New Generation SDH Multiplexer

DATACOM

DmSTM-1

Operation and Configuration Manual

17/02/2006 Rev.05 204-0067-05

WARRANTY

This product is guaranteed to be free against manufacturing and raw material defects, during the period specified in the sales receipt.

The warranty includes only the repair and replacement of components or defective parts, free of charge. We do not cover damages caused by any one of the following conditions: improper use, energy failures, natural phenomena (lightning, for example), failure in equipments connected to this product, improper grounding or repairs done by personnel unauthorized by DATACOM.

This warranty does not cover repairs done at the customer's site. All equipments must be sent to DATACOM to be repaired.

Quality Management System certified by DQS according to ISO9001 Register Nº (287097 QM)

NOTE

This equipment uses invisible laser radiation transmitters. Never look directly to the laser terminals or to the optical fibre: the exposition to laser emission can cause permanent eye injury.

Although this document has been written with care, the company does not assume responsibility for occasional mistakes and omissions in its content. Likewise, DATACOM is not liable for any damages that may result from the use of the information contained in this manual. Specifications provided in this manual are subject to changes without any previous notice and should not be construed as a commitment of any kind by DATACOM.

REVISION HISTORY

January, 2005	204-4067-00 – Firmware version 5
September, 2005	204-4067-04 – Firmware version 7 and 8
February	204-4067-05 – Firmware version 9

INDEX

FIGURE INDEX

TABLE INDEX

1 CONNECTING TO THE DMSTM-1

The DmSTM-1 can be configured by using the DmView management software, by terminal or VT100 emulator, or by telnet, through the Ethernet port. For DmView details please check the accompanying user manual.

1.1. PC or terminal connection using the serial port

The DmSTM-1 presents a female DB9 connector in its front panel and another in the back panel for connecting a PC or a terminal. The connection is performed by a male DB9-ended cable at the DmSTM-1 side and by either a DB9 or DB25 female connector at the PC side.

1.2. Access terminal serial configurations

The terminal must be configured for 9600bit/s, 8 data bits, no flux control, 1 stop bit, no parity. When Windows 2000 is used for configuration, it is not recommended to use HyperTerminal due to some operating problems that have been reported under this platform. The recommended software is the Tera Term Pro freeware, which can be downloaded from:

http://www.vector.co.jp/authors/VA002416/teraterm.html

1.3. Telnet PC connection

The DmSTM-1 management can also be performed by Telnet by means of the Ethernet port. Before accessing the equipment via Telnet it is necessary to set the network and configuration parameters.

The telnet management is identical to the one performed through the DmSTM-1 serial port.

When using Windows 2000, it is not recommended to use the default telnet, for there are operating problems regarding some special keys, like Page Up and Page Down. The recommended software is the PuTTY freeware, which can be downloaded from:

http://www.chiark.greenend.org.uk/~sgtatham/putty/

1.4. Authentication

All users must pass by an authentication procedure, providing username and password to be able to access the equipment terminal. The default equipment user is ***"admin***" and the default password is ***"admin***". Some equipments may be configured with default user "**datacom**" and default password "**datacom**".

```
Linux 2.4.4-rthal5 (DmSTM-1) (ttyp1)

Busy Box on DmSTM-1 login:
Password:
```

Figure 1 – Terminal Authentication Screen

After the equipment installation, it is recommended to change the default password.

1.5. Main terminal menu

The main equipment menu allows accessing the configuration, administration, status checking and tests screens. Figure 2 presents the main menu. The available options are now described.

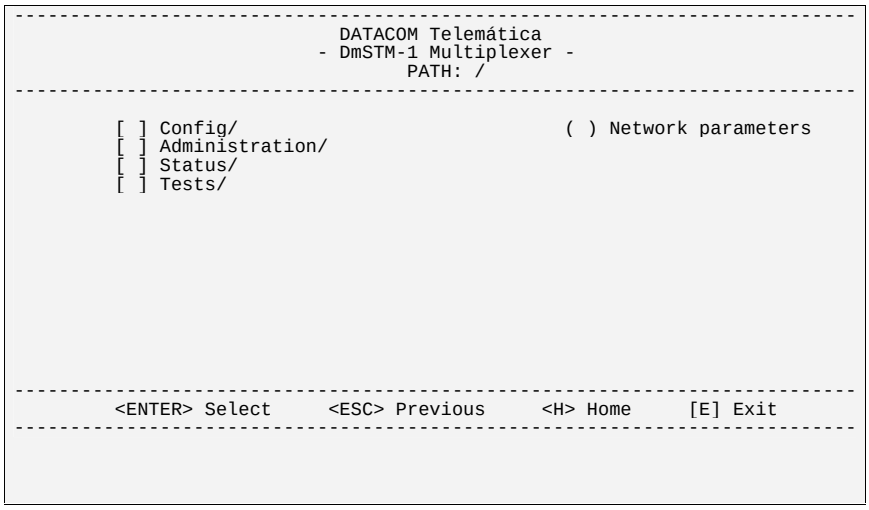


Figure 2 – Main menu

Using the Main menu, the user has access to:

- Administration: equipment configuration and system information;
- Status: equipment status visualisation;
- Tests: equipment test activation and visualisation;
- Network Parameters: equipment network access configuration.

1.6. PC Connection using the Ethernet port – Telnet and DmView

After performing the DmSTM-1 IP Ethernet interface configuration, it is possible to manage using the DmView management software.

Step 1: IP number Configuration (The equipment is factory configured with IP number 192.168.0.25/24)

To change the equipment IP number, the following steps must be taken: The user must access the terminal and choose the Network_Parameters option on the main screen. From this moment on, the configuration is done by the Zebra software. The user has to execute the following command sequence to change the IP number:

Command	Description
Enable	Enables access to the Privileged mode
conf t	Enables access to the Configuration mode
Inter eth0	Enables access to the DmSTM-1 Ethernet interface mode
no ip address AAA.BBB.CCC.DDD/M	Removes the IP number AAA.BBB.CCC.DDD. It is always necessary to remove the previous IP address before setting a new one.
ip address AAA.BBB.CCC.DDD/M	Inserts a new user-defined IP number

wr mem	Writes the new configuration into non-volatile memory
End	Takes the user back to the Privileged mode
Exit	Gets out of the initial mode and ends access to Zebra

Table 1 - IP change in Zebra

Step 2: Including the element in the DmView software

1. Run DmView management software
2. When the login screen is displayed, enter default password "**administrator**"
3. The Network Browser screen will be displayed. Select the "ADD" button and add the equipment IP.

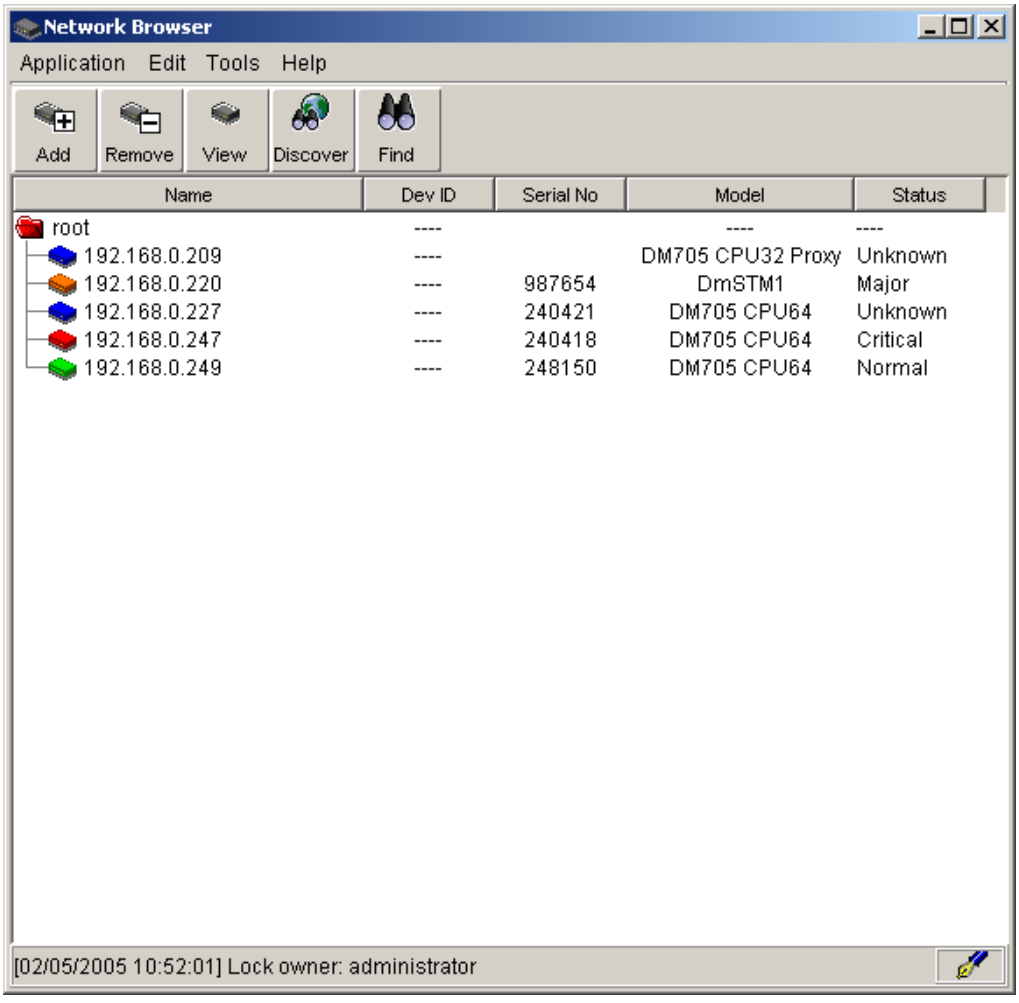


Figure 3 – Network Browser Screen

2 ADMINISTRATION (TERMINAL)

System_parameters – Visualises the system parameters

Current_logs - Visualises the current equipment log

Saved_logs - Visualises the previously saved equipment logs

Set_boot_parameters - Configures the initialisation and auto-recovering equipment parameters

Set_snmp_parameters - Configures the SNMP management parameters

Set_ntp_parameters - Configures the equipment date/time server parameters

Del_user – Delete user

Add_user – Create user

Set_password – Set user password

Date - Configures equipment date and time

Kill_vtysh – Closes vtysh connections

The Administration menu allows adjustment of the normal equipment operating parameters and also displays some of the equipment configuration.

2.1. System parameters visualisation

The System_parameters menu allows visualising the system parameters. These parameters are unchangeable equipment-specific information. The figure below displays the System_parameters menu.

```
--------------------------------------------------------------------------------
                            DATACOM Telemática
                          - DmSTM-1 Multiplexer -
                           PATH:/Administration/
--------------------------------------------------------------------------------

             Administration/System_parameters


             <> Boot Version             [ 1.1 ]
             <> Firmware Version         [ 1 ]
             <> Hardware Version         [ 3 ]
             <> Release Date             [ Wed Apr  2 16:17:54 BRT 2003 ]
             <> MAC Address              [ 40.00.00.00.00.FD ]
             <> Number of resets         [ 14 ]
             <> Serial Number            [ 400324 ]




--------------------------------------------------------------------------------
                              <ESC> Back to Menus
--------------------------------------------------------------------------------
```

Figure 4 – System_parameters Menu

Boot Version – Boot Firmware version.

Firmware Version – Equipment firmware version. The firmware can be upgraded by the user.

Hardware Version - Equipment hardware version.

Release Date - Equipment software release date.

MAC Address - Medium Access Control address – physical Ethernet interface address.

Number of Resets - Number of equipment reset times since factory release.

Serial Number - Equipment serial number.

2.2. System Logs

The Current_logs menu allows visualisation of the system logs. Every alarm, activation and error equipment logs are available. Date and time changes are also logged. The Figure below illustrates the Current_logs menu.

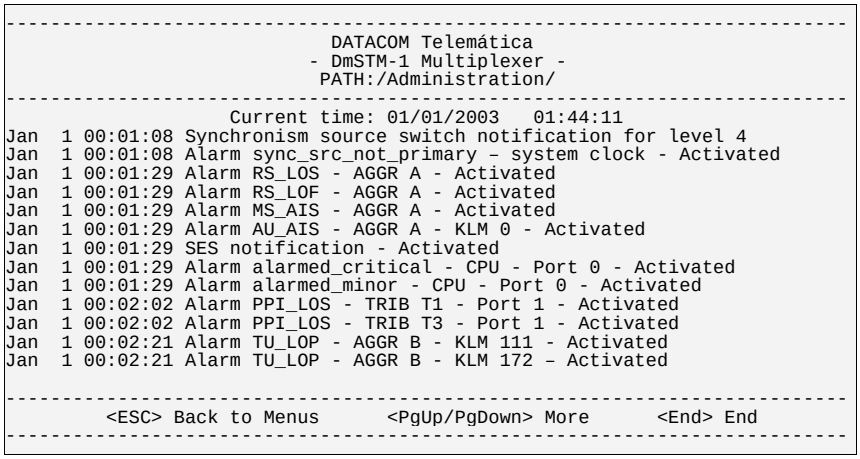


Figure 5 – Current_logs Menu

Note: The log file is saved and cleared by the equipment in non-volatile memory periodically. To visualise the saved logs, use the Saved_logs command.

2.3. Saved Logs

The Saved_logs menu allows visualising the system logs that have been saved. Every alarm, activation and error equipment logs are available. The Figure below illustrates the Saved_logs menu.

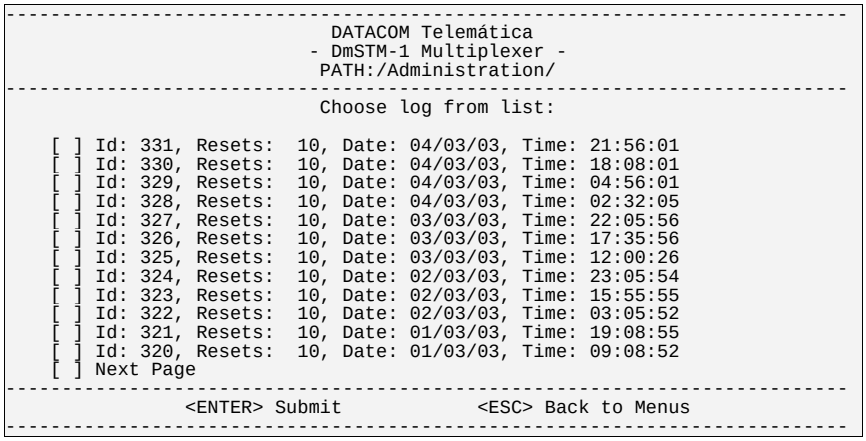


Figure 6 –Saved_logs Menu

The first entry corresponds to the last saved log (the most recent). The others are older, according to the ID number.

ID - Saved log ID number.

Resets - Number of equipment resets since factory release, from the moment this log was recorded.

Date - Log save date.

Time - Log save time.

Next Page – Jumps to next page (older logs). Shortcut key: Page Down

Previous Page – Jumps to previous page (newer logs). Shortcut key: Page Up

Note: The first entry shown on-screen always points to the last saved log, that is, to the log preceding the present one (visualised with the Current_logs command).

2.4. Initialisation parameters configuration

The Set_boot_parameters menu allows visualising and configuring the equipment initialisation parameters. These parameters have system recovering information for equipment use in the event of a major failure. The Figure below illustrates the Set_boot_parameters menu.

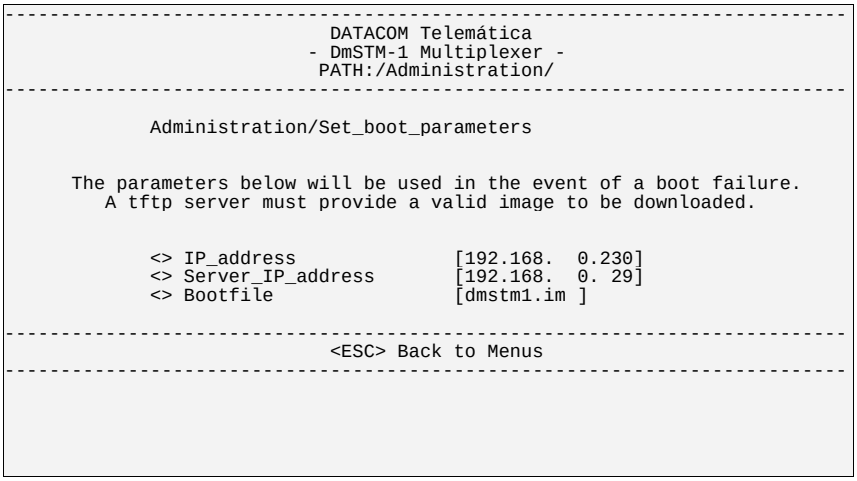


Figure 7 – Set_boot_parameters Menu

IP address - Equipment IP number when operating in boot mode.

Server IP address – TFTP server IP number, containing a valid equipment firmware image.

Bootfile - Equipment firmware image residing on the TFTP server.

The information configured in this menu is not used by the equipment under normal operating conditions. These parameters are necessary so that the equipment can recover from any interruption during firmware upgrade or physical failure during the writing processes in the non-volatile memories.

It is important to note that the equipment IP number when operating in boot mode is not the same as the equipment IP number under normal operation (unless this operation is manually done by the equipment user). So, extra care must be taken so as to avoid the equipment to have invalid or conflicting IP numbers.

2.5. SNMP management parameters configuration

The Set_snmp_parameters menu allows visualising and configuring the SNMP (*Simple Network Management Protocol*) management parameters. The management station that gets the equipment-generated traps has its IP number configured and also the name of the writing and reading communities. The figure below illustrates the Set_snmp_parameters menu.

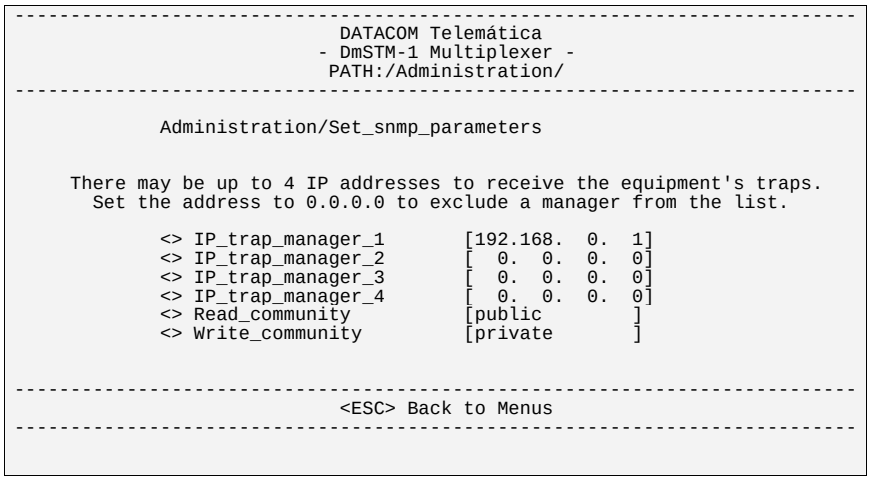


Figure 8 – Set_snmp_parameters Menu

Note: when the IP number 0.0.0.0 is configured, the equipment does not generate traps (for this particular IP entry).

IP_trap_server - Management station IP number that will receive the equipment-generated traps (when the IP number 0.0.0.0 is set, the equipment will NOT generate traps for any manager in this IP).

Read_Community – Read community to access the SNMP management.

Write_Community – Read/write community to access the SNMP management.

Sys_name - Parameter that allows reading/writing the sysName object, pertaining to the system table (mib-II).

NOTE 1: The DmSTM-1 SNMP agent allows management via the SNMPv1 and SNMPv2c protocol. The traps are generated in the SNMPv2c format, however.

The Set_snmp_parameters menu allows:

- Visualising and configuring the IP number of the management station that will receive the equipment-generated traps (for a total of four IPs);
- Visualising and altering the read and read/write SNMP management communities (SNMPv1 and SNMPv2c);
- Visualising and altering the system name identification (sysName).

NOTE 2: To access the SNMP management through the DmView software it is necessary to configure the reading and writing communities in the DmView. For more details, see the DmView Manual.

2.6. Date/time server parameter configuration

The Set_ntp_parameters menu allows visualising and configuring the IP number of the station that will provide the date and time updating for the equipment. The configured IP must have an NTP software server. The date and time updating is done at the equipment initialisation and at every other day. If there is any failure in getting the correct time, the equipment tries again, with an interval of five minutes between each trial.

IP_NTP_server - NTP server IP address.

Time_zone - Allows configuring the equipment time zone parameter. If set to 0, the equipment will use the Greenwich Time.

Note 1: When the IP number is set to 0.0.0.0, the equipment will use no NTP server.

Note 2: No summer time automatic adjustment is done. To do the manual adjustment, change the time zone.

Note 3: The time zone configuration is mandatory; otherwise the equipment will use the Greenwich Time.

2.7. System User Deletion

The Del_user menu allows excluding a user from equipment.

Username - Name of user to be deleted

Note 1: If an invalid user name is keyed, no user will be deleted from the equipment access.

Note 2: Only the default use (**datacom**) is allowed to add or delete users.

Note 3: It is not possible to delete the default user (**datacom**).

2.8. Adding System Users

The Add_user menu allows adding a user to the equipment, allowing his or her access to it.

Username - Name of user to be added

New Password - The password to be used by the new user

Retype new Password - New user password confirmation

Note 1: Only the default user (**datacom**) is allowed to add or remove users.

Note 2: It is not possible to add existing users.

Note 3: The user name will be listed in the activation logs, keeping track of the operations that he or she performed on the equipment.

2.9. Changing the user password

The Set_password menu allows changing the user password presently logged in the equipment.

Username – automatically filled

New Password – The new password to be employed by the user

Retype new Password - New user password confirmation

Note 1: The user is allowed to change only his or her own password. The exception is the user **datacom**, who can change any user password.

Note 2: Only the user **datacom** has access to the Username object. For the other users, this object is automatically filled.

Note 3: The user name will be listed in the activation logs, keeping track of the operations that he or she performed in the equipment.

2.10. System Date Change

The Date menu allows setting the system date and time.

Date - Sets the system Date, in the format: MM/DD/YYYY

Time - Sets the system time

Note 1: If the equipment has no configured NTP server, the system date and time must be set every time that the equipment is turned on.

Note 2: If the system has an NTP server, it is recommended not to set date/time by using this menu, for that information will be lost after the next NTP update.

2.11. System Pending Connection Removal

Old (pending) connections can prevent the user from accessing the DmStm-1 via telnet. By using the Kill_vtysh menu, these connections are killed.

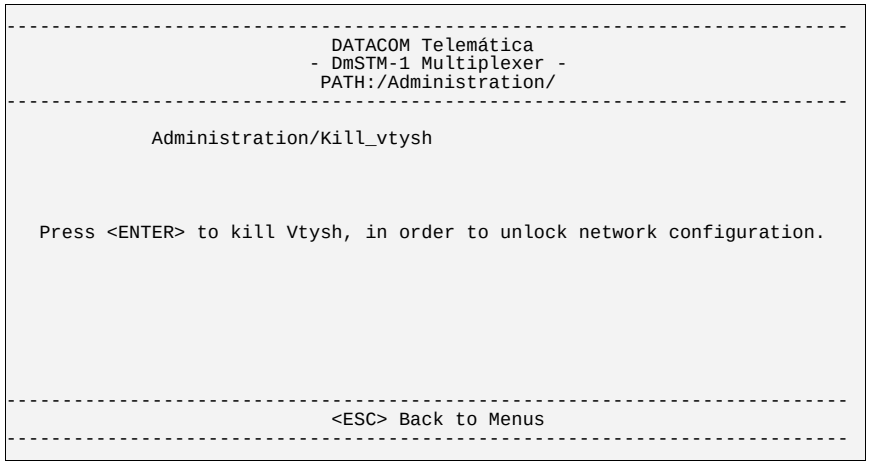


Figure 9 – Pending connections elimination menu

2.12. Restarting Network Router

For some cases, there can be problems when reconfiguring the equipment network parameters. The Restart_inetd object restarts the section responsible for network routing, so as to force the network interfaces to operate in the same way as dictated by the stored configuration.

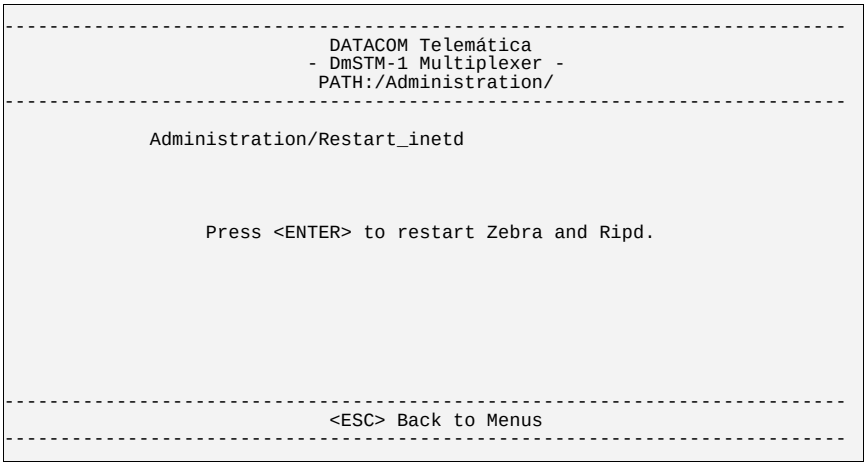


Figure 10 – Network Router restart menu

3 CONFIGURATION

The DmSTM-1 configuration is performed by the DmView application software.

3.1. DmSTM-1 Configuration

It is possible to access the DmSTM-1 configuration screens through the DmView Configuration/Device Config option

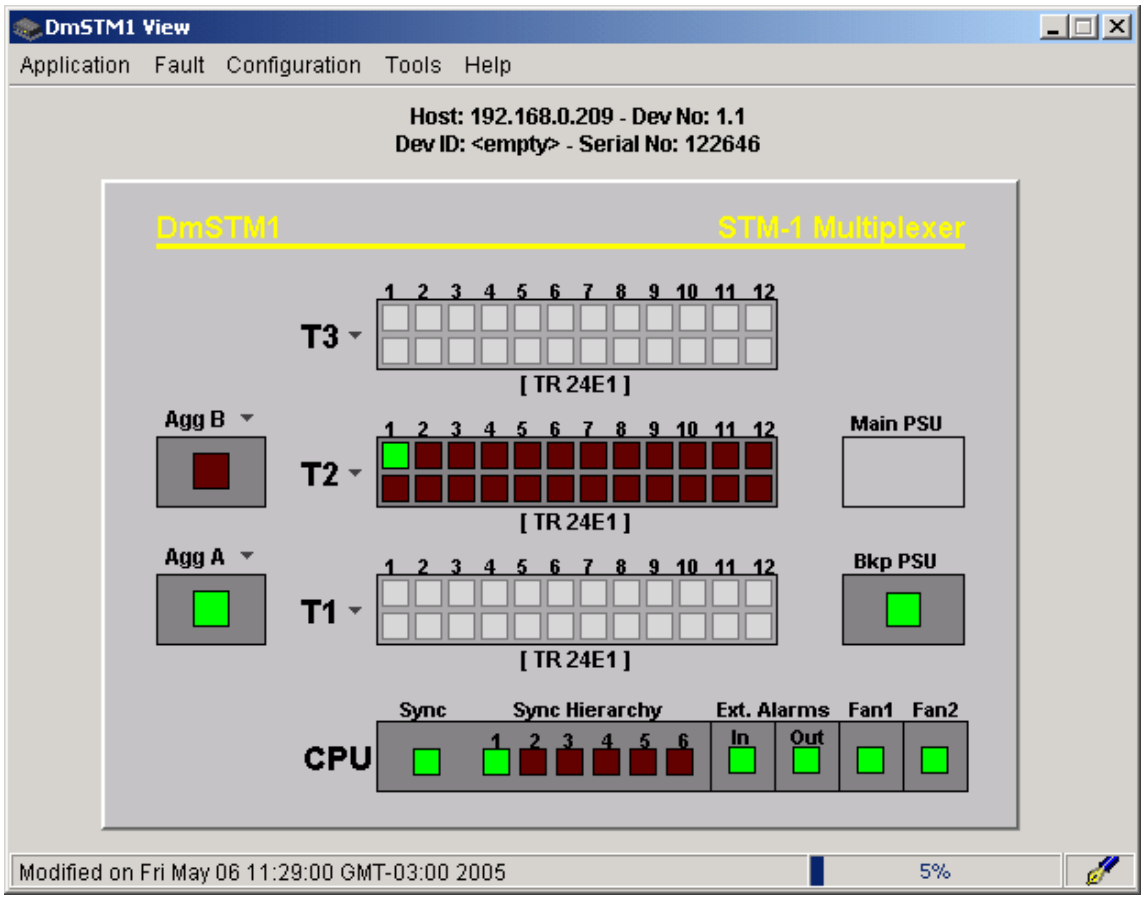


Figure 11 – DmSTM-1 bayface screen

3.2. Network Topology Configuration

From the Configuration/Device Config/NE Config menu it is possible to configure the DmSTM-1 operation topology. For point-to-point operation, the Terminal mode should be used, which allows using the MSP 1+1 protection scheme. The MSP requires that the equipment be equipped with two STM-1 aggregate interface cards.

For ring or linear ADM operation the ADM mode should be used, equipping the DmSTM-1 with two STM-1 aggregate interface modules. For ring operation, the SNC protection scheme can be used. For linear topology the SNC protection should not be used.

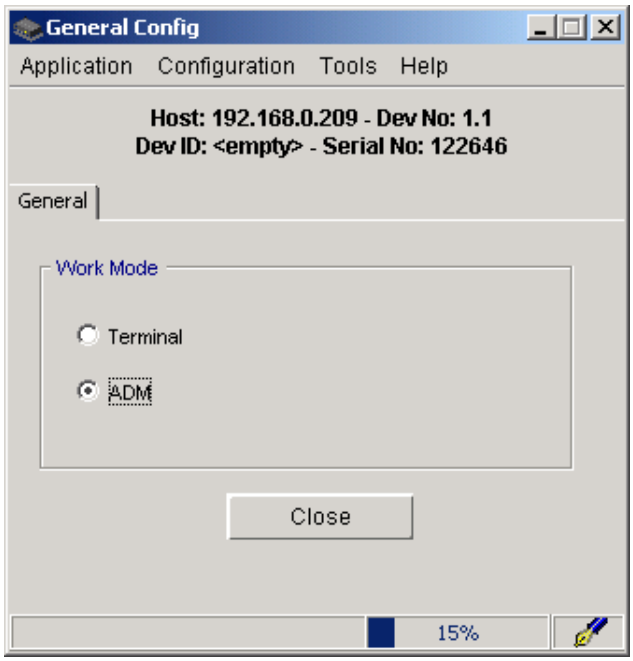


Figure 12 – Topology Configuration Screen

Terminal - Point-to-point topology, optionally using MSP 1+1 protection.

ADM - The equipment is connected to an SDH ring, inserting and deriving only the locally mapped data with pass-through of the other network traffic. It can operate with or without SNC protection.

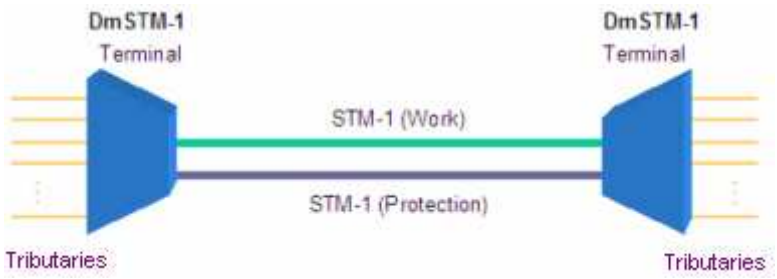


Figure 13 – DmSTM-1 using point-to-point topology

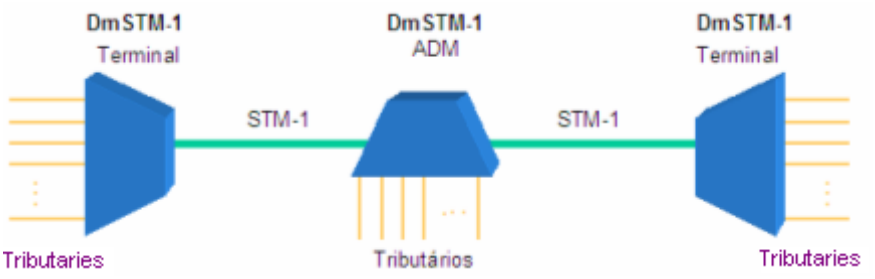


Figure 14 – DmSTM-1 in the ADM and Terminal modes, linear topology

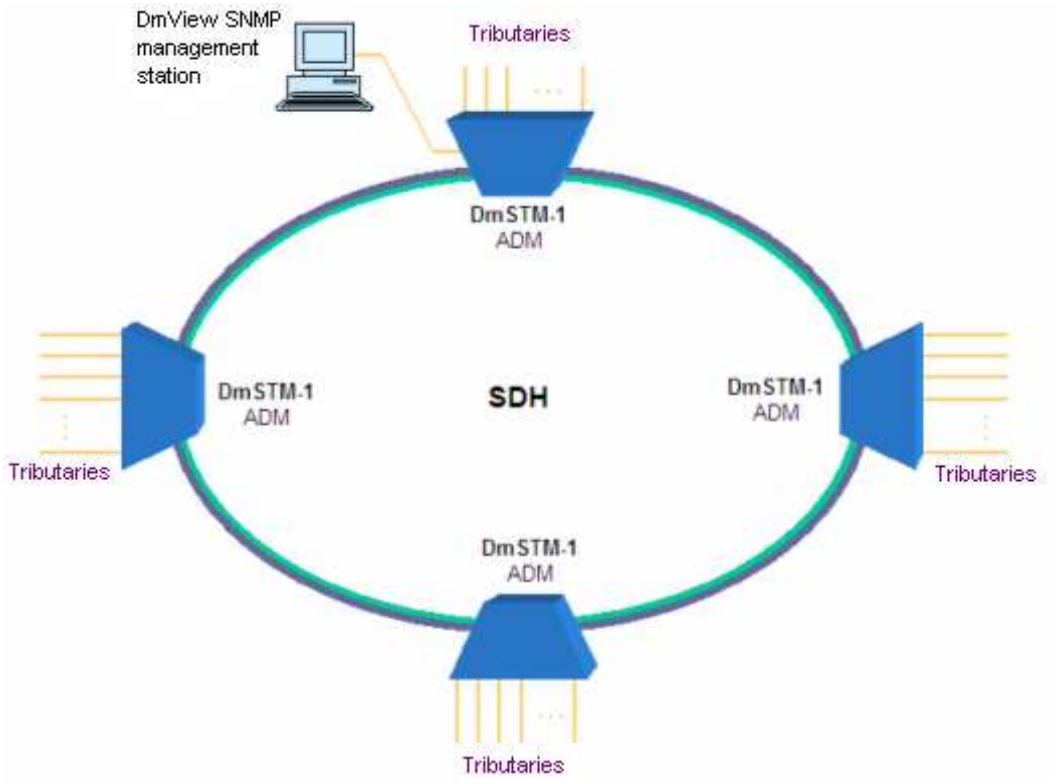


Figure 15 – DmSTM-1 in the ADM modes, ring topology

3.3. Protection Configuration

3.3.1. SNC Protection Global Parameters

The SNC protection is used for the ADM operating mode. The SNC Config menu allows performing the SNC protection global parameters configuration. The global parameters are valid for every mapping that has SNC protection.

