(device) and PC shall be set and kept at the identical IP segment. For example, if the device IP is 192.168.0.155, while the IP of PC is 202.194.192.2, you should set the IP of PC as 192.168.0.154(for example), make the PC and device IP in the same IP segment, and the TCP/IP communication can be set up, and then change the IP of NE and IP of PC.

1.12 Trap IP

Purpose

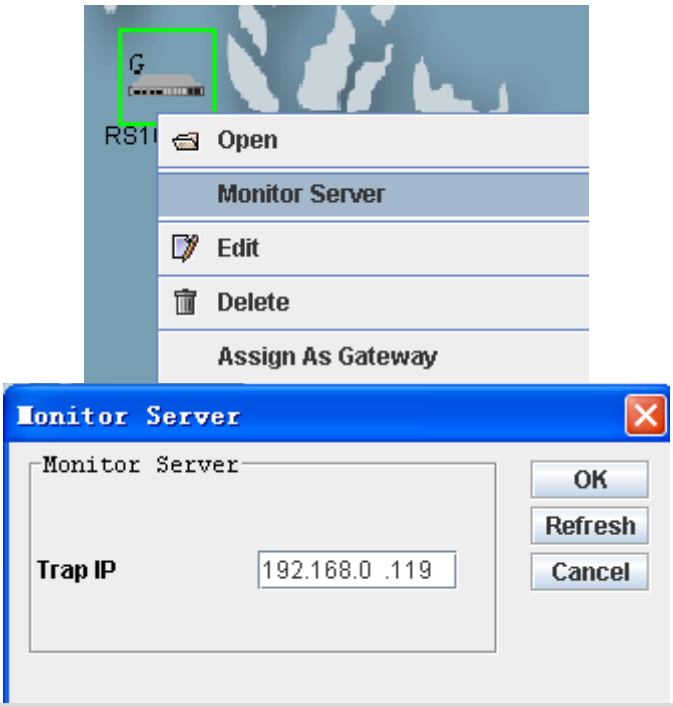
This part introduce how to configure alarm trap IP

Steps

1, right-click the NE icon ,select "Monitor Server"

2, input the monitor IP of PC.

3, click <OK>.



Note

The trap IP is the monitor sever IP address, that is the current IP address of PC.

The monitoring server helps engineers grasp the operating status of the network at any time. If an alarm occurred from the device, it will be transferred to the server and passed on to the client side.

1.13 User group management

1.13.1 New user group and group restriction

Purpose

This operation is for the users who are capable of system maintenance right at least in the group restriction item

Steps

Step1: select [system-security-user group];

Step2: Right-click to select [new] in the pop up menu;

Step3: Type the new user group information in the popped up dialog box, click<OK>.

Note: step1~3 is used to create user group.

Step4: After creating user group, the system will pop up [group restriction] menu, select the restriction for the user group and click<OK>.

Note: step4 is used to assign restriction for each user group.

1.13.2 Edit restriction of user group

Purpose

This operation is for the users who are capable of system maintenance right at least in the management restriction item

Steps

Step1: select [system-security-user group];

Step2: right-click group list to select [group restriction];

Step3: the [group restriction] menu will be popped up, edit restriction of user group, click <OK>.

1.14 User management

1.14.1 New user and user restriction

Purpose

This operation is for the users who are capable of system maintenance right at least in the management restriction item

Steps

Step1: select [system-security-user];

Step2: Right-click to select [new] in the popup menu;

Step3: Type the new user information in the popped up dialog box, click<OK>.

Note: Step1~3 is used to create users.

Step4: After creating user, the system will pop up [user restriction] menu, select the restriction for the user and click<OK>.

Note: step4 is used to assign restriction for each user.

1.14.2 Edit user restriction

Purpose

This operation is for the users who are capable of system maintenance right at least in the management restriction item

Steps

Step1: select [system-security-user];

Step2: right-click group list to select [user restriction];

Step3: the [user restriction] menu will be popped up, edit restriction of user, click <OK>.

1.15 Log viewer

Purpose

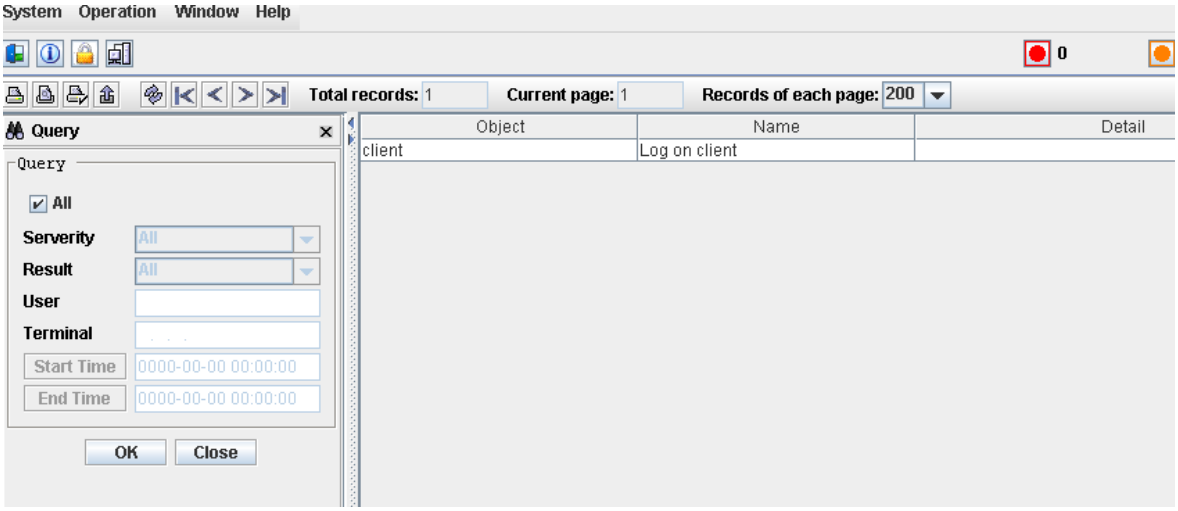
The operation log records all kinds of operations (includes device operation and system operation);

Steps

In the main menu of network topology layer, select [system - log viewer], to view the operation records;

Right-click-<query>, pop up query interface, you may set the query condition to view the log records freely.

Note: Currently, the log cannot be deleted



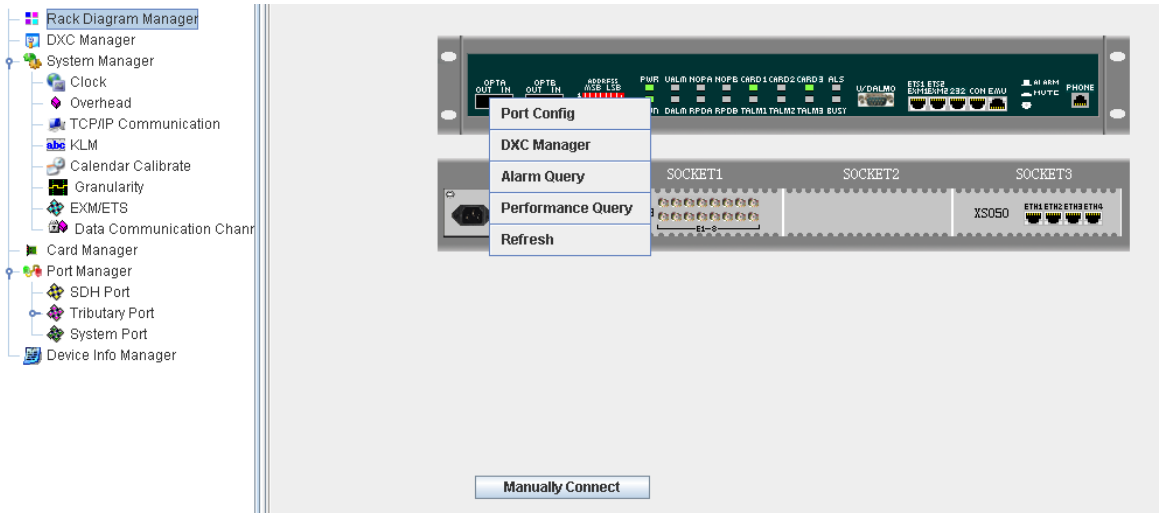
RS1010 Functional Modules

1.16 Rack Diagram Manager

Steps

1 In the navigation tree, select [Rack Diagram Manager],the rack diagram is shown ;

2 Right-click the ports on the rack panel,the configuration window will pop up, this is the shortcut way for configuration;



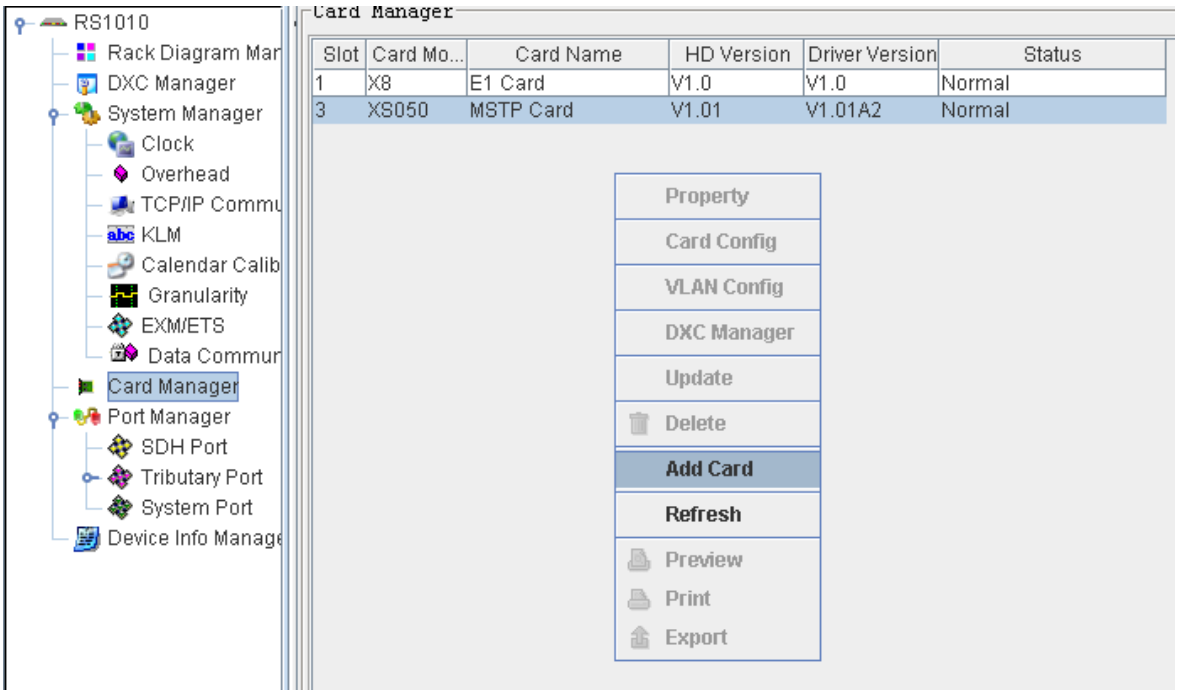
1.17 Card Manager

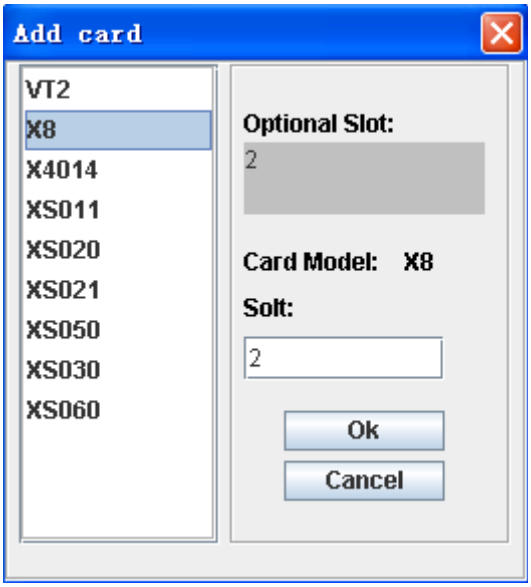
RS1010 provides several service cards such as E1 card, Ethernet card and to meet user's various requirements.

Steps

1 In the navigation tree, select [Config-card Manager],the card manager window is shown ;

2 Right-click and select "add card" ,the add card window will pop up.





Note

Socket1 and socket 2 are only for E1 card, and socket3 is only for Ethernet card.

1.18 Create DXC

RS1010 supports cross-connection, by which, the E1 traffic and Ethernet traffic can be assigned to any timeslot of OPTA/B, the creation and deletion of cross-connection can be implemented by management software. The protection type can be 1+1, 1+0.

Steps

1 In the navigation tree, select [DXC manager- DXC] to enter DXC circuit;

2 Right-click the blank and select [create], the DXC creator window pop up;

3 In the "DXC creator" window, select RS1010 and port from the source part, and E1 port/ VCG path from the destination part.

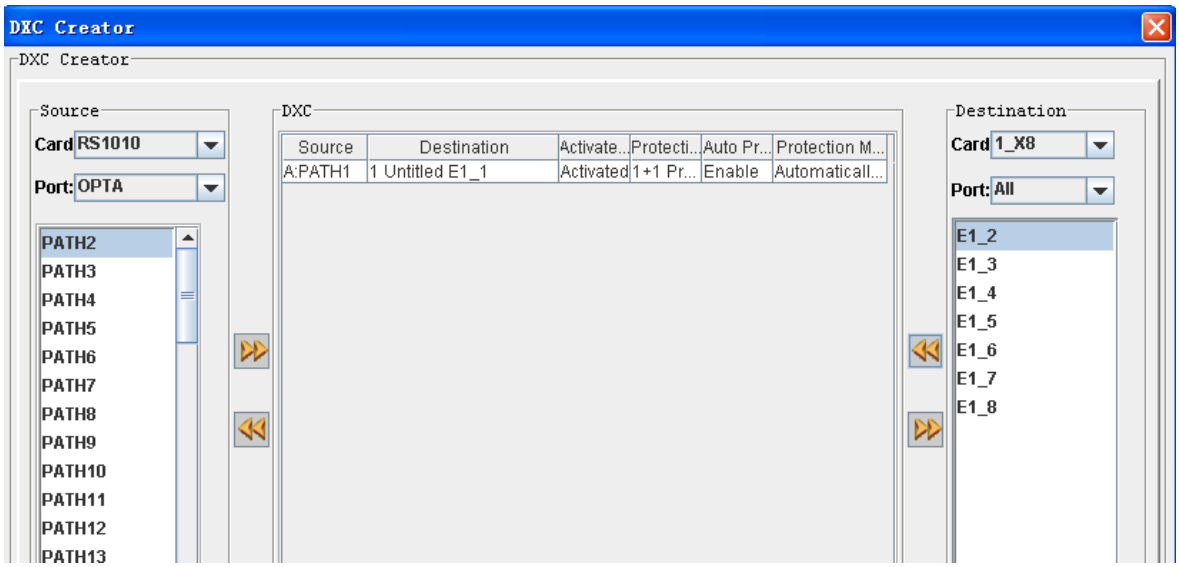
4 Select source path, such as PATH2, click Shift or Ctrl tab to select multiple continuous or intermittent paths. Click 

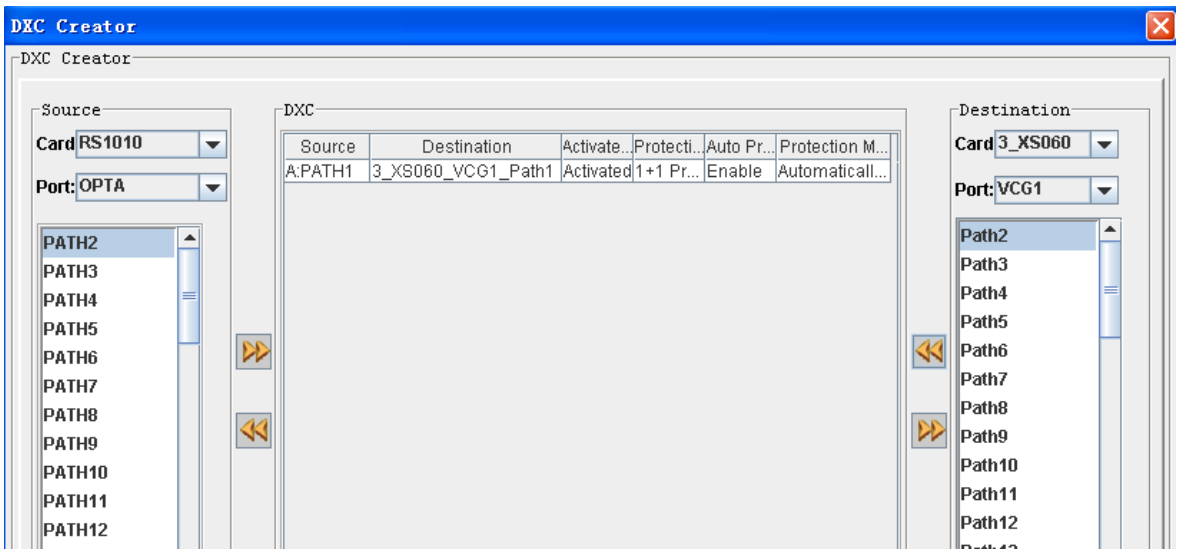
5 Click the created circuit, and then select the ;select the same number of destination E1 path. Click  . Thus the cross-connection circuit is created.

