BlackBox ETHERLINK IV

RACKCARD (RC) DEVICES

TECHNICAL DESCRIPTION AND OPERATIONS MANUAL

Version	1.14
Document name	_SAUM_BB_ETHERLINK_IV_RC_V1-1_20104APR02
Revision	10.FEB 2017

© Copyright 2017 by BlackBox GmbH. The content of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of BlackBox GmbH. Published by BlackBox GmbH. All rights reserved.

VERSION CONTROL

Manual Version	Date	Software Version	Major changes to previous version
1.0	02.11.2009	1.0.0	Initial Version
1.1	15.12.2009	1.0.0	Ethernet LED table corrected, Page 32 DB15 to 2xRJ45 adapter included, Page 89 Wetting Current Supply Jumper corrected, Page 12
1.2	19.8.2010	1.2.3	Nx64 added
1.3	27.9.2010	1.2.5	Cable corrected N21-DCE/N35-DCE, Page 96-97 Update remote power configuration, Page 13
1.4	03.01.2011	1.2.15	RSTP added
1.5	29.08.2011	1.4.8	WEB interface added, Software commands updated
1.6	27.03.2012	1.4.8	Alarm Connector corrected, Alarm Command updated, RS-485 Connector added
1.7	03.12.2012	1.4.37	Status Ext changed, Commands adapted, MAC Filtering, 4xRS-232 Connector
1.8	07.05.2013	1.4.38	MIB's adapted, WEB Interface, G.703 Interface included
1.9	22.10.2013	1.5.4	Connector 4xRS-232 corrected. SSH & RADIUS added.
1.10	24.06.2014	1.6.6	SNMP& RADIUS updated, Commands updated incl. SD-Card
1.11	15.08.2014	1.6.6	2xRS485/422/232 interface card included
1.12	09.07.2015	1.6.19	LLDP chapter included
1.13	11.02.2016	1.7.2	802.1x included 4I4O daughter card included
1.14	10.02.2017	1.7.5	RADIUS Server setup with defined Service-Type Attribute RFC-4133 Entity-MIB partially supported RTS-CTS | DTR-DCD or RTS-DCD | DTR-CTS trigger for RSIP Rate example improved for IRATE, CRATE, ERATE commands RSTP commands improved

SAFETY REGULATIONS

IF THE UNIT IS NOT USED IN ACCORDANCE TO REGULATIONS DESCRIBED AND DEFINED IN THE CHAPTERS "TECHNICAL DESCRIPTION" AND "TECHNICAL SPECIFICATIONS", BLACKBOX GMBH REFUSES TO TAKE ANY RESPONSIBILITY. FURTHERMORE, NO WARRANTY IS GRANTED IN SUCH CASE!

IT'S ONLY ALLOWED TO USE EXTERNAL POWER SUPPLYS THAT ARE APPROVED ACOORDING TO THE SAFETY STANDARD IEC/EN 60950-1.

IT'S ONLY ALLOWED TO USE THE UNITS WITH HOUSINGS SUPPLYED FROM BLACKBOX GMBH (SUBRACKS, MINIRACK, SA-DESKTOP-X). THE RACK MUST BE CONNECTED PERMANENTLY TO A RELIABLE PROTECTIVE ERTH CONDUCTOR. THE LTU UNIT MUST BE FIXED TO THE RACK PERMANENTLY WITH THE TWO PANEL SCREWS.

INCORRECT USE OF THIS DEVICE, USE IN ANY OTHER ENVIRONMENT AND/OR HOUSING THAN PROVIDED BY BLACKBOX MIGHT LEAD TO HARMFUL CONDITIONS. FAILURE TO FOLLOW THESE PRECAUTIONS MAY RESULT IN DEATH, SEVERE INJURY OR PROPERTY DAMAGE.

Please read this manual carefully before operating the system.
Installation of this equipment must be done by **qualified** personnel only.