The enabling and configuration of the SNC protection parameters is performed at the DmView tributary mapping menu.

Figure 16 – SNC Protection Configuration Screen

WTR (Wait to restore) – Time that the equipment will wait to switch to the main path, when that path recovers from a failure state.

Enable HP-TIM – Enables switching to protection path when a HP-TIM alarm is detected.

Enable HP-EXC – Enables switching to protection path when a HP-EXC alarm is detected.

3.3.2. MSP Protection Scheme

The MSP 1+1 protection scheme is used in point-to-point topology, when the equipment is configured to operate in the terminal mode.

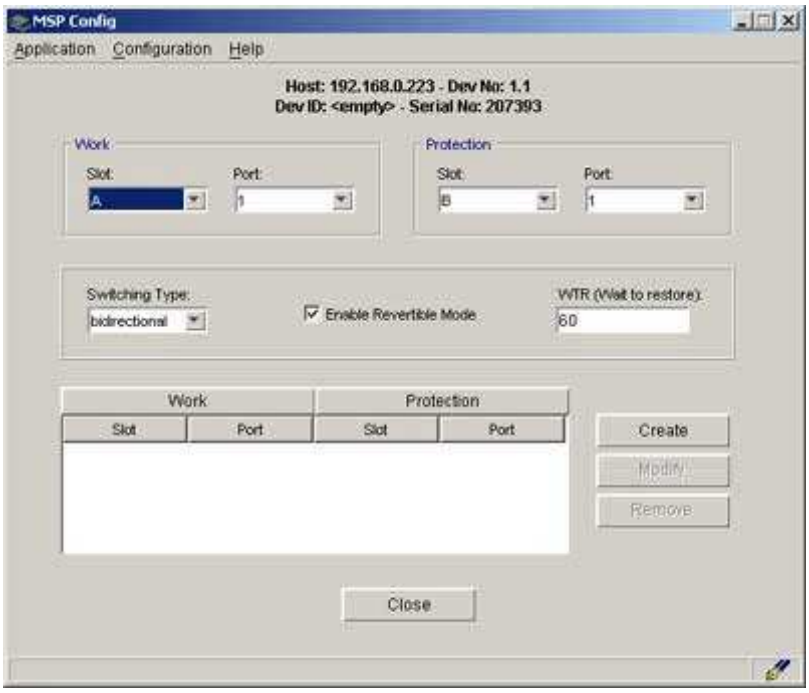


Figure 17 – MSP Protection Configuration Screen

Work - Selects the main aggregate interface.

Protection - Selects the protection aggregate interface.

Switching Type - Selects bi-directional or unidirectional protection switching.

Enable Revertible Mode - Enables revertible mode. In revertible mode equipment will switch back to the work interface after it recovers from a failure state.

WTR (wait to restore) - Time that the equipment will wait to switch to the main aggregate, when that aggregate recovers from a failure state.

3.4. STM-1 Aggregate Configuration

At the Ports Config screen it is possible to select the tributary to be configured. By selecting the STM-1 aggregate in the Slot and the Port tab, the aggregate configuration options are made available.

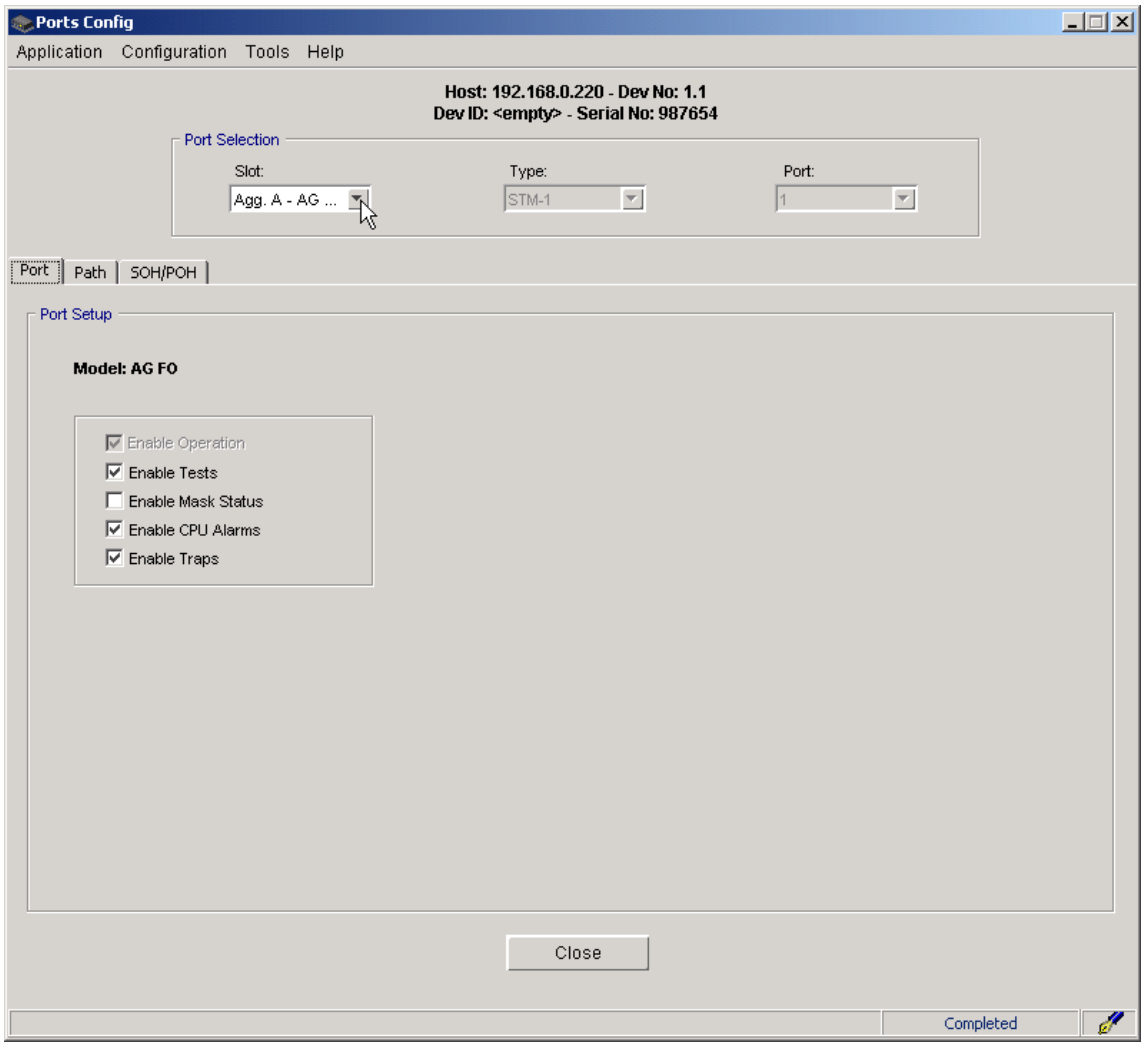


Figure 18 – Aggregate Ports Config Screen

Enable Operation - Enables interface operation.

Enable Tests - Allows running diagnose interface tests.

Enable Mask Status - Enables interface status masking. When disabled interface alarms are not propagated.

Enable Traps - Enables sending traps. When disable no traps are sent when an alarm event occurs.

3.4.1. Path Configuration

Using the Path tab, the user can configure the path identifiers, the alarm threshold and the path label.

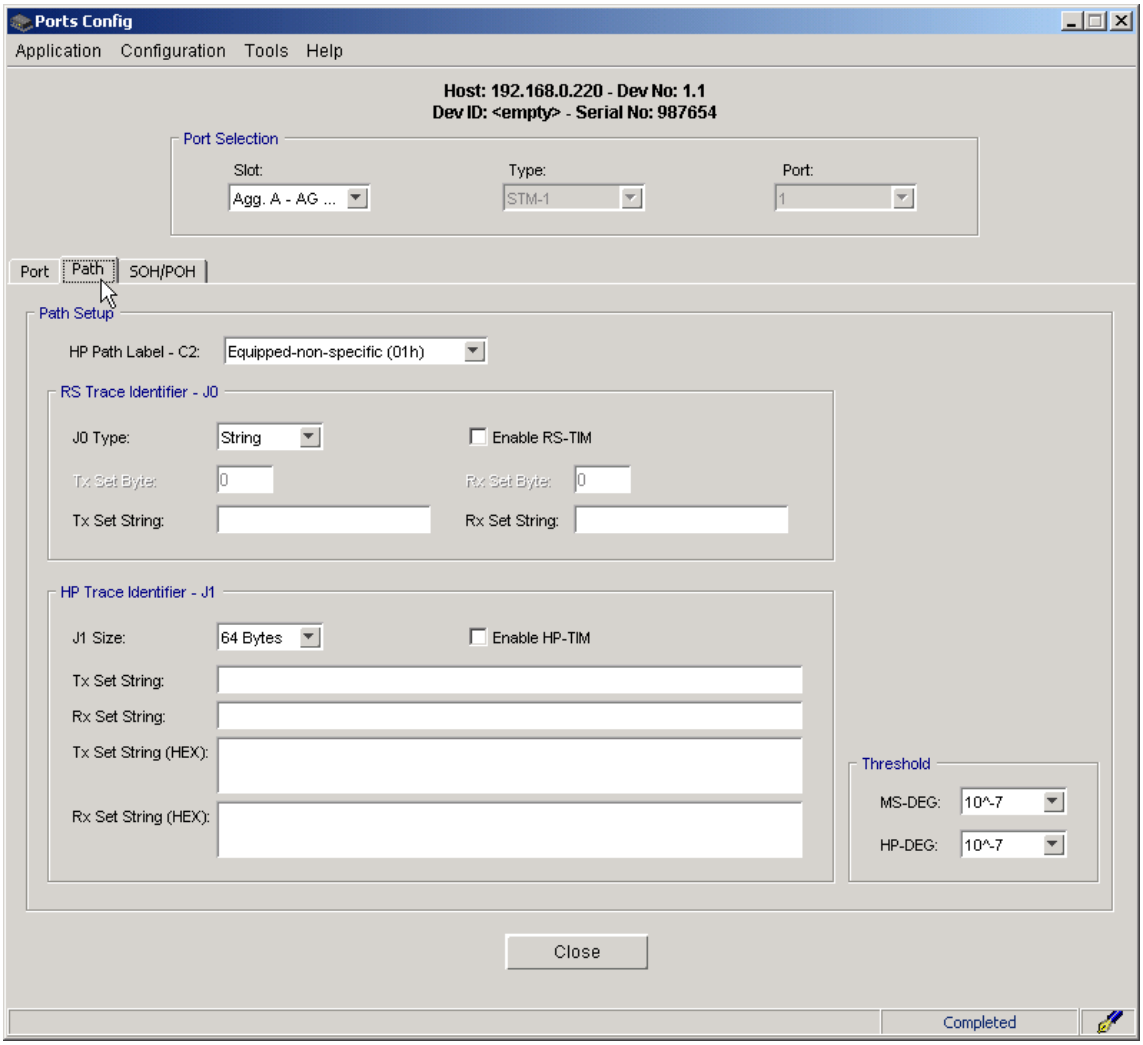


Figure 19 – Aggregate Path Config Screen

3.4.2. Payload Identifier - Path Label C2

Allows the VC-4 Payload Identifier configuration. The HP Path Label – C2 configuration values are listed below.

Equipped-non-specific (01h) - Not specific.

TUG-structure (02h) - TUG Structure.

Mapping under development (05h) – Mapping coding not defined.

3.4.3. Path Identifier- Trace Identifier J0

Performs the Path Identifier configuration for the regenerating section.

J0 Type - Defines the type of path trace used, byte or 16 character string.

Tx Set Byte - Defines the value of the J0 transmitted byte (when configured as byte).

Tx Set String - Defines the value of the J0 transmitted string (when configured as string).

Rx Set Byte - Defines the value of the expected J0 byte (when configured as byte).

Rx Set String - Defines the value of the expected J0 string (when configured as string)

Enable RS-TIM – Enables RS-TIM alarm generation if the received Trace Identifier is different of the expected value as configured in Rx Set String.

3.4.4. Path Identifier- Trace Identifier J1

J1 Size - Defines the path name size, string of 16 or 64 characters.

Tx Set String - Defines the value of the transmitted J1 string.

Rx Set String - Defines the value of the expected J1 string.

Tx Set String (HEX) - Defines the value of the transmitted J1 string in hexadecimal.

Rx Set String (HEX) - Defines the value of the expected J1 string in hexadecimal.

Enable HP-TIM - Enables HP-TIM alarm generation if the received Path Identifier is different of the expected value, as configured at Rx Set String.

3.4.5. Thresholds - MS-DEG and HP-DEG

MS-DEG - Configures error rate for MS-DEG alarm generation.

HP-DEG - Configures error rate for HP-DEG alarm generation.

3.4.6. SOH/POH Configuration

The SOH/POH configuration guide allows configuring the VC-4 SOH and POH bytes. It is possible to perform the mapping of the overhead bytes for the following interfaces: aggregate A, aggregate B, voice interface and HDLC (0-3) routing channels. When the overhead bytes are not mapped, they assume the configured fixed values (stuff). The overhead bytes having specific functions that cannot be mapped are shown with a grey background.

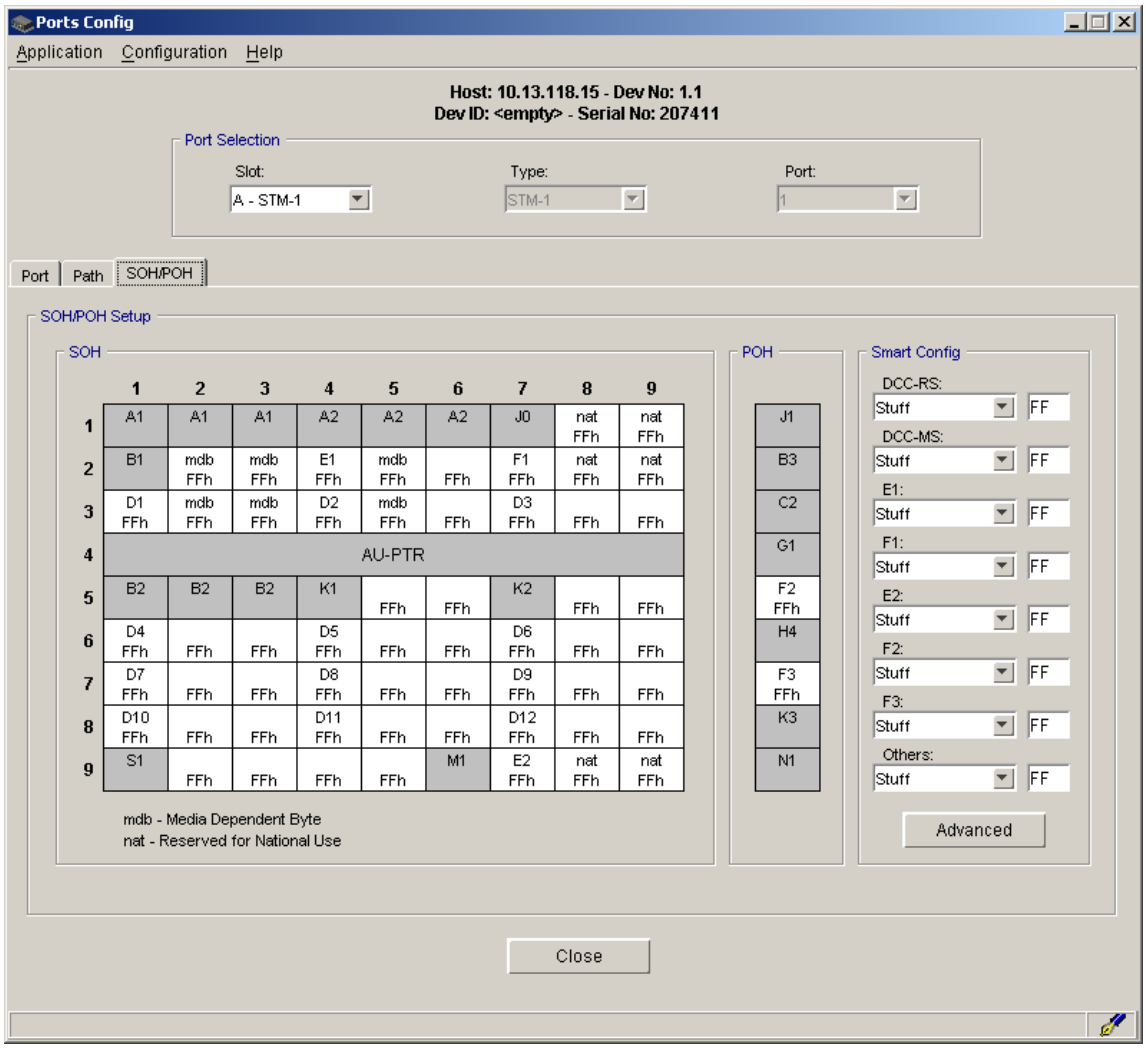


Figure 20 – STM1 overhead configuration bytes menu

The overhead bytes configuration options are listed below:

Stuff – Fills the byte with the configured value.

Agg A – The transmitted overhead byte will be the byte received at aggregate A.

Agg B - The transmitted overhead byte will be the byte received at aggregate B.

Voice - The overhead byte will be mapped to the equipment voice interface.

HDLC 0 – The configured bytes will be mapped to the router channel 0 *

HDLC 1 – The configured bytes will be mapped to the router channel 1 *.

HDLC 2 – The configured bytes will be mapped to the router channel 2 *.

HDLC 3 – The configured bytes will be mapped to the router channel 3 *.

The total number of bytes sent to the ROUTER HDLC (0-3) should not be more than 1280 kbit/s.

3.4.7. Multiframe Indicator - H4

The indicating byte of multiframe H4 is configured through the VC-4 Structure screen (see item 3.10.1). It defines the type of used sequence as indicating of multiframe in the H4 byte of the POH. (see Figure 21)

In the screen it is necessary to choose TUG-3 Structure option and, after that, choose the multiframe H4 that will be used.

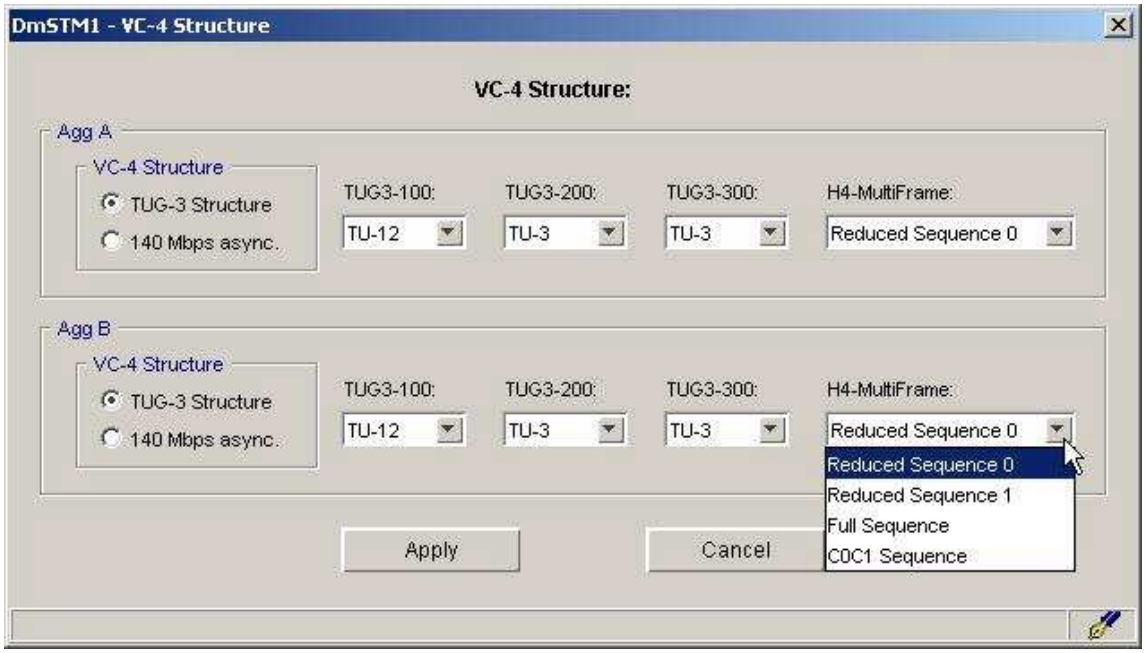


Figure 21 – H4_multiframe configuration screen

Reduced Sequence 0 - Reduced sequence of 4 bytes. Bits not used with standard 000000.

Reduced Sequence 1 - Reduced sequence of 4 bytes. Bits not used with standard 111111

Full Sequence - Complete sequence with 48 bytes

C0C1 Sequence - Reduced sequence of 4 bytes. Bits not used with standard 110000

3.5. 2Mbit/s (TR-24E1) tributary configuration

By selecting the slot with TR-24E1 card at the Configuration/Ports Config menu, the user has access to the configuration menu for the 2Mbit/s (E1) ports.

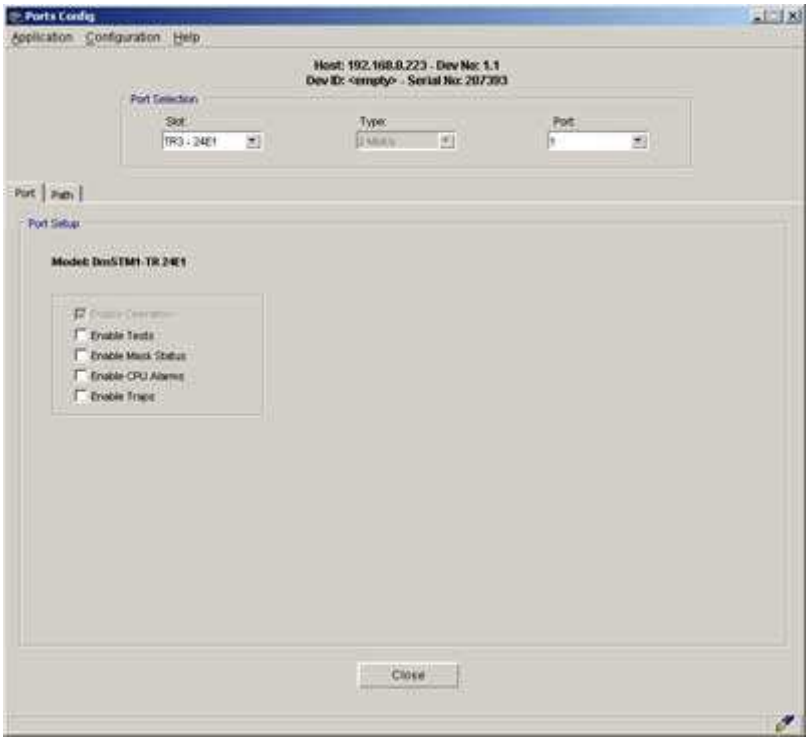


Figure 22 – TR-24E1 interface port setup screen

Enable Operation - Enables interface operation.

Enable Tests - Allows running interface diagnostic tests.

Enable Mask - Enables interface status masking. When disabled interface alarms are not propagated.

Enable Traps - Enables sending traps. When disable no traps are sent when an alarm event occurs.

The Path tab allows configuring the path parameters.

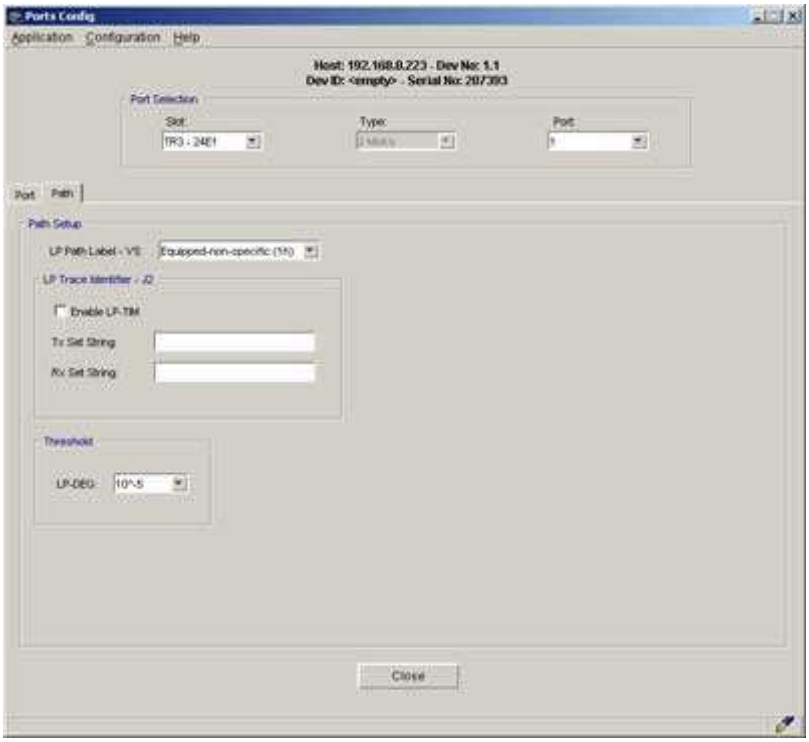


Figure 23 – TR-24E1 Interface path setup screen

3.5.1. Payload Identifier - Path Label V5

Allows configuring the VC-12 Payload Identifier. The LP Path Label V5 configuration values are listed below.

Equipped-non-specific (1h) – Not specific.

Asynchronous (1h) – Asynchronous mapping

3.5.2. Path Identifier - Trace Identifier J2

Enable LP-TIM - Enables LP-TIM alarm generation if the received Path Identifier is different of the expected value as configured in Rx Set String.

Tx Set String - Defines the value of the transmitted J2 string.

Rx Set String - Defines the value of the expected J2 string.

3.5.3. Threshold - LP-DEG

LP-DEG - Configures the error rate for LP-DEG alarm generation.

3.6. 34/45Mbit/s (TR-E3E) Tributary Configuration

By selecting the slot with the TR-E3E card at the Configuration/Ports Config menu, the user has access to the 34/45Mbit/s tributaries configuration menu.

The interface will have 45Mbit/s support when it is identified as 34/45Mbit/s in the panel stamping and in DmView. If such identification does not exist, the interface operates at 34Mbit/s.

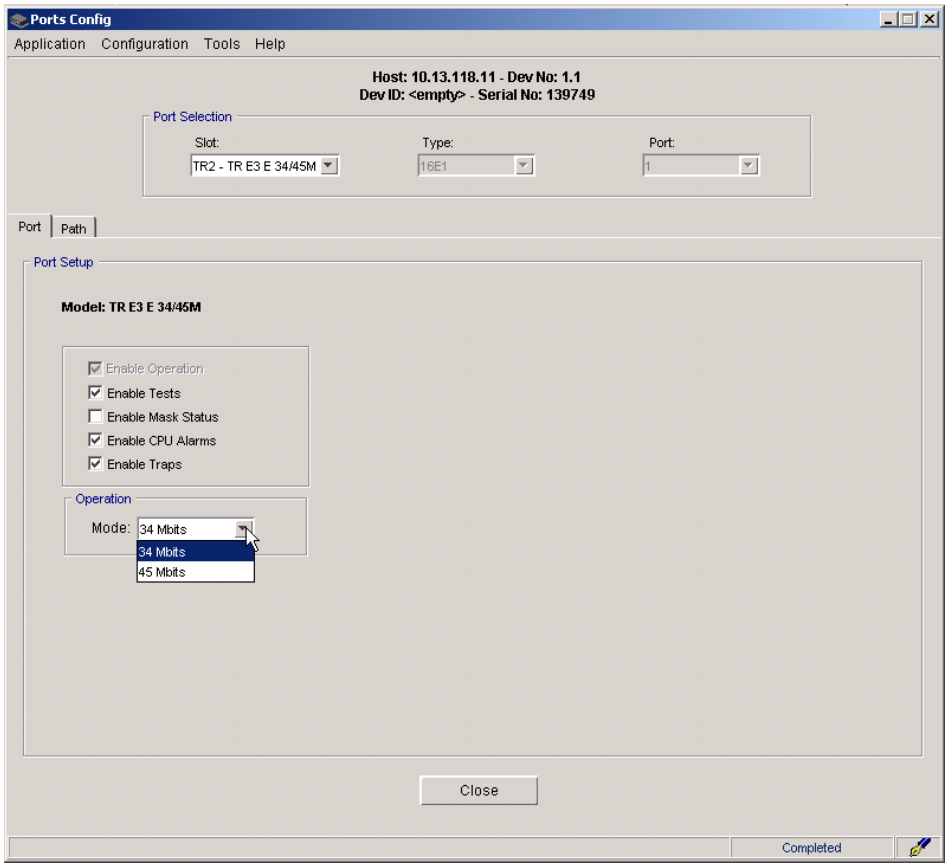


Figure 24 – E3E Interface Port setup Screen

Enable Operation – Enables interface operation.

Enable Tests - Allows running interface diagnose tests.

Enable Mask Status - Enables masking the interface status.

Enable Traps - Enables sending traps.

Operation Mode - Selects the operational mode of the tributary. The possible options are 34Mbit/s and 45Mbit/s.

3.6.1. Path configuration

In the Path label the configuration of the path parameters, alarm threshold and path label is done.

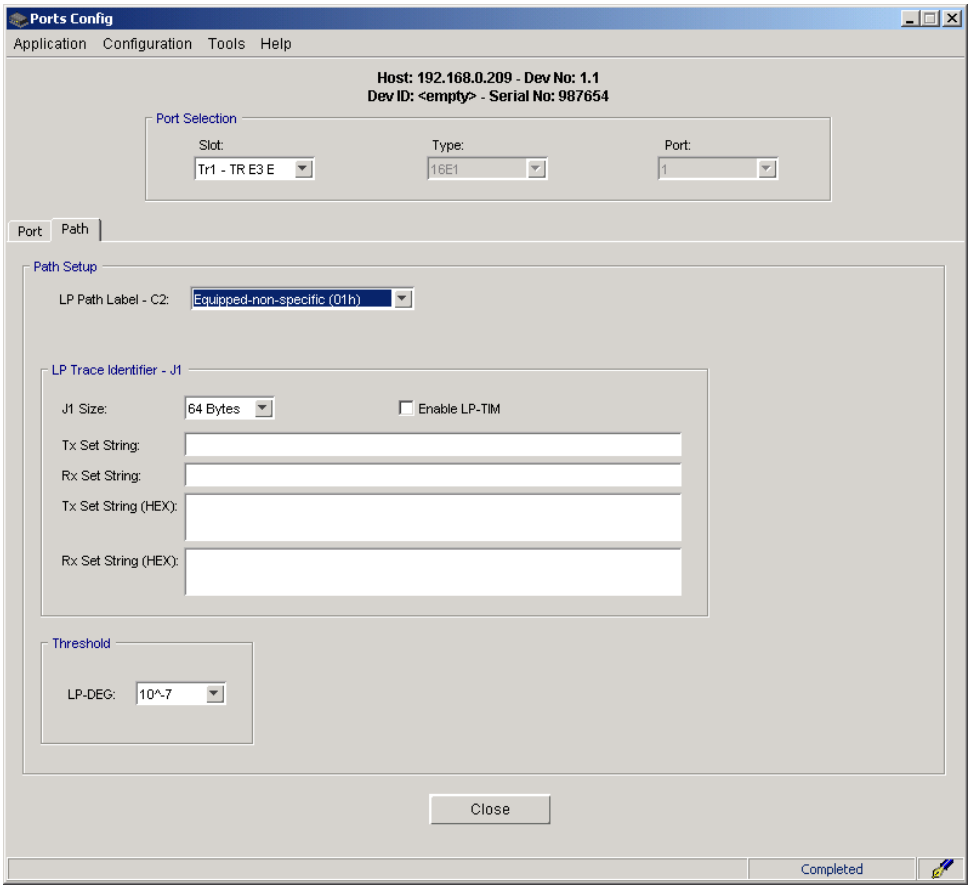


Figure 25 - E3E Interface path setup screen

3.6.2. Payload Identifier - Path Label C2

The LP Path Label – C2 configuration values are listed below.