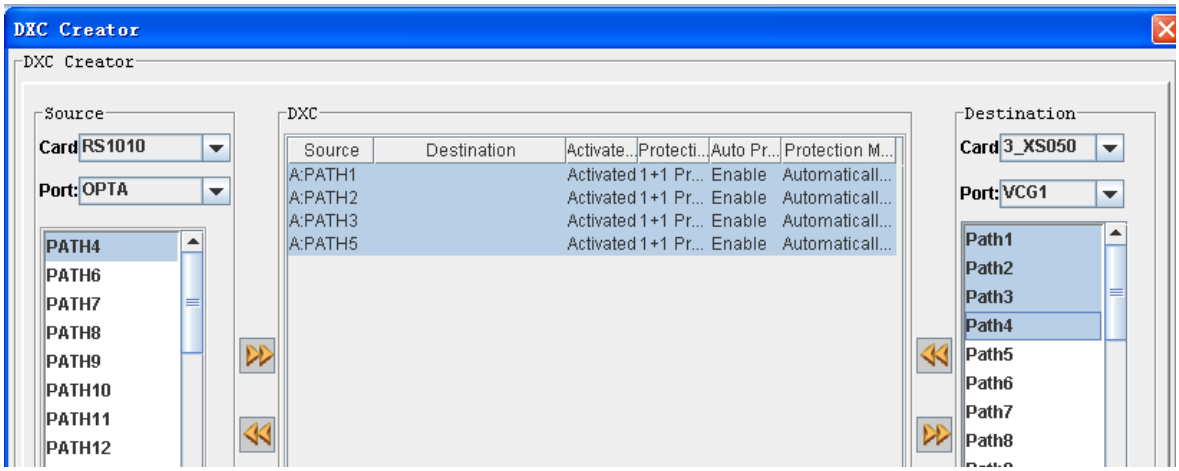
6 To modify the DXC circuit, select one or more records, right-click to do the “open/close protection” or “activate/inactivate” operation.

7 To reconfigure the circuit, right-click to select “clear table” to clear all the records.

8 Click “OK” button, the DXC circuit status is “pre-adding”.







Note

1. By default, there is no cross-connection, and all the timeslot resource is free.

2 The menu item description:

field	range	description
ID	e.g.:1, 2, 3, 4, 5	The number of the DXC circuit
Source	e.g.:A_ PATH1	The source of the circuit (including plate, slot, channel and timeslot)
Destination	e.g.E1_2	The destination of the circuit (including plate, slot, channel and timeslot)
Activated Status	Activate, inactivate	Indicate the circuit is available or not
Protection Type	1+1 mode 1+0 mode	1+1 mode:the client traffic is always transmitted in two directions, taking the same time slot, over the both working and protection path (VC12 or timeslot) simultaneously. 1+0 mode: the client traffic is transmitted over the dedicated working path without protection path standby. There is no protection path so the path of port A and port B with the same VC12 No. can be transmitted to different client traffic,
Auto Protection	ON ofF	（1）the DXC circuit for pass-through service do not supports protect function, it is "—" （2）when protection is 1+1 mode, it can be enabled or disabled; when protection is 1+0 mode, it is "—"
Protection Mode	Prefer switch to A Prefer switch to B Auto protection Force switch to A Force switch to B	For 'prefer switch to A/B' operation, the alarm (TU-AIS, TU-LOP) will be checked for the corresponding timeslot of optical A/B. If there is alarm, this operation will not be executed; while for 'force switch to A/B' operation, the system will switch to the pointed port without checking any alarm.
Actual source	e.g.:A	Show the actual source of circuit
DXC description	e.g.:XX bank	Show the user information

3 right-click menu

Menu Name	Function	Note
DXC Property	Pop up DXC Property window	
Create	Pop up create DXC manager window	
Delete	Delete that DXC circuit	
Open auto	Enable the 1+1 protection to that DXC circuit	

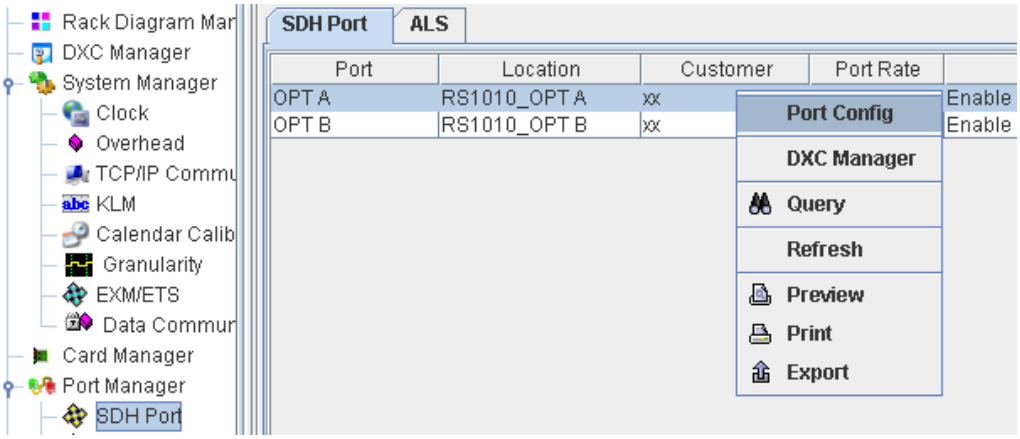
protect		
Close auto protect	Close the 1+1 protection to that DXC circuit	
Activate	Make that DXC circuit available for use	
Inactivate	Make that DXC circuit unavailable for use	
Query	Pop up DXC query window	
Refresh	Refresh DXC circuits	

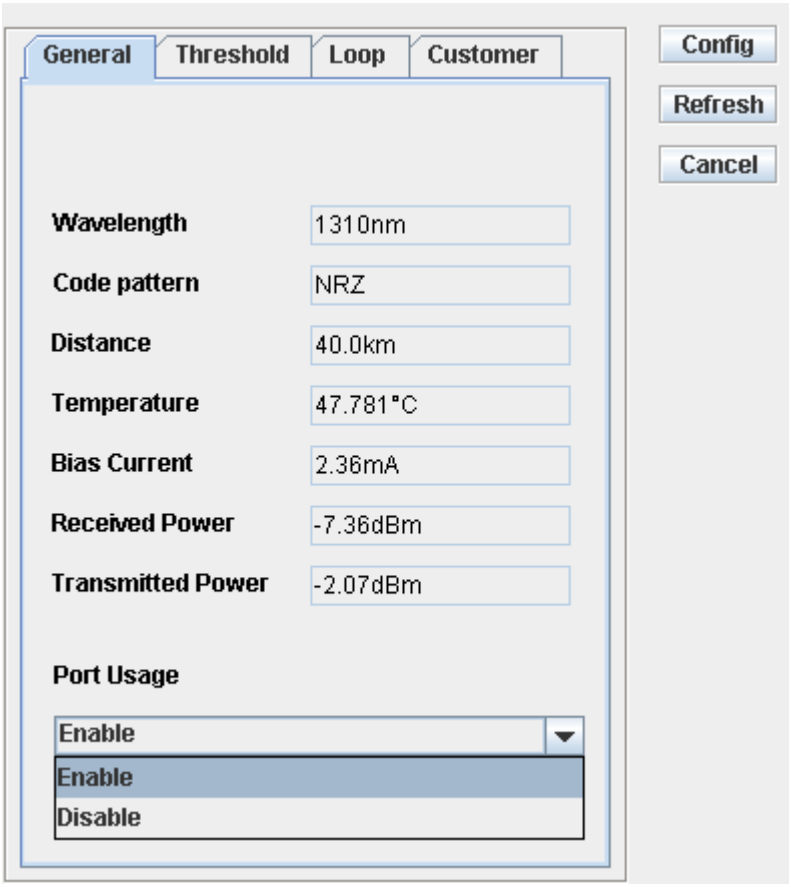
1.19 Optical port

1.19.1 Enable /Disable port

Steps

1. In the navigation tree, select [config/port Manager/SDH Port/SDH Port].
2. Choose a record and right-click and select "Port Config".
3. click "General" tab, under port usage, select Enable/Disable





1.19.2 View Optical interface information

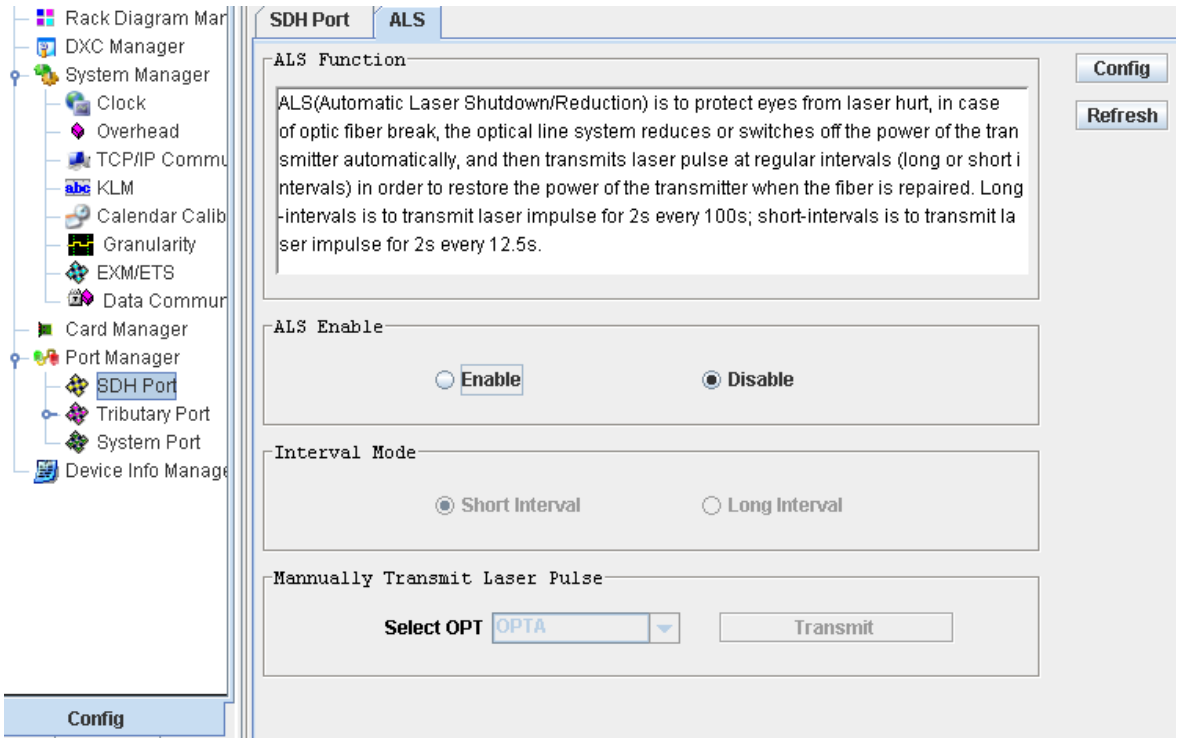
Steps

1. In the navigation tree, select [config/port Manager/SDH port/SDHport] .
2. Choose a record and right-click and select "Port Config".
3. click "General","Threshold" tab, click "refersh" button to view the information.

1.19.3 ALS Configuration

Steps

1. In the navigation tree, select [config/port Manager/SDH port/ALS] .
2. do operations such as enable/ disable ALS, manual send pulse, long interval/short interval settings and so on,.



Note

The ALS function of the OPTA, OPTB port must be configured as enabled or disabled simultaneously; only when the corresponding optical interface detects a Loss of signal and the ALS is enabled by SNMP, that particular optical interface will enter into the ALS state.