EU DIRECTIVE 2002/96/EC AND EN50419

Our equipment is marked with the recycling symbol. It means that at the end of the life of the equipment you must dispose it separately at an appropriate collection point and not place it in the normal domestic unsorted waste stream. (European Union only)

1 SELECTION GUIDE

BlackBox Etherlink_IV RC SHDSL Overview

Etherlink IV - RackCard -Models	Standalone	Rail Mounting	Subrack Module	Protected Housing	Single Pair	Dual Pair Bonding	Triple Pair Bonding	Quadruple Pair Bonding	Point-to-Point	Point-to-Multipoint	E1 (120Ohm)	E1 (75Ohm) optional	Ethernet Bridge	Ethernet Add/Drop	Nx64kbps Interface	E1 Cross Connect	Remote Power Receiver	Remote Power Source	Console Port Management	Telnet Management	Web Management	SNMP Management
SA-RC-Etherlink_IV-2E1-DSL-4ETH	*1		√		√				√		√	√	√			*2		√	√	√	√	√
SA-RC-Etherlink_IV-2E1-Nx64-DSL-4ETH	*1		√		√				√		√	√	√		√	*2		√	√	√	√	√
SA-RC-Etherlink_IV-2DSL-4E1-4ETH	*1		√		√	√			√	√	√	√	√	√		*2		√	√	√	√	√
SA-RC-Etherlink_IV-2DSL-2E1-nx64-4ETH	*1		√		√	√			√	√	√	√	√	√	√	*2		√	√	√	√	√
SA-RC-Etherlink_IV-4DSL-4E1-4ETH	*1		√		√	√	√	√	√	√	√	√	√	√		*2		√	√	√	√	√
SA-RC-Etherlink_IV-4DSL-4ETH	*1		√		√	√	√	√	√	√			√	√					√	√	√	√
SA-RC-Etherlink_IV-4DSL-2nx64-4ETH	*1		√		√	√	√	√	√	√			√	√	√				√	√	√	√

*1 Yes, if you use SA-DESK-TOP-1

*2 Not yet supported, future development

Attention: The models with Nx64 (N64) could be mounted with V.24 (V24), RS-485 (485), G.703 or E0 (703), or 4I4O or any other future interfaces

2 PRECAUTION

The present document describes devices of the BlackBox Etherlink IV LTU family. The document contains the technical description of the devices, installation, configuration, and operation instructions. Appendices and installation manuals containing additional information about the system are also an integral part of the present document.

WARNING
BEFORE STARTING OPERATING THE EQUIPMENT, READ CAREFULLY THE CURRENT MANUAL AND THE INSTALLATION MANUAL. BLACKBOX GMBH REFUSES NEITHER TAKING ANY RESPONSIBILITY NOR GRANTING ANY WARRANTY TO ANY DEVICE MALFUNCTIONING OR ANY DAMAGES DUE TO FAILURE TO COMPLY WITH THE REQUIREMENTS STATED IN THE MANUALS, ESPECIALLY IN THE SECTION RELATED TO “SERVICE INSTRUCTIONS”.

WARNING
IMPROPER USE OF OUR EQUIPMENT, USE IN ANY OTHER ENVIRONMENT OR IMPROPER INSTALLATION AND MAINTENANCE MIGHT LEAD TO HARMFUL CONDITIONS. FAILURE TO FOLLOW THESE PRECAUTIONS MAY RESULT IN DEATH; SEVERE INJURY OR PROPERTY DAMAGE.
BLACKBOX GMBH REFUSES NEITHER TAKING ANY RESPONSIBILITY NOR GRANTING ANY WARRANTY IN SUCH CASE.

WARNING
ELECTRONIC MODULES CAN BE DAMAGED OR DECREASED IN RELIABILITY BY STATIC ELECTRICAL DISCHARGE. BEFORE HANDLING MODULES, WEAR AN ANTISTATIC DISCHARGE WRIST STRAP TO PREVENT DAMAGE TO ELECTRONIC COMPONENTS. PLACE MODULES IN ANTISTATIC PACKING MATERIAL WHEN TRANSPORTING OR STORING. WHEN WORKING ON MODULES, ALWAYS PLACE THEM ON AN APPROVED ANTISTATIC MAT THAT IS ELECTRICALLY GROUNDED. TO PREVENT ELECTRICAL SHOCK, DO NOT INSTALL EQUIPMENT IN A WET LOCATION OR DURING A LIGHTNING STORM.