Equipped-non-specific (01h) - Not specific.

34Mbit/45Mbit in C3 async (04h) – Asynchronous C3 mapping

Mapping under development (05h) – Mapping coding not defined.

3.6.3. Path Identifier - Trace Identifier J1

J1 Size – Defines the size of the trace identifier, 16 or 64 string characters.

TX Set String - Defines the transmitted J2 string value.

Rx Set String - Defines the expected J1 string value.

TX Set String (HEX) - Defines the transmitted J1 string value in hexadecimal.

Rx Set String (HEX) - Defines the expected J2 string value in hexadecimal.

Enable LP-TIM - Enables LP-TIM alarm generation if the received Trace Identifier is different of the expected value as configured in Rx Set String.

3.6.4. Threshold - LP-DEG

LP-DEG - Configures the error rate for LP-DEG alarm generation.

3.7. (TR-ETH) Ethernet Tributary configuration

By selecting a slot with TR-ETH card in the Configuration/Ports Config menu, the user has access to the Ethernet tributary configuration Menu. To better understand the configurations, figure 25 shows a block diagram representing the tributary structure.

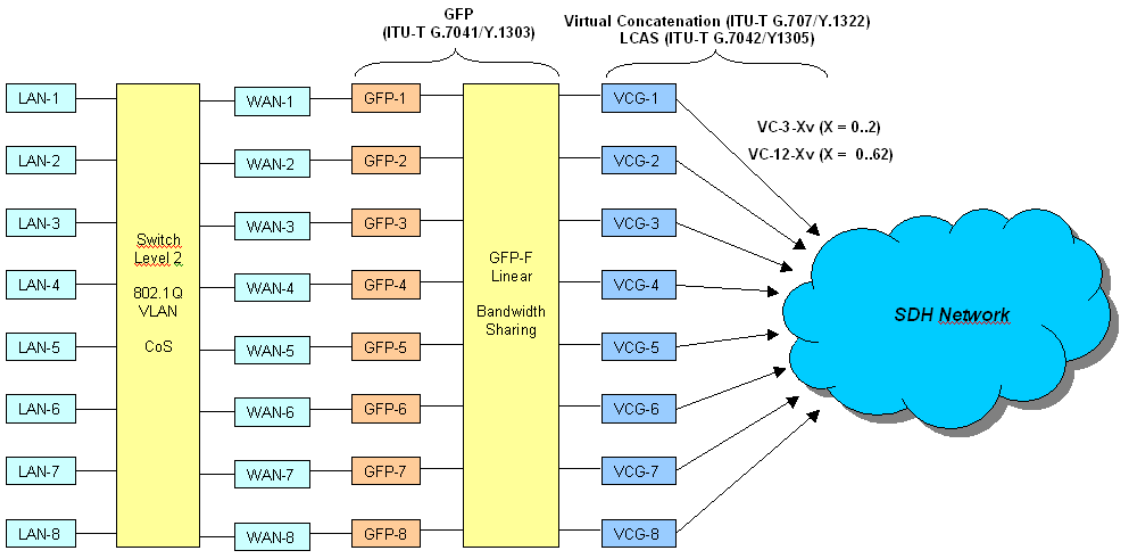


Figure 26 – Tributary block diagram

The Ethernet Tributary configuration is divided in four parts that can be selected in the Port Selection panel type menu. Items 3.7.1, 3.7.2, 3.7.4 and 3.7.5 will each show one of those four parts, describing its features and configurations.

3.7.1. Ethernet Interfaces (LAN)

In this panel all eight tributary LAN interfaces can be configured, as described below:

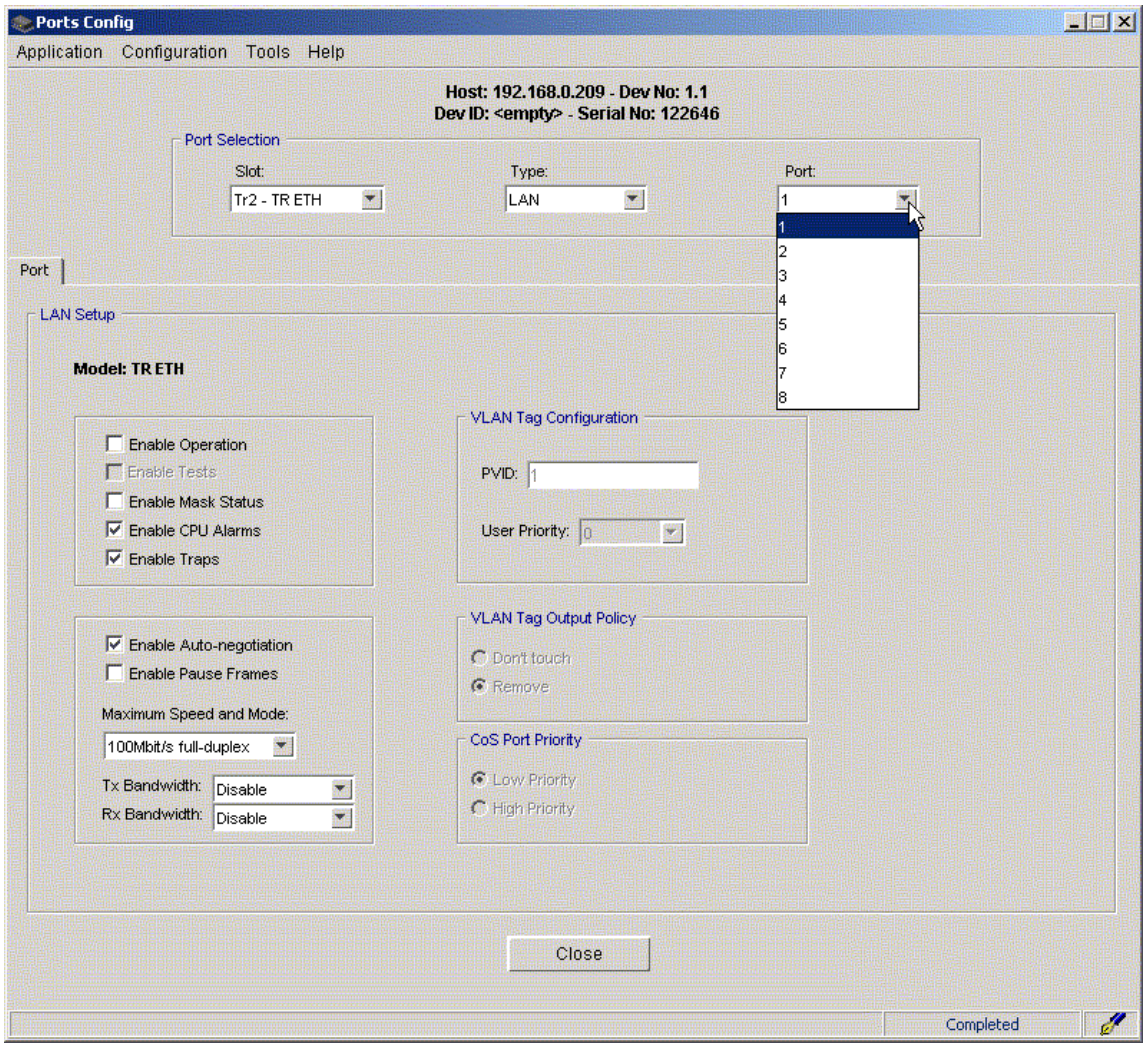


Figure 27 – LAN Interfaces configuration screen

Enable Operation – Enables interface operation.

Enable Mask Status - Enables masking the interface status.

Enable Traps - Enables sending traps.

Enable Auto-negotiation – Enables port auto-negotiation

Enable Pause Frames – Enables flow control to the Full-duplex operational mode, through the generation of Pause Frames.

Maximum Speed and Mode – In case the auto-negotiation option is enabled, this option allows the user to select the maximum speed and the interface auto-negotiable modes. In case the auto-negotiation option is disabled, the selection of speed and operational mode of the Ethernet interface can be done.

TX Bandwidth – Configuration of the interface maximum bandwidth transmission.

Rx Bandwidth – Configuration of the interface maximum bandwidth reception. In case the data reception rate exceeds the configured, the flow control (pause-frames or backpressure) will be activated in the interface, as long as it is enabled.

VLAN Tag Configuration – This panel is only enabled when the Switch is in the VLAN Aware operation mode (see item 3.7.2). The interface default VID configurations, as well as the priority are configured in this panel. The values configured here are inserted as VLAN tag in the Ethernet frames that arrive at the interface without tag. Packets with tag are not altered.

VLAN Tag Output Policy – Defines the packets outgoing policy in the interface relating to the VLAN tag. The Remove option makes so that all Ethernet frames leave the interface without tag. In case the option is Don't Touch, the frames will be sent in the same way as they reached the Switch, with or without VLAN tag.

CoS Port Priority – In this item, the port priority is defined. See item Class of Service, in 3.7.2.

3.7.2. Switch

In this window all Ethernet Tributary Switch functionalities are configured. The configurations enclose operational mode, VLANs mapping and service classes configuration. The window is divided in two parts. In the first are the Switch configurations and in the second, the VLANs mapping.

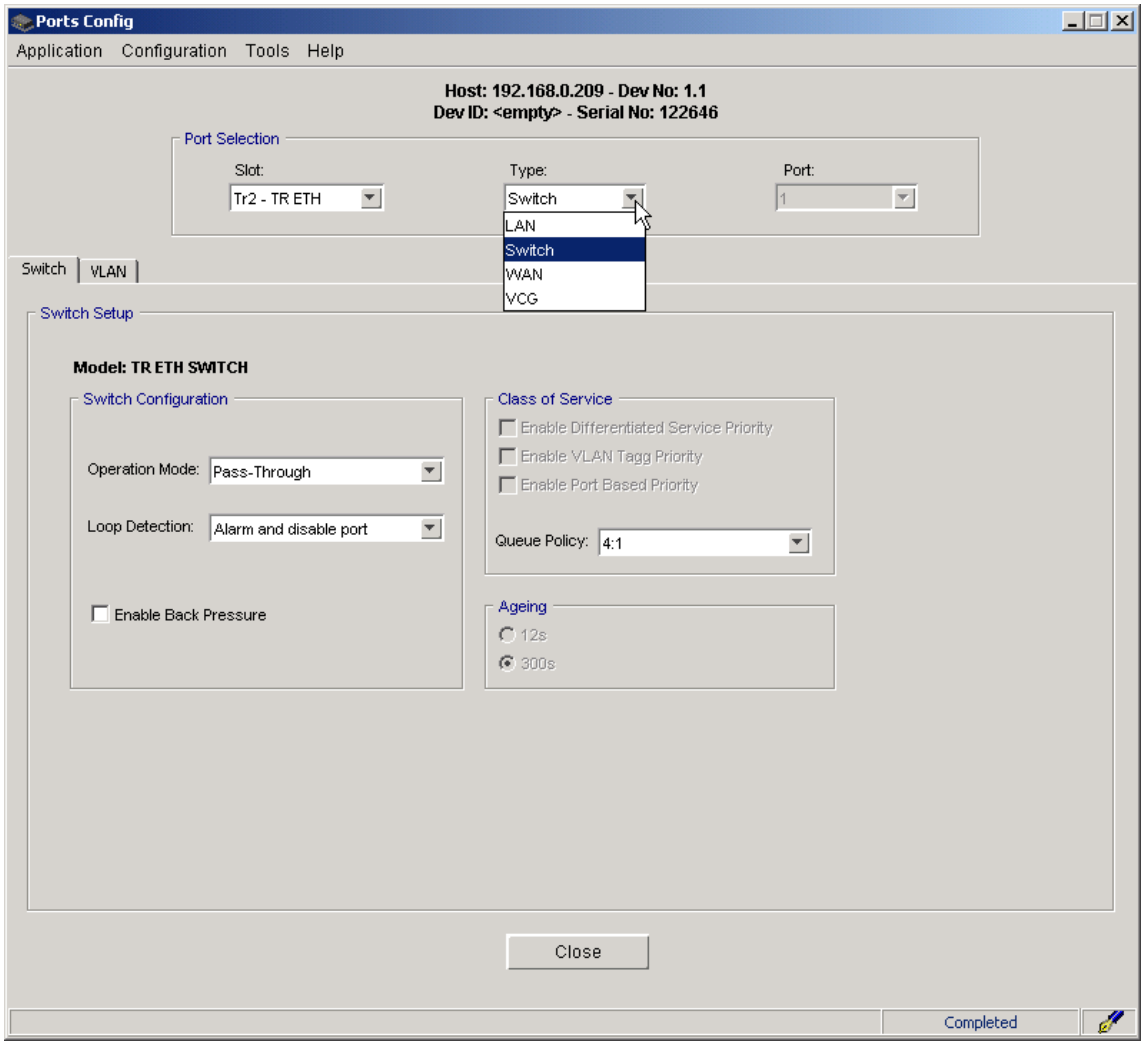


Figure 28 – Switch configuration screen

Operation Mode – Configuration of the Switch operation mode. Below are described the four possible operation modes:

- **Pass-through:** Switch disabled. When this mode is selected, the eight LAN interfaces of the tributary are connected directly to the WANs and all Switch functions are disabled.
- **VLAN-Unaware:** In this operation mode the Switch is enabled, however without the VLAN functions. The CoS functions operate regularly in this mode. It is also good to note that, in this operation mode, broadcast packets or unicast packets with MAC unknown by the switch that arrive at the interfaces, LANs or WANs, are sent to all 16 Switch ports.
- **VLAN-Aware:** Enables the Switch operation with recognitions of the VALN tags. In this mode VLANs in the switch can be configured, as well as default VIDs in the LAN interfaces can be defined (see item 3.7.1).
- **Port Based VLAN:** Enables the Switch operation and the configuration of Port Based VLANs. In this case, port groups can be created, forming broadcast domains. Each group

traffic is isolated from the other groups. Each Switch port (LANs and WANs) can only take part in one group.

Loop Detection – This menu allows configuring the functionality loop detection in the LAN or WAN tributary interfaces. The detection is done through the periodical generation of special Ethernet frames. When one of these frames returns to the switch, a detected loop alarm is activated. The configuration allows disabling the generations of these frames and consequently the loop detection. It is also possible to configure the Switch to disable the port (LAN or WAN) where the loop was detected.

Enable Back Pressure – Enables the back-pressure method flow control. This configuration is used by all the eight tributary LAN interfaces.

Class of Service – Configuration of the service classes. The frames are classified as high or low priority through 3 possible methods. When more than one method is enabled, the frame classification as high priority in any of the 3 methods defines it as high priority. The two outgoing lines operate in the weighted round robin mode and the Queue Policy menu allows the configuration of the line weights. Below, the 3 packets classification types are described with more details:

- **Differentiated Service Priority:** The frame is classified according with the DS field value, called Differentiated Services Code point (DSCP) defined in the RFC2474. The recommended code points for the traffic classification are defined in the RFC2597. The Expedited Forwarding (101110), Assured Forwarding (001010, 010010, 011010 and 100010) and Network Control (111000 e 110000) values, classify the frames as high priority. The remaining are classified as low.
- **VLAN Tag Priority:** The frame classification is done from the User Priority field, present in the VLAN Tag. Values from 4 to 7 classify the frame as high priority and values from 0 to 3 as low priority.
- **Port Based Priority:** The classification is done from the frame origin port. Packets originated from low priority ports are put in the low priority line and the ones originated from high priority ports are sent to the high priority lines. Each Switch port can be configured as high or low priority (see item 3.7.1).

Ageing – Configuration of the permanence time of an entry in the dynamic MAC address table of the switch.

3.7.3. VLAN

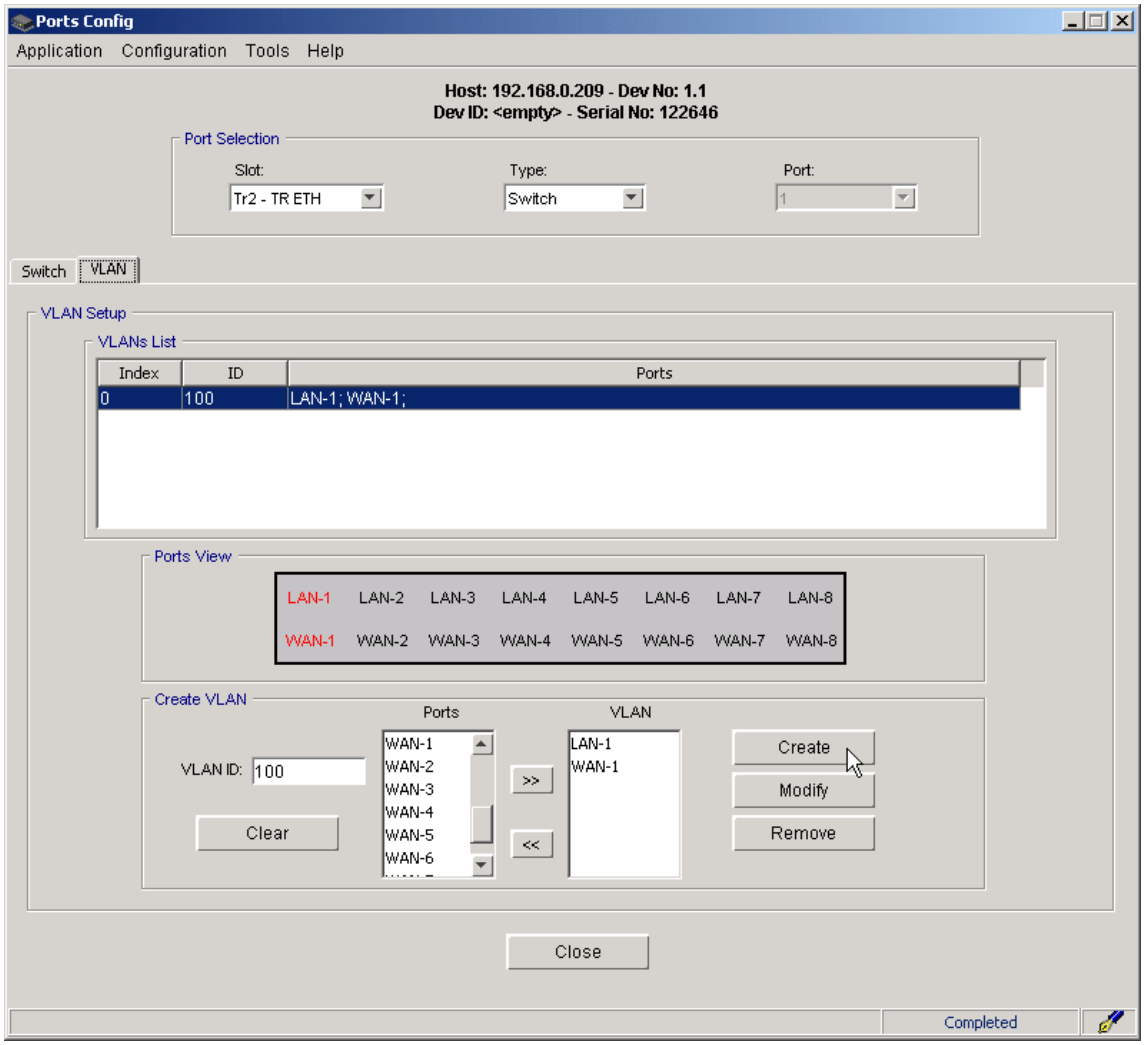


Figure 29 – VLANs configuration screen

In this screen the mapping of the VLANs is done. It is only possible to map VLANs when the Switch is in the VLAN Aware or Port Based VLAN operation modes. The screen is made of 3 main panels that show a list of VLANs, port visualization and the interface for VLANs creation.

VLANs List – This panel shows the VLANs already created In the VLAN Aware mode, up to 32 VLANs can be created. When one VLAN in this list is selected, the ports belonging to it are marked in the Ports View panel.

Ports View – In this panel the 16 Switch ports f the Ethernet Tributary are represented, being made of 8 LAN interfaces and 8 WANs. When the user selects one port in this panel, all the VLANs containing this port are marked in the VLANs List panel.

Create VLAN – This panel should be used to operate with the VLANs, allowing its creation, alteration or removal. Below are described the necessary steps for each of these operations:

- **Creating a VLAN**:

  1. If you so wish, clear the VLAN ID and VLAN field values, by clicking the Clear button;

2. In case the Switch is in the VLAN Aware mode, insert the VLAN ID in the VLAN ID field. Any value from 1 to 4094 is accepted, as long as there isn't another VLAN with the same ID. For the Port Based VLAN mode, this field is not necessary;
3. Configure the ports belonging to the VLAN through the >> e << buttons;
4. Click the Create button to create the VLAN;

- **Editing a VLAN**:
  1. Select in the VLANs List panel the VLAN to be edited;
  2. Alter the VID field value, if so wished;
  3. Make the desired alterations in the ports belonging to the VLAN through the << e >> buttons.
  4. Click the Modify button to alter the VLAN.
- **Removing a VLAN**:
  1. In the VLANs List panel, select the VLAN to be removed;
  2. Click the Remove button.

3.7.4. WAN

The type WAN represents the eight tributary internal ports, connected to the Switch. In this screen are configured ports features as CoS and encapsulation protocol.

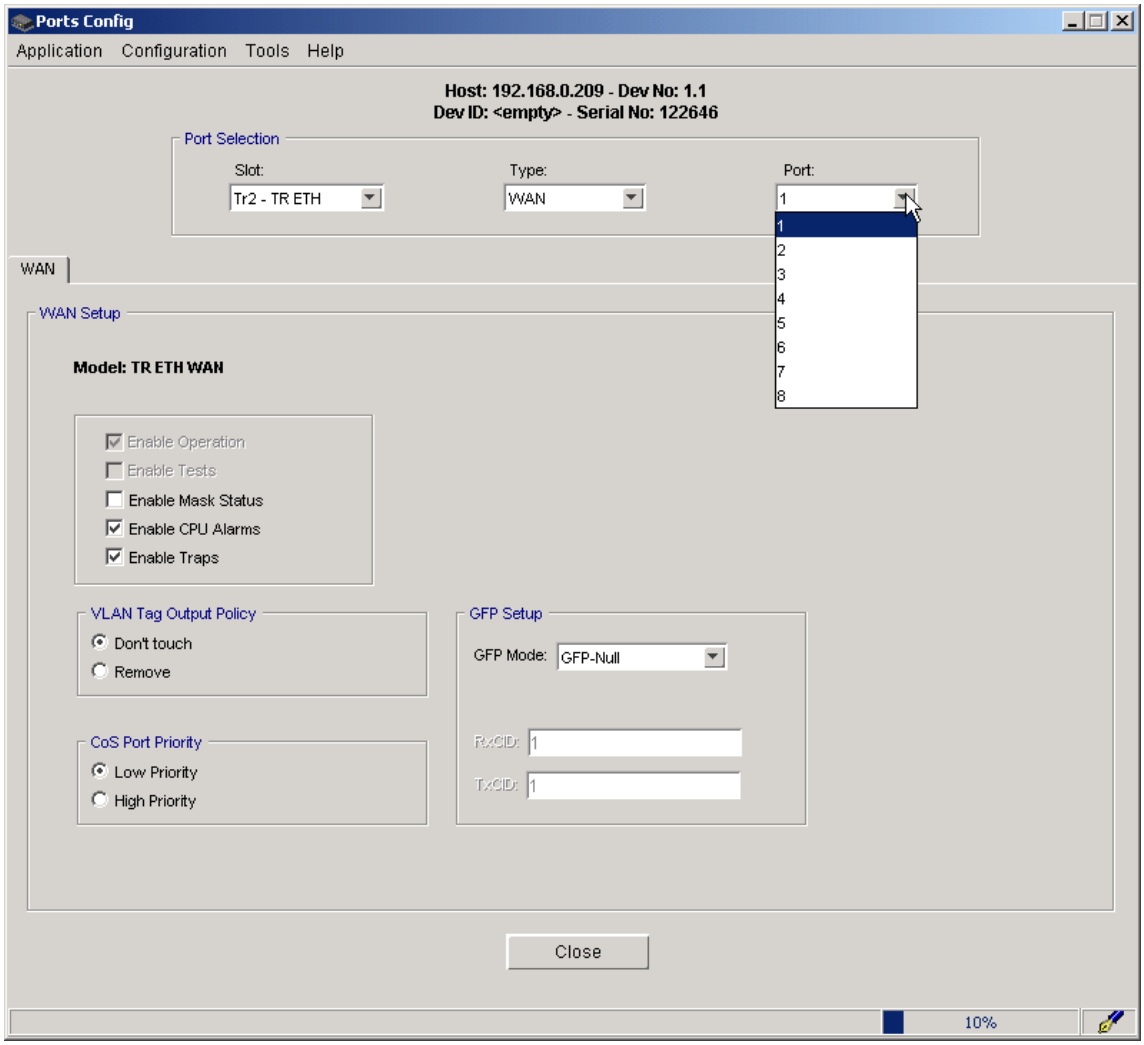


Figure 30 – WANs configuration screen

VLAN Tag Output Policy: In the same way as in the LANs, this configuration defines the outgoing policy of the packets relating to the VLAN tag.

CoS Port Priority – In this panel the WAN port priority is defined. See item Class of Service, in 3.7.2.

GFP – GFP protocol configuration, for Null or Linear mode operation. In the linear mode, Channel Ids are attributed in the encapsulated frames, allowing band sharing (see item 3.7.5). The TX and RX CIDs for each WAN port should be configured when the protocol is GFP-Linear. The same CID cannot exist in two different ports. In case any VCG receives GFP frames with CID different from the configured, the GFP-CID_Mismatch alarm is generated.

3.7.5. VCG

In this screen the Virtual Concatenation Groups (VCG) configuration is done. The screen is made of two borders, in the first the VCG configurations are done and in the second the SDH path parameters configurations.

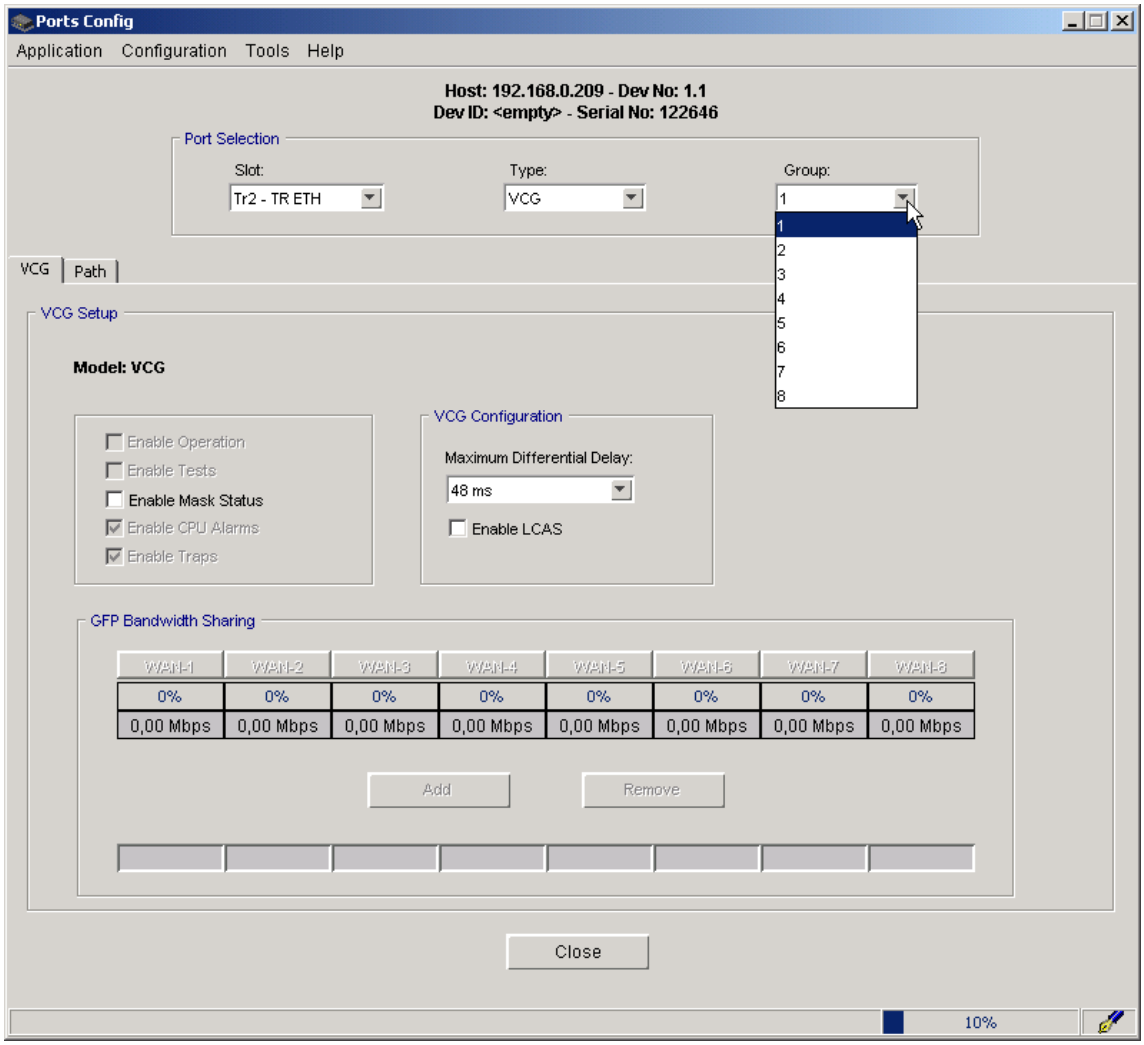


Figure 31 – VCGs configuration screen

This border contains the following configurations:

Enable Mask Status – Enables masking the interface status.

Enable Traps – Enables sending traps.

Maximum Differential Delay – Maximum differential delay configuration among the VCG members. The bigger this value is the bigger is the delay in the data transported by this VCG.

Enable LCAS - Enables LCAS protocol in the VCG.

GFP Bandwidth Sharing – When the WAN ports are operating with GFP protocol in the Linear mode, it is possible to share the band of a VGC among different WANs. In this panel the mapping of this sharing is done. When the band sharing is used, the VCG is composed by a set of up to 8 spaces that can be filled by the WAN ports, whose GFP protocol is configured in the Linear mode. To map, the WAN must be selected and the Add and Remove buttons should be used to add or remove WANs from the VCG composition. Below each WAN, is shown a bar containing the percentage of the band used by it as well as the band numerical value, considering the mapping

done for the selected VCG. It is important to note that it is not necessary that all 8 spaces composing the VCG are filled for the band to be completely used. Figure 31 shows an example where the WANs 1, 3 and 4 share the VCG-7 band.

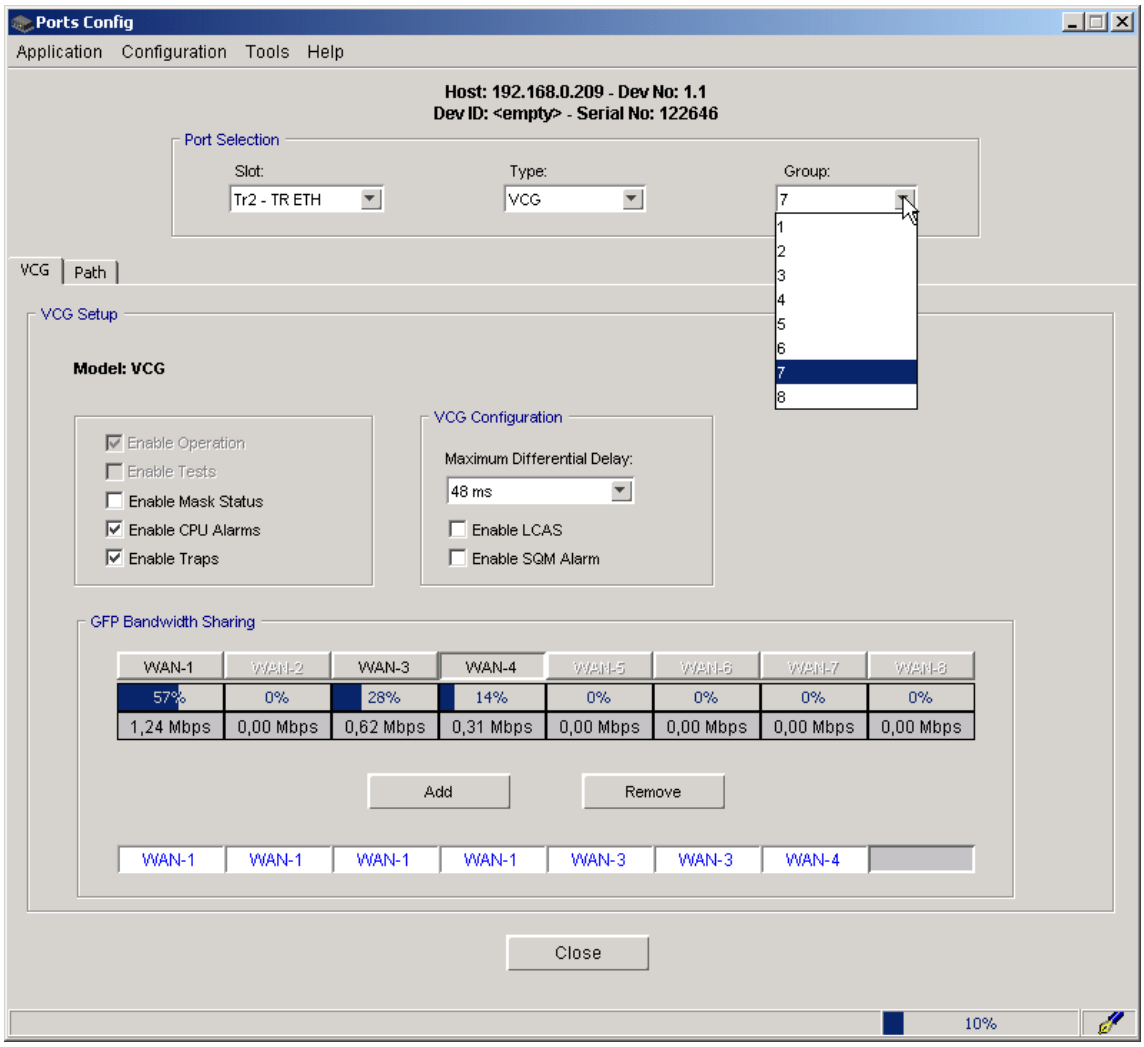


Figure 32 - GFP Bandwidth Sharing

3.7.6. Path configuration

In the Path borders are done the path configurations for all the VCs mapped for the selected VCG. This screen depends on the TUG-3 Structure configuration, done in the SDH Map. Figure 32 shows the configuration screen for VC-3 mapping and figure 33 shows the path configurations for VC-12 mapping.