1.20 E1 port

1.20.1 E1 loop

Steps

1. In the navigation tree, select [config/port Manager/Tributary port/E1 port].
2. Click "E1 port" tab
3. Choose a record and right-click and select "Port Config".
3. Click "loop" tab, select line loop or device loop

1.20.2 BERT testing

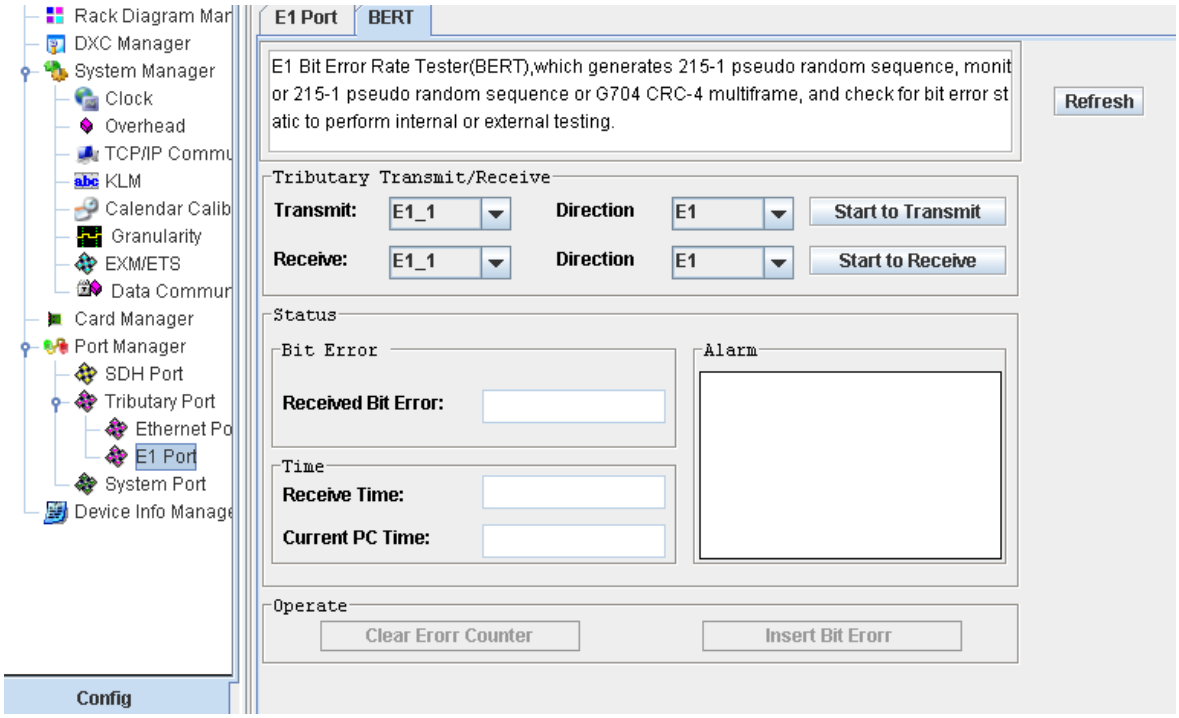
RS1010 provides an embedded BERT (Bit Error Ratio Tester) for maintenance actions such as fault localization and failure detection. It makes a great facility for operator in environment without any external BERT.

The embedded BERT can detect any E1 line (it only detects the existed E1), note that the E1 used for BERT testing cannot be employed for traffic transmitting, but other E1 can work normally.

Steps

1. In the navigation tree, select [config/port Manager/Tributary port/E1port].

2. Click "BERT" tab



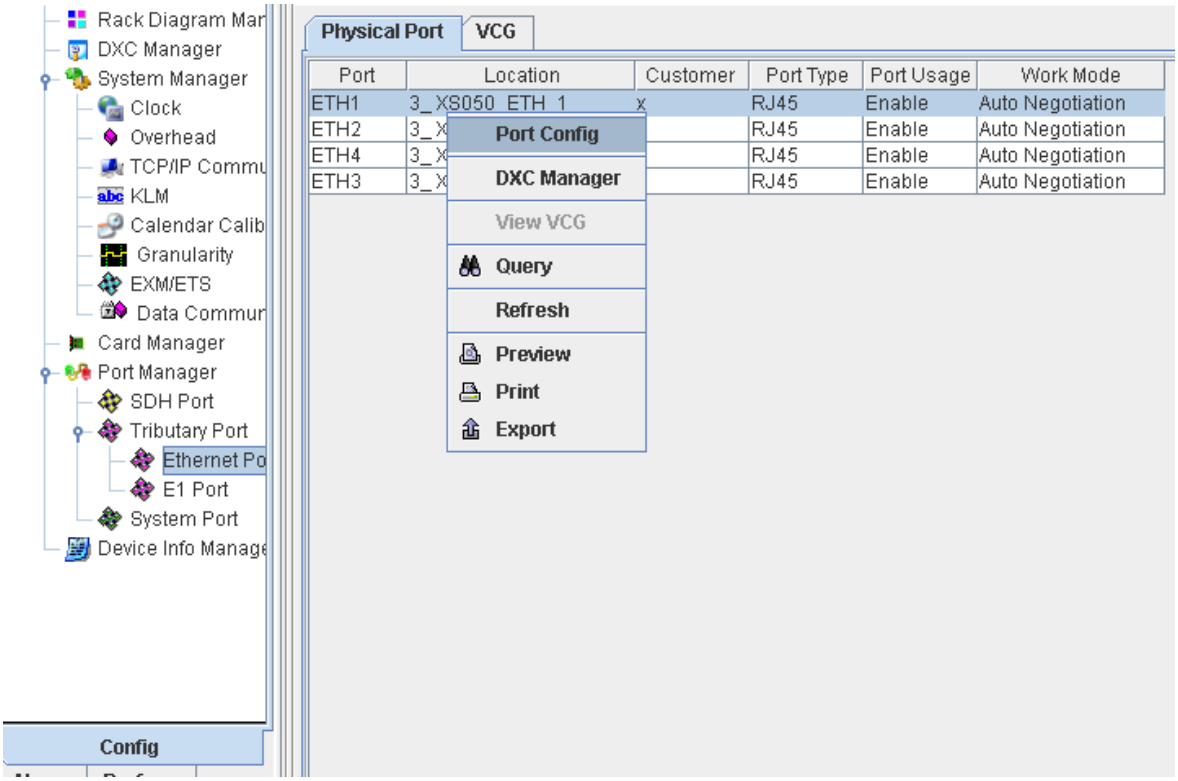
1.21 Ethernet port（XS050）

This part takes XS050 as an example, to describe the configuration of Ethernet port.

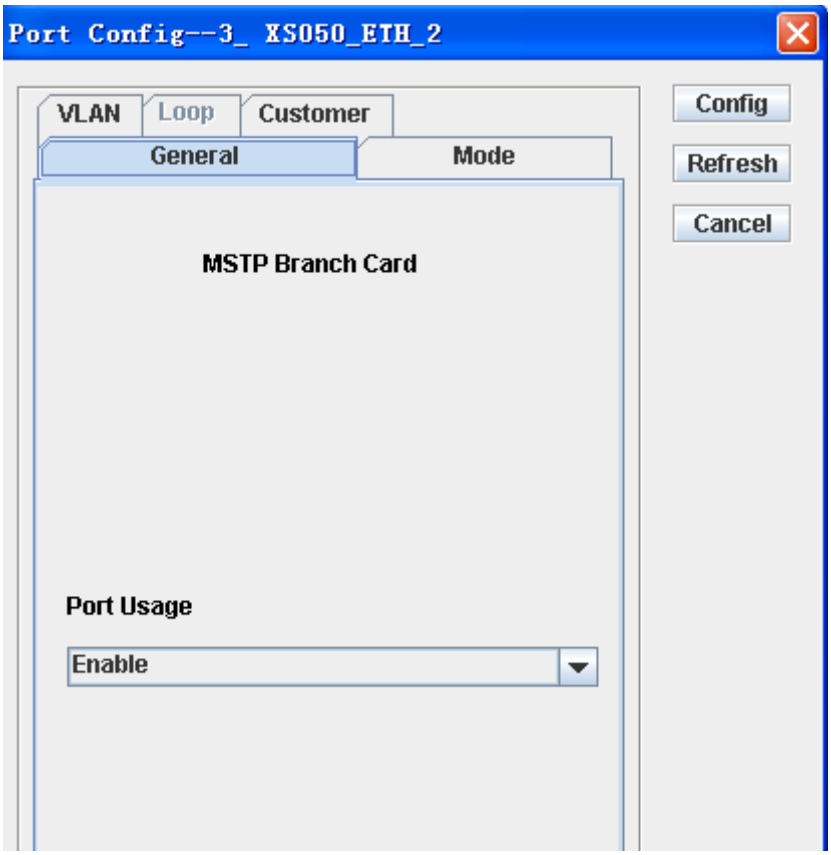
1.21.1 Physical port configuration

Steps

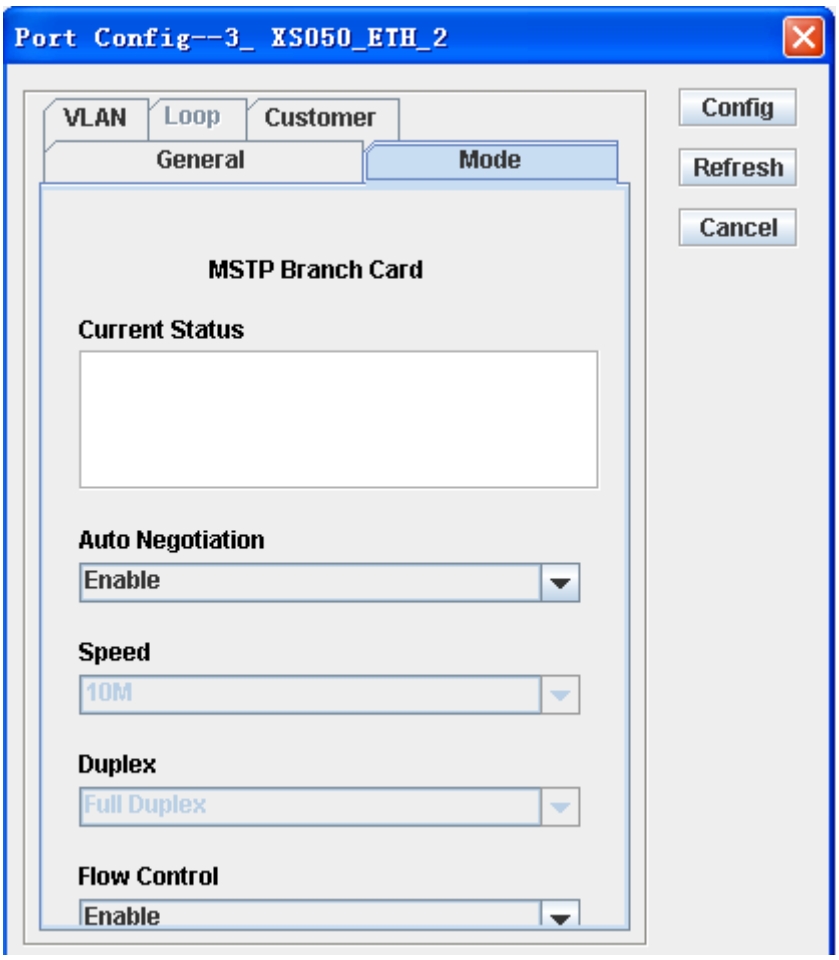
1. In the navigation tree, select [config/port Manager/Tributary port/Ethernet port].
2. Click [Physical port] tab.
3. Select a port record and right-click and select "Config".



4. Click [General] tab to enable/disable port



5. Click [Mode] tab to do operation such as "auto negotiation" and "flow control"



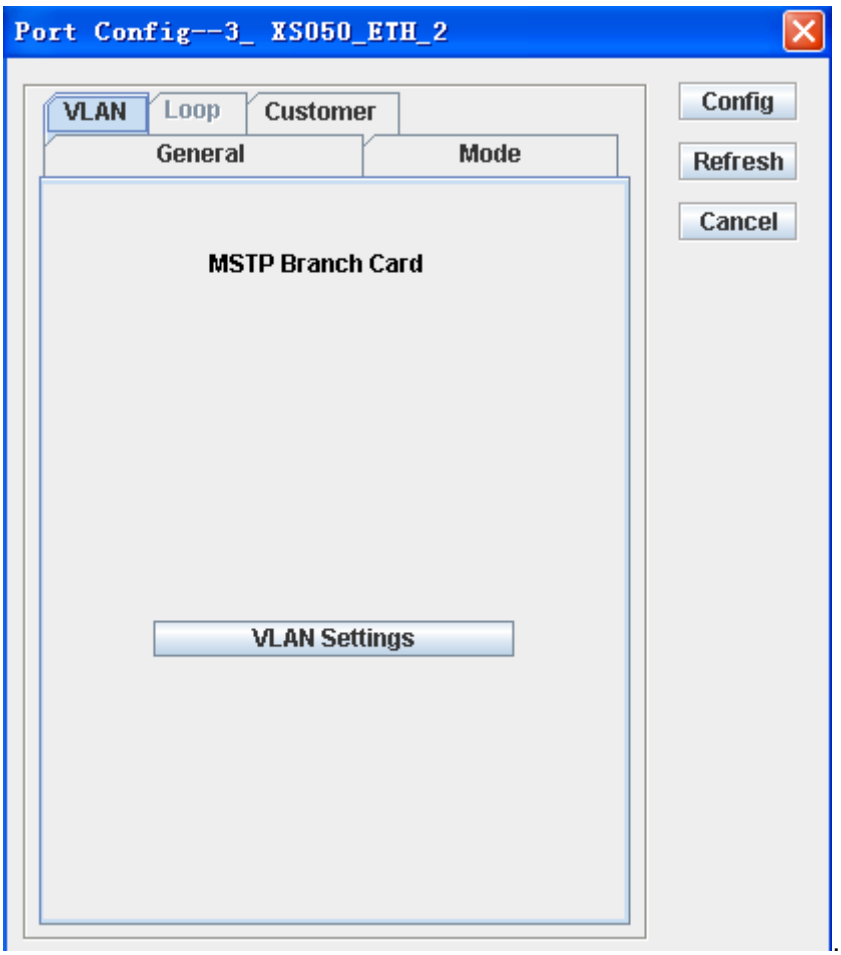
1.22 VLAN Management

XS030,XS050 and XS060 are the Ethernet card of RS1010, all cards supports two VLAN modes: 802.1Q tag-based VLAN, port-based VALN. VLAN mode can be configured via Management software.

For XS030/XS050, do the following steps to enter into windows of VLAN configuration

Steps

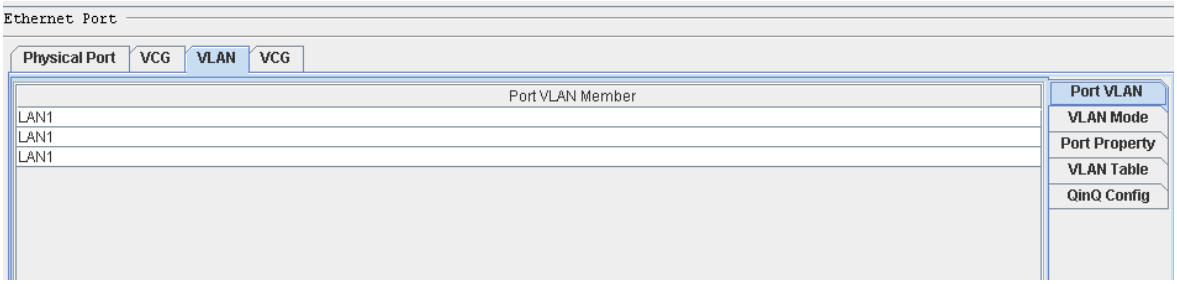
1. In the navigation tree, select [config/port Manager/Tributary port/Ethernet port].
2. Click [Physical port] tab.
3. Select a port record and right-click and select "Config".
4 Click [VLAN] tab, click "VLAN Settings".