WARNING
SOME MODULES CAN BE CONFIGURED TO HAVE REMOTE POWER. THIS MEANS, THAT THERE COULD BE A HIGH VOLTAGE ACCORDING TO EN 60950-1 SAFETY REGULATION. BE CAREFUL AND DO NOT TOUCH ANY COMPONENTS OF ANY MODULE. ALSO IN NOT POWERED STATUS, SOME CAPACITORS MAY STILL CARRY A HIGH VOLTAGE. PLEASE DO NOT TOUCH INSIDE OF ANY HOUSING (SUBRACK, MINIRACK, SA-DESK-TOP-1 OR SA-DESKTOP-4).

WARNING
THE PROTECTIVE GROUND CONNECTION MUST BE APPLIED TO THE UNIT. MAKE SURE THAT THE UNIT AND ALL EQUIPMENT CONNECTED TO IT USE THE SAME PROTECTIVE GROUND TO REDUCING NOISE INTERFERENCE AND SAFETY HAZARDS.

3 TECHNICAL DESCRIPTION

3.1 General Information about BlackBox Etherlink IV

The BlackBox **Etherlink IV SHDSL.bis Extended** product family offers a broad range of products, which are based on the latest SHDSL.bis standards (ITU-T G.991.2 & ETS TS 101 524), while also being fully interoperable with all our existing SHDSL equipment (Etherlink1 & Etherlink2). The BlackBox Etherlink IV supports TC-PAM16/32 and the new TC-PAM4/8/64/128-line coding. The support of these line codes ensures compatibility with existing SHDSL equipment that is already installed, to protect customer investments, while at the same time providing an upgrade path to the newest DSL technologies.
SHDSL.bis Extended allows symmetrical data and voice transmission at speeds up to 15.2Mbps over a single pair of copper. In addition, the BlackBox Etherlink IV modem range also supports DSL channel bonding for up to 4 copper pairs to achieve speeds to 60.8Mbps! BlackBox Etherlink IV SHDSL.bis Extended modems can provide up to 4 complete E1 interfaces, which support framed and unframed services (G.703/G.704). An integrated 2 or 4 port Ethernet layer 2 managed switch with VLAN support (10/100BaseT) ensures connectivity to IP services. Beside of E1 and Ethernet we have additional interfaces like Nx64 that can be configured to be a V.35, V.36, X.21 or V.24 (RS-232) interface by software. This makes BlackBox Etherlink IV SHDSL.bis Extended modems a perfect solution for a wide range of applications in which TDM and IP services need to be transmitted over copper wires.
Like all BlackBox Etherlink products, the Etherlink IV SHDSL.bis Extended modems family is based on industrial components and is manufactured according to highest quality standards providing additional value due to the extended temperature range and higher reliability.

The BlackBox **Etherlink IV SHDSL.bis Extended** product family consists of

LTU devices (Line Termination Units)
Usually Central Office Equipment.
LTU's can be powered from local DC power supply. (36-72VDC)
LTU's has the possibility to have an on board remote power (120/200VDC).

NTU devices (Network Termination Units)
Usually Customer Premise Equipment.
NTU's can be powered from local DC power supply.
NTU's can be powered remotely from LTU's.

RR devices (Repeater, Regenerator)
Increase (double) the distance.
RR's can be powered:

- locally with DC voltage.
- remotely from LTU's.

Supported management features:

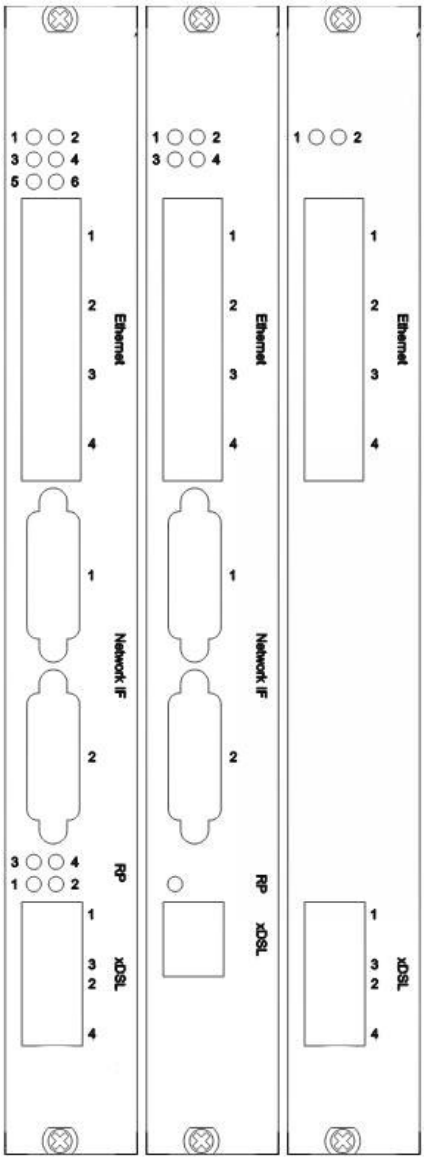
- Local Craft Terminal (RS-232), Telnet, SNMP and WEB
- Two levels of system users: administrator and user, protected with passwords