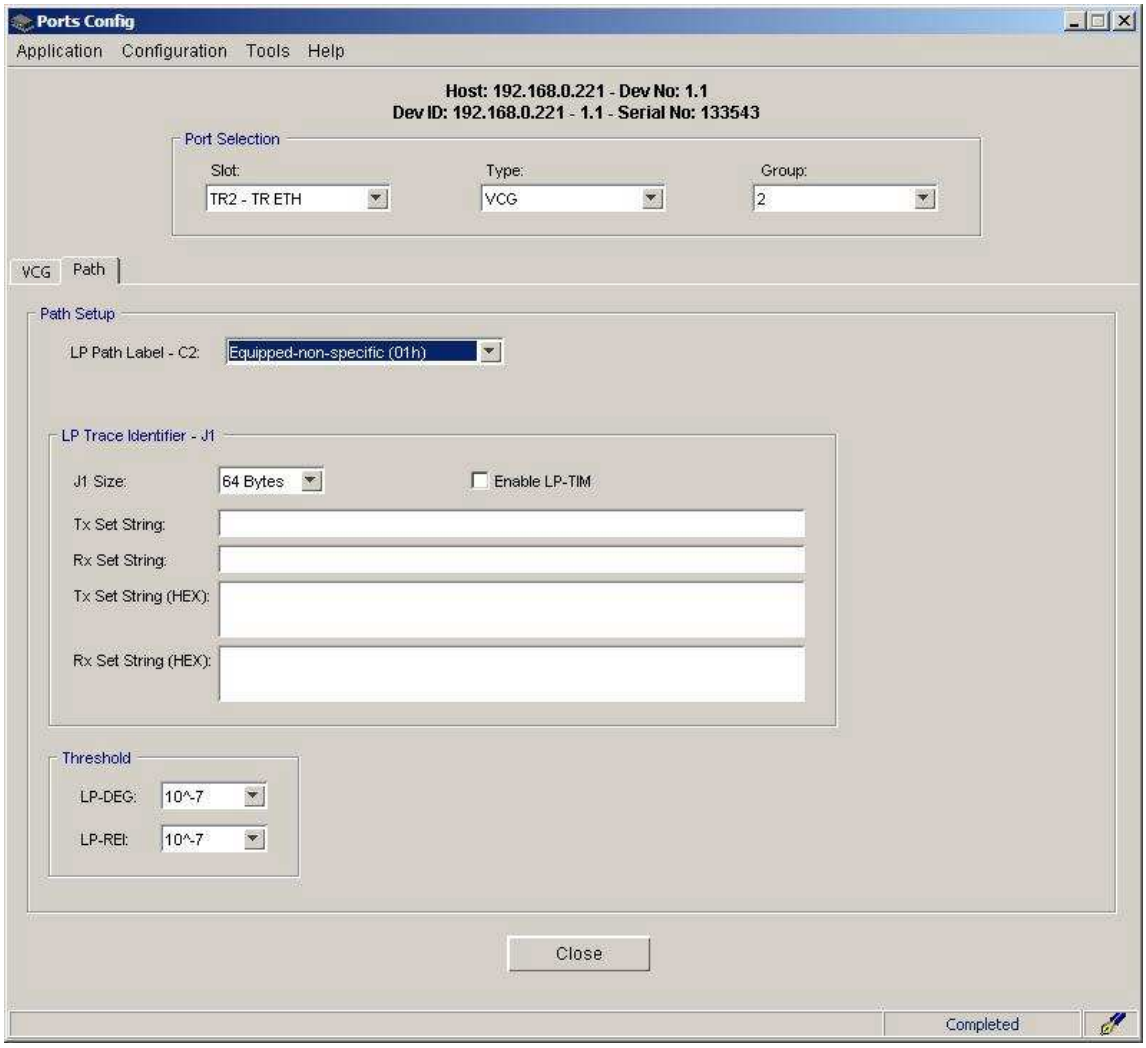


Figure 33 - VC-3 Path configurations

3.7.7. Payload identifier – LP Path Label C2

The Path Label values in the DmSTM-1 for the Ethernet mapping are:

Equipped-non-specific (01h) – Non specific.

GFP Mapping (1Bh) – GFP Mapping.

3.7.8. Path Identifier- LP Trace Identifier J1

Defines the size of the path name, a string of 16 or 64 characters.

Tx Set String - Defines the value of the transmitted J1 string.

Rx Set String - Defines the value of the expected J1 string.

Tx Set String (HEX) - Defines the value of the transmitted J1 string, in hexadecimal.

Rx Set String (HEX) - Defines the value of the expected J1 string in hexadecimal.

Enable HP-TIM - Enables HP-TIM alarm generation if the received Path Identifier is different of the expected value, as configured in Rx Set String.

Threshold (LP-DEG) – Configures the error rate for the LP-DEG alarm generation.

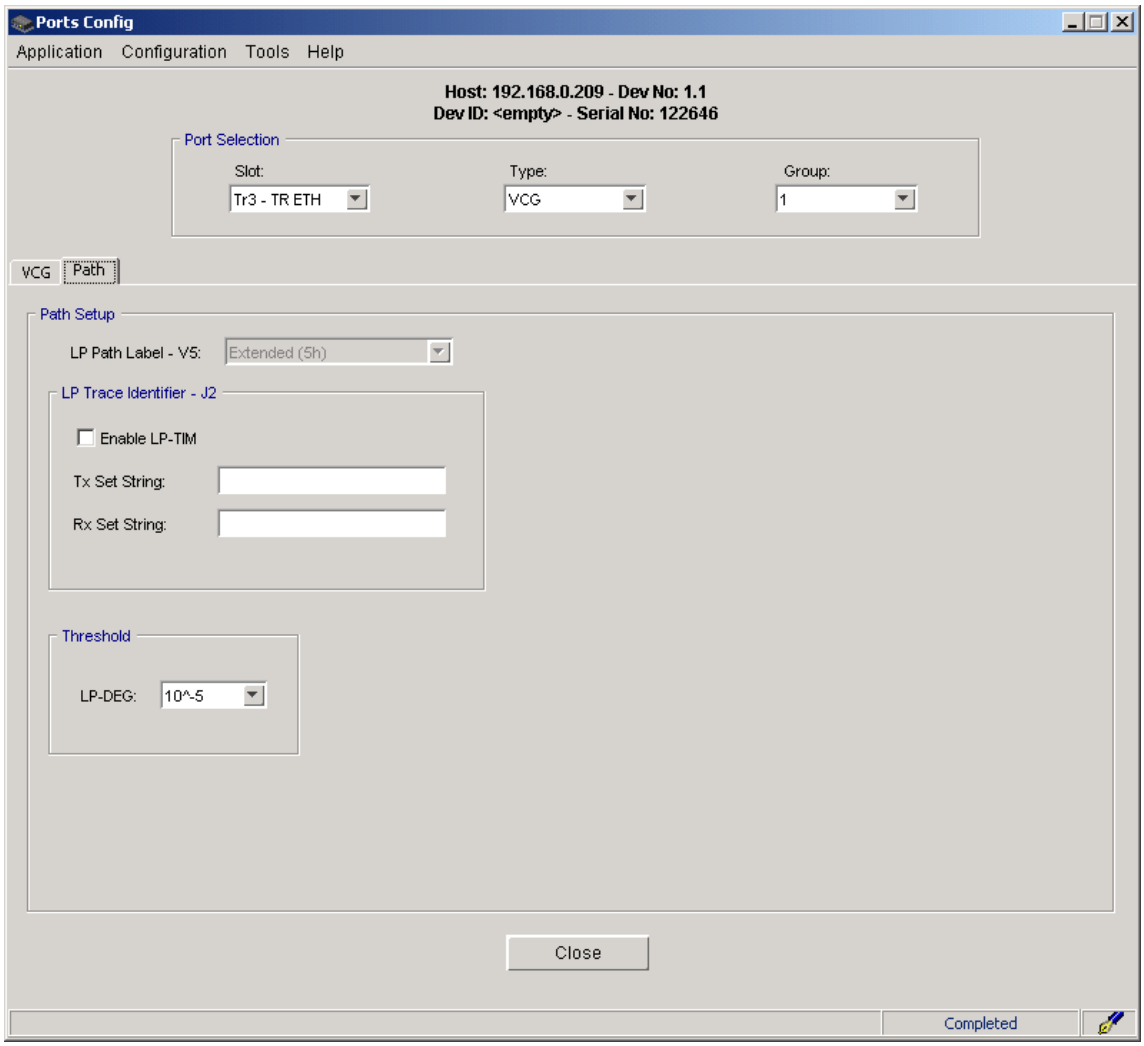


Figure 34 - VC-12 Path configuration

3.7.9. Payload Identifier– LP Path Label V5

The Path Label (V5) value for Ethernet mapping is Extended (5h).

3.7.10. Path Identifier - LP Trace Identifier J2

Enable LP-TIM - Enables LP-TIM alarm generation if the received Path Identifier is different of the expected value as configured in Rx Set String.

TX Set String - Defines the value of the transmitted J2 string.

Rx Set String - Defines the value of the expected J2 string.

Threshold (LP–DEG) – Configures the error rate for the LP-DEG alarm generation.

3.8. STM-1 (TR-STM1) Tributary Configuration

By selecting a slot with TR STM-1 card at the Configuration/Ports Config menu, the user has access to the STM1 ports configuration menu.

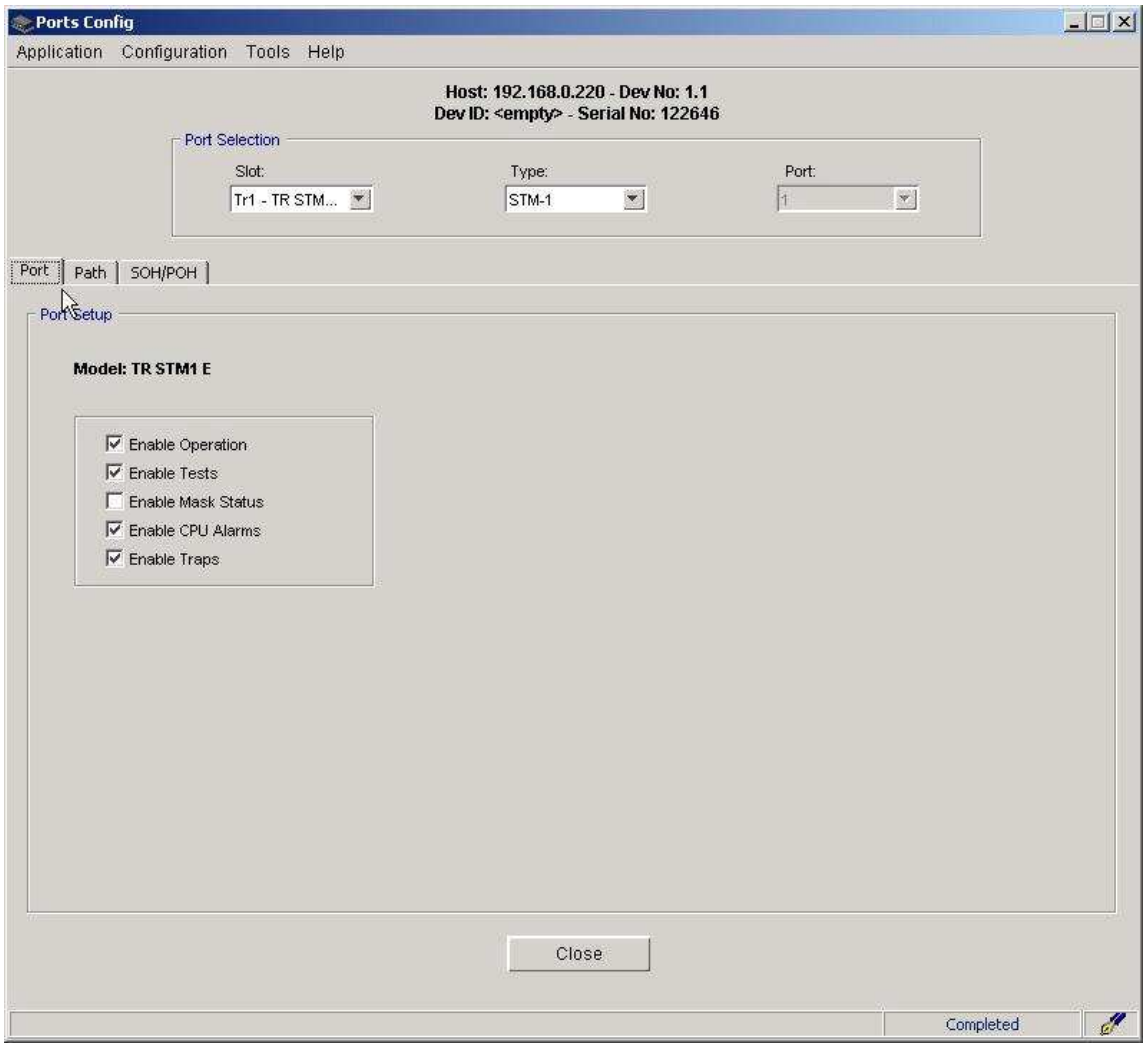


Figure 35 - STM-1 Tributary Ports setup screen

Enable Operation - Enables interface operation.

Enable Tests - Allows running diagnose interface tests.

Enable Mask Status - Enables interface status masking.

Enable CPU Alarms – Enables the propagation of the aggregate alarms to the CPU.

Enable Traps - Enables sending traps.

3.8.1. Path configurations

In the Path border is done the configuration of the path identifiers, alarm threshold and path label.

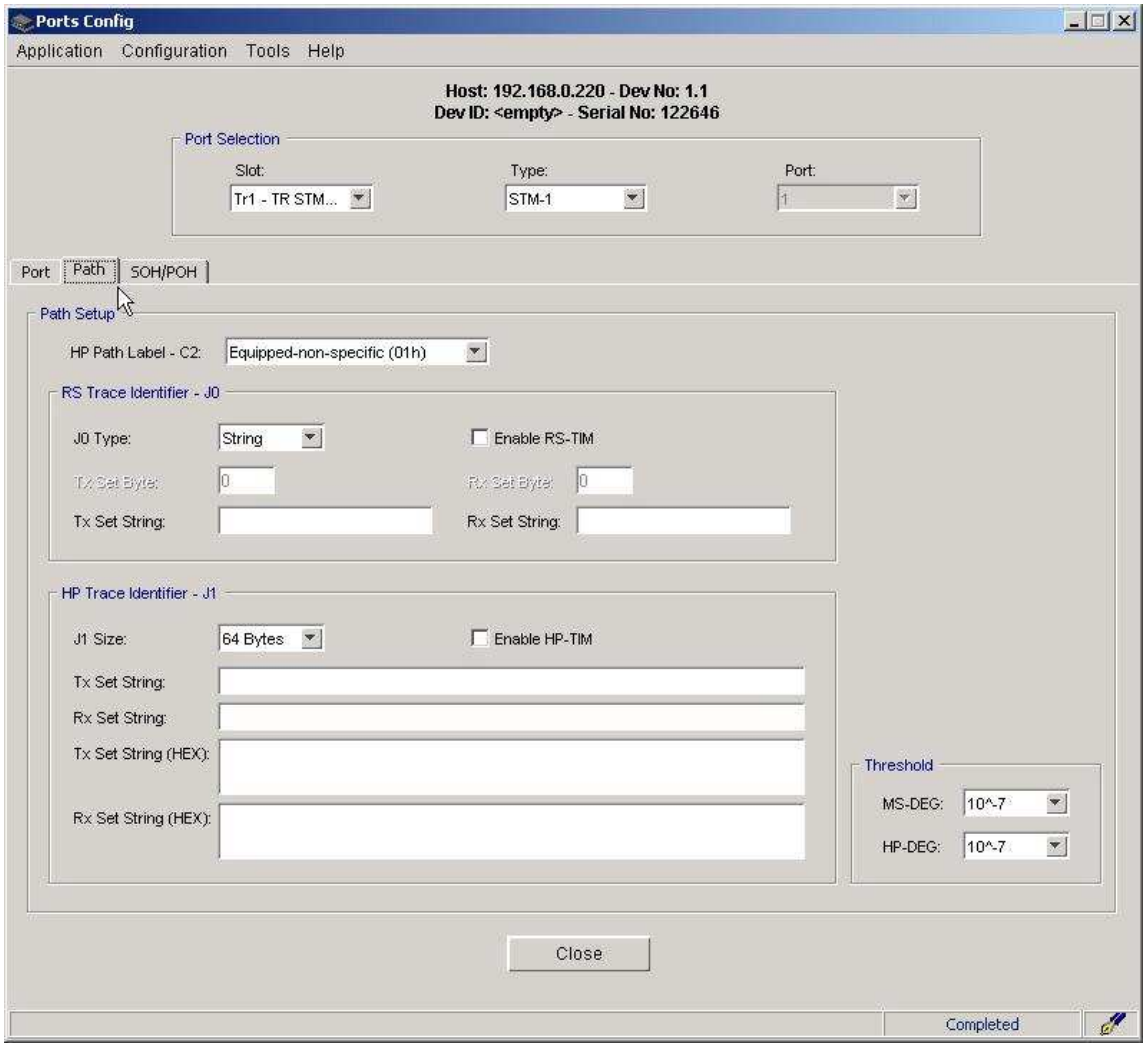


Figure 36 - STM-1 Tributary Path Config screen

3.8.2. Payload Identifier - Path Label C2

Allows configuring the VC-4 Payload Identifier. The HP Path Label – C2 configuration values are listed below.

Equipped-non-specific (01h) - Not specific.

TUG-structure (02h) - TUG Structure.

Mapping under development (05h) – mapping code undefined

3.8.3. Trace Identifier- Trace Identifier J0

Performs the Trace Identifier configuration for the regeneration section.

J0 Type - Defines the type of trace name used, byte or 16-character string.

Tx Set Byte - Defines the value of the J0 transmitted byte (when configured as byte).

Tx Set String - Defines the value of the J0 transmitted string (when configured as string).

Rx Set Byte - Defines the value of the J0 expected byte (when configured as byte).

Rx Set String - Defines the value of the J0 expected string (when configured as string)

Enable RS-TIM – Enables alarm generation RS-TIM if the received Trace Identifier is different of the expected value as configured in Rx Set String.

3.8.4. Path Identifier- Trace Identifier J1

J1 Size - Defines the size of the path name, a string of 16 or 64 characters.

Tx Set String - Defines the value of the transmitted J1 string.

Rx Set String - Defines the value of the expected J1 string.

Tx Set String (HEX) - Defines the value of the transmitted J1 string, in hexadecimal.

Rx Set String (HEX) - Defines the value of the expected J1 string in hexadecimal.

Enable HP-TIM - Enables HP-TIM alarm generation if the received Path Identifier J1 is different of the expected value, as configured in Rx Set String.

3.8.5. Thresholds - MS-DEG and HP-DEG

MS-DEG - Configures the error rate for MS-DEG alarm generation.

HP-DEG - Configures the error rate for HP-DEG alarm generation.

3.8.6. KLM Configuration

In the Type TU-3/12 it is possible to configure traps and propagation of alarms individually for each KLM of the STM-1 tributary.

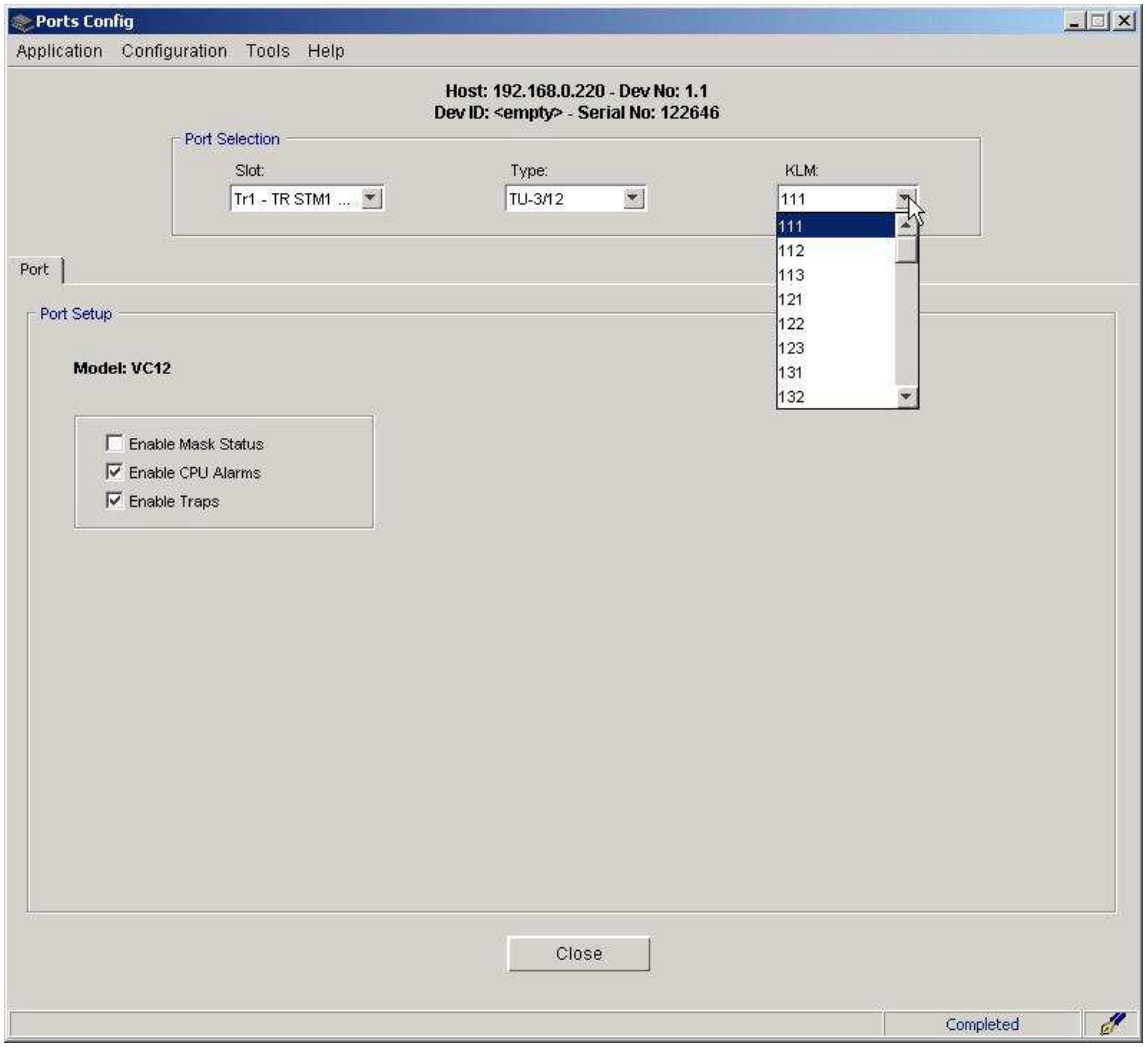


Figure 37 - STM-1 Type TU-3/12 Port setup screen

Enable Mask Status - Enables interface status masking.

Enable CPU Alarms – Enables the propagation of the tributary alarms to the CPU.

Enable Traps - Enables sending traps.

3.9. V.11 Interface configuration

The V.11 interface of the basic unit is configured through the Config/Ports/V11 menu in the equipment terminal, which can be accessed by Telnet or serial port. It is important to note that the v.11 interface requires mapping and port configuration. The interface can be mapped to the overhead bytes of the STM frame of one of the aggregate interface ports or to a router channel.

3.9.1. Port enabling (V11 / Operation)

The Operation menu allows enabling or disabling the interface V.11 port operation.

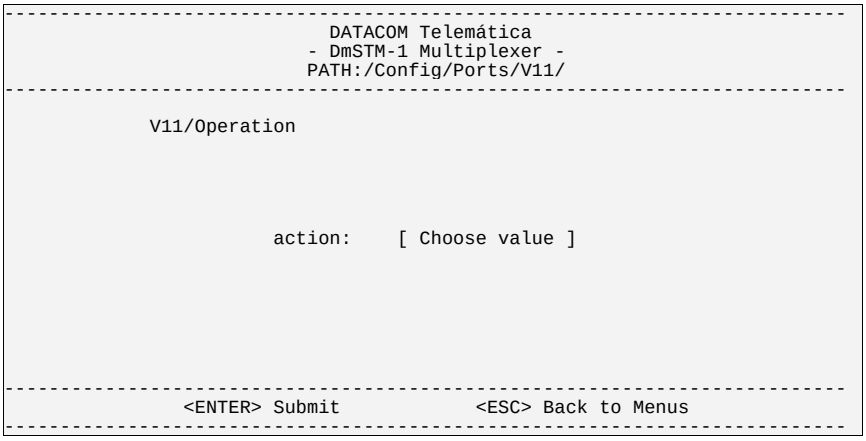


Figure 38 –V.11 Operation Configuration

The V.11 interface port enabling is done automatically by the mapping function.

Command: /Config/Ports/V11/Operation		
Object	Value	Description
Action	Enable	Enables the V.11 interface port operation.
	Disable	Disables the V.11 interface port operation

3.9.2. Tests Enabling (V11 / Enable_tests)

The Enable_tests menu inhibits or enables the possibility of test execution in the V.11 interfaces.

Command: /Config/Ports/V11/Enable_tests		
Object	Value	Description
Action	Enable	Enables tests in the V.11 interface.
	Disable	Disables tests in the V.11 interface.

3.9.3. Operation speed (V11 / Rate)

The Rate menu allows configuring the number of timeslots used in the V.11 interface, defining the operation speed. Figure 38 shows the speed configuration menu of the V.11 interface port.

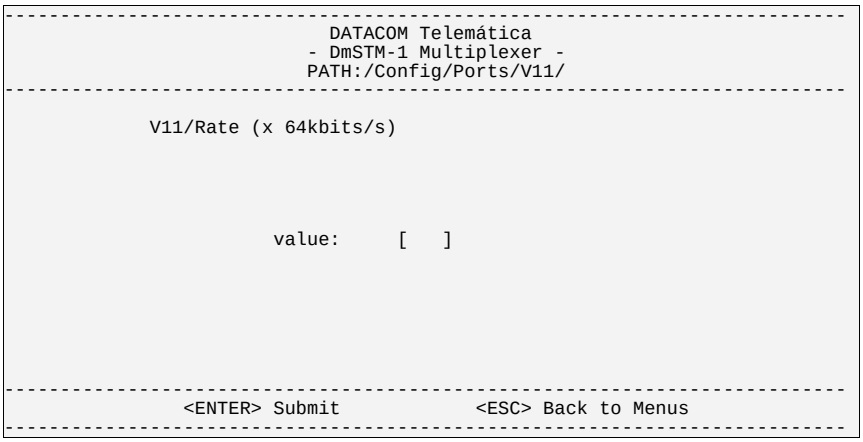


Figure 39 – V.11 Interface speed configuration

The interface speed is defined in multiples of 64Kbit/s, or Nx64kbit/s, where N is the number of timeslots from 1 to 20. Note that the number of configured timeslots should be the same configured in the mapping.

Command: /Config/Ports/V11/Rate		
Object	Value	Description
Value	1 – 32	Defines the number of timeslots allocated to the V.11 interface. The interface speed will be adjusted to Nx64kbit/s, where N is the number of timeslots form 1 to 32.

3.9.4. Reception Clock (V11 / Rx_clk_src)

The Rx_clk_src menu configures the origin of the V.11 interface reception clock.

Command: /Config/Ports/V11/Rx_clk_src		
Object	Value	Description
Rx_clk_src	CT113, CT115	Define V.11 interface reception clock origin.

3.9.5. Reception clock phase (V11 / Rx_clk_inv)

The Rx_clk_inv allows configuring the V.11 interface reception clock phase.

Command: /Config/Ports/V11/Rx_clk_inv		
Object	Value	Description
Action	Enable	Enables V.11 interface reception clock phase inversion.
	Disable	Disables V.11 interface reception clock phase inversion.

3.9.6. Transmission clock (V11 / Tx_clk)

The Tx_clk menu allows configuring the V.11 interface transmission clock. Together with the Tx_clk configuration, the E6 to E8 straps of the basic unit should be configured as described in the Equipment Manual.

Command: /Config/Ports/V11/Tx_clk		
Object	Value	Description
Tx_clk	CT113, CT114	Defines the V.11 interface transmission clock.

3.9.7. Transmission clock selection (V11 / Tx_clk_src)

The Tx_clk_src menu allows configuring which clock will be used as the V.11 interface transmission clock.

Command: /Config/Ports/V11/Tx_clk_src		
Object	Value	Description
Tx_clk_src	CT113, CT114, CT115	Defines the V.11 interface transmission clock origin.

3.9.8. Transmission clock phase (V11 / Tx_clk_inv)

The Tx_clk_inv menu allows configuring the V.11 interface transmission clock phase.

Command: /Config/Ports/V11/Tx_clk_inv		
Object	Value	Description
Action	Enable	Enables V.11 interface transmission clock phase inversion.
	Disable	Disables V.11 interface transmission clock phase inversion.

3.9.9. CTS/RTS (V11 / Cts_rts) Configuration

The Cts_rts menu configures the CTS/RTS signal of the V.11 interface. The use of the signals is exclusive, meaning that the user should choose to use either the CTS or the RTS. Together with the CTS/RTS configuration the E3 to E5 straps of the main unit should be configured, as described in the Equipment Manual.

Command: /Config/Ports/V11/Cts_rts		
Object	Value	Description
Cts_rts	CT105	Defines the use of CTS as control signal.
	CT106	Defines the use of RTS as control signal.

3.9.10. Mapping (V11 / Map)

Configures which type of mapping will be used for the V.11 interface. The interface can be mapped to overhead bytes of the STM or to a router channel.

Command: /Config/Ports/V11/Map		
Object	Value	Description
Map_to	Overhead	Defines that the V.11 interface mapping will be done to overhead bytes of the STM frame. The bytes mapping in the SOH/POH of the overhead should be done via terminal and not via DmView.
	Router_2	Defines that the V.11 interface mapping will be done to router channel number 2.

3.9.11. Visualization (V11 / View)

Allows visualizing the V.11 interface port configurations. The V11/View menu is shown in Figure 40.

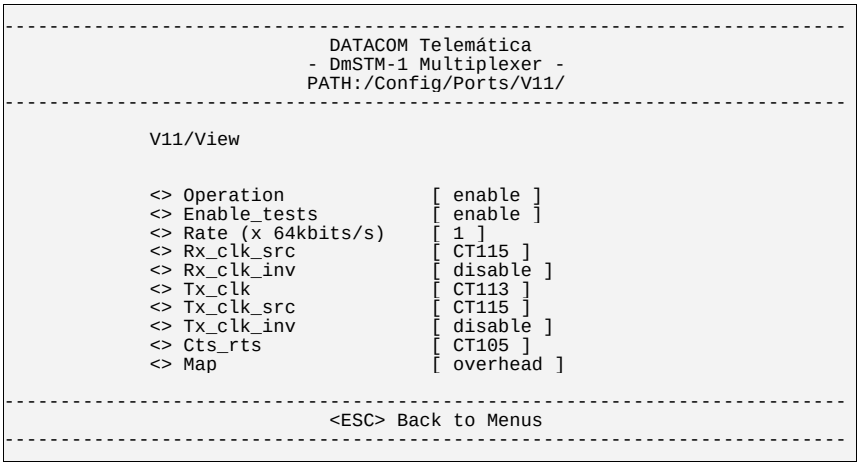


Figure 40 –V.11 interface configurations visualization

3.10. Mapping of the Tributaries

The Configuration/SDH_Map menu allows performing the mapping of the signals of the tributaries in the STM-1 payload containers. Before starting the mapping of the tributaries, the VC-4 structure should be defined.