For XS060, do the following steps to enter into windows of VLAN configuration

Steps

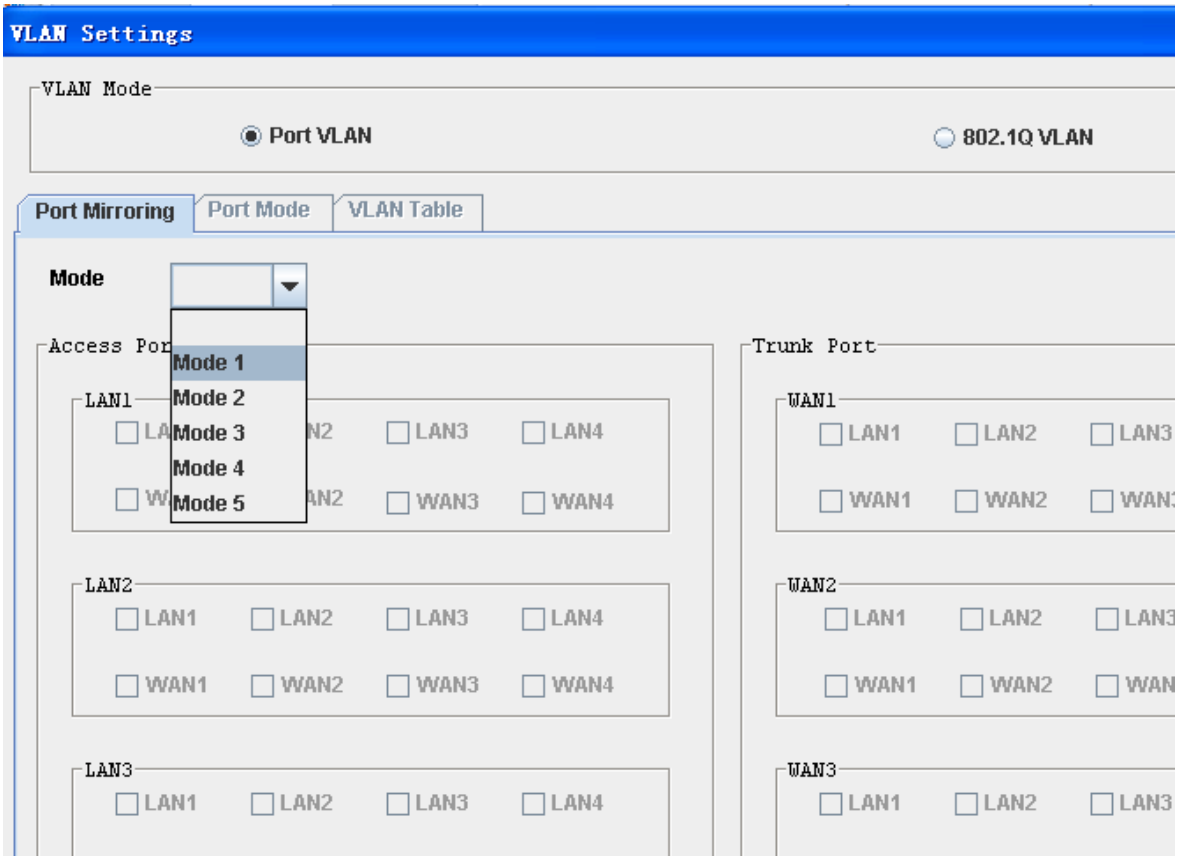
1. In the navigation tree, select [config/port Manager/Tributary port/Ethernet port].
2. Click [VLAN] tab.



1.22.1 Port-based VLAN of XS050

Steps

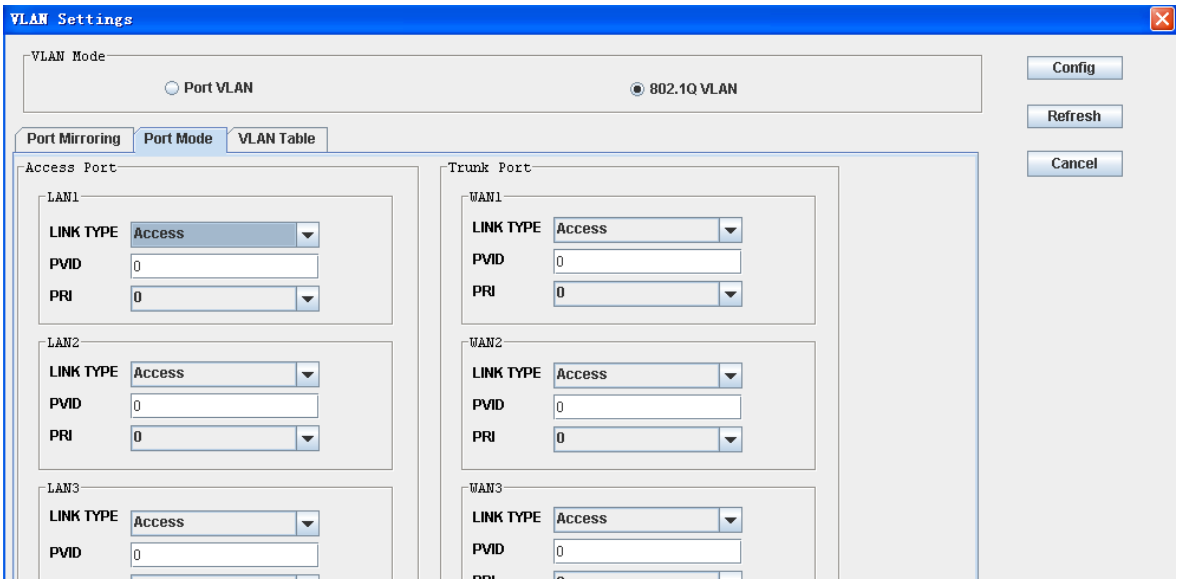
1. Click "port VLAN"
2. Select mode1/2/3/4/5 from mode list



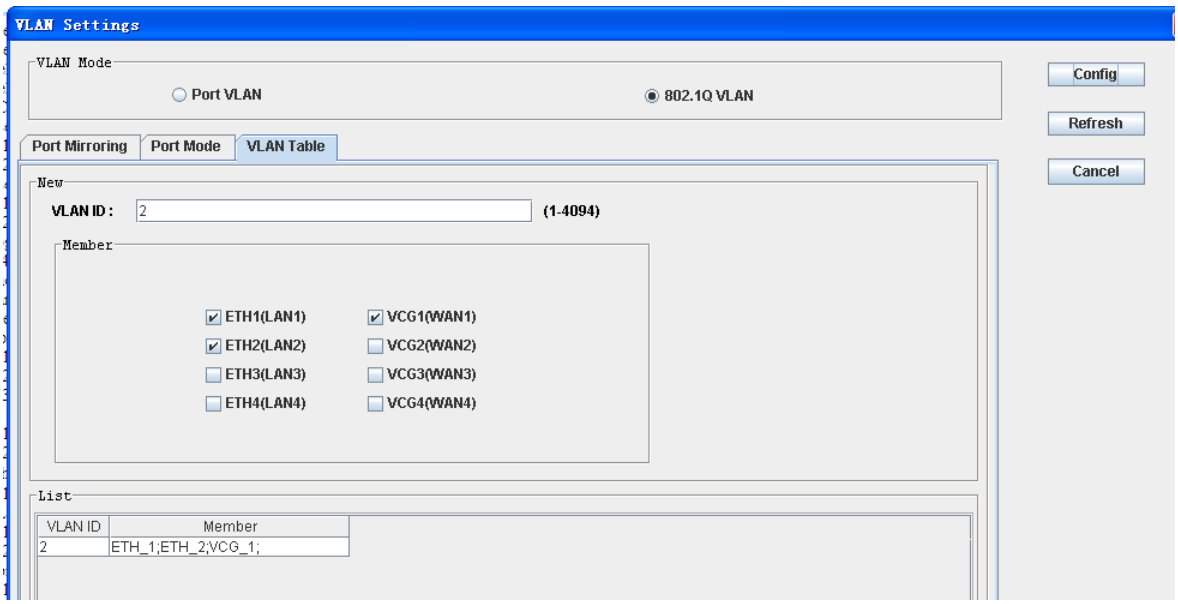
1.22.2 802.1Q VLAN of XS050

Steps

1. Click "802.1Q VLAN"
2. Click "port mode" tab. Config LINK type and port PVID.



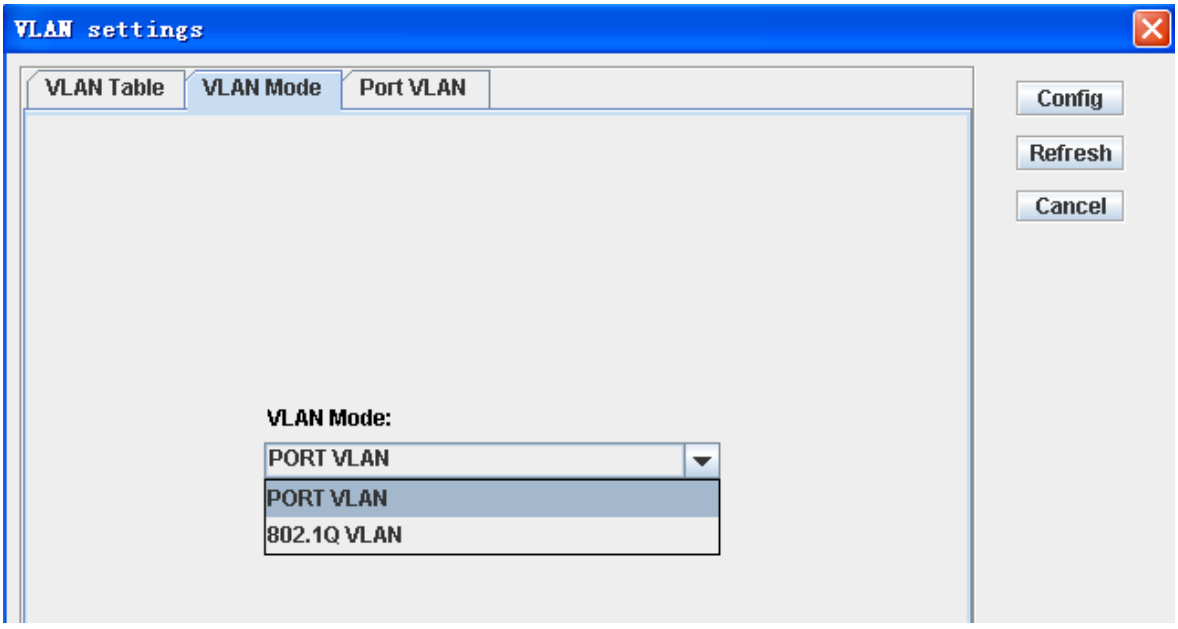
3. Click "VLAN table" tab, add VLAN table



1.22.3 Port-based VLAN of XS030

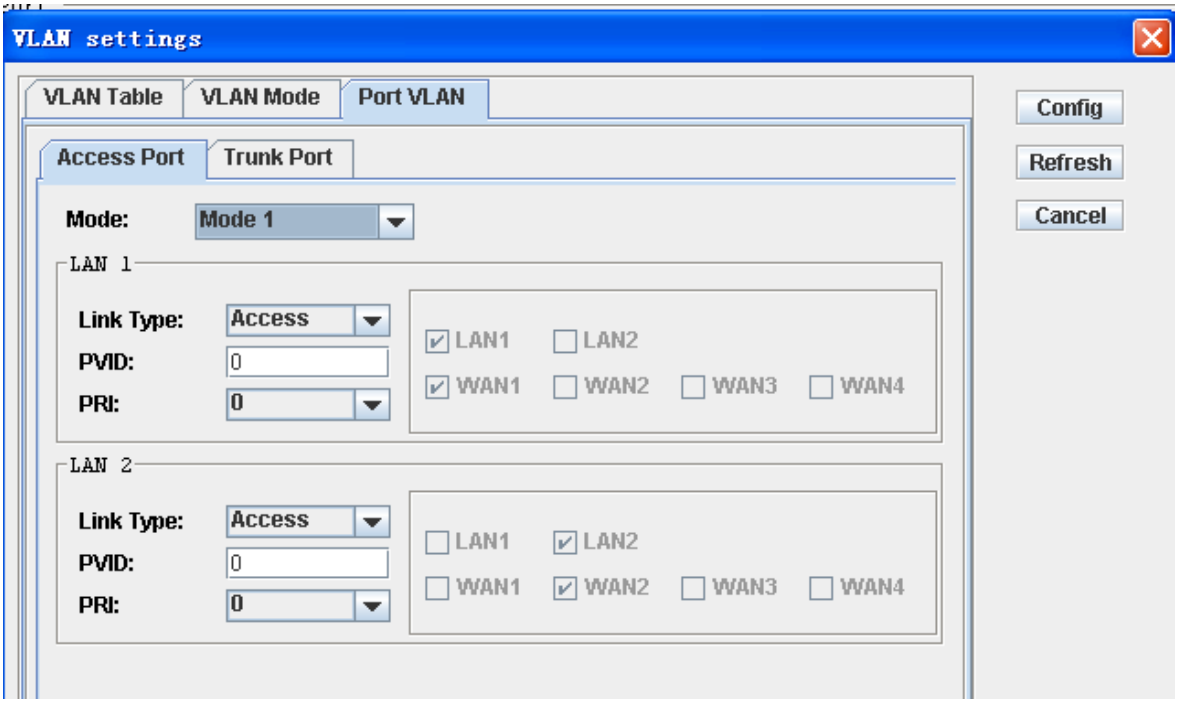
Steps

1. Click [VLAN mode] tab



2. Select "PORT VLAN" from the VLAN mode list

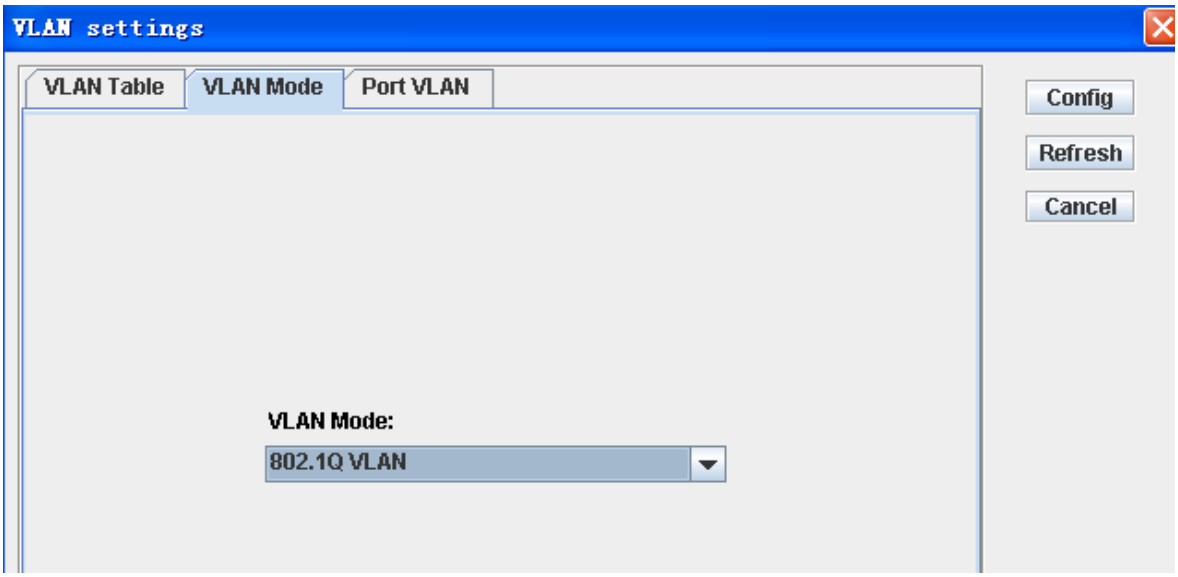
3. Click "port vlan " tab and select port mode1/2/3/4/5 from the port mode list,