Supported operating modes:

- Multi-Service Operation, Point-to-Point, Point-to-Multipoint and Ring Applications

3.2 Description of Etherlink IV LTU Devices

Etherlink IV subrack devices represent a printed circuit board with a front panel. The following LEDs and connectors are located on the front panel of the device:



Element			Description	
1	**2**		LED: status local device	LED: status remote device
3	**4**		LED: status 1st E1 port	LED: status 2nd E1 port
5	**6**		LED: status 3rd E1 port	LED: status 4th E1 port
	1	**Ethernet**	RJ45: 1st Ethernet Interface	
	2		RJ45: 2nd Ethernet Interface	
	3		RJ45: 3rd Ethernet Interface	
	4		RJ45: 4th Ethernet Interface	
	1	**Network IF**	SA-RC-ETHERLINK_IVL-2E1B/4Eth-	DB15 (Male): 1st E1
			SA-RC-ETHERLINK_IVL-	DB15 (Male): 1st/2nd E1
			SA-RC-ETHERLINK_IV2L-4E1B/4Eth-	DB15 (Male): 1st/3rd E1
			SA-RC-ETHERLINK_IV2L-	DB15 (Male): 1st/2nd E1
			SA-RC-ETHERLINK_IV4L-4E1B/4Eth-	DB15 (Male): 1st/3rd E1
	2		SA-RC-ETHERLINK_IVL-2E1B/4Eth-	DB15 (Male): 2nd E1
			SA-RC-ETHERLINK_IVL-	HD26 (Fem.): Nx64
	2		SA-RC-ETHERLINK_IV2L-4E1B/4Eth-	DB15 (Male): 2nd/4th E1
			SA-RC-ETHERLINK_IV2L-	HD26 (Fem.): Nx64
			SA-RC-ETHERLINK_IV4L-4E1B/4Eth-	DB15 (Male): 2nd/4th E1
3	**4**	**RP**	LED: Status RP (remote power) 3rd DSL	LED: Status RP 4th DSL
1	**2**		LED: Status RP (remote power) 1st DSL	LED: Status RP 2nd DSL
	1 **3**	**SHDSL**	RJ45 con. 1st and 3rd DSL line + two LEDs	
	2 **4**		RJ45 con. 2nd and 4th DSL line + two LEDs	

A) SA-RC-ETHERLINK_IV2L-4E1B/4Eth-RP, V93 / SA-RC-ETHERLINK_IV2L-2E1B/N64/4Eth-RP, V94 / SA-RC-ETHERLINK_IV4L-4E1B/4Eth-RP, V96
B) SA-RC-ETHERLINK_IVL-2E1B/4Eth-RP, V90 / SA-RC-ETHERLINK_IVL-2E1B/N64/4Eth-RP, V91
C) SA-RC-ETHERLINK_IV4L-4Eth, V98

Table 3.1 Connectors and LEDs on the front panel of the LTU devices

3.2.1 Remote Power Supply and Wetting Current

The wetting current and remote power supply modes can be changed by jumpers and the configuration management. Despite the safe voltage on each DSL copper wire with respect to the ground (<120 Volts according to EN 60950), the use of the remote power supply must be done strictly according to the following rules:

- When working with DSL copper lines make sure that the remote power is switched off.
- The insulation of cable pairs, junctions (junction boxes, distribution frames, etc.) should be checked against the remote power voltage (norms and standards of the network)

3.2.1.1 Compatibility of Remote Power and Wetting Current Supply Modes

Devices operating in pairs should be configured for mutual operation! The mode «√» means recommended and possible.
The use of the mode «**-**» is not recommended because it may cause high power consumption, degradation of communication (communication stability), and additional safety measures.
The mode «**inc**» (incompatible) will not allow the devices to establish communication (because in this case one or both devices will be de-energized).