3.10.1. VC-4 Structure

In the SDH Map Configuration Screen, select the VC-4-Structure option to open the corresponding configuration window.

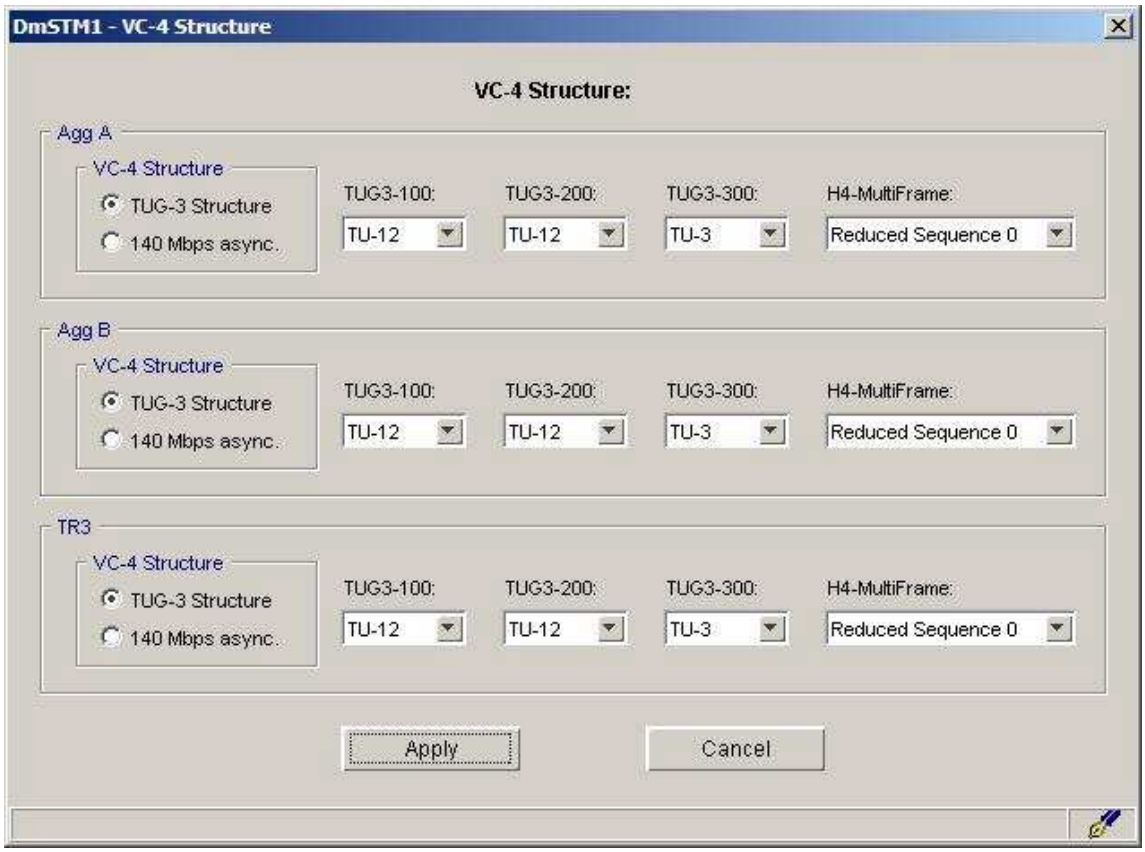


Figure 41 – VC-4 Structure Configuration Screen

TUG-3 Structure – TUG-3 Structure

140Mbps async. – Not structure

3.10.2. Mapping of the 2Mbit/s tributaries

The Configuration/SDH_Map menu allows performing the mappings of the signals of the tributaries for the STM-1 payload containers.

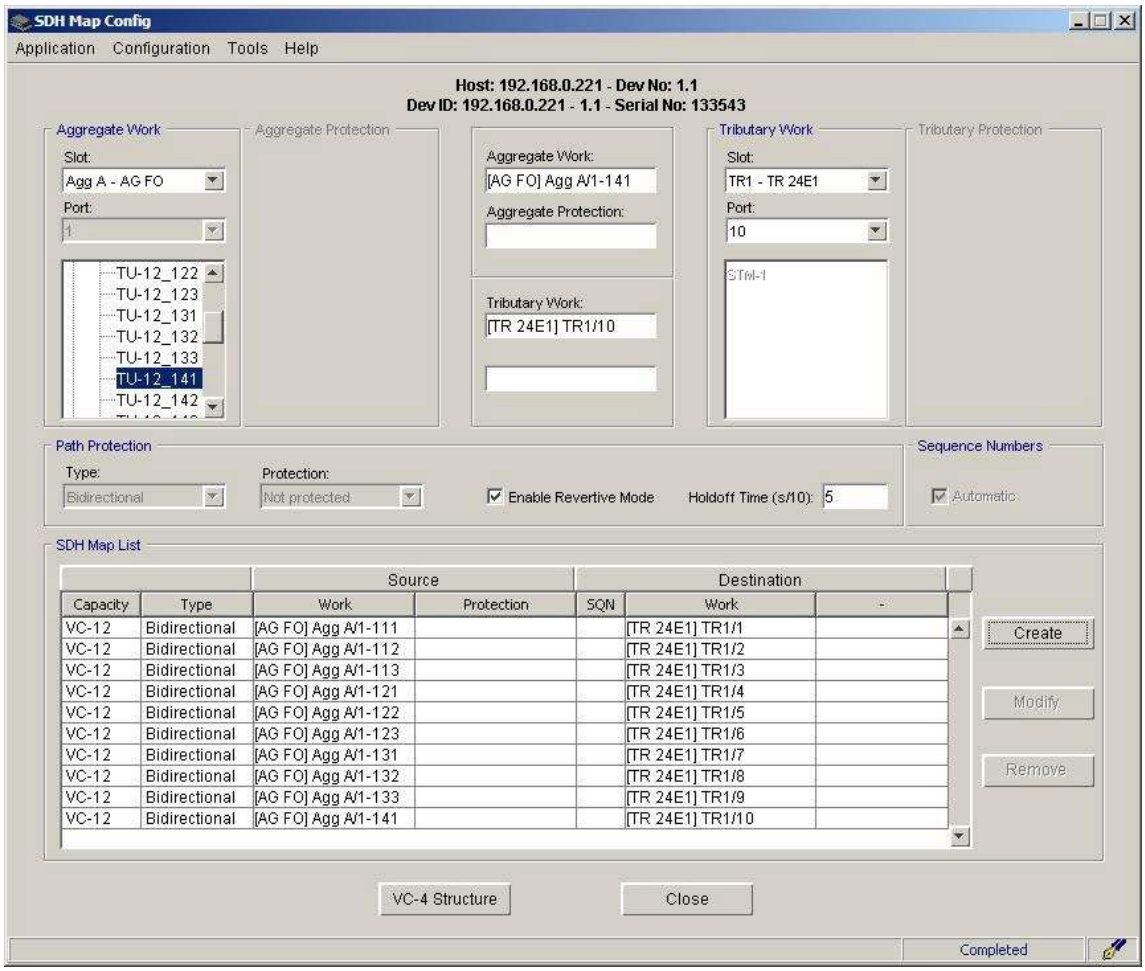


Figure 42 – SDH Map Configuration Menu

The mapping must be done after the VC-4 structure selection (see item 3.10.1). The process of mapping a tributary comprises the following steps:

1) Select the aggregate and timeslot (KLM) of the work path, in the Aggregate Work panel.
2) Select the tributary and port at the Tributary Work panel.
3) Configure the SNC protection in the Path Protection panel, when applicable.
4) Create the mapping using the Create button of the SDH Map List panel.

When the protection is enabled, the path will be protected by the same timeslot (KLM) of the work path in the aggregate which is opposite to the selected as work path. That is, if the work path is configured for aggregate A, the protection path will be mapped for aggregate B and vice-versa.

To change the mapping, select it in the SDH Map List panel. After changing all that is needed at the Aggregate Work, Tributary Work and Path Protection panels, use the Modify button of the SDH Map List to make changes effective.

To remove the mapping, use the Remove button of the SDH Map List panel.

The Aggregate Work panel offers the following options.

Slot - Selects an aggregate port for which the mapping will be performed.

Port – For the aggregate, the parameter value is 1.

STM1 - Allows selecting the VC-3/VC-12 timeslot (KLM) or VC-4 for which the mapping will be performed.

The Tributary Work panel offers the following options.

Slot - Selects the tributary card slot that will be mapped.

Port - Selects the tributary port that will be mapped.

The Path Protection panel provides the following options.

Type - The default protection type is bi-directional.

Protection - Enables/disables creation of the protection path.

Enable Revertive Mode - Enables reversible mode.

Hold off Time - Defines the link failure period until switching occurs.

Sequence Numbers – Only for virtual concatenated mappings. Enables the automatic numbering of the VC sequence numbers.

3.10.3. Ethernet Tributaries Mapping

The Ethernet tributaries mapping is different from the others because it is possible to map an Ethernet port to many VCs using virtual concatenation (VCX). Up to eight VCGs can be created for each Ethernet tributary card, corresponding to the Ethernet ports of the DmSTM-1 TR-ETH card. The maximum number of VCs for each virtual concatenation group or Ethernet tributary card is 63xVC-12 and 3xVC-3.

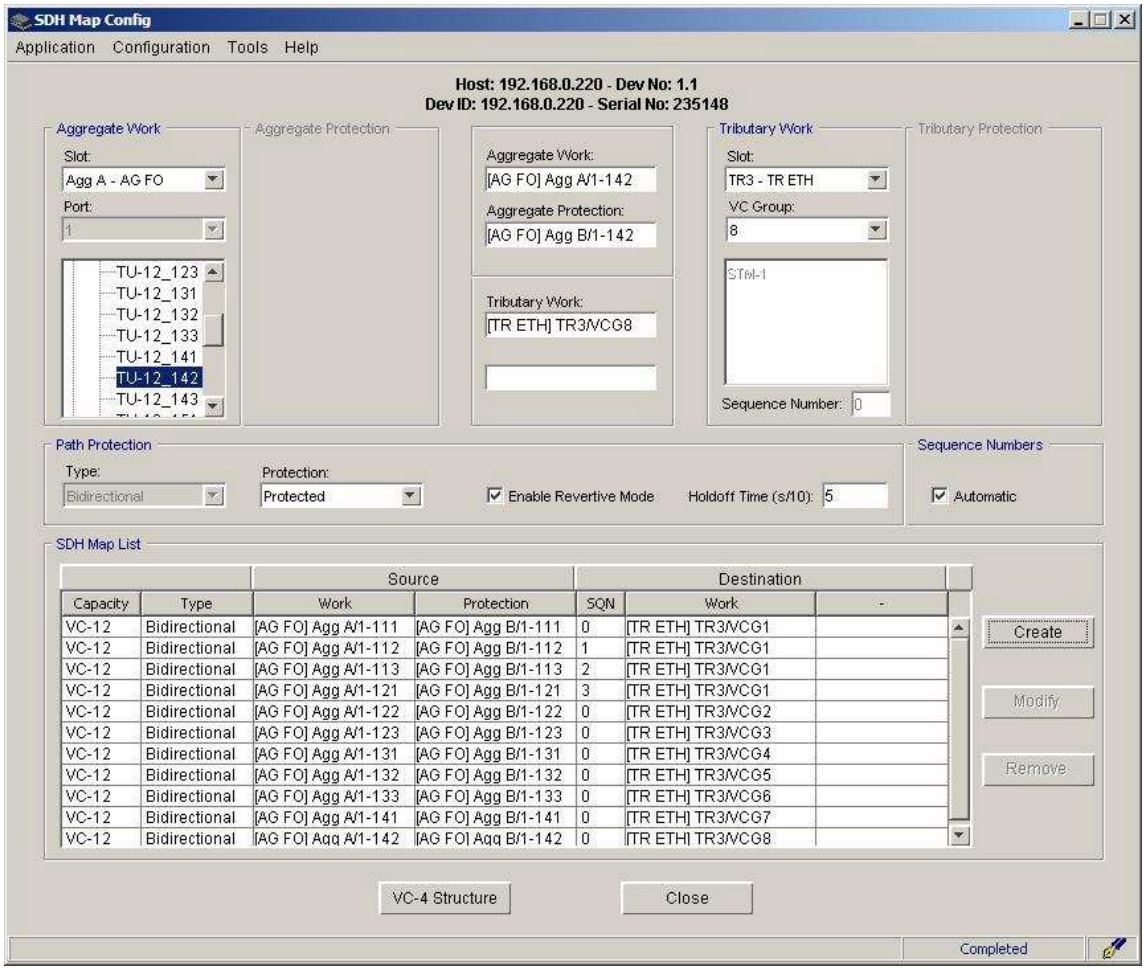


Figure 43 – SDH Map Configuration Menu– Ethernet Tributaries

The mapping of Ethernet tributaries follows the same mapping procedure for the tributaries, but for the virtual concatenation group (VCG) to which the mapping belongs. The VCG is configured in the Tributary Work panel, VC Group option.

The Sequence Number of the VCs that belong to a VCG can be manually configured, if the Automatic option of the Sequence Numbers panel is disabled.

Example: to create the Ethernet mapping with a 6Mbit/s bandwidth, the user must perform the individual mapping of three VC-12, selecting the same VCG for all mappings.

3.10.4. 34/45Mbit/s Tributary mapping

The mapping should be done after the selection of a TU-3 in the TUG-3 structure. The remaining of the E3 tributary mapping process is similar to the mapping of a 2Mbps tributary (see item 3.10.2).

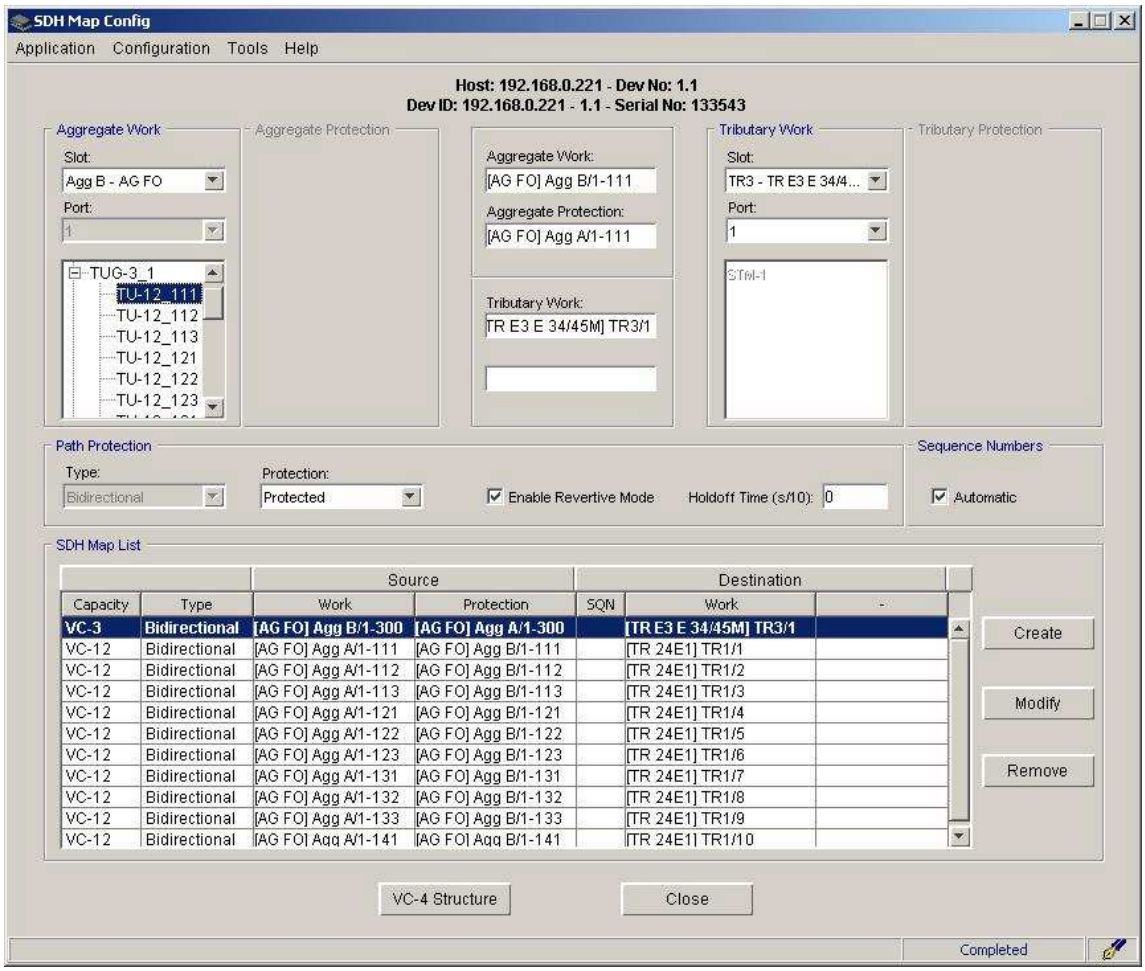


Figure 44 - SDH Map configuration menu – 34/45Mbit/s tributary

3.10.5. STM-1Tributary mapping

The STM-1 tributaries mapping follows the same steps as for the 2Mbps tributaries mapping (see item 3.10.2). The STM-1 tributaries KLM's can be mapped to any position in the STM-1 aggregate payload (VC-3/VC-12).

To pass-throug of VC-4, select "*140 Mbps async.*" option at the VC-4 Structure Configuration Menu (see item 3.10.1)

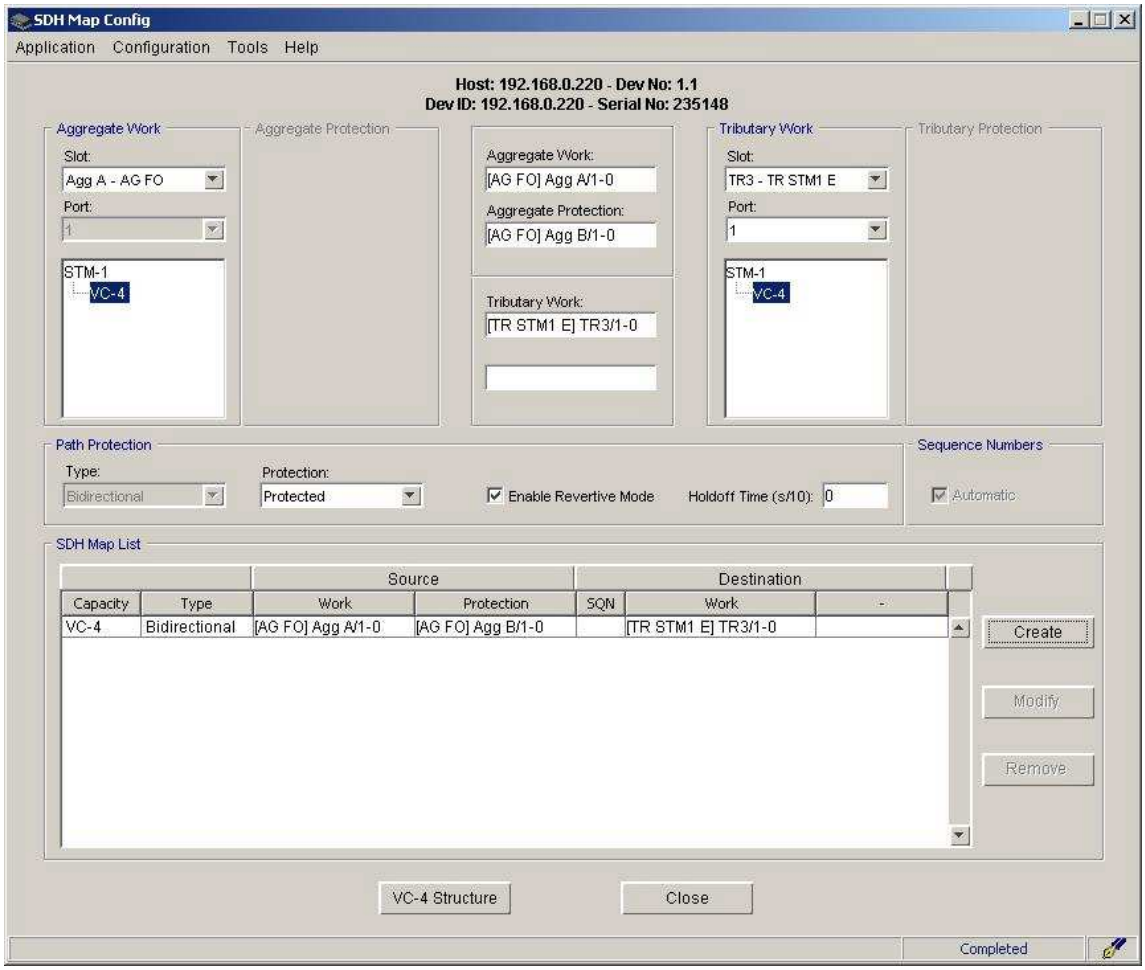


Figure 45 - SDH Map configuration menu– Tributary STM-1

3.11. Synchronism

At the Configuration/Device Config/Sync Source Config menu it is possible to define the system synchronism references and the switching criteria for the sync reference. The equipment synchronism is independent of the protection scheme employed or of the network topology used.

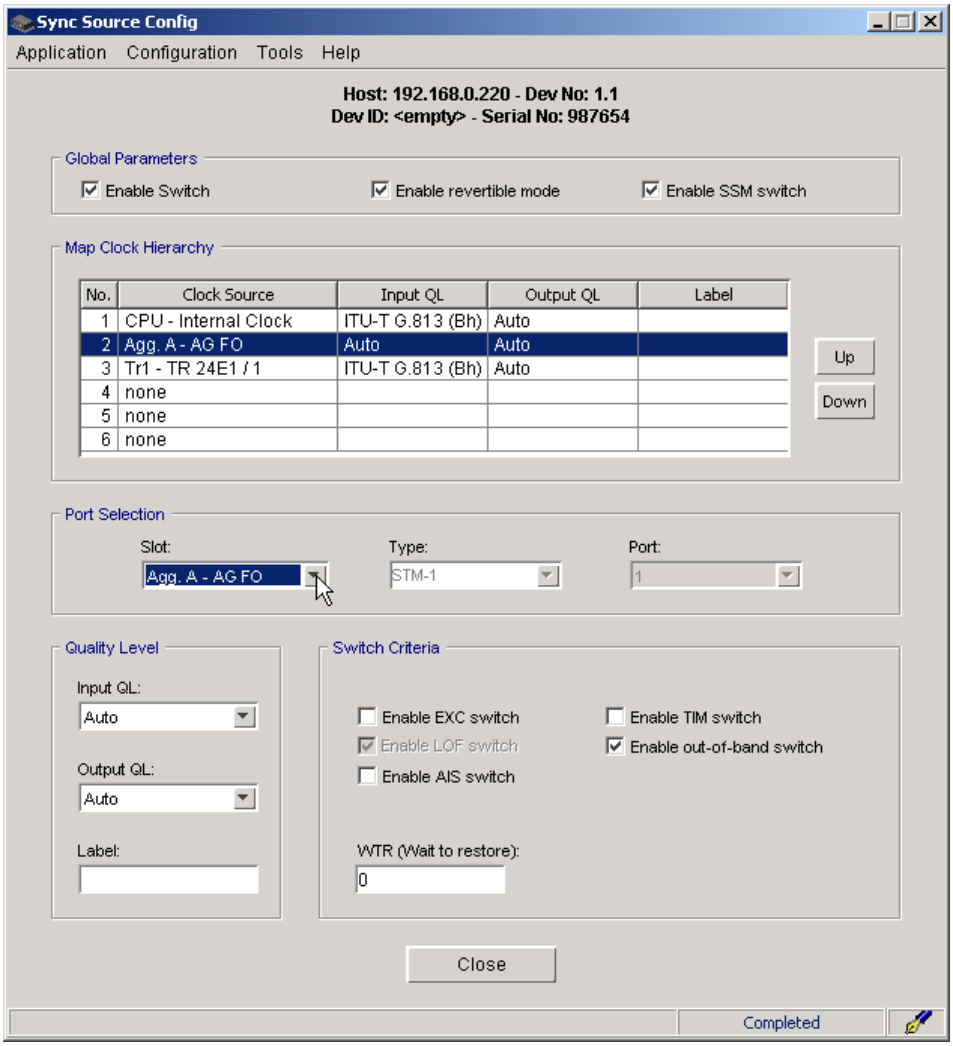


Figure 46 – Synchronism Configuration Screen

Enable Switch – Enables switching the synchronism reference.

Enable Revertible Mode – Enables revertible mode.

Enable SSM switch – Enables the switching by synchronism source quality.

Map Clock Hierarchy – Shows the table with the synchronism configured references.

Port Selection - Allows selecting the slot, type of slot and port for configuring the associated synchronism source.

Quality Level – Defines the quality of the input and output of the selected synchronism reference.

Switch Criteria – Allows enabling the synchronism switching reference when the EXC, LOF, AIS, TIM or out of band alarms are detected.

WTR (Wait to restore) – Time that the equipment will wait to go back to the highest hierarchy or quality sync source, after going back to the failure state.

3.12. Performance Monitoring (DmView)

The configuration and qualification of Performance Monitoring may be done using the menu Configuration/Device Config/Performance Config, from DmView as the following structure.

Structure from Menu Configuration/Device Config/Performance Config

Configuration - Access the Performance Config module

Performance Config – Enables the access to the Configuration module

- Global - Enables performance monitoring

- STM - Configures the PMP´s from STM hierarchy

- HP - Configures the PMP´s from HP hierarchy

- LP - Configures the PMP´s from LP hierarchy

- PPI - Configures the PMP´s from PPI hierarchy

Closing Time (24h) - Configures the 24 hours period of closing schedule.

3.12.1. Introduction

Performance Monitoring is a continuous collection process and data analysis in a series of Performance Monitoring Points (PMPs, Performance Monitoring Points) distributed during the transmission pathway. Informations about performance are collected and stay available to offered service quality. These informations assist in the detention of problems in the net.

3.12.2. Performance Monitoring Periods

The informations from monitoring performance are collected in determined periods: to each 15 minutes and/or to each 24 hours. For 15 minutes periods, the performance registers are generated in fixed times, to each quarter of hour. In 24 hours periods, the performance registers are generated daily according to the schedule specified by the operator. Any period can be finished prematurely by the operator. In this case, a new period immediately begins, and it will be finished in the schedule where the original period should be finished, respecting the keeping time of 7 minutes and 30 seconds between two consecutive closings.

3.12.3. Storing Registers

To each PMP, keep storing the last 32 registers of 15 minutes and the last 8 registers of 24 hours. If these limits are exceeded while occuring the generation of new registers, these oldest registers automatically are excluded to allocate new registers. Very old registers also are automatically excluded: registers of 15 minutes are stored for up to 24 hours, and 24-hour registers are stored for up to 240 hours (10 days), counted from the moment of the generation of the register. All the registers are kept in volatile memory, being lost if the equipment turn off or will be restarted. To prevent lost of information, it is recommended that the performance information are collected periodically by the applicatory of management.

3.12.4. Types of PMPs

In DmSTM-1 exists 3 differents types of PMPs, following described.

3.12.4.1. Type OOF

Store information about Out-Of-Frame (OOF) indications, detected by the equipment.

3.12.4.2. Type PJE

Store information about justifications pointers (PJE, Pointer Justification Events) realized or detected by the equipment.

3.12.4.3. Type BIP

Store information about errors detected by local equipment or informed by remote equipment. The main forms of detention these errors are parity (BIP, Bit Interleaved Parity) and alarms. For this type of period, are stored the following countings:

Errored Seconds (ES): seconds that occurred at least one anomaly or defect.

Severely Errored Seconds (SES): seconds which occurred an extreme number of anomaly or at least defect. A SES is also, for definition, an ES. The limit for amount of errors that separates a SES from an ES is defined at Annex C from norm G.826 ITU-T, as 30% of the total of covered blocks in a second by PMP.

Background Errored Block (BBE): blocks that contain anomalies and they are not part of a SES.

Unavailable Seconds (UAS): seconds that belong to the unavailability period (UAT, Unavailable Time). An UAT begins with ten consecutive SES and it finishes with ten seconds consecutive non-SES. During an UAT, the occurrences of ES, SES e BBE are not registered.

For all the types of PMP, are also stored with a number of seconds that each register it relates (AS, Assessed Seconds).

3.12.5. Performance Monitoring Points

In DmSTM-1 are defined the following performance monitoring points:

Hierarchy	PMP	TIPO	Defects	Description
RS	RS-OOF	OOF	-	Out-Of-Frame Indication
RS	RS-NE	BIP	RS-LOS RS-LOF	RS Near-End Error
MS	MS-NE	BIP	RS-LOS RS-LOF MS-AIS MS-EXC	MS Near-End Errors
MS	MS-FE	BIP	-	MS Far-End Errors
HP	HP-NE	BIP	AU-LOP AU-AIS HP-LOM HP-PLM HP-UNEQ HP-TIM	HP Near-End Errors
HP	HP-FE	BIP	HP-RDI	HP Far-End Errors
HP	PJE-NE	PJE	-	Justification in the transmission
HP	PJE-FE	PJE	-	Justification in the reception
LP	LP-NE	BIP	TU-LOP TU-AIS LP-UNEQ LP-TIM	LP Near-End Errors
LP	LP-FE	BIP	HP-RDI LP-RDI	LP Far-End Errors
PPI	PPI	BIP	PPI-LOS PPI-AIS	Errors in the lines of tributaries.

3.12.5.1. Performance Monitoring Configuration

In menu Configuration/Device Config/Performance Config is possible to define the performance monitoring points during the pathway.

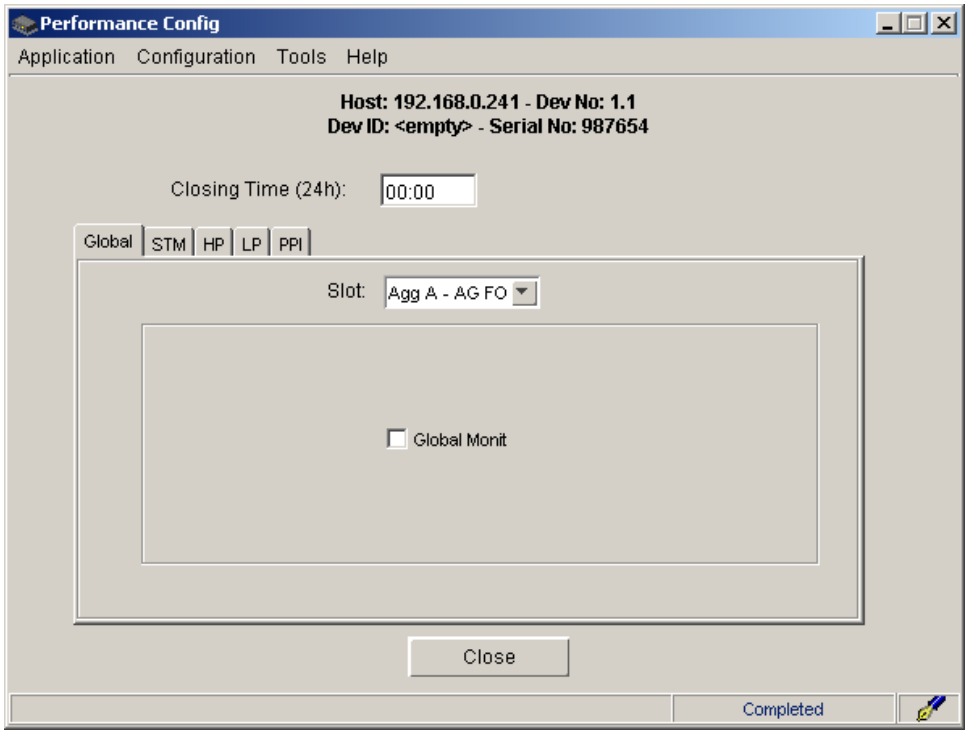


Figure 46 – Monitoring Configuration Screen

The menu Configuration/Device Config/Performance Config/Global allows the qualification performance monitoring in the equipment as a whole or to each slot individually, using separate configurations to the periods of 15 minutes and 24 hours.

Object	Value	Description
Slot	A, B, T1, T2, T3	Defines which slot would like to enable the performance monitoring. The CPU slot represents the equipment as a whole.

Obs: It is necessary to enable the performance monitoring in the equipment and slot simultaneously to make the qualification of PMPs specific performance monitoring has effect.