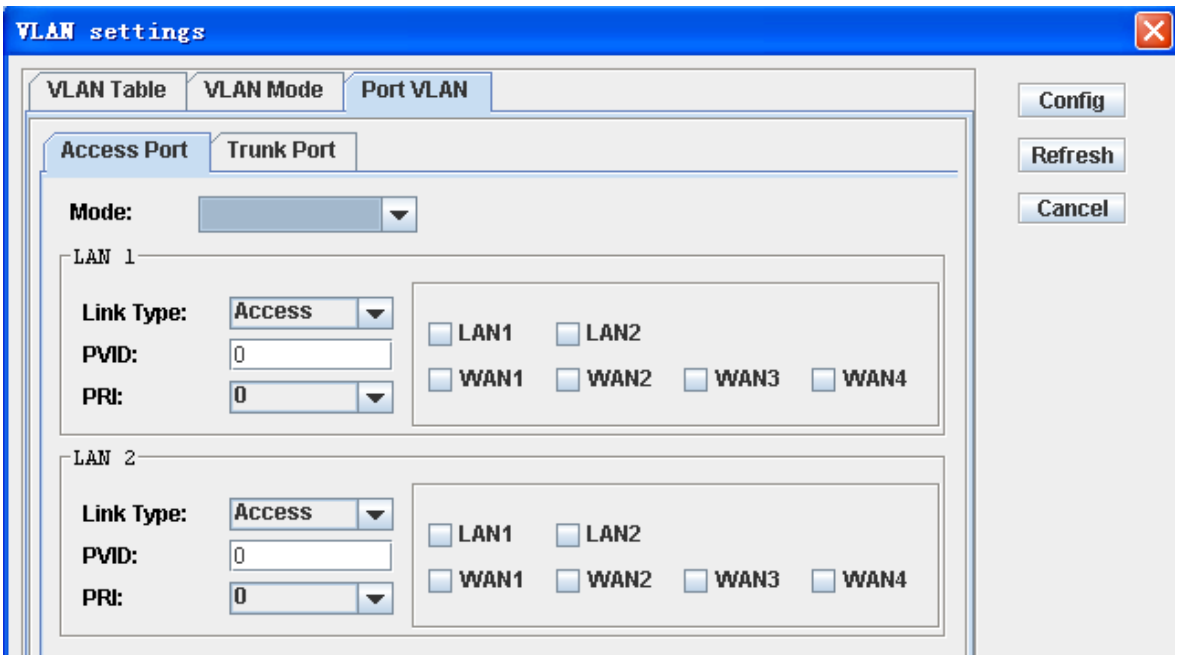
1.22.4 802.1Q VLAN of XS030

Steps

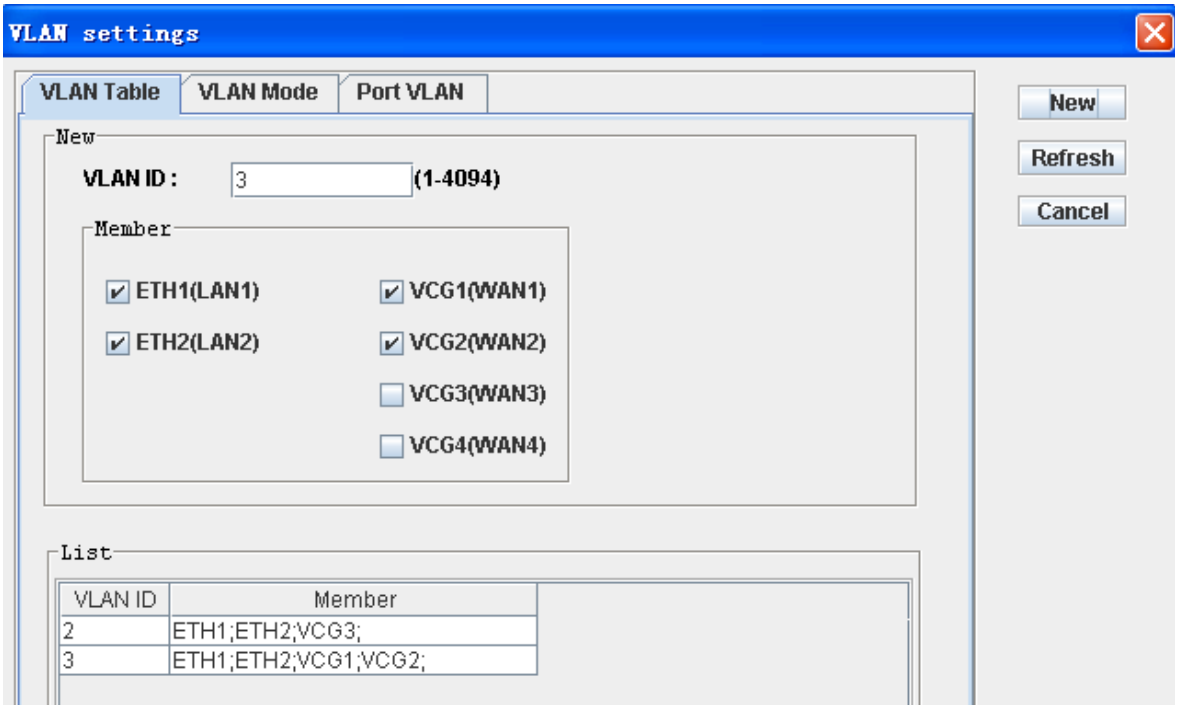
1. Click [VLAN mode] tab, Select "802.1Q VLAN" from the VLAN mode list



2 Select mode 5, and then select Link Type and type PVID



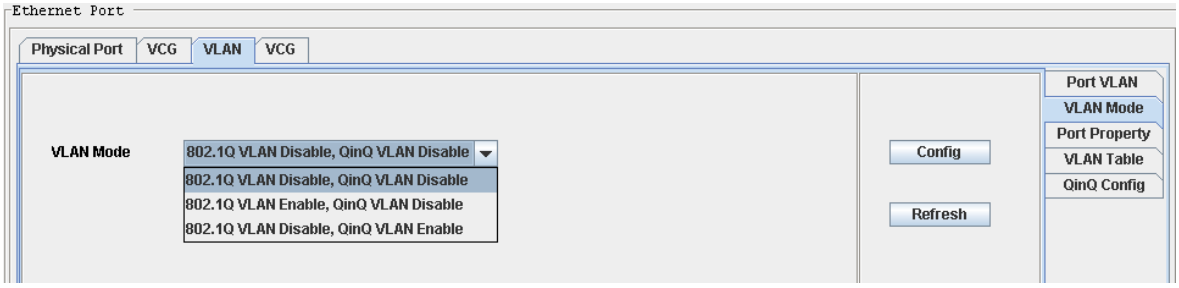
3 Click "VLAN table" tab, add VLAN table



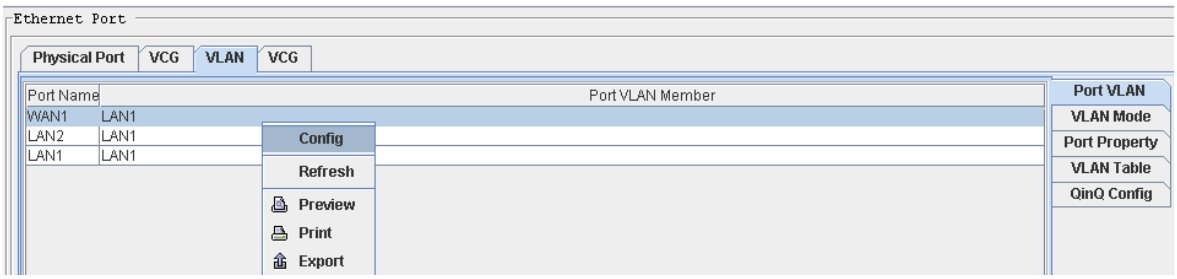
1.22.5 Port-based VLAN of XS060

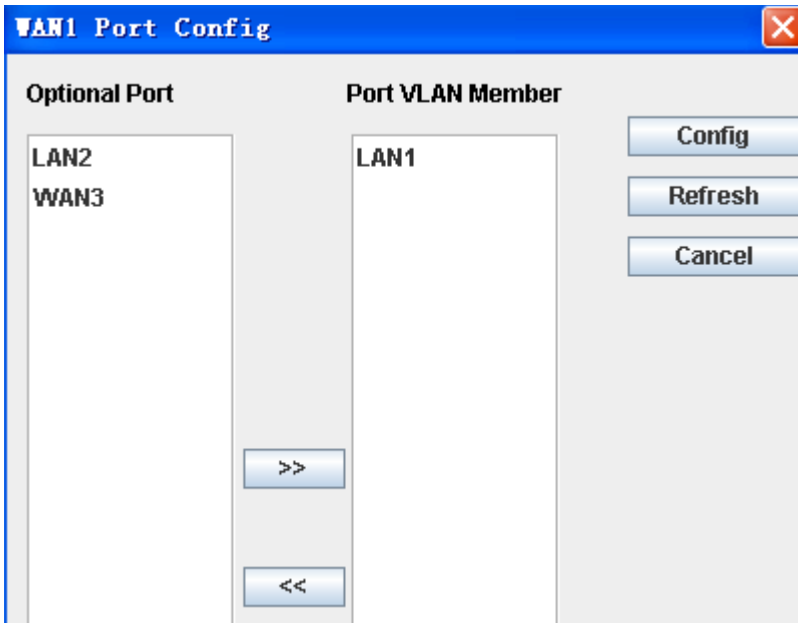
Steps

1. Click [VLAN mode] tab on the right side.



2.Click [Port VLAN] tab on the right side,right-click the record and click "config".



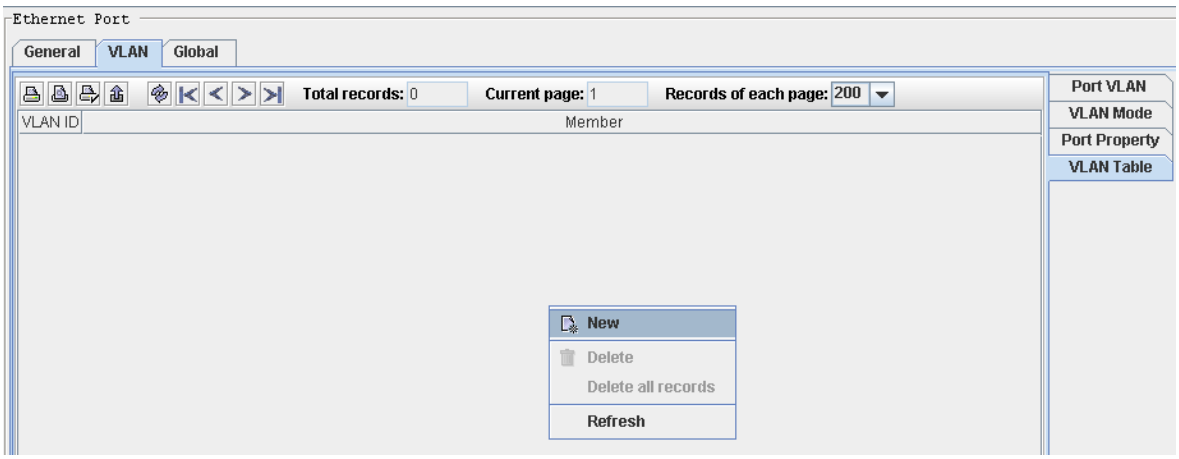


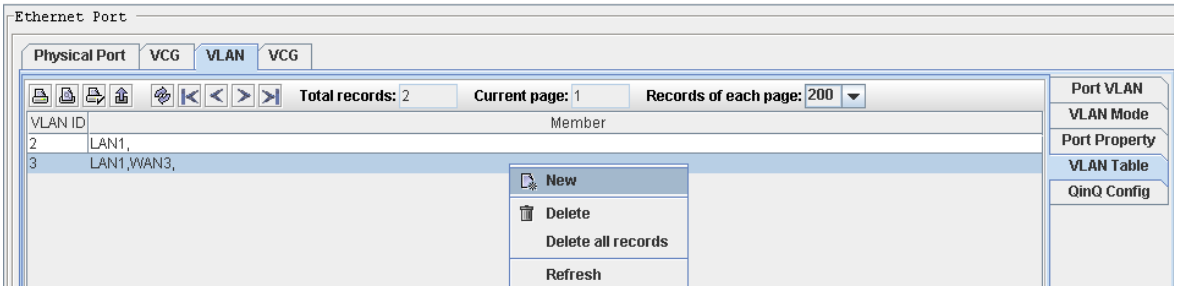
1.22.6 802.1Q VLAN of XS060

Steps

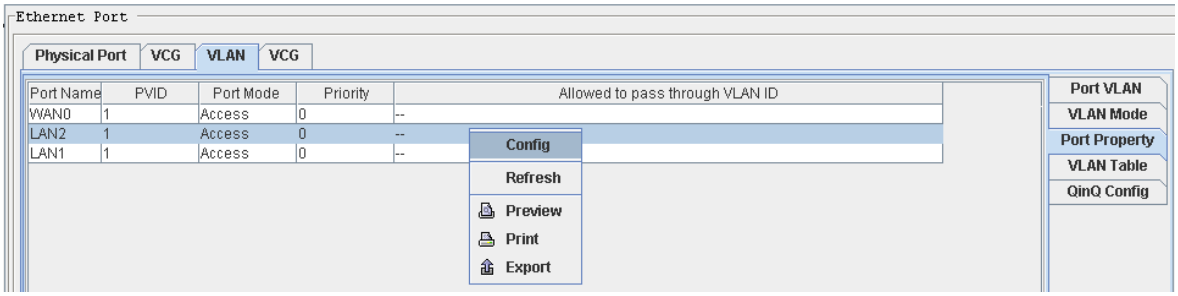
1. Click [VLAN mode] tab, Select "802.1Q VLAN" from the VLAN mode list

2. Add VLAN table, click "VLAN Table" tab on the right side, right-click on the left blank, select "New" from the pop up menu.





3. Config port mode and port PVID. click " port property" tab on the right side, right-click on the left records , select "config" from the pop up menu,select port mode and type PVID.



1.23 Configure Clock

Purpose

This part introduces how to configure SDH clock, including:

▲ Clock mode

▲ Clock PRI

▲ Frequency offset overrun switch

▲ Reference restoring time

▲ External timing source

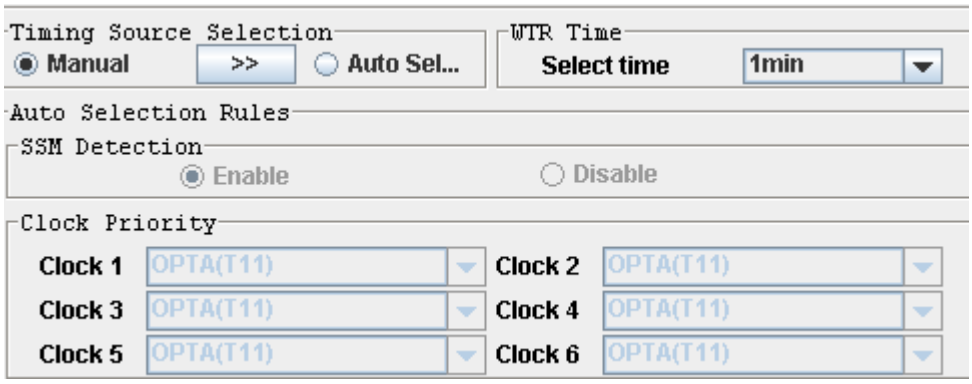
▲ SSM

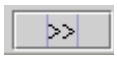
▲ current clock status

1.23.1 Clock mode Configuration

Steps

Steps1: in the navigation tree, select [config/system manager/clock], select in the “Timing source selection” item. Note : SSM and clock priority is only available in the “auto mode”.



Step 2: click “manual” and click 

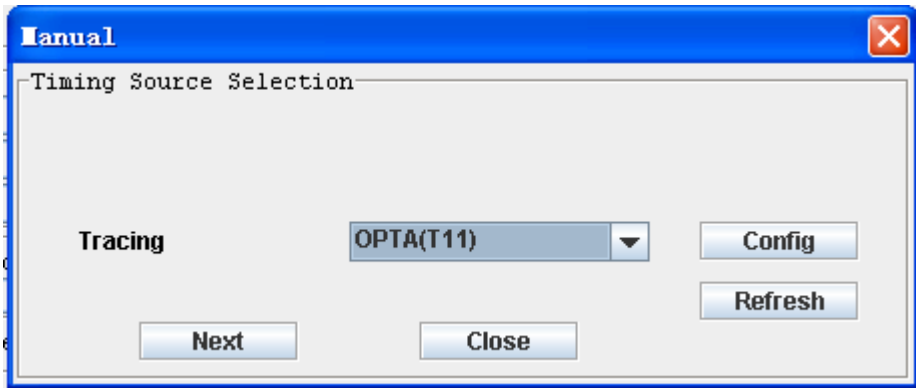
button, pop up the manual mode settings window. First, set tracing clock as the following figure, when the settings is successful, it will send 3 commands:

A, clock mode is manual

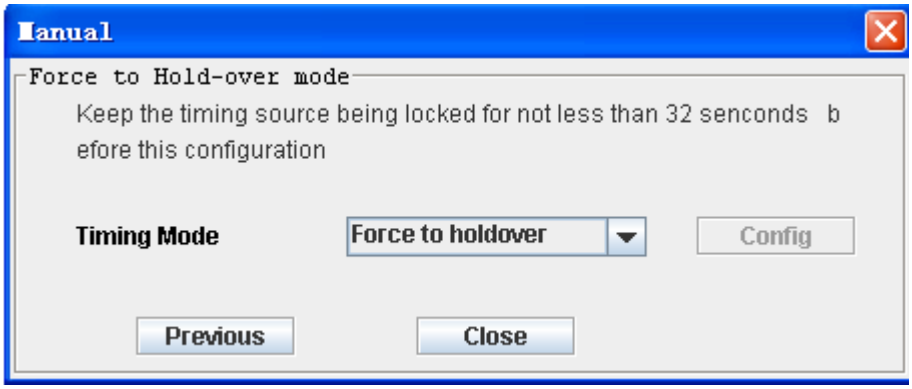
B, the clock reference assigned by manual

C, not force to holdover mode

Click “next” button, to assign timing mode



Step3: in [timing mode] interface, only when the current timing source is identical with the timing source assigned manually, and it is locked status, the <force to holdover> can be configured.



1.23.2 Clock PRI Configuration

Purpose

This part introduce how to configure the priority of clock.

the equipment will always tracing the current available clock with the highest priority, only when the clock with the highest priority is deteriorate or manual swith clock, the equipment may switch to trace clock with lower priority.

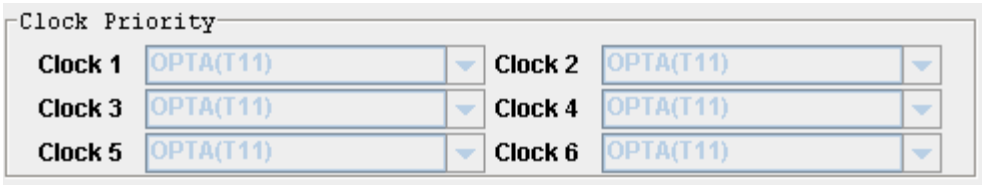
For clock protection, two clock reference at least must be configured. Usually, tributary clock should not be used as the equipment clock.

Steps

Step1: in the navigation tree, select [config/system manager/clock], select in the “clock Priority(PRI)" item. Select the timing reference according to the PRI

Step2: click <config>.

Step3: for the equipment which needs to be activated, click <config activate> button;



1.23.3 Frequency offset overrun switch

Purpose

This part introduce how to set the frequency offset overrun switch.

when the frequency offset is out of normal range, the system will determine whether switch to the next clock according to this settings.

Steps

Step1: in the navigation tree, select [config/system manager/clock], select “switch when overrun” or “not switch when overrun”.

Step2: Click <config>.

1.23.4 Reference restoring time

Purpose

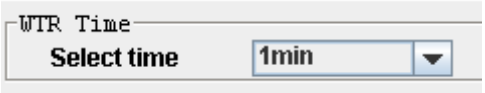
This part introduces how to configure reference restoring time.

The equipment will wait for a period of time- the restoring time, when the timing source is from failure to available. If the timing source is always available in this period of time, the equipment will automatically set this timing as the available timing source. E.g. the degraded clock with highest PRI can be reused as the equipment timing source after being resorted.

Steps

Step1: in the navigation tree, select [config/system manager/clock], set the reference restoring time(WTR time) from “select time” dropdown box .

Step2: Click <config>.



1.23.5 ETS(external timing source) config

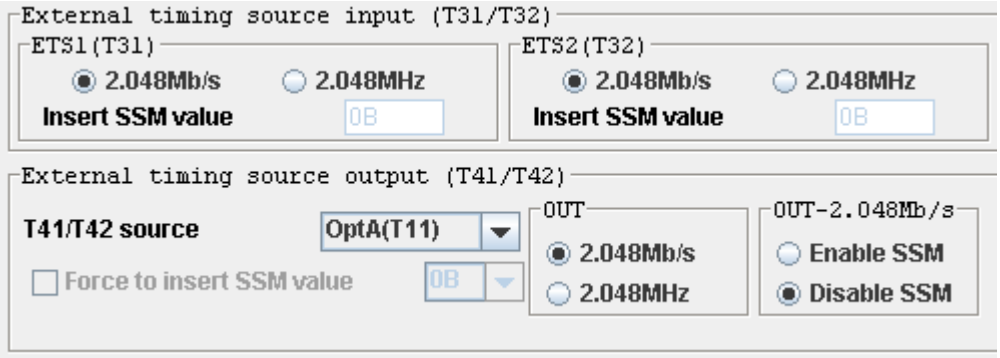
Purpose

The device can trace the ETS which can be 2.048Mb/s(HDB3) or 2.048MHz

Steps

Step1: in the navigation tree, select [config/system manager/clock], select 2.048Mb/s or 2.048MHz for input and output.

Step2: Click <config>.



1.23.6 SSM config

Purpose

SSM（Synchronization Status Message） is used for indicating quality level (QL) of clock reference timing, which make the SDH node acquire the upstream clock information by SSM, and transfer the information to the downstream. It adopts 4 bits code to indicate 16 types of message.

SSM channel :SSM can be transmitted through S1 byte of the multiplex section overhead as defined in ITU-T G.707. bit 5, 6, 7, 8 of S1 byte indicate 16 codes to reprensent quality level. The SSM generator can be closed and 1111 can be inserted, which means it can not be used for synchronization.

Steps

Step1: in the navigation tree, select [config/system manager/clock], configure SSM

Step2: Click <config>.

1.23.7 View the current clock status

Purpose

This part will introduce how to view the current clock status.

Steps

Step1: in the navigation tree, select [config/system manager/clock],

Step2: Click <refresh>.

Step3: view the current clock status.

Field	Range	Description
Current clock status	Locked, tracing, holdover, freerun mode	Show the current clock mode Locked mode: the clock of SDH will trace the same or higher quality input clock source, and locked the timing source. Holdover mode: if all the timing source supply fail, the clock signal is kept relatively accurate by controlling the oscillator and applying the stored frequency correction values for the previous signal. Free run mode: if the oscillator don't store the previous signal or is on the hold-over mode over 24 hours, the device will work on the free run mode..
Reference source	Such as: OPTA	Show the current reference source being traced. Normally, the clock of SDH will trace the highest quality clock source.
SSM information	Quality unknown, Rec. G.811, Rec.G.812 transit, Rec.G.812 local, Synchronous Equipment Timing Source(the internal oscillator of the equipment), Do not use for synchronization	Show the SSM information
S1 byte	Such as: no information	Show the S1 byte information
SSM value	00, 02, 04, 08, 0b, 0f	
Frequency offset		

1.24 Calendar calibrate

Purpose

The occurrence time of alarm and performance event is important for the maintenance, but the system time of NE and the management software may be different, so it is necessary to keep the time of NE in steps with that of the software.

Note:

1, please ensure the clock synchronization of the NEs in the network before configuring

the time calibrate;

2, please ensure the server and client PC time is correct.

3, currently the calibrate only supports 24 hour clock.

Steps

Manually calibrate

1, in the navigation tree, select [config/system manager/calendar calibrate-manually.

2, input the NE time

3, click<OK>.

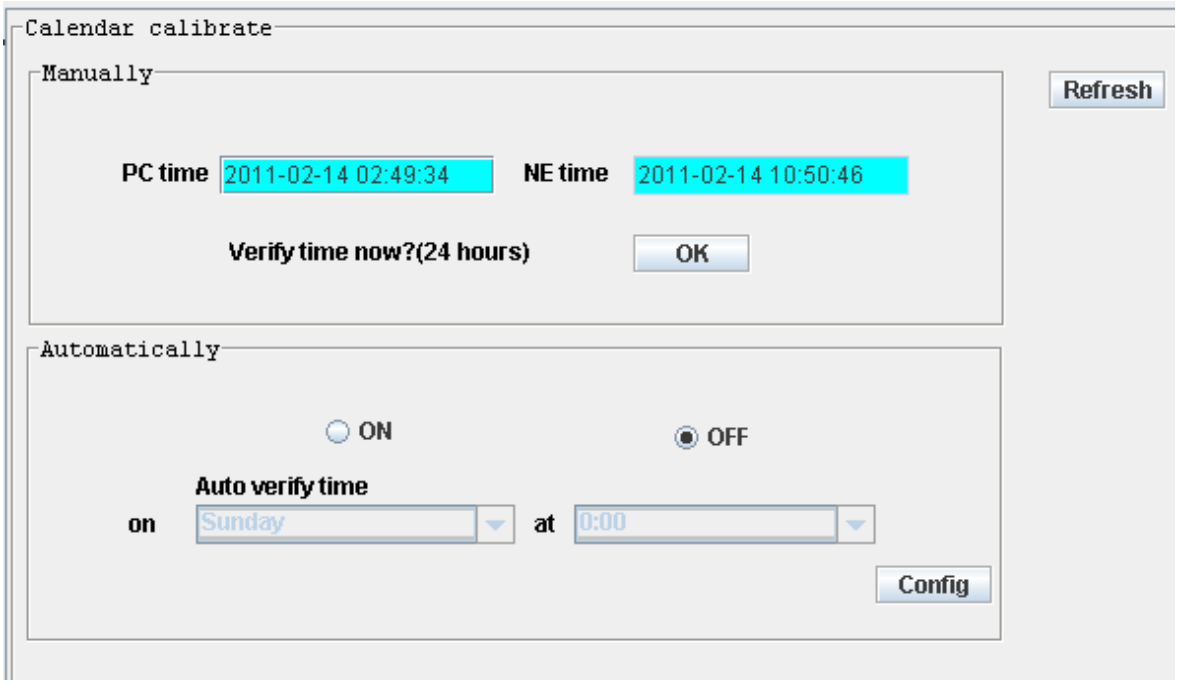
Automatically calibrate

1, in the navigation tree, select [config/system/calendar calibrate-automatically.

2, select “ON”.

3, select the automatic calibrate cycle（based on the server time）

4, Click<config>.



1.25 KLM

Purpose

In order to be able to communicate with the equipment from other vendors, the management system provides three different concatenation types simultaneously: logic order, path order and line order.

Steps

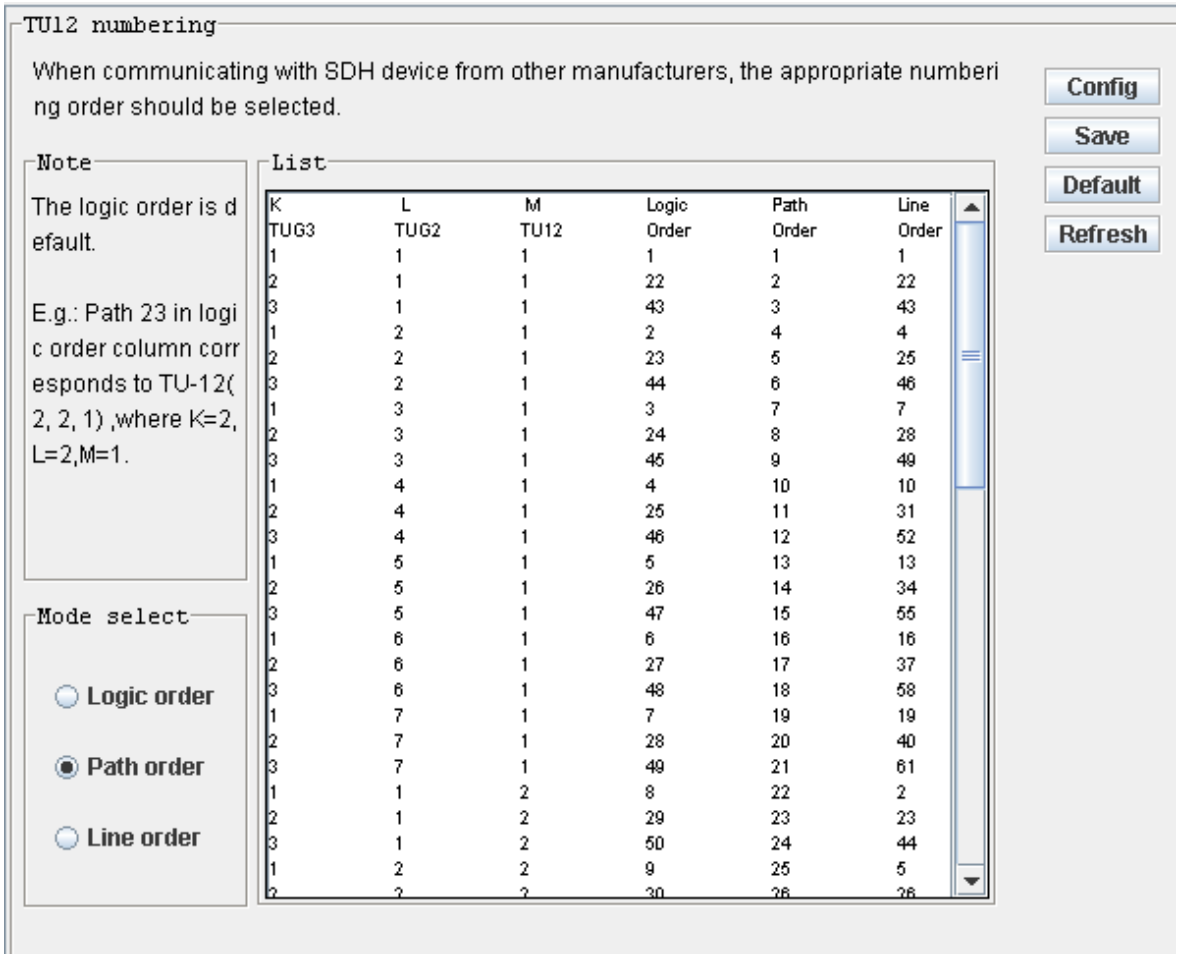
Step1: in the navigation tree, select [config/system manager/ KLM].