The menu Configuration/Device Config/Performance Config/STM allows the qualification performance monitoring in PMPs from STM hierarchy (RS and MS), with separate configurations to the periods of 15 minutes and 24 hours. The following figure illustrates this menu:

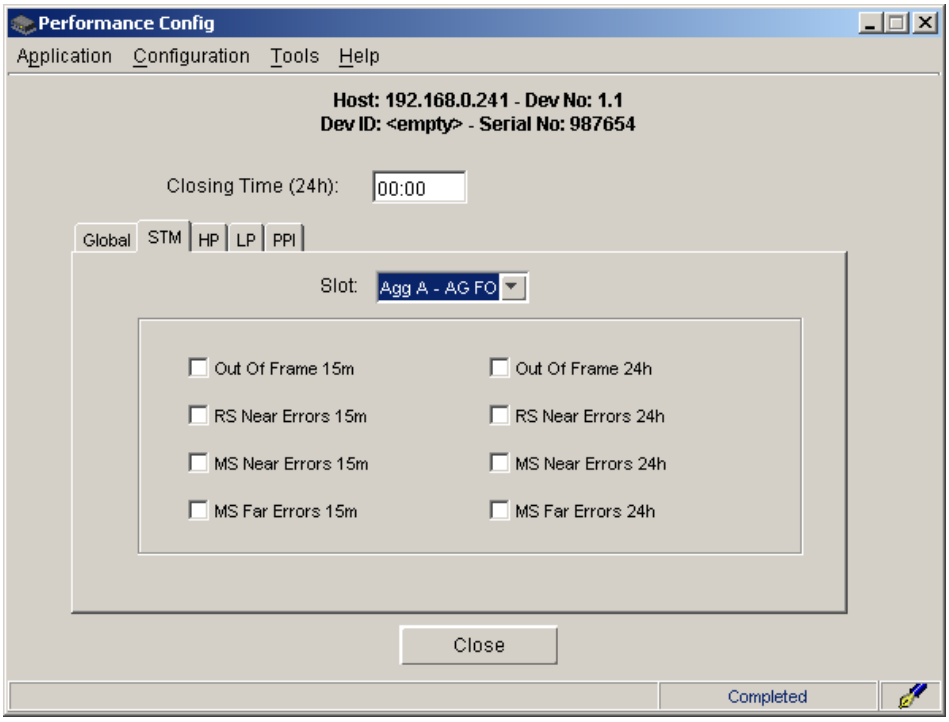


Figure 47 – STM Performance Configuration

The following objects described are observed in the qualification screen from PMP RS-OOF. The objects for others PMPs and respective periods are analogous.

Object	Value	Description
Slot	Agg.A, Agg.B	Defines which aggregate enables the performance monitoring

The menu Configuration/Device Config/Performance Config/HP allows the qualification performance monitoring in PMPs from HP hierarchy, with separate configurations to the periods of 15 minutes and 24 hours. The following figure illustrates this menu:

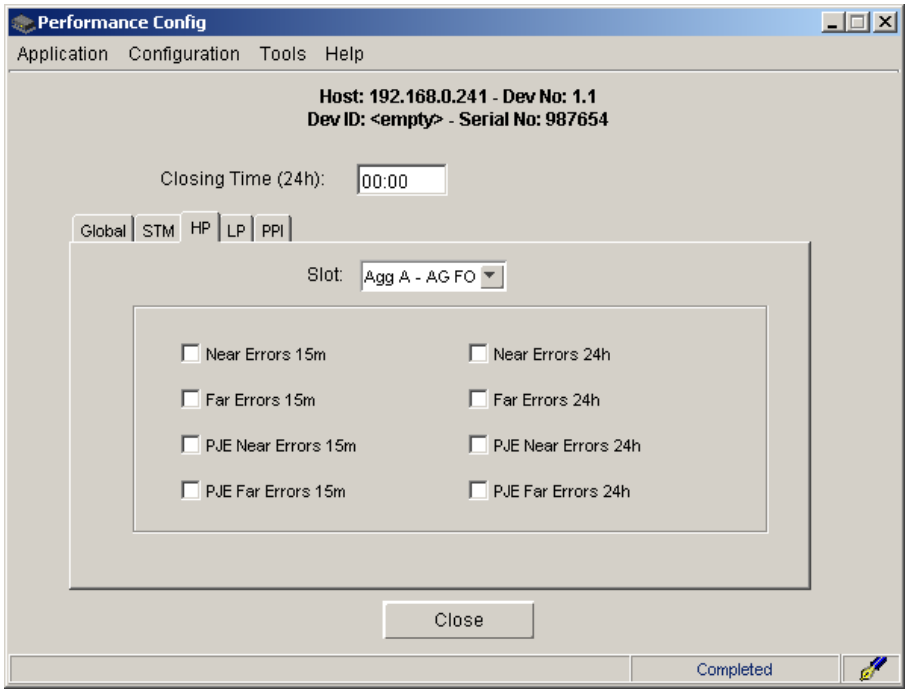


Figure 48 – HP Performance Configuration

The menu Configuration/Device Config/Performance Config/LP allows the qualification performance monitoring in PMPs from LP hierarchy, with separate configurations to the periods of 15 minutes and 24 hours. The following figure illustrates this menu:

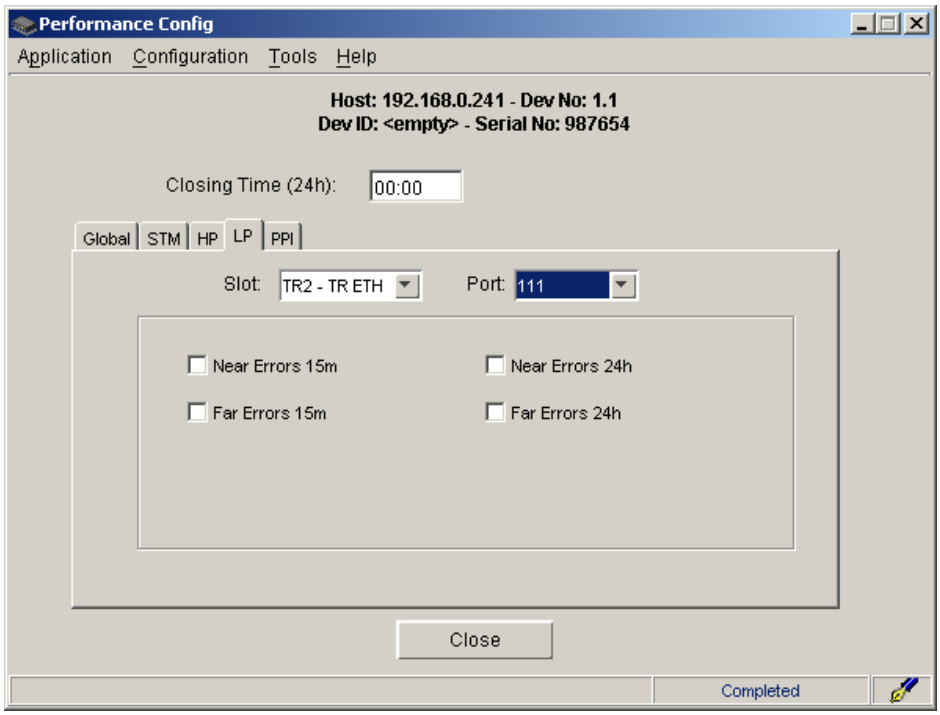


Figure 49 – LP Performance Configuration

The objects presents in LP configuration have the following meanings:

Object	Value	Description
Slot	T1, T2, T3	Defines which slot it desires to qualify the performance monitoring.
KLM	111-333	Indicates which VC-12 it desires to qualify the performance monitoring.

It is necessary to exists a configured mapping in VC-12 specified to makes qualification of the performance monitoring has effect. If the mapping will be removed, the registers stored until the moment will be excluded automatically.

The menu Configuration/Device Config/Performance Config/PPI allows the qualification performance monitoring in PMPs from PPI hierarchy, with separate configurations to the periods of 15 minutes and 24 hours. The following figure illustrates this menu:

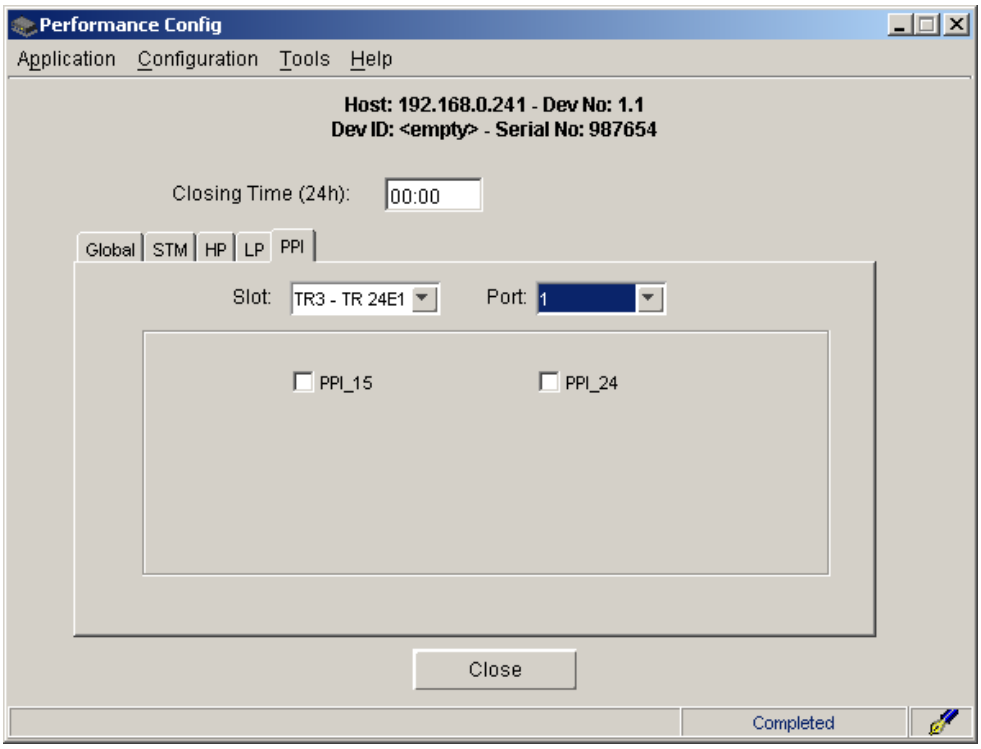


Figure 50 – PPI Performance Configuration

The objects for configuring sub_menus from PPI menu have the following meanings:

Object	Value	Description
Slot	T1,T2,T3	Defines which slot it desires to qualify the performance monitoring.
Port	1-24	Indicates which tributary it desires to qualify the performance monitoring.

It is necessary to exist a configured mapping in VC-12 specified so that the qualification of the performance monitoring has effect. If the mapping will be removed, the registers stored until the moment will be excluded automatically.

The menu Configuration/Device Config/Performance Config/Closing Time 24h allows the qualification the time of closing the “Closing Time 24h”, with separate configurations to the periods of 15 minutes and 24 hours. The following figure illustrates this menu:

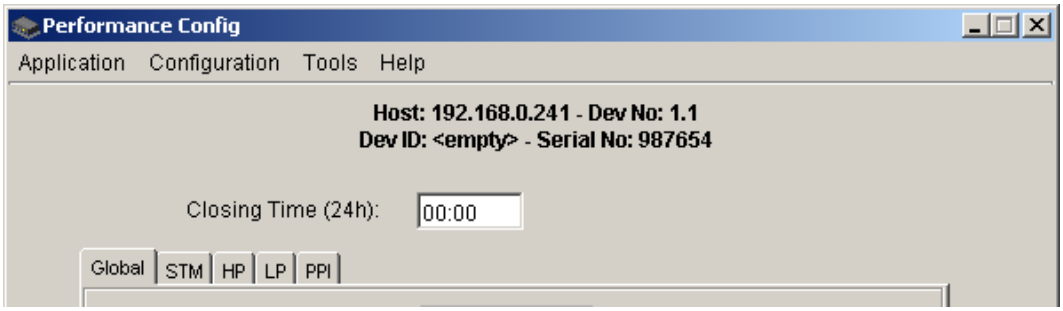


Figure 51 – "Closing Time 24h" Configuration

3.13. Generation of Performance Monitoring Report

Using DmView is possible to build reports where it has the control of performance monitoring. So that it is possible the visualization and confection of these reports, first some described parameters in the table below must be verified.

NMS JMS Service - It must be initiated

NMS Apache Tomcat Service - It must be initiated

NMS Probe Service - It must be initiated

To verify if these parameters are initiated, go to the folder Services that if it inside locates of administrative Control Panel/Administrate Tools. If the same ones will be stopped, select and go to the option "Start" that will appear in the top of the screen.

For more information about it, consults the DmView manual that is installed with the software.

The reports generation will be created in agreement to the equipment date, therefore verifies the date so that it has a standard in the creation of the reports.

It is good for remembering that all the corresponding parameters to performance monitoring are in accordance with the values stipulated in the option "*Threshold Alarms Config"* and so the report will go to be based on these values. To verify or to modify these values it, follow the pathway Configuration/Device Config/Threshold Alarms Config through the DmView.

After established the parameters to be monitored in agreement it explains item 3.12, go to Network Manager/Tools/Reports/Web, however, to login itself it is necessary to use a password already registered in cadastre.

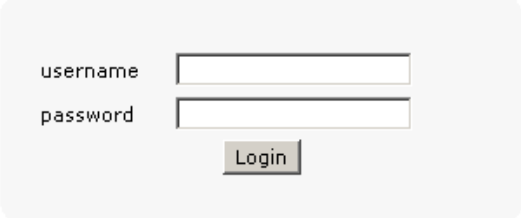


Figure 52 – Login Report Web

The initial screen will appear, as it shows the figure below, the creation of reports SDH is concentrated in the two selected options.

SDH Performance Chart - Creation of graphical reports

SDH Performance Report - Creation of described reports for tables

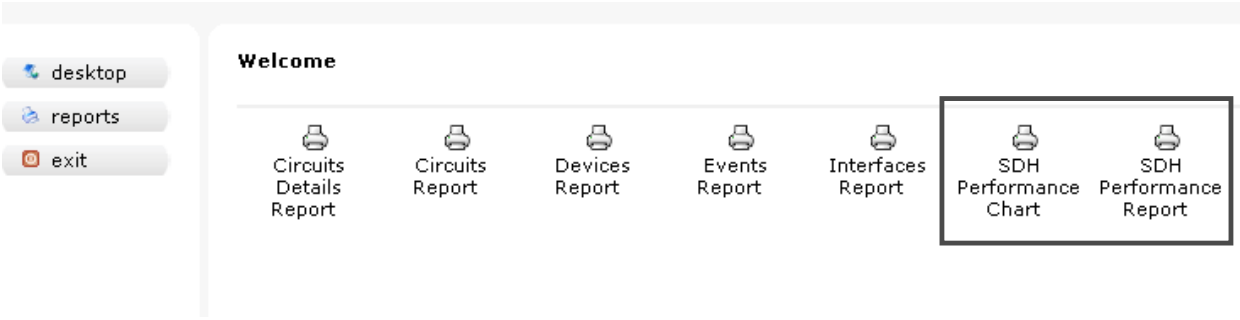


Figure 53 – "Welcome" screen from Report Web

3.13.1. SDH Performance Chart:

It is possible to filter the information desired for the report, specifies the parameters described in itens below. Selects the option that it desires to show, but ypu want a complete report just leave the options without specific description (as it shows the follow figure).

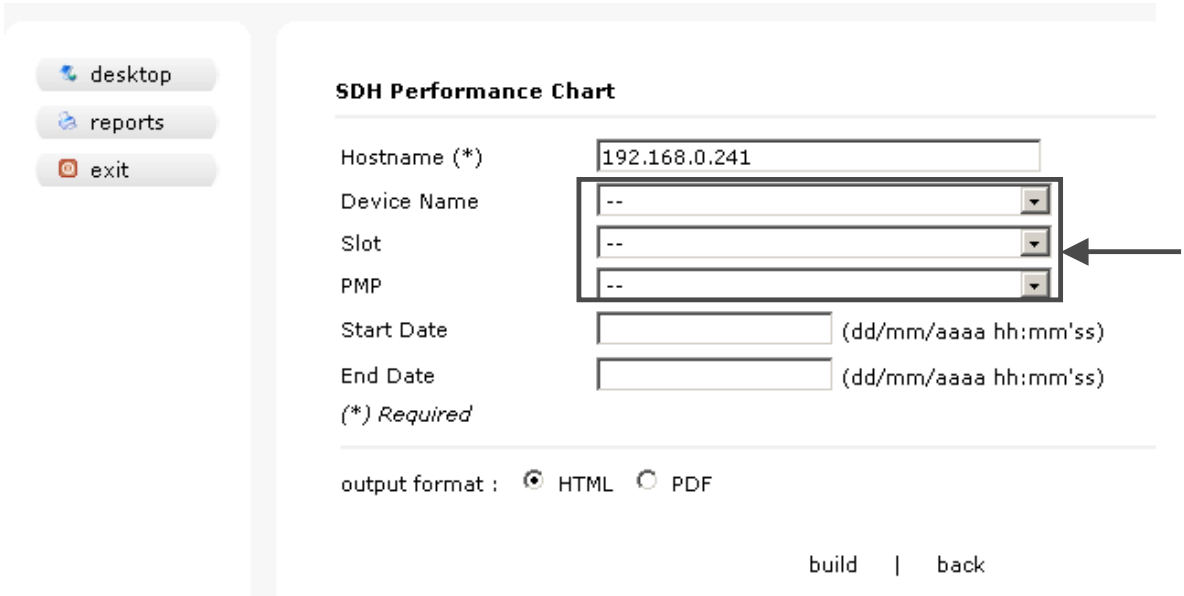


Figure 54 – Choosing Filters

Hostname – Source Host for creating the reports.

Device Name (*) - Equipment SDH that belongs to the host.

Slot (*) - Slot is mentioned to it to be told.

PMP (*) - Options of the filtering.

Start Date – Beginning Date of the filtering and creation the report.

End Date – Finishing Date of the filtering and creation the report.

HTML / PDF - Choice of the document format

Build / Back - Builds the report or comes back toward the previous menu

(*) In case that none of these parameters is specified, a specific filter will not occur, but yes a referring filtering to all the pertaining parameters to each option.

The report possesses, beyond the graphs of each chosen test, a heading contends information on the same, so that thus if they can better organize the reports of each monitoring.

SDH PERFORMANCE CHART

Filters:

Hostname:	192.168.0.241	Start Date:	20/09/2005 00:00'00
Device Name:	DmSTM1	End Date:	23/09/2005 23:59'59
Slot:	Agg A		
PMP:	---		

Date: 26/09/05 14:12 **Created by:** ADMINISTRATOR **Total of pages:** 34

Figure 55 – SDH Performance Chart Heading

The figures below show an example of the reports appearance. Where axle "X" shows the hour and date of each quadrant and axle "Y" shows the time represented in seconds.

RS-OOF / Assessed seconds (15 mins)

HOSTNAME: 192.168.0.241
DEVICE MODEL: DmSTM1 **SLOT/PORT:** Agg A/STM-1 **MODEL:** STM1 **START DATE:** 20/09/05 00:00

Figure 56 – Example of the graph from report model

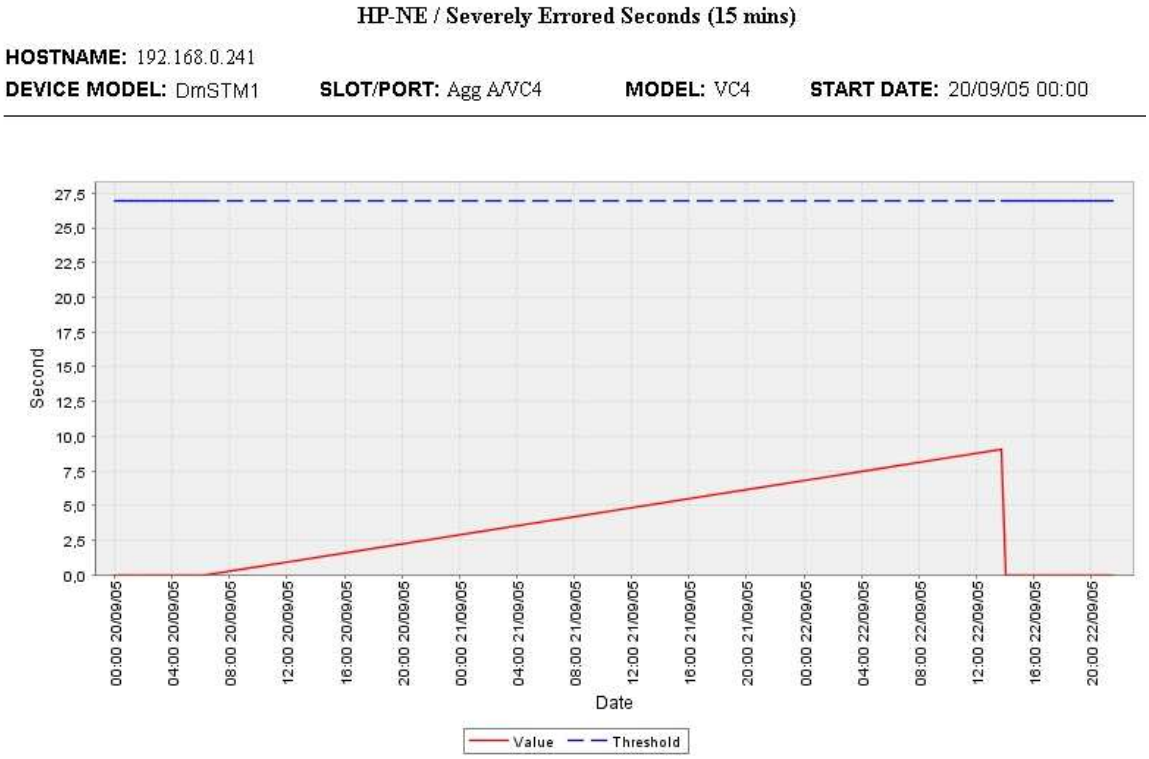


Figure 57 – Example of the graph from report model

3.13.2. SDH Performance Report:

The configuration parameters are the same ones used in the SDH Perfomance Chart, however the report is seen in a different form.

In the following figures, we have heading after that Chart Performance is presented very similar to the SDH and, then, the format of the report.

SDH PERFORMANCE REPORT

Filters:

Hostname:	192.168.0.241	PMP:	---
Device Name:	DmSTM1	Start Date:	20/09/2005 00:00'00
Slot:	---		
End Date:	23/09/2005 23:59'59		

Date: 26/09/05 10:05 **Created by:** ADMINISTRATOR **Total of pages:** 300

Figure 58 – SDH Performance Report Heading

Date	Serial No	Hostname	Slot/Port	Model	PMP	Counter	Value
20/09/2005 00:00	987654	192.168.0.241	Agg A/STM-1	STM1	RS-OOF	Assessed seconds (15 mins)	642
20/09/2005 00:15	987654	192.168.0.241	Agg A/STM-1	STM1	RS-OOF	Assessed seconds (15 mins)	904
20/09/2005 00:30	987654	192.168.0.241	Agg A/STM-1	STM1	RS-OOF	Assessed seconds (15 mins)	900
20/09/2005 00:45	987654	192.168.0.241	Agg A/STM-1	STM1	RS-OOF	Assessed seconds (15 mins)	900
20/09/2005 01:00	987654	192.168.0.241	Agg A/STM-1	STM1	RS-OOF	Assessed seconds (15 mins)	900
20/09/2005 01:15	987654	192.168.0.241	Agg A/STM-1	STM1	RS-OOF	Assessed seconds (15 mins)	900
20/09/2005 01:30	987654	192.168.0.241	Agg A/STM-1	STM1	RS-OOF	Assessed seconds (15 mins)	900
20/09/2005 01:45	987654	192.168.0.241	Agg A/STM-1	STM1	RS-OOF	Assessed seconds (15 mins)	900
20/09/2005 02:00	987654	192.168.0.241	Agg A/STM-1	STM1	RS-OOF	Assessed seconds (15 mins)	900
20/09/2005 02:15	987654	192.168.0.241	Agg A/STM-1	STM1	RS-OOF	Assessed seconds (15 mins)	900
20/09/2005 02:30	987654	192.168.0.241	Agg A/STM-1	STM1	RS-OOF	Assessed seconds (15 mins)	900
20/09/2005 02:45	987654	192.168.0.241	Agg A/STM-1	STM1	RS-OOF	Assessed seconds (15 mins)	900
20/09/2005 03:00	987654	192.168.0.241	Agg A/STM-1	STM1	RS-OOF	Assessed seconds (15 mins)	900
20/09/2005 03:15	987654	192.168.0.241	Agg A/STM-1	STM1	RS-OOF	Assessed seconds (15 mins)	900
20/09/2005 03:30	987654	192.168.0.241	Agg A/STM-1	STM1	RS-OOF	Assessed seconds (15 mins)	900
20/09/2005 03:45	987654	192.168.0.241	Agg A/STM-1	STM1	RS-OOF	Assessed seconds (15 mins)	900

26/09/05 10:05 Page 2 of 300

Figure 59 – Example of SDH Performance Report

4 STATUS AND ALARMS (DMVIEW)

The Event Browser is used for checking the equipment and interfaces alarms. The DmSTM-1 alarms can be divided in four levels of severity: critical, major, minor, and warning.

The interface status and alarm logs can also be accessed from the DmSTM-1 terminal via telnet or by an RS-232 serial interface connection.

4.1. Event Browser

The Event Browser can be accessed by the equipment bayface at the Tools/Events/Events Browser menu. In this screen the user can check the equipment-generated alarms and their severity, as well as DmSTM-1 configuration information.

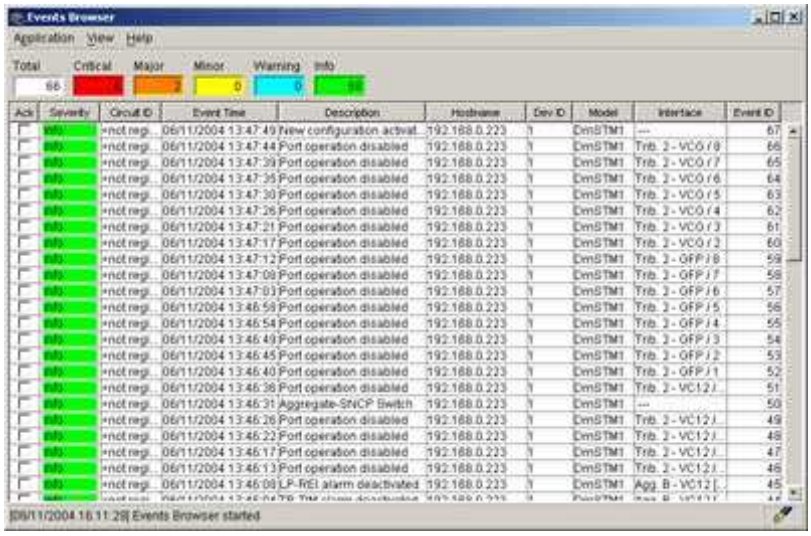


Figure 47 – Event Browser Screen

4.2. Checking the Interface Status

It is also possible to check the alarms clicking twice at the bayface interface port, displaying detailed status and alarms information.

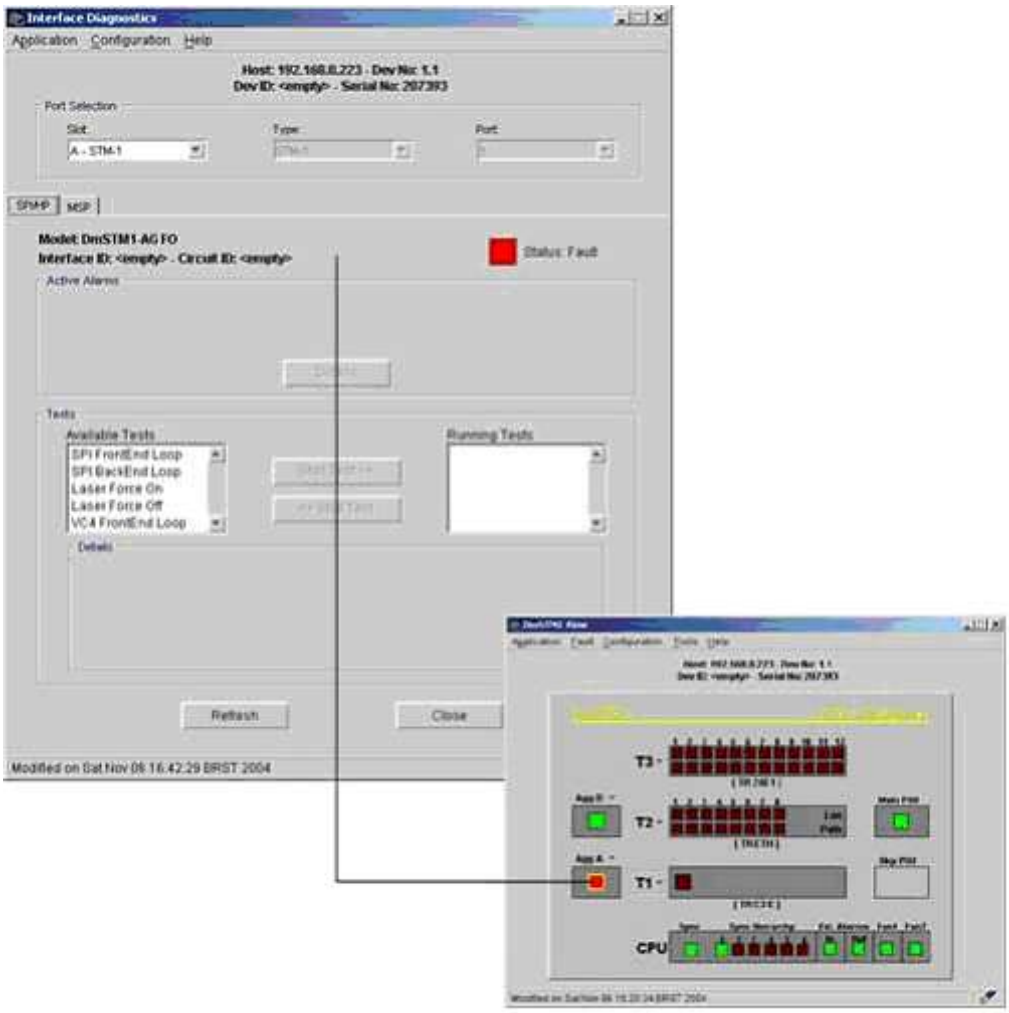


Figure 48 – Interface Diagnostics Screen

5 TESTS (DMVIEW)

The DmSTM-1 allows diagnostic tests to check failures at the link, protection switching and synchronism sources. To be possible to activate tests at the interface ports, this option must be enabled at the port configuration window.

The carrying out of tests can be done by the DmView or directly by the equipment terminal.

5.1. Interface Tests - Interface Diagnostics Screen

There are three ways to access the test facilities of the equipment interfaces, always starting from the bayface:

1) Press the right mouse button over the desired interface (tributary or aggregate) and choose Tributary/Aggregate Diagnostics.
2) Select the desired interface and go to the Fault -> Interface Diagnostics menu.
3) Double-click the left mouse button over the interface.

5.2. Aggregate Interface Tests

5.2.1. SPI/HP Tests

At the Interface Diagnostics window, choose Slot A - STM-1 or B - STM-1.

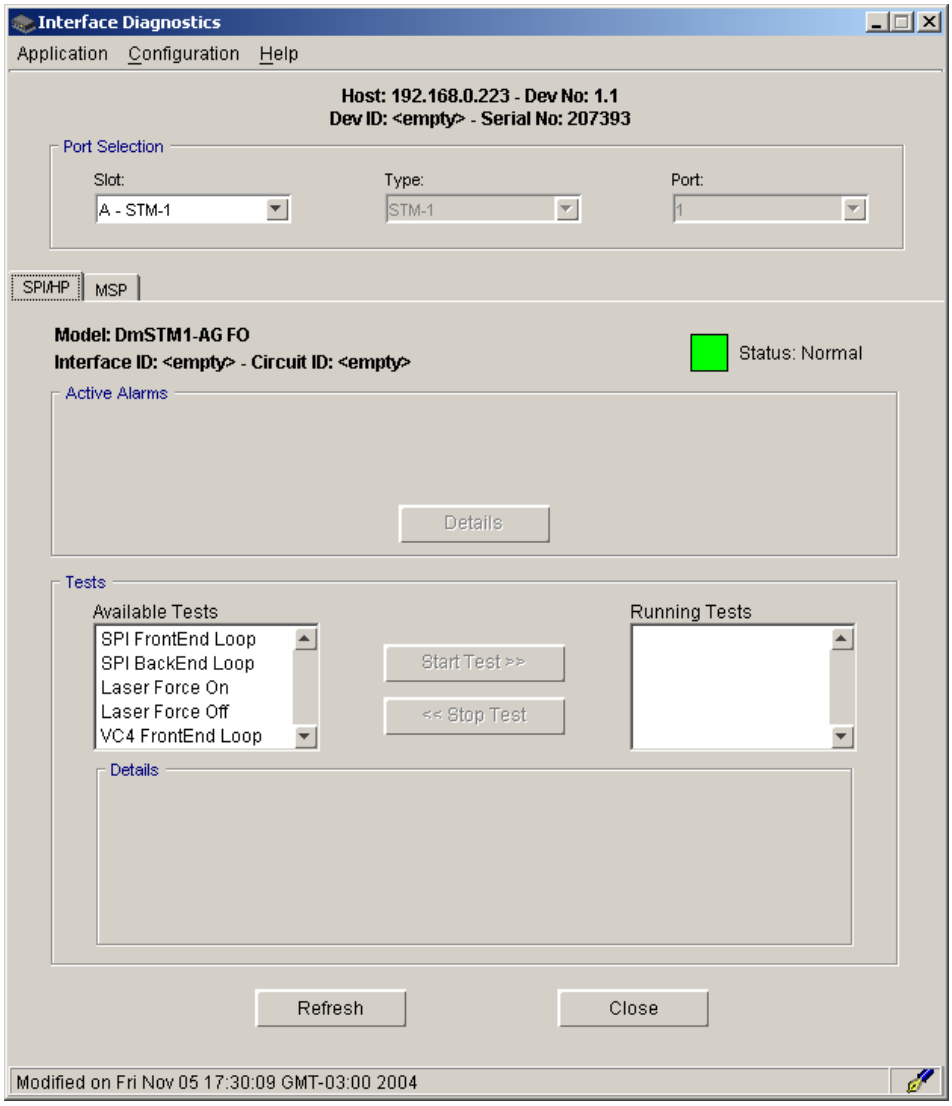


Figure 49 – Interface Diagnostics Screen for Aggregate SPI/HP tests

The available tests for this interface are:

SPI BackEnd Loop: Starts internal loopback test at the STM-1 aggregate interface

SPI FrontEnd Loop: Starts external loopback test at the STM-1 aggregate interface

Laser Force On: Forces the laser to remain on for the predefined time

Laser Force Off: Forces the laser to remain off for the predefined time

VC4 FrontEnd Loop: Starts internal VC-4.loopback test

The figures below display the test diagram of the aggregate interfaces.