Step2:Select optical interface:

1, view the TU-12 numbering: click <refresh> to view the TU-12 numbering.

2, set the TU-12 numbering: select the corresponding mode;

3, Click <config>.



1.26 Data communication channel

Purpose

In order to communicate with the equipment from other vendors, you need to configure the data communication channel.

Steps

Step1: in the navigation tree, select [config/system manager/data communication channel].

Step2: Select optical interface:

1, view the data communication channel: click <refresh> to view the data communication channel..

2. Set the data communication channel.: select the “mode”, “allow DCC”, “the other OHs source”;

3, Click <config>.

field	range
mode	select 'non-standard' mode to avoid overhead collision when communicating with device of other vendor
allow DCC	Control whether the network management software can manage this optical interface or not
the other OHs source	Set other OH source to pass-through or loopback the current free overhead when communicating with device of other vendor

Note

1, in standard mode: EOW occupy E1, RS232 channel occupy F1, DCC channel occupy D1, D2, D3;

Other overhead:D4 V1 V2 D5 V3 V4 D6 V5 V6 D7 V7 V8 D8 V9 V10 D9 V11 V12 D10 D11 D12

2, in non-standard mode:EOW occupy D4, RS232 channel occupy D5, DCC channel occupy D6, D7, D8.

Other overhead: E1 F1 D1 D2 D3 V1 V2 V3 V4 V5 V6 V7 V8 V9 V10 D9 V11 V12 D10 D11 D12

1.27 EXM/ETS

Purpose

For RS1010 equipment, the 23rd, 24th E1 in this interface can be used as ETS or XE1.

T3/T4 port: external timing source interface, the equipment can extract the timing information from the T3 port and then recovery the system clock;

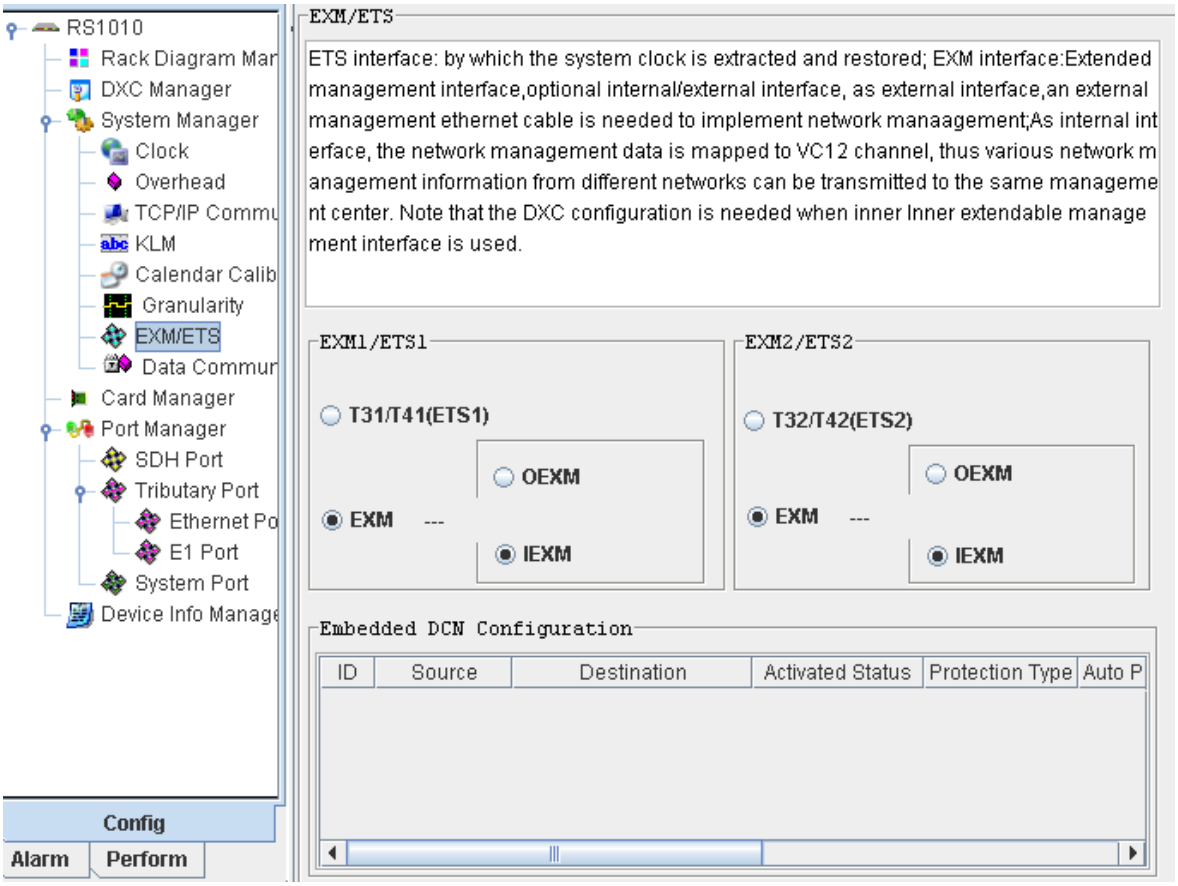
XE1 port: extended management interface, as external interface, an external management cable is needed to implement management; as internal interface, the management information is mapped to VC-12 channel, thus various network management information from different networks can be transmitted to the same management center. Note that the DXC configuration is needed when inner extendable management interface is used.

Steps

Step1: in the navigation tree, select [config/system manager/EXM/ETS].

Step2: select ETS1/2 or EXM, click <config>.

Step3: if select the IEXM, you need to configure the DXC circuit, refer to "DXC manager".


RS1010
Rack Diagram Mar
DXC Manager
System Manager
Clock
Overhead
TCP/IP Commu
KLM
Calendar Calib
Granularity
EXM/ETS
Data Commur
Card Manager
Port Manager
SDH Port
Tributary Port
Ethernet Po
E1 Port
System Port
Device Info Manage
Config
Alarm
Perform
EXM/ETS
ETS interface: by which the system clock is extracted and restored; EXM interface:Extended management interface,optional internal/external interface, as external interface,an external management ethernet cable is needed to implement network manaagement;As internal interface, the network management data is mapped to VC12 channel, thus various network management information from different networks can be transmitted to the same management center. Note that the DXC configuration is needed when inner Inner extendable management interface is used.
EXM1/ETS1
T31/T41(ETS1)
OEXM
EXM

IEXM
EXM2/ETS2
T32/T42(ETS2)
OEXM
EXM

IEXM
Embedded DCN Configuration
ID
Source
Destination
Activated Status
Protection Type
Auto P

Alarm and Performance

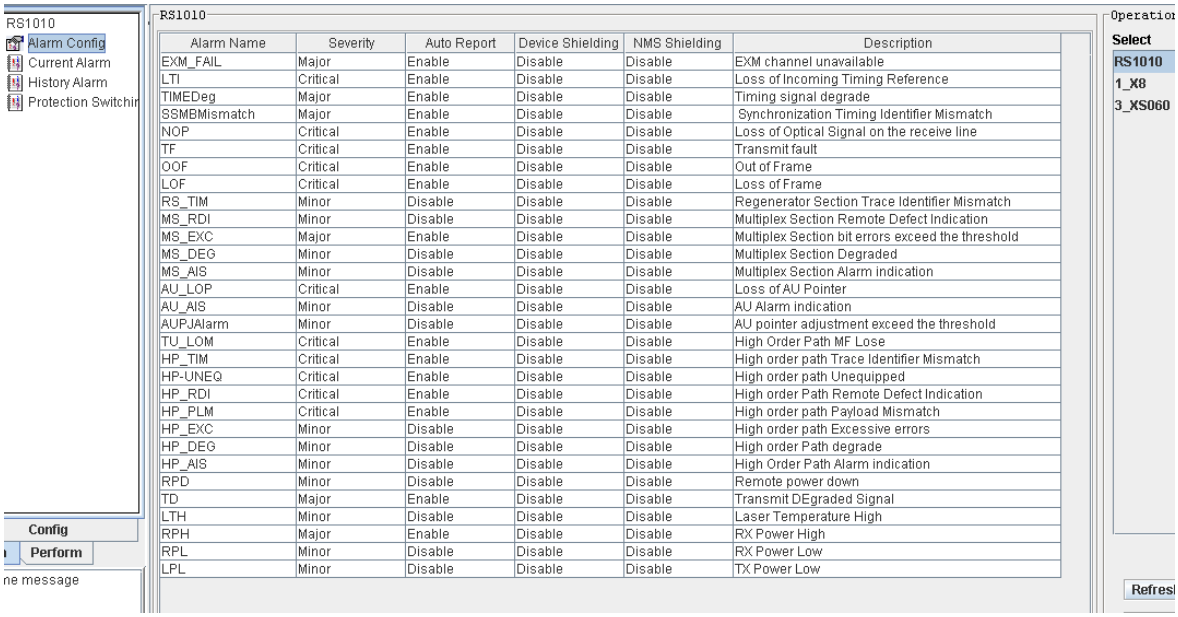
1.28 Alarm Managment

1.28.1 Alarm Severity

Steps

1.In the NE manager, click "alarm" tab at the left corner, In the navigation tree, click [alarm config]

2. Choose a record and right-click and select "critical alarm/major alarm/minor alarm/warning alarm".



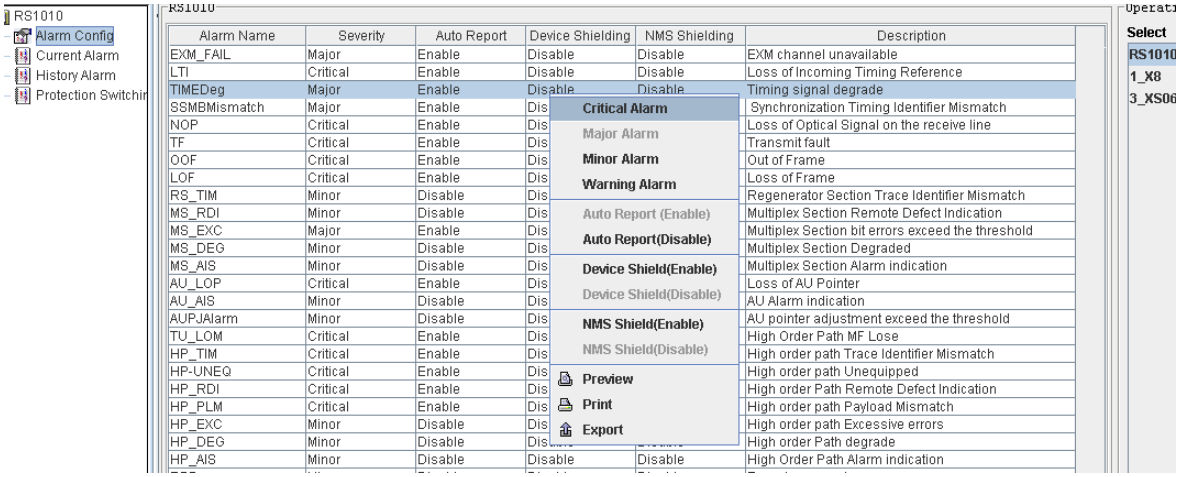
Alarm Name	Severity	Auto Report	Device Shielding	NMS Shielding	Description
EXM_FAIL	Major	Enable	Disable	Disable	EXM channel unavailable
LTI	Critical	Enable	Disable	Disable	Loss of Incoming Timing Reference
TIMEDeg	Major	Enable	Disable	Disable	Timing signal degrade
SSMBMismatch	Major	Enable	Disable	Disable	Synchronization Timing Identifier Mismatch
NOP	Critical	Enable	Disable	Disable	Loss of Optical Signal on the receive line
TF	Critical	Enable	Disable	Disable	Transmit fault
OOF	Critical	Enable	Disable	Disable	Out of Frame
LOF	Critical	Enable	Disable	Disable	Loss of Frame
RS_TIM	Minor	Disable	Disable	Disable	Regenerator Section Trace Identifier Mismatch
MS_RDI	Minor	Disable	Disable	Disable	Multiplex Section Remote Defect Indication
MS_EXC	Major	Enable	Disable	Disable	Multiplex Section bit errors exceed the threshold
MS_DEG	Minor	Disable	Disable	Disable	Multiplex Section Degraded
MS_AIS	Minor	Disable	Disable	Disable	Multiplex Section Alarm indication
AU_LOP	Critical	Enable	Disable	Disable	Loss of AU Pointer
AU_AIS	Minor	Disable	Disable	Disable	AU Alarm indication
AUPJAlarm	Minor	Disable	Disable	Disable	AU pointer adjustment exceed the threshold
TU_LOM	Critical	Enable	Disable	Disable	High Order Path MF Lose
HP_TIM	Critical	Enable	Disable	Disable	High order path Trace Identifier Mismatch
HP-UNEQ	Critical	Enable	Disable	Disable	High order path Unequipped
HP_RDI	Critical	Enable	Disable	Disable	High order Path Remote Defect Indication
HP_PLM	Critical	Enable	Disable	Disable	High order path Payload Mismatch
HP_EXC	Minor	Disable	Disable	Disable	High order path Excessive errors
HP_DEG	Minor	Disable	Disable	Disable	High order Path degrade
HP_AIS	Minor	Disable	Disable	Disable	High Order Path Alarm indication
RPD	Minor	Disable	Disable	Disable	Remote power down
TD	Major	Enable	Disable	Disable	Transmit DEgraded Signal
LTH	Minor	Disable	Disable	Disable	Laser Temperature High
RPH	Major	Enable	Disable	Disable	RX Power High
RPL	Minor	Disable	Disable	Disable	RX Power Low
LPL	Minor	Disable	Disable	Disable	TX Power Low

1.28.2 Alarm shield

Steps

1.In the NE manager, click "alarm" tab at the left corner, In the navigation tree, click [alarm config]