Figure 50 –SPI BackEnd Aggregate Loop Diagram

Figure 51 – SPI FrontEnd Loop Aggregate Diagram

Figure 52 –VC-4 FrontEnd Loop Diagram

5.2.2. MSP Protection Tests

Figure 53 – Interface Diagnostics Screen for aggregate MSP protection tests

The available tests for this interface are:

Manual to work: Manual switching for the work link. If there is a failure, no switching will occur.

Manual to protect: Manual switching for the protection link. If there is a failure, no switching will occur.

Force to work: Forced switching for the work link.

Force to protect: Forced switching for the protection link.

Lockout: Prevents switching.

Clear: Removes link protection switching request.

5.3. 2Mbit/s Tributary Interface Tests

At the Interface Diagnostics window, choose Slot TRx-24E1 (x = 1, 2 or 3 indicates the equipment slot). On the port field, choose the port at which the test will be activated.

5.3.1. Physical Interface Tests

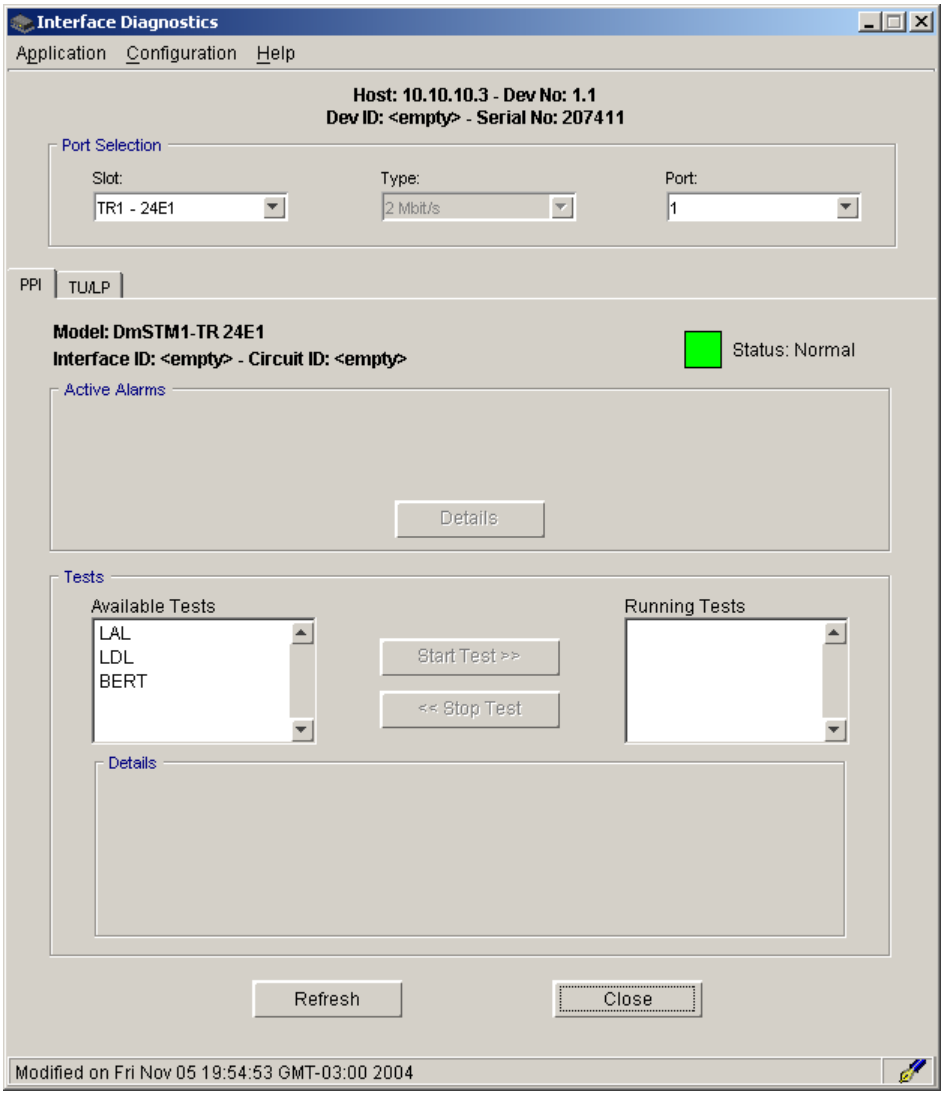


Figure 54 – Interface Diagnostics Screen for E1 tributary PPI tests

The available tests for this interface are:

LDL: Starts local digital loopback test on the E1 tributary.

LAL: Starts local analogue loopback test on the E1 tributary.

BERT: Generates and detects bit error rate pattern test. The BERT is generated towards the aggregate, being transmitted to the remote equipment.

The figures below display the 2Mbit/s interface tests diagram.

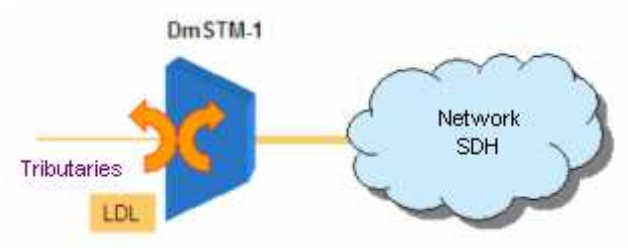


Figure 55 – LDL test diagram for the E1 tributaries

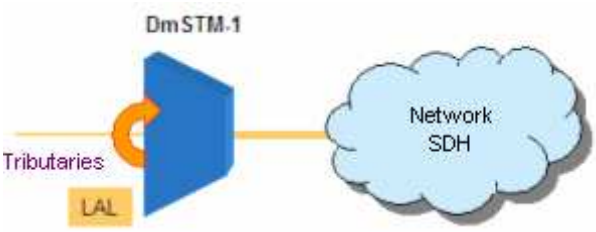


Figure 56 – LAL test diagram for the E1 tributaries

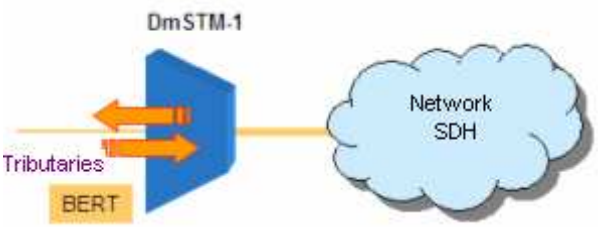


Figure 57 – BERT test diagram for the E1 tributaries

5.3.2. SNC Protection Tests

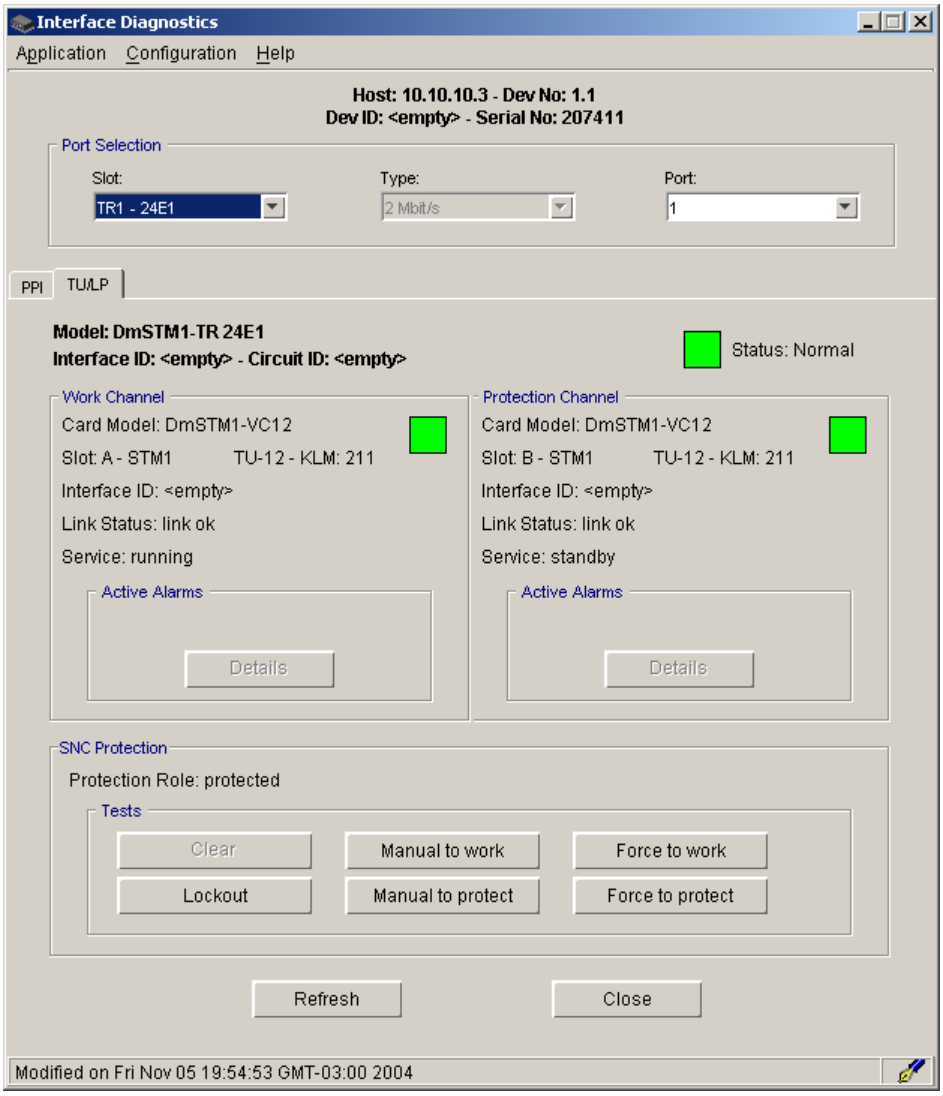


Figure 58 – Interface Diagnostics Screen for E1 tributary SNC protection tests

The tests available for this interface are:

Manual to work: Manual switching for the work link. If there is a failure, no switching will happen.

Manual to protect: Manual switching for the protection link. If there is a failure, no switching will happen.

Force to work: Forced switching to the work link.

Force to protect: Forced switching to the protection link.

Lockout: Prevents switching.

Clear: Removes link protection switching request.

5.4. E3 Tributary Interface Tests

At the Interface Diagnostics window, select Slot TRx – E3 (where x = 1, 2 or 3 indicates the equipment slot).

5.4.1. Physical Interface Tests

Figure 59 – Interface Diagnostics Screen for E3 Tributary PPI tests

The tests available for this interface are:

PPI BackEnd Loop: Runs internal loopback test at the E3 tributary interface

PPI FrontEnd Loop: Runs external loopback test at the E3 tributary interface

BERT FrontEnd: Generates and detects error rate test pattern. The BERT is generated towards the E3 interface.

BERT BackEnd: Generates and detects error rate test pattern. The BERT is generated towards the aggregate, being transmitted to the remote equipment.

LDL: Starts local digital loopback test at the E3 Tributary interface

5.4.2. SNC Protection Tests

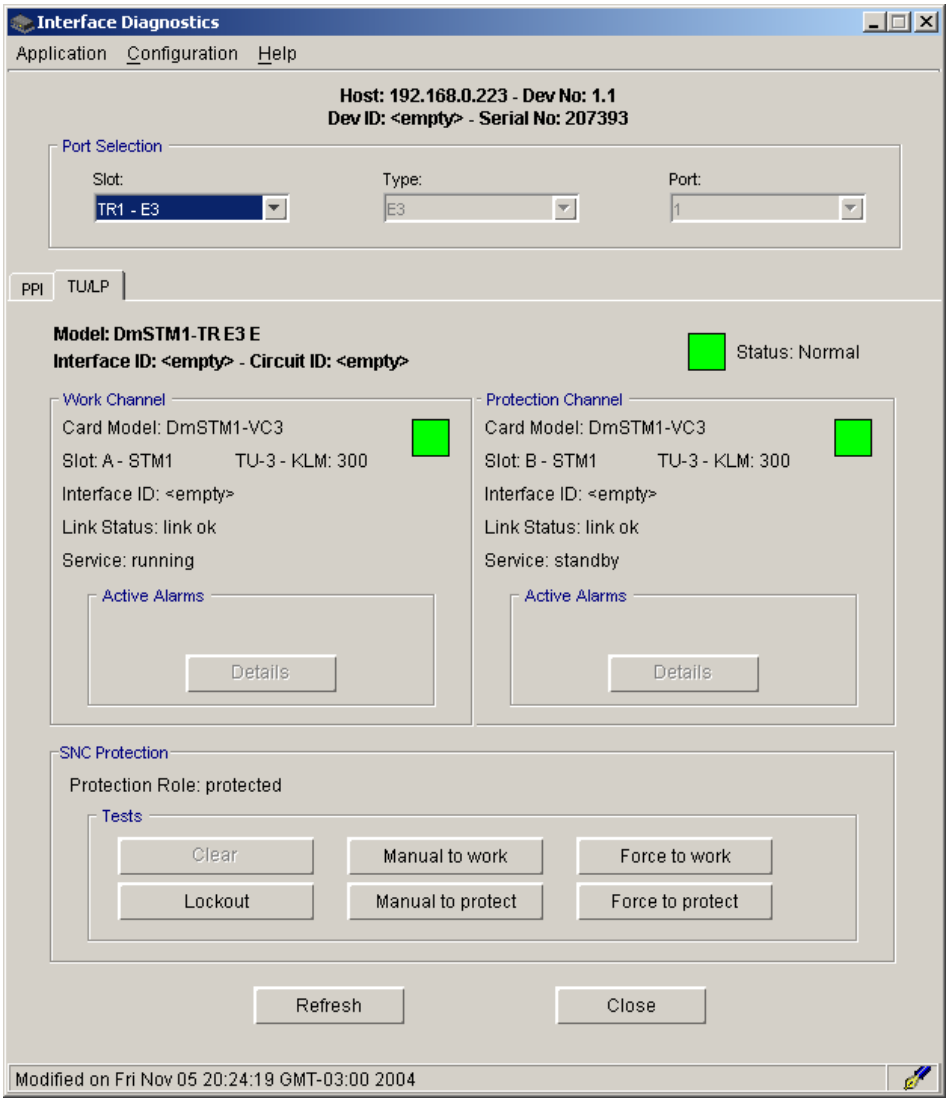


Figura 60– Interface Diagnostics Screen for SNC protection tests at the E3 Tributary

The tests available for this interface are:

Manual to work: Manual switching for the work link. If there is a failure, no switching will happen.

Manual to protect: Manual switching for the protection link. If there is a failure, no switching will happen.

Force to work: Forced switching for the work link.

Force to protect: Forced switching for the protection link.

Lockout: Prevents switching.

Clear: Removes link protection switching request.

5.5. STM-1 Tributary Tests

At the Interface Diagnostics window, select Slot TRx - STM-1 (where x = 1, 2 or 3 indicates the equipment slot).

5.5.1. SPI/HP Tests

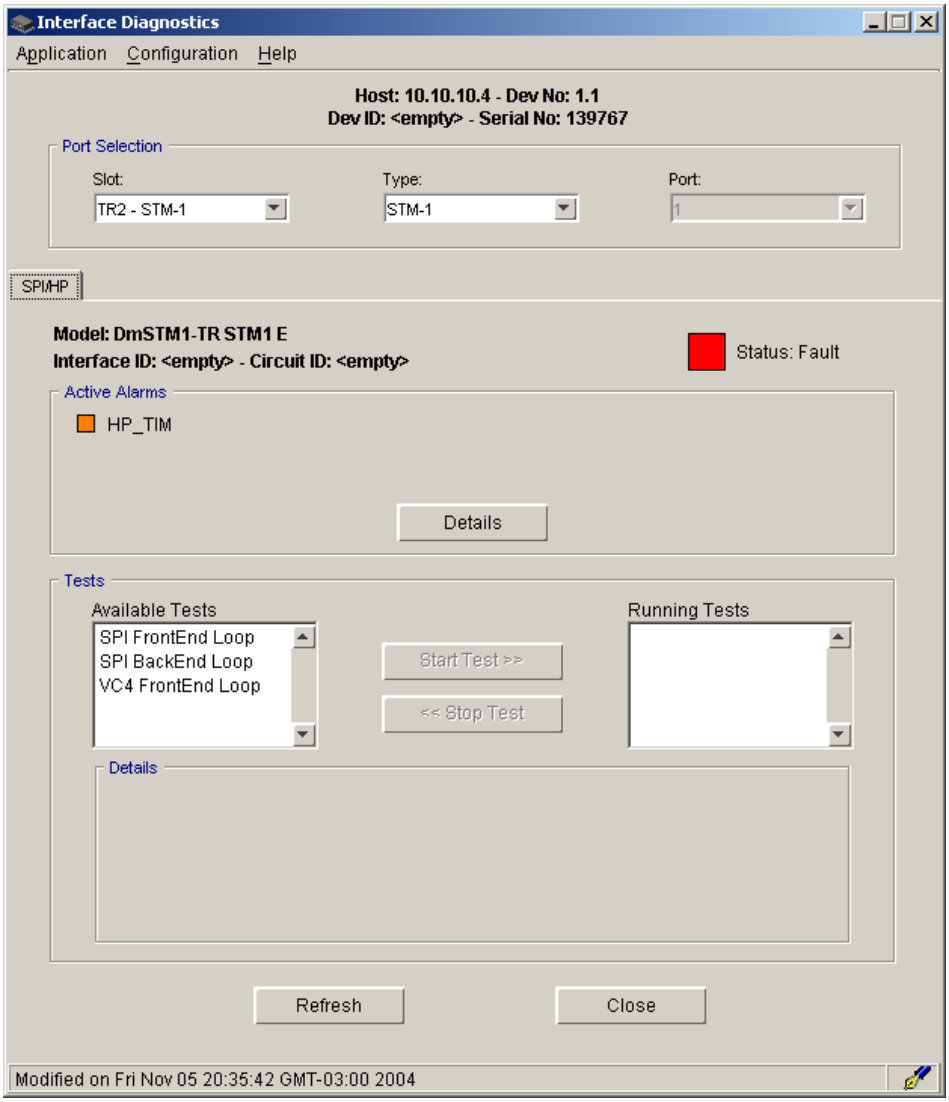


Figure 61 – E3 Tributary PPI Tests Interface Diagnostics Screen

The tests available for this interface are:

SPI BackEnd Loop: Starts internal loopback test at the STM-1 tributary interface.

SPI FrontEnd Loop: Starts external loopback test at the STM-1 tributary interface.

VC4 FrontEnd Loop: Starts VC4 external loopback test.

5.6. Switching Reference Synchronism Test

There are two ways to access the switching reference synchronism test facility, always from its bayface:

1) Go to the menu Fault -> Sync Source Status.

2) Double-click the left mouse button over one of the available CPU clock hierarchies.

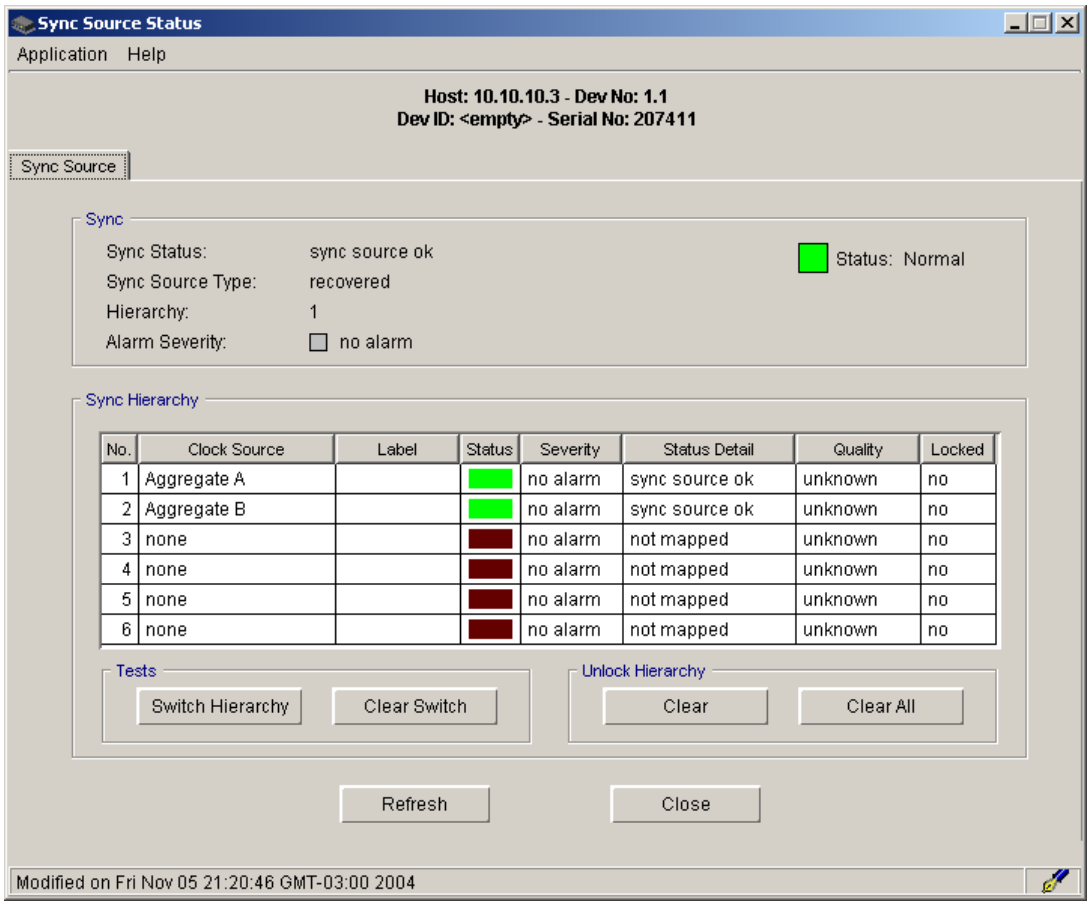


Figure 62 – Switching reference synchronism test window

Choose the hierarchy to which it is desired to switch and click on Switch Hierarchy. To remove the test request, click on Clear Switch.

6 SYNCHRONISM

6.1. Notes on synchronism quality

The ITU-T Recommendations define the following synchronism reference types for STM-1 equipments:

- PRC – Primary Reference Clock – also known as G.811. It is the most trustworthy clock available, hence its name. It is recommended that big STM-1 rings have at least a primary synchronism source.
- SSU – Synchronization Supply Unit – Also known as G.812. It is also a trustworthy clock for it is derived from the PRC, but it has already passed by a lot of equipments since the main clock input.
- SEC – SDH Equipment Clock – This clock source refers directly to the clock generated by any SDH equipment. That is, it comes from an internal clock source. It is not trustworthy for big networks, but it can be used as reference for smaller networks.

6.2. Hierarchy Synchronism Switching

The hierarchy clock switching is based upon the user-configured clock priority sequences to define which sync source will be used by the equipment.

This kind of synchronism is easier to use, but it does not assure that the equipment is using the best sync source available on the network. The only safety feature of this method comes from a good network planning, such that the operator always sets the best sync sources for the higher hierarchy levels.

For performing the sync reference switching, the DmSTM-1 has six levels on the sync source table, which will always be used from the highest to the lowest. The highest hierarchy is the one with the lowest number.

The sync reference switching criteria change the way the equipment will deal with each of the clocks. It is important to note the following characteristics when configuring the equipment with hierarchy sync reference switching. These configurations are related to the clock hierarchies.

- Enable Switch – Defines if the equipment can switch to the sync reference as configured in the sync hierarchy table. This is a global parameter.
- Reversible Mode – Defines if the equipment will reuse a sync reference that has previously failed, if this source becomes trustworthy again. This is a global parameter.

The option below refers to the switching selection method used in the equipment. To use the hierarchy switching, leave this option always disabled:

- SSM Switch – Defines if sync reference switching will occur by sync reference status messages. This is a global parameter.

The rest of the configurable characteristics refer to the criteria to evaluate if a sync reference has good quality, or not:

- EXC Switch – Defines if sync reference switching will be caused by alarm EXC detection.
- LOF Switch – Defines if sync reference switching will be caused by alarm LOF detection.

- TIM Switch – Defines if sync reference switching will be caused by alarm TIM detection.
- AIS Switch – Defines if sync reference switching will be caused by alarm AIS detection.
- Out_of_band Switch – Defines if switching will occur if it is detected that the sync reference is out of the expected frequency band.

Using these configurations, the equipment will choose the sync reference to be used for synchronism. The most important options are Enable_switch, Reversible_mode and SSM_Switch.

Enable_Switch will enable the sync reference switching. If that option is disabled, the equipment does not switch among the sync sources.

Reversible_mode will define if the sync source can be used again if it becomes operational once more. This is an important option if it is needed that the equipment consistently tries to go back to the lowest hierarchy levels (where the best quality sources are mapped). If the reversible mode is disabled, the operator will still be able to release the switching back to a sync source by unblocking it (please check the source unblocking item for further information). An unblocked source behaves as if no failure was detected, that is, if it fails again, it will be blocked once more.

6.3. Synchronism Status Message Switching

The synchronism status message clock switching is based on the condition that every sync source has a quality indicator and this indicator can be automatically updated for STM-1 links or manually inserted for the other cases.

The quality indicators are used to define the received clock quality for every clock hierarchy and, in this way, provide information so that the equipment can decide which the best available clock option is.

Within the STM-1 network, the clock quality indicators circulate in the S1 byte of the multiplexing section and they are changed by the equipments when failures are observed in sync sources or network switching.

The clock quality indicators are defined in ITU-T Recommendation G.707 and are presented in the following table:

Sync source quality description		
S1Bits (b5-b8)	Nomenclature	Description
0000	Quality Unknown (Existing Synchronization Network)	Unknown quality. This clock is considered to have a quality close to the DNU clock, so its use is not recommended (note 1)
0001	Reserved	Reserved for operator use (note 2)
0010	G.811 (PRC)	Primary reference clock
0011	Reserved	Reserved for operator use (note 2)
0100	G.812 Transit (SSU-A)	Clock traceable to a node with G.812 reference in transit
0101	Reserved	Reserved for operator use (note 2)
0110	Reserved	Reserved for operator use (note 2)
0111	Reserved	Reserved for operator use (note 2)
1000	G.812 Local (SSU-B)	Clock traceable to a node with local G.812 reference
1001	Reserved	Reserved for operator use (note 2)
1010	Reserved	Reserved for operator use (note 2)
1011	SEC - SDH Equipment Clock	It is the SDH equipment clock, that is, the internal clock or the holdover of a faulty source
1100	Reserved	Reserved for operator use (note 2)
1101	Reserved	Reserved for operator use (note 2)
1110	Reserved	Reserved for operator use (note 2)
1111	DNU - Don't Use for Synchronization	This clock should not be used for network synchronisation

Some notes concerning the table above:

1. The lowest values in the table correspond to better quality clocks. The only exception is the clock with quality 0000 (UNKNOWN), which has a quality that is evaluated as being a little better than the DNU, but in most cases this means that this clock should not be used. For the DmSTM-1, the Unknown clock is considered as having identical quality to the DNU.

2. The reserved values correspond to values that can be used by the operator to indicate specific references. Some cares must be taken when using reserved values:

    a. The reserved values with the lowest numbers assigned to them have, by definition, better qualities than the values with higher numbers assigned to them;

    b. When using reserved values in networks that intermix equipments from different makers, the user should check that every equipment interprets the reserved values in the same way;

    c. It is recommended that the reserved values are not used, for they depend only on the operator and they can lose meaning with time, bringing trouble or maintenance complication on the networks.

Based upon the values on this table, it is possible for the operator to define the qualities that the equipment will take into account for the input of each of the sources.

Concerning the quality indicators of the STM-1 system clock references, it is possible to individually configure, for each clock hierarchy, the input quality that will be taken into account, and also which output quality will be sent to the STM-1 links (at byte S1) when each of these sources is being used.

6.4. Input Quality Indicators

To do that the Input_QL command is used at the clock hierarchy configuration. In this command it is possible to configure which value of the clock source quality indicator will be linked to each of the sync sources. The values include every existing option in the quality indicator table and also allow the user to choose the automatic configuration (*auto*).

When the sync quality indicator is chosen as *auto*, the input quality value will be recovered from the S1 byte, that is, the equipment will consider the values received at the STM-1 line as being valid and will make decisions based on the variation of these sync quality indicators.

Important: the *auto* value is only applicable to sync sources that have valid quality indicators, that is, only for sync sources derived from the STM-1 lines. So, the value *auto* should not be used for the input quality of tributary clock links and external equipment sync inputs.

When an input that carries valid information in S1 has its quality forced to any value other than *auto*, the equipment will ignore the value received at the line and it will use the one that is configured by the user.

6.5. Output Quality Indicators

In the same way that it is possible to define the input quality configuration, it is possible to manually or automatically define the output quality value (which will be sent on the equipment aggregate S1 bytes).

Differently of the input quality system, the output quality indicator can be configured as automatic for all clock hierarchies, such that, when working automatically, the equipment will copy the input quality value to the equipment output quality. That is, the output will behave according to the quality value which is received (or configured) at the input.

Another existing difference between the output quality indicator and the input quality indicator is that, even if an output quality level is forced, if the reference indicates that the input signal quality is worse than the output quality forced value, the equipment will consider the output quality to be the same as the input quality. This ensures that the equipment is not able to indicate erroneously a quality value that the synchronism source does not actually have. If it is not necessary, this behaviour can be altered, forcing the input quality of the equipments connected to these links.

6.6. The working of synchronism message switching

Using the information configured in the input and output qualities for each hierarchy and its own synchronism mappings, the equipment defines which the best clock source available is at the moment (considering the input quality received and configured) and also from the position of the clock hierarchy.

If a better quality synchronism source is available, the equipment will switch to it and will spread its new clock quality by means of the S1 bytes of its aggregates.

There exists an important mechanism that is used by the equipments that use SSM switching to avoid that equipments (inside a network) get into a clock loop. When an equipment (A) is using the clock coming from another equipment (B), it will automatically indicate to equipment B (using its S1 byte) that the clock should not be used (DNU). In that way, it is avoided that, if any clock switching takes place, A tries to recover the clock from B while B is simultaneously trying to recover clock from A.

The example below better illustrates the operation of the clocks in SSM equipments:

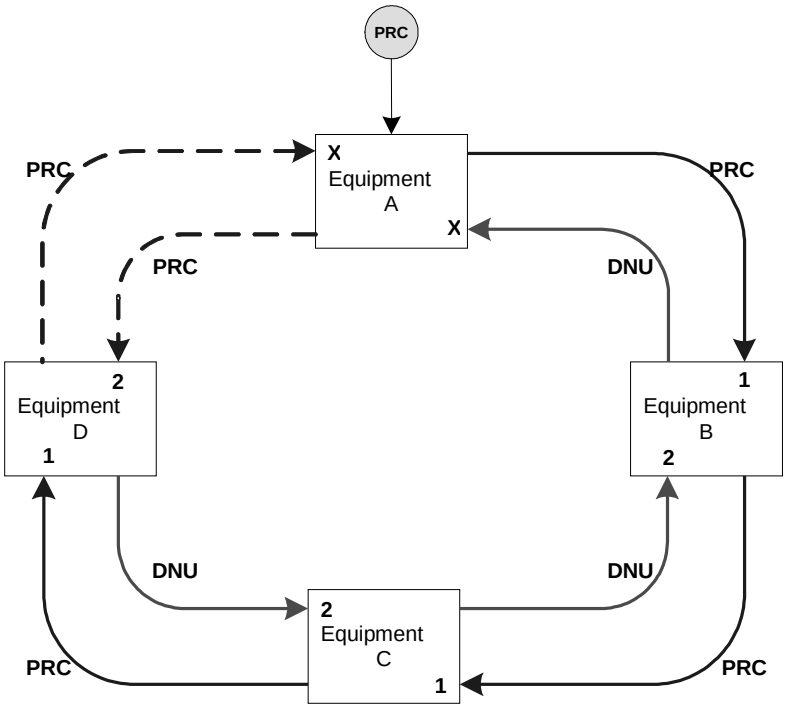


Figure 63 – Clock diagram using SSM

Consider the ring depicted above, where Equipment A receives the clock from a primary sync source *(PRC)* and distributes this synchronism through its aggregates for equipments B and D.

The clock quality indicator has the value PRC only because the operator configured the Input_QL from Equipment A primary synchronism source as being a PRC type clock and the Output_QL as being automatic. Having this type of configuration, equipment A will spread to its neighbours that the clock derived from it is of PRC quality.

Equipment B has as its main sync source the STM-1 link (indicated by number 1) and as secondary source the link received from Equipment C. As it is receiving from equipment A a PRC quality clock and as this is its primary source, even if it received the PRC clock from equipment C, Equipment B would opt for the clock received from Equipment A.

Due to the fact that it is using the clock coming from equipment A, and to avoid forming network clock loops, Equipment B will answer to A that its clock should not be used (DNU).

The same happens to the Equipment C concerning the clock received from equipment B. It will opt for its primary clock, and will respond to equipment B that its clock should not be used.

Equipment D completes the ring, and it receives PRC clock from both aggregates, but as its primary clock is the clock received from Equipment C, even if the quality of both sides is the same, the selection criterion will be the lowest hierarchy sync source. In that way Equipment D starts to send DNU to equipment C to avoid clock loops.

In this way the sync network will become stable according to the equipment configuration and by always selecting the best sync source available at every equipment.

Let us consider a failure situation, where there is total interruption of the clock path, as illustrated by the figure below:

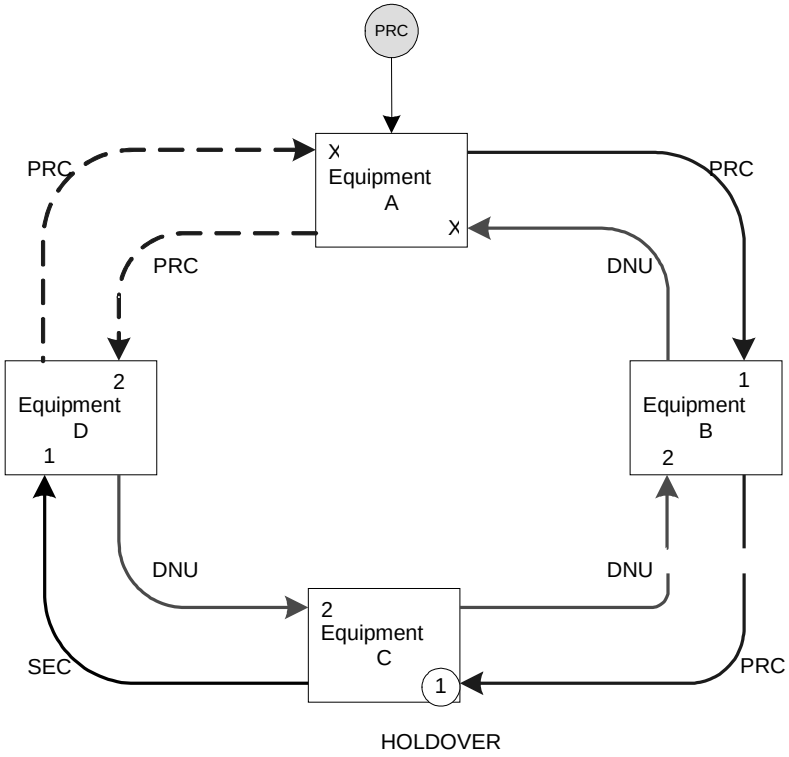


Figure 64 –Example diagram of the failure situation

If there is any interruption in the path that connects equipment B to C, the network will try to recover in the least traumatic way, always looking for situations in which every equipment will use the best available sync sources.

In the exact moment that the line is interrupted, equipment C, which used that clock as sync, faces the following situation:

- Primary clock – failure;
- Secondary clock – DNU;

So the normal decision for equipment C is to go to the holdover of the sync source that it already had.

With that, the clock quality that equipment C will send to its remote equipments will be the SEC, which is the clock derived from a sync source of the equipment C itself (that is, holdover or free run).

This forces equipment D to react, for it was using the clock that was received from equipment C and that had its quality reduced. Looking at its clock hierarchy table, equipment D will note that the clock coming from equipment A has better quality than the one coming from equipment C. At once equipment D will switch its clock to the one coming from Equipment A, and this will cause a change in the behaviour of the automatic DNU responses from equipment D, for it now is receiving a clock from equipment A, and so it will answer DNU to equipment A. As the clock in D is PRC, it will tell equipment C that its clock from now on is PRC.

Equipment C, which is still in holdover mode, for its primary source is in failure and got DNU from D, starts to get the news that the D clock is now PRC. With that, it will switch to the sync source coming from D. C, now, will start to answer DNU to equipment D, for it is already using clock from it. This generates a new stable situation in the network, for every equipment is using the best sync source available.

In the figure below, it is possible to check how the network has re-established itself in regard to clock sync:

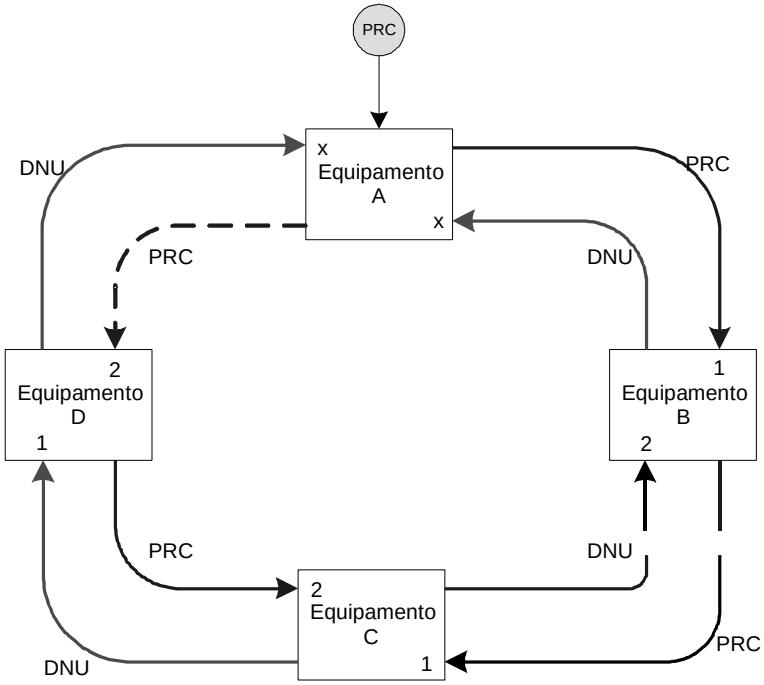


Figure 65 – Example diagram of synchronism re-establishing

When the link between C and B is re-established, the network will return to the original condition, for C will start to receive the clock from B as PRC, and the clock coming from D is also PRC, hence it will opt for the lower hierarchy one (B).

C will again tell D that its clock is PRC, and this will make D also choose its primary clock, going back to the INITIAL network condition.

6.7. Some cares that must be taken concerning the design of networks using SSM

SSM can be used to increase the sync quality to failures like fibre interruption (for example). It can also be used in networks that carry data/sensible services (such as video signals).

The SSM simplifies some operational aspects of the synchronism architecture. However, care must be taken to avoid sync loops during the SSM message transitions. The following is recommended when using SSM:

- The clock hierarchy will define the possible sync sources for the equipment. Sources that are not mapped will not be used, even if they have better SSM quality;
- If there is any need of switching, the equipment will look for the sources with higher level of quality and will switch to the best available quality. If there is a quality conflict, the equipment will choose the source with the lowest hierarchy;
- The equipment will always respond DNU to the clock source that it is using to avoid sync loops. Notwithstanding this action, the user must take care to avoid putting the network in clock loops;
- When the input quality of a sync source is forced, it does not matter if there is an SSM message indicating if the source has better or worse quality than what is configured. To the equipment, the input quality of this source will be the same as the value forced by the user;

- The SSM system provides a network sync quality indication through message spreading. These messages are sent through the multiplexing section as described in Recommendation G.707. When an STM-1 output transmits a sync quality, the sync message will indicate the quality or sync traceability that has originally generated it. Note that this does not reflect the accumulation of jitter and wander resulting from the clock retransmission through the network. To avoid jitter and/or wander problems in very large networks, the operator must force output qualities in some equipments to adequate the quality indication to the actual clock quality;
- Sync sources with quality indicator equal to 0 (Unknown) are considered as sync sources with DNU quality. When a hierarchy receives a clock whose quality is Unknown, that source is considered as untrustworthy, that is, that source will only be used if the rest of the sources are DNU, invalid or blocked.
- Equipments using sync source from the historic of a source (holdover) or with free-running clock spread SEC quality level to its remotes;
- Care must be taken from the moment that SSM is fired in a network for the first time to avoid clock loops to be formed and to avoid sync oscillations to happen for an undefined period of time. The necessary cares are related to good network design, for the equipments will become stable only when their higher hierarchy sources display the best clock qualities;
- For networks that do not employ SSM, it is recommended that the source quality indicators be configured as DNU or Unknown;
- If you are upgrading a network that does not employ SSM, do not use SSM;
- Define exactly which is the desired configuration for the SSM network;
- Develop a detailed plan for configuring the SSM network;
- Define the quality levels and priorities for every equipment before starting to implement SSM;
- Start using SSM at the equipment that is directly connected to the best sync source;
- Start SSM in the next network equipment. Continue enabling SSM for each equipment that will follow the clock in the network, in the appropriate sequence of the use of this clock;
- Avoid sync loops:
    - During SSM configuration, make sure that there are no equipments which have no initialised SSM located between equipments in which SSM is operating;
    - If any of the network equipments does not support SSM, DO NOT USE SSM in that network;
    - If no port is defined as Auto in the SSM, one of the qualities (input or output) must be defined as 15 (DNU), but not both. For the DmSTM-1, it is highly recommended that the QL of the output sources be configured. That is, a source can receive the sync signal or transmit it, but never do both simultaneously;
    - Normally, an STM-1 port should only be set without SSM (that is, with fixed QL) only when the other end of the link does not support SSM, or if it is required that SSM should not be used for that link. This is the case of a network threshold, for example, in a control threshold, operator threshold or links between rings.
    - When an equipment uses its internal sync source as reference signal, it is recommended that the quality levels for that source be configured with a value lower than 11. This happens because the internal clock source has level equal to 11, which is the same as the holdover quality value.

- If a single equipment brings synchronism to the network, do not include its aggregates within the clock hierarchies used in that equipment. This avoids the situation where the aggregates could receive a quality level greater than all others in this NE (network element) and the equipment starts to use one of them as sync source. In this situation, every equipment will synchronize from the aggregates, resulting in sync loops and loss of external clock reference. To solve that, the sync hierarchy will have to be reconfigured.

7 MANAGEMENT

From the Network_parameters equipment terminal menu it is possible to configure the equipment network parameters.

After entering the Network_Parameters menu, the equipment can be configured through the Zebra software, which presents a standard interface for configuring the Ethernet network devices and router. In this application, any change is valid from the moment the command is entered.

Zebra on-line help can be reached using the "?" key. By pressing "?" the available commands are shown for the present configuration mode. That help is context-sensitive, showing the options for the command that is being keyed in. There are also three more interface shortcut keys: TAB, which completes the command that is being keyed, CTRL-Z, that takes the user back to the initial configuration mode, and CTRL-D that takes the user out of this interface, back to the equipment main menu.

Zebra operates in five modes: INITIAL, PRIVILEGED, CONFIGURATION, INTERFACE and ROUTER.

When running the software (from the Network_Parameters menu), the user starts Zebra in the Initial mode.

To go from the Initial mode to the Privileged mode, the user must key in the **enable** command.

To go from the Privileged mode to the Configuration mode, the user must key in the **configure terminal** command.

To go from the CONFIGURATION mode to the INTERFACE mode, the user must key in the **interface <interf>** command (where **<interf>** is the interface name; usually **<interf>** is chosen as **eth0**).

To go from the CONFIGURATION mode to the ROUTER mode, the user must key in the **router rip** command.

To exit the modes, it is necessary to key in the **exit** command. If the present mode is the INITIAL or the PRIVILEGED mode, the **exit** command exits the network configuration application software.

7.1. Protocols

Use of the DataCom Protocol allows configuring a single network in the ring. It is not necessary to employ sub-networks. It also presents performance gains between the management software and the NEs. Below follows a brief description of the DATACOM Protocol configuration.

7.1.1. Using the DATACOM Protocol

An IP address of the same segment of the network is necessary for each dc interface of the DATACOM Protocol.

For ring operation, two HDLC interfaces are used, encapsulated within the DATACOM Protocol. An HDLC channel must be mapped in the aggregate A overhead bytes and the other in the aggregate B ones.

Enable the rip and the route redistribution for the dc interface. Example:

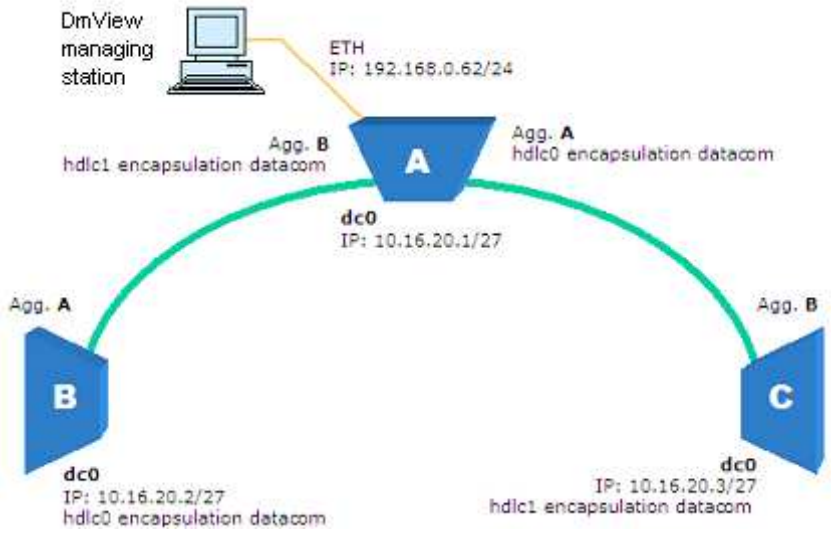


Figure 66 – Example using DATACOM Protocol

7.1.2. Using the PPP protocol

Uses a network IP address for each HDLC interface. One is directed to aggregate A and the other to Aggregate B, in the Overhead bytes. The user should enable the rip and the route redistribution for both HDLC interfaces.

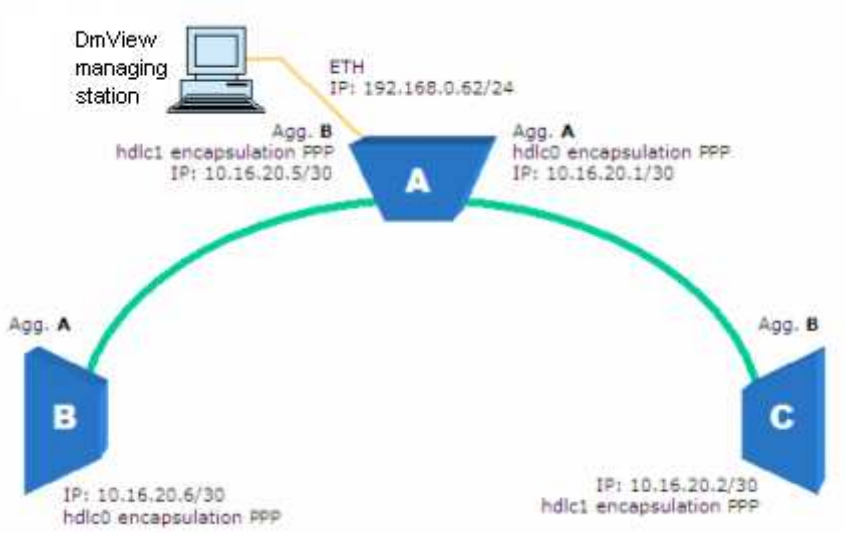


Figure 67 – Example using PPP protocol

7.2. Migrating to the DATACOM Protocol

This chapter presents the necessary steps for migrating from a PPP encapsulation management system to a DATACOM encapsulation. Consider the system displayed below, configured with HDLC interfaces PPP encapsulation:

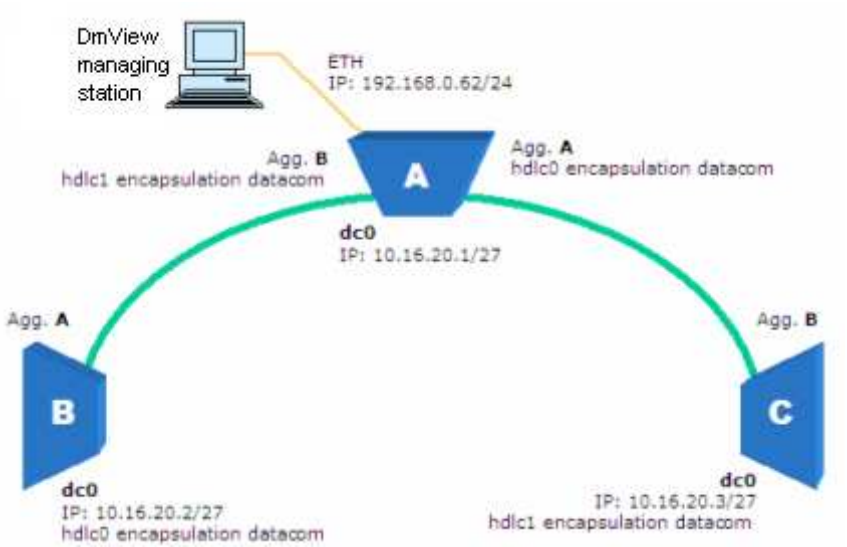


Figure 68 – Example migration to DATACOM Protocol

To maintain management during the migration process, it is recommended to first replace one side of the ring and after it enters operation, replace the other side. Example

Let us first configure the hdlc1 direction for equipment A. Network parameters:

```
>enable
>configure terminal
>interface hdlc1
>encapsulation datacom
>exit
>interface dc0
>show interface dc0

>no ip address <address shown in the last command >
>ip address 10.16.10.1/27
>exit
>router rip
>no network hdlc1
>exit
>write memory
>exit
>exit
```

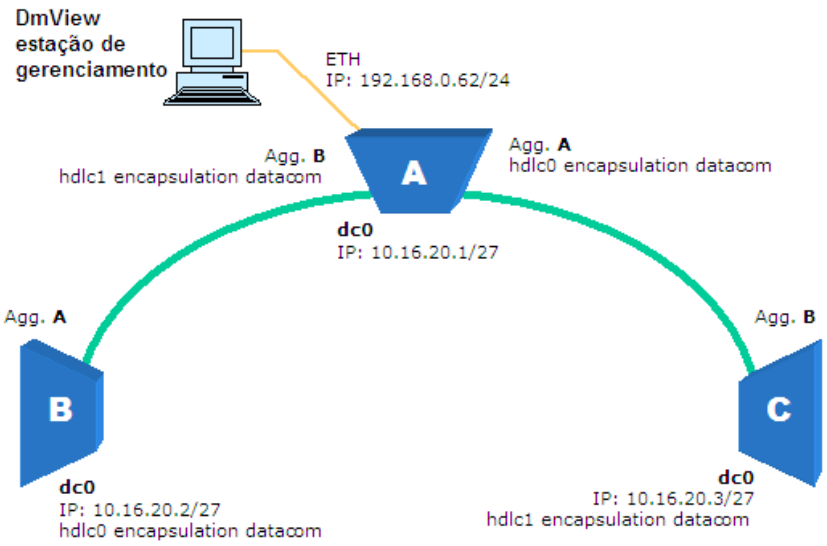
Repeat the procedure for every NE in the same direction, keeping the sequence from equipment A to B, from B to the next and proceeding up to the last ring segment before equipment A.

To complete the process on the other direction, it suffices to configure the hdlc interface encapsulation. Follow the example:

Equipment A, network parameters:

```
>enable
>configure terminal
>interface hdlc0
>encapsulation datacom
>exit
>router rip
>no network hdlc0
>exit
>write memory
>exit
>exit
```

Repeat the procedure for the other ring equipments to complete the migration.



7.3. Zebra Commands

The tables below present some basic Zebra commands.

Command	Operating mode	Description
Enable	**INITIAL**	Enables access to the Privileged mode
configure terminal	**Privileged**	Enables access to the Configuration mode
interface eth0	**Configuration**	Enables access to the Interface mode
router rip	**Configuration**	Enables access to the ROUTER mode

Table 2 – Commands to alternate among the Zebra modes

Command	Operating mode	Description
show <Command>	**INITIAL**	Displays information about the network interface. To visualize the <Command> options, key in **show**
show interface	**INITIAL**	Displays information about the network interface

Table 3 –Initial Mode Commands

Command	Operating mode	Description
show interface	**Interface**	Displays information about the network interface
no ip address IP/M	**Interface**	Removes the IP number **IP** mask **M**. Example: **no ip address 192.168.0.1/24**
ip address IP/M	**Interface**	Inserts the IP number **IP** mask **M**.
no shutdown	**Interface**	Enables the interface
Shutdown	**Interface**	Disables the interface

Table 4 –Interface Mode Commands

Command	Operating mode	Description
ip route 0.0.0.0/0 IP/M	**Configuration**	Configures the standard gateway (**IP/M** being the IP and mask of the standard gateway)
no ip route 0.0.0.0/0 IP/M	**Configuration**	Removes the standard gateway **IP/M**
ip route IP/M IPg/Mg	**Configuration**	Inserts a static route for the network **IP/M** with standard gateway at **IPg/Mg**
no ip route IP/M IPg/Mg	**Configuration**	Removes the static route for the network **IP/M** with standard gateway at **IPg/Mg**

Table 5 –Configuration Mode Commands

Command	Operating mode	Description
network eth0	**ROUTER**	Enables the RIP for the equipment Ethernet interface.
no network eth0	**ROUTER**	Disables the RIP for the equipment Ethernet interface.
redistribute static	**ROUTER**	Enables the static routes redistribution. The standard is not to redistribute.
no redistribute static	**ROUTER**	Disables the static routes redistribution. That option is default.
redistribute connected	**ROUTER**	Enables the redistribution of the routes corresponding to the equipment interfaces.
no redistribute connected	**ROUTER**	Disables the redistribution of the routes corresponding to the equipment interfaces. That option is default.

Table 6 –Routing Mode Commands

Command	Operating mode	Description
write memory	**All**	Writes the configuration into non-volatile memory
write terminal	**All**	Displays the present configuration
exit	**All**	Goes back to the previous mode
end	**All**	Goes back to the Privileged mode

Table 7 – Commands for all modes

Command	Operating mode	Description
show datacom <name>	**INITIAL, Privileged and interface**	Displays the equipments known by the DataCom Protocol to the interface <name>, or for every interface if <name> is omitted
encapsulation datacom <name>	**Hdlc interface**	Places the hdlc interface in the same group as interface <name>. If <name> is not specified, every DataCom interface is displayed
no encapsulation datacom <name>	**Hdlc interface**	Removes the hdlc interface hdlc from the interface <name> group

Table 8 – Commands for the DATACOM Protocol

Note: each hdlc channel must be configured for a single DataCom interface.

Command	Operating mode	Description
datacom reset	**Configuration**	Resets the DataCom Protocol
datacom drop max	**Configuration**	Defines the maximum number of packets that must be rejected for having sequence error.
datacom keep alive period	**Configuration**	Defines the period (in seconds) to send keep alive to the interface
datacom keep alive limit	**Configuration**	Defines the limit of keep lives not received before dropping the interface
datacom keep alive hdlc period	**Configuration**	Defines the period (in seconds) to send group hdlc interface keep lives
datacom keep alive hdlc limit	**Configuration**	Defines the limit of keep lives sent without answer to the group hdlc interface

Table 9 – Commands for the DATACOM Protocol

Note: Placing **"no"** in front of the DATACOM Commands causes Zebra to configure the default values.

Command	Operating mode	Description
show frame-relay <name>	**INITIAL, Privileged and interface**	Displays the frame-relay information for interface <name>
encapsulation frame-relay <name>	**Hdlc interface**	Places the hdlc interface in the group of interface <name>. If <name> is not specified, all DataCom interfaces are displayed.
no encapsulation frame-relay <name>	**Hdlc interface**	Configure interface with PPP encapsulation.
frame-relay lmi-type (ansi|q933a|none)	**Hdlc interface**	Defines the lmi type (q933a = CCITT)
no frame-relay lmi-type	**Hdlc interface**	Configure interface with PPP encapsulation.
frame-relay intf-type (dce|dte)	**Hdlc interface**	Configures the interface type (DTE or DCE)
frame-relay interface-dlci <DLCI>	**Hdlc interface**	Creates the PVC with the specified DLCI
frame-relay keep alive <TIME>	**Hdlc interface**	Sets the indicated parameter
frame-relay lmi-t391 <TIME>	**Hdlc interface**	Sets the indicated parameter
frame-relay lmi-t392 <TIME>	**Hdlc interface**	Sets the indicated parameter
frame-relay lmi-n391 <TIME>	**Hdlc interface**	Sets the indicated parameter
frame-relay lmi-n392 <TIME>	**Hdlc interface**	Sets the indicated parameter

Table 10 – Zebra Commands for the Frame-Relay protocol

Note: Placing **"no"** in front of the DATACOM commands, causes Zebra to configure the default values.

It is not necessary to key in the full command name. After keying in the first characters, so as Zebra can unequivocally distinguish the desired command, it is automatically understood.

Defaults:

Timer	Default
t391	10
t392	15
n391	6
n392	3
n393	4

Example:

To change the equipment IP number, it is necessary to perform the following steps:

Command	Description
Enable	Enables access to the Privileged mode
conf t	Enables access to the Configuration mode
Inter eth0	Enables access to the DmSTM-1 interface Ethernet mode
no ip address AAA.BBB.CCC.DDD/M	Removes the IP number AAA.BBB.CCC.DDD. it is always necessary to remover the ip address before configuring a new one
ip address AAA.BBB.CCC.DDD/M	Inserts a new user-defined IP number
wr mem	Writes the new configuration into non-volatile memory
End	Takes back to the Privileged mode
Exit	Gets out of the Initial mode and ends Zebra access

To visualise the equipment configured IP number it is necessary to do the following steps:

Command	Description
show interface	Displays the equipment interfaces configuration list – eth0 is the DmSTM-1 Ethernet interface port

Note: Do not try to change the IP number of the interface being used to configure the equipment. After executing the **no ip address AAA.BBB.CCC.DDD/M** command, the interface loses the address and the user that is performing the configuration is disconnected. That means it is not possible to change the Ethernet interface IP address by the telnet.

8 FIRMWARE UPDATE

8.1. How to identify the present Firmware version

To identify your equipment version, from the bayface equipment interface go to the Fault -> Device Information menu, General guide. If it is necessary to install a newer firmware version, follow the procedure described at the item below.

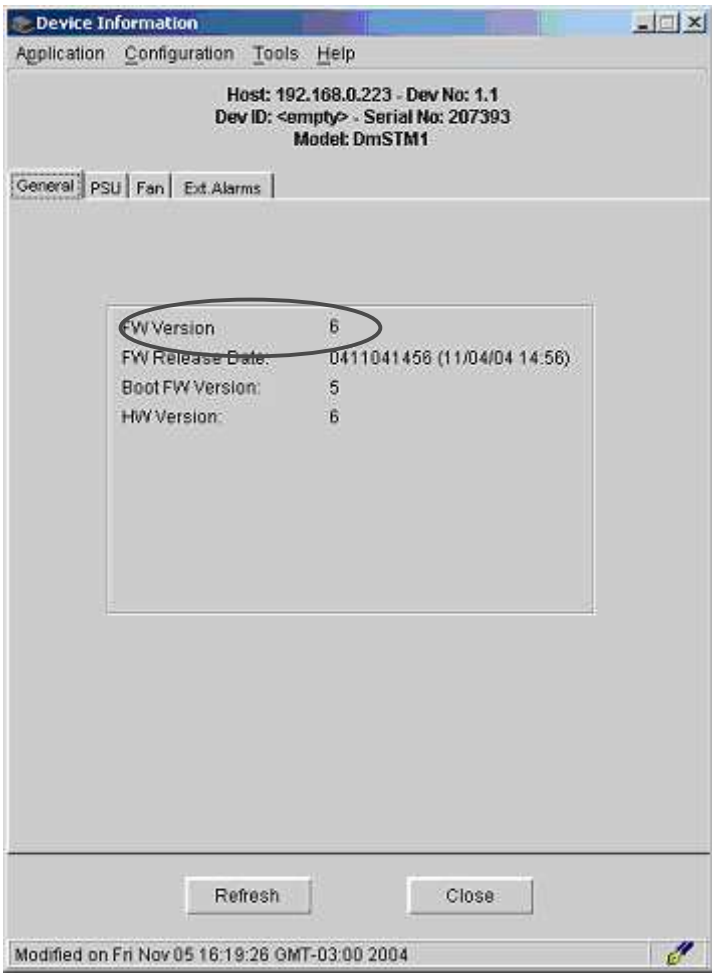


Figure 69 – Device Information

8.2. Firmware Update

To perform the firmware download, at first the user must get the file containing the desired firmware version. The files normally have the extension ".im ".

After getting the file, follow the instructions below to perform the download.

From the equipment bayface or from the Network Browser go to the Tools -> Firmware Update -> Firmware Update menu.

1) In the Model field, select the equipment model. Every equipment of this type that is present in the DmView database will be listed under Current Devices.

2) Using the Browse... button, find the file containing the new firmware, which will become visible in the File field after it is selected.

3) In the Current Devices field, choose one or more equipments for which the firmware will be sent, respecting the preset limit in the Max. Simult. Uploads field.

4) Click the Send FW to Selected Devices... button to start the download. In the Log field it is possible to follow the updating process status. At the end of this updating it is possible to save this log, which will indicate success or failure in the operation.

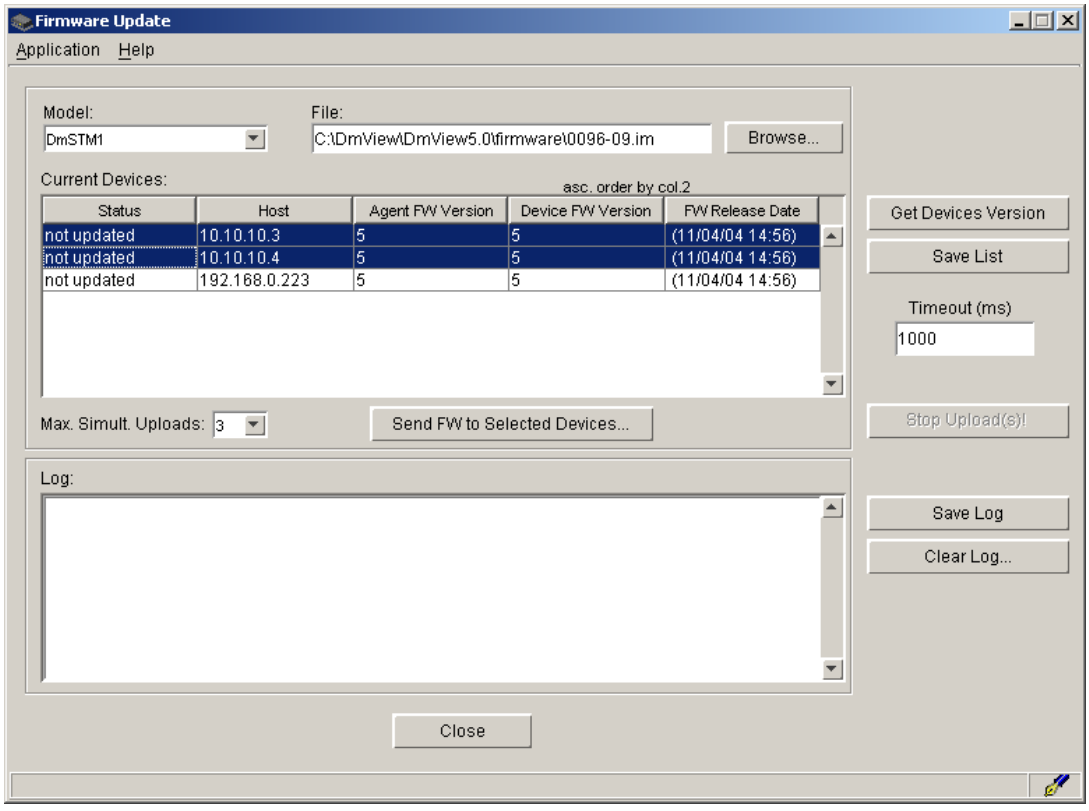


Figure 70 – Firmware Update

8.3. Important Notes

8.3.1. Boot Parameters

The boot parameters must be correctly configured, especially if the update is done by the “In Band” process. If there is no TFTP server IP and if there is any failure in the update process, it will not be possible to recover the previous firmware image, thus requiring local intervention.

If local intervention is needed, the user must connect a TFTP server to the DmSTM-1 Ethernet port. The user must have previously configured in the equipment boot parameters both the TFTP server IP and the filename to be used. Recovering is automatically done.

8.3.2. Power failure

During the update, there must be no power failure until the equipment is restarted, so as to validate the new firmware. In case of power loss, the equipment will try to recover its firmware from a TFTP server. If it can’t find it, local intervention will be necessary.

8.3.3. Failure in Ring-installed Equipment

If there is a firmware update failure at an equipment that is inserted in a ring without an Ethernet port connection, the recovery must be performed locally.

8.3.4. Data traffic interruption

According to the firmware version that is being installed on the equipment and to the present firmware version, there can be data traffic interruption for up to three minutes.

DATACOM

Phone: (51) 3358-0100
Support: (51) 3358-0122
Fax: (51) 3358-0101
http://www.datacom-telematica.com.br/