2. Choose a record and right-click and select alarm shield configuration items.



Alarm Name	Severity	Auto Report	Device Shielding	NMS Shielding	Description
EXM_FAIL	Major	Enable	Disable	Disable	EXM channel unavailable
LTI	Critical	Enable	Disable	Disable	Loss of Incoming Timing Reference
TIMEDeg	Major	Enable	Disable	Disable	Timing signal degrade
SSMBMismatch	Major	Enable	Dis		Synchronization Timing Identifier Mismatch
NOP	Critical	Enable	Dis		Loss of Optical Signal on the receive line
TF	Critical	Enable	Dis		Transmit fault
OOF	Critical	Enable	Dis		Out of Frame
LOF	Critical	Enable	Dis		Loss of Frame
RS_TIM	Minor	Disable	Dis		Regenerator Section Trace Identifier Mismatch
MS_RDI	Minor	Disable	Dis		Multiplex Section Remote Defect Indication
MS_EXC	Major	Enable	Dis		Multiplex Section bit errors exceed the threshold
MS_DEG	Minor	Disable	Dis		Multiplex Section Degraded
MS_AIS	Minor	Disable	Dis		Multiplex Section Alarm indication
AU_LOP	Critical	Enable	Dis		Loss of AU Pointer
AU_AIS	Minor	Disable	Dis		AU Alarm indication
AUPJAlarm	Minor	Disable	Dis		AU pointer adjustment exceed the threshold
TU_LOM	Critical	Enable	Dis		High Order Path MF Lose
HP_TIM	Critical	Enable	Dis		High order path Trace Identifier Mismatch
HP-UNEQ	Critical	Enable	Dis		High order path Unequipped
HP_RDI	Critical	Enable	Dis		High order Path Remote Defect Indication
HP_PLM	Critical	Enable	Dis		High order path Payload Mismatch
HP_EXC	Minor	Disable	Dis		High order path Excessive errors
HP_DEG	Minor	Disable	Dis		High order Path degrade
HP_AIS	Minor	Disable	Disable	Disable	High Order Path Alarm indication

Note

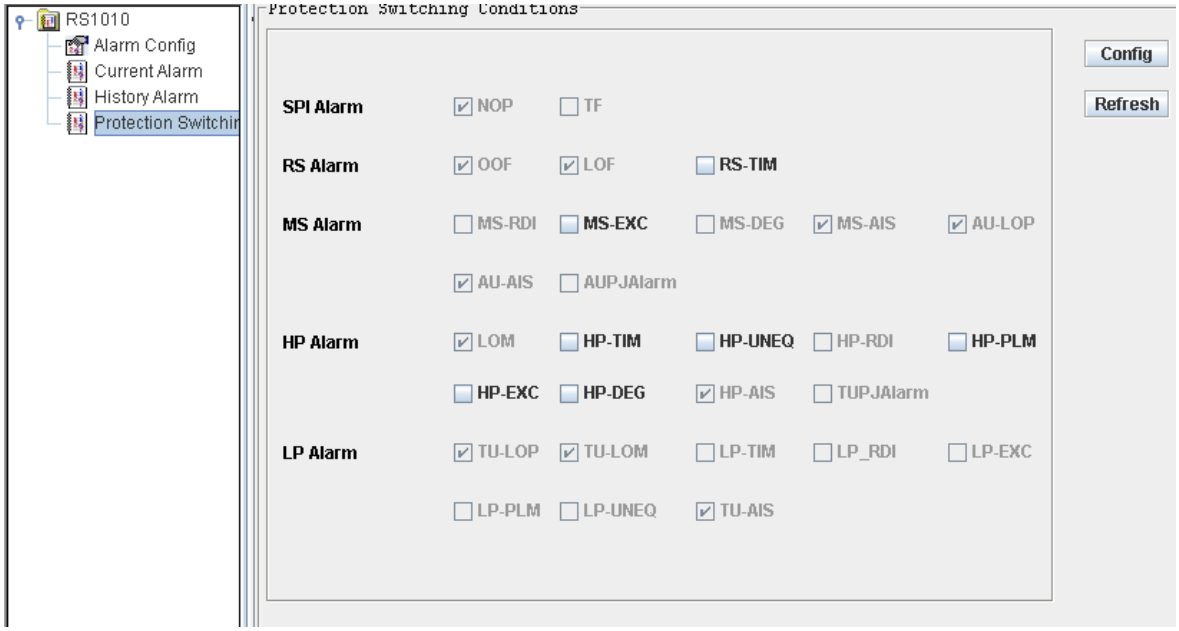
configuration item	description
Severity	Alarm level: Critical (red), major(orange), minor(yellow), warning(purple)
Auto report	Auto update is on: NE trap the alarm generated automatically (that is NE send the alarm to PC automatically when the alarm is occurred); Auto update is off: NE do not trap the alarm generated automatically, refresh alarm manually can update the alarm shown in PC (if alarm is not disappeared)
Device shield	If device shield is on, NE do not trap the alarm, and refresh alarm manually can not update the alarm shown in PC when alarm is occurred in device
NMS shield	NMS shield is on: NMS will discard the alarm when receiving; NMS inhibit alarm is off: the alarm will be saved into the database when received by NMS

1.28.3 Protection

Steps

1.In the NE manager, click "alarm" tab at the left corner, In the navigation tree, click [alarm config-Protection switching conditions]

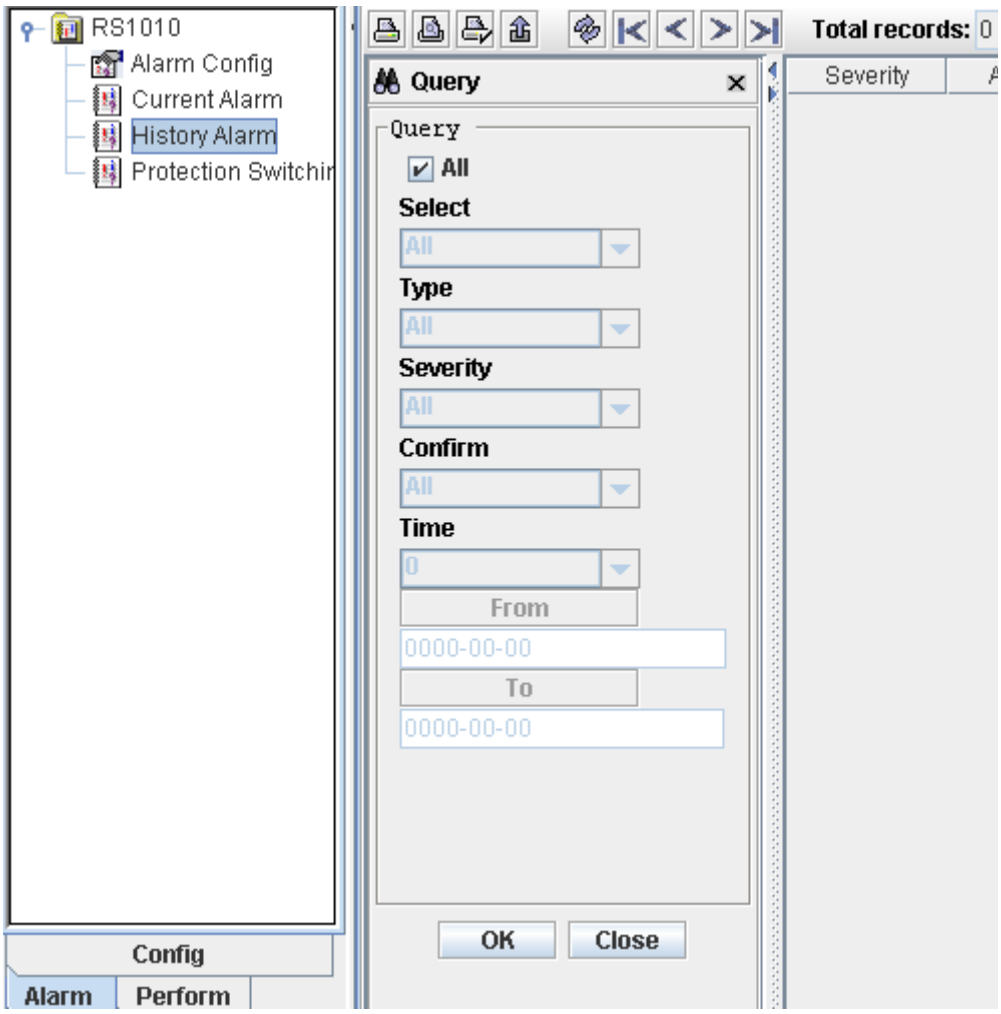
2 select the alarm as the condition of protection switching



1.28.4 Alarm View

Steps

1. In the NE manager, click "alarm" tab at the left corner, In the navigation tree, click [alarm config-current alarm/history alarm]

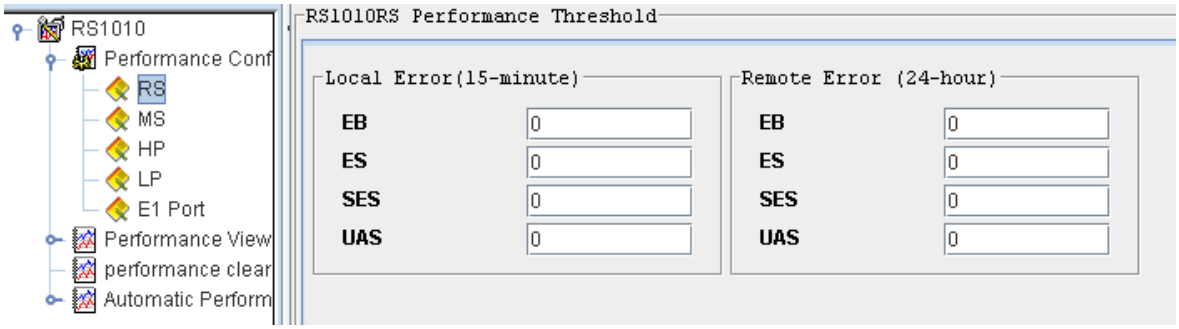


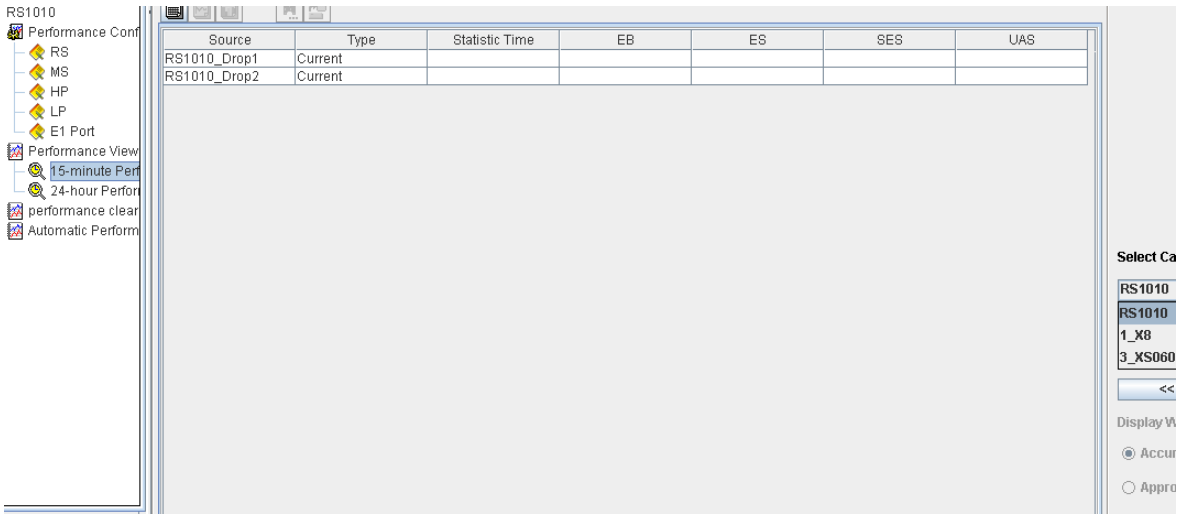
1.29 Performance Management

Steps

1. In the NE manager, click "perform" tab at the left corner, In the navigation tree, click [Perform]

2. do performance threshold configuration,performance view or performance clear




RS1010
Performance Conf
RS
MS
HP
LP
E1 Port
Performance View
15-minute Perf
24-hour Perfor
performance clear
Automatic Perform
Source
Type
Statistic Time
EB
ES
SES
UAS
RS1010_Drop1
Current
RS1010_Drop2
Current
Select Ca
RS1010
RS1010
1_X8
3_XS060
<<
Display W
Accur
Appro

Questions

Q1:Alarm can not be refresh to interface

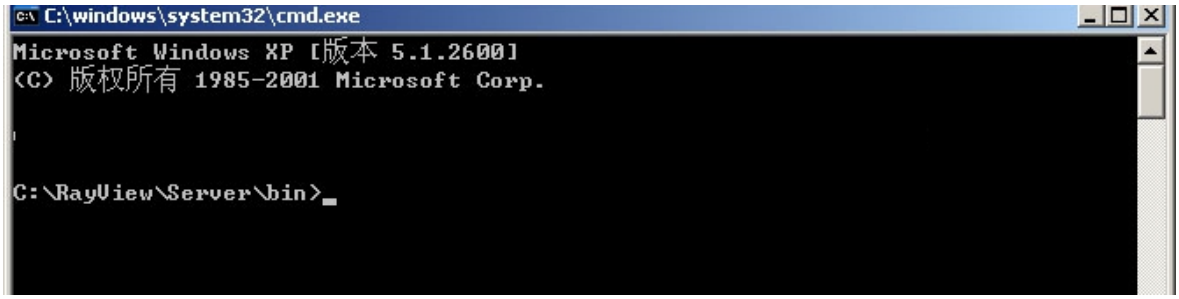
A1:Troubleshoot:

A: Make sure the IP address of monitor is correct; you can Right-click –monitor server--Refresh

B: If the IP address of monitor is correct, make sure process 'knTrapServer.exe' is open, view process in task manager to confirm that.

C: If there is no problem in step A and B, make sure if 'knTrapServer.exe' is stop by firewall.

You can click start--Run—CMD to enter DOS window: Enter into the installation folder of RAYVIEW, such as: C:\RAYVIEW\Server\bin



type 'start kntrapserver' and then enter

If the firewall prevention tip window pop up, allow or release prevention. Restart server and client terminal, refresh alarm.

Q2 the TCP/IP communication between device (NE) and PC failed (PC can not connect to device, the NE is offline)

A2:Troubleshoot:

First, you should know the default NE(device) address. The default NE IP address is 192.168.0.155. The address of NE(device) and PC shall be set and kept at the identical IP segment. For example, if the device IP is 192.168.0.155, while the IP of PC is 202.194.192.2, you should set the IP of PC as 192.168.0.154(for example), make the PC and device IP in the same IP segment, and the TCP/IP communication can be set up, and then change the IP of NE and IP of PC.

Q3 Client terminal link server failed

A3:Troubleshoot:

Check the IP address of server that client terminal connect with, make sure the communication between client and server is correct, and make sure the server is open. There is 4 processes (kncenter.exe\knmaster.exe\raynescan.exe\kntrapserver.exe) at

least.

Q4:The client and server are in two PC separately, and the client terminal runs slowly.

A4:Troubleshoot:

Check the IP settings of the client terminal to see if there is DNS server IP, make sure the communication between client and the DNS server is correct, if the connection is break, delete the DNS server IP.