Remote Power and Wetting Current Supply Modes		**NTU/RR**		**LTU**			
		Power DP Distance P.	Power LP Local P.	Remote Power Supply	Wetting Current Supply	Wetting Current Consumption	No
NTU/RR	Power DP Distance Power	**inc**	**inc**	√	**inc**	**inc**	**inc**
	Power LP Local Power	**inc**	√	**-**	**-**	√	√
LTU	Remote Power Supply	√	**-**	**X**	**X**	**X**	**-**
	Wetting Current Supply	**inc**	**-**	**X**	**X**	√	**-**
	Wetting Current Consumption	**inc**	√	**X**	√	√	√
	No	**inc**	√	**-**	**-**	√	√

Table 3.2 Compatible operation of remote power supply and wetting current supply modes

WARNING
TO PREVENT THE FAILURE OF THE EQUIPMENT, THE USE OF "X" MODES IS STRICTLY PROHIBITED!

3.2.1.2 Configuration of Remote Power and Wetting Current Supply

Each LTU SHDSL channel can be configured to supply wetting current, to consume wetting current, to supply remote power or being passive. The switching between these modes is performed by setting the corresponding jumpers separately for each DSL channel of the modem and to use one configuration command in the modem software menu (POWER [OFF/ON] N).

Be aware, that you can configure up to 4 SHDSL channels at 120Volts each or up to 2 SHDSL channels at 200Volts (200Volts mode is supported for DSL-1 and DSL-2 only).

The default delivery setting for any LTU is 120VDC and 60mA. It is short circuit protected and at any failure the system will restart automatically.

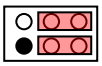
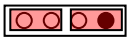
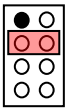
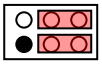
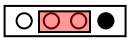
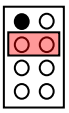
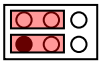
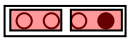
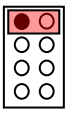
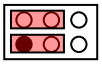
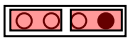
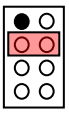
Remote Power and Wetting Current Supply Modes		Voltage		Current	Restrictions
Remote Power Source		120VDC		60, 90	
					125mA not available for 120VDC
XM60 DSL-1 XM38 DSL-2 XM65 DSL-3 XM35 DSL-4	XM52 DSL-1 XM54 DSL-2 XM51 DSL-3 XM53 DSL-4	XM42 DSL-1/2 XM50 DSL-3/4	XM47 DSL-1/2 XM48 DSL-3/4	XM55 DSL-1 XM58 DSL-2 XM56 DSL-3 XM57 DSL-4	Configuration SW: POWER [OFF/ON] N
Remote Power Source		200VDC		60, 90, 125mA	
					200VDC only, if half of the SHDSL channels are used
XM60 DSL-1 XM38 DSL-2 XM65 DSL-3 XM35 DSL-4	XM52 DSL-1 XM54 DSL-2 XM51 DSL-3 XM53 DSL-4	XM42 DSL-1 XM50 DSL-2	XM47 DSL-1 XM48 DSL-2	XM55 DSL-1 XM58 DSL-2 XM56 DSL-3 XM57 DSL-4	Configuration SW: POWER [OFF/ON] N
Wetting Current Supply		47VDC		3.5mA	
					
XM60 DSL-1 XM38 DSL-2 XM65 DSL-3 XM35 DSL-4	XM52 DSL-1 XM54 DSL-2 XM51 DSL-3 XM53 DSL-4	XM42 DSL-1/2 XM50 DSL-3/4	XM47 DSL-1/2 XM48 DSL-3/4	XM55 DSL-1 XM58 DSL-2 XM56 DSL-3 XM57 DSL-4	
Wetting Current Consumption		Termination			
					
XM60 DSL-1 XM38 DSL-2 XM65 DSL-3 XM35 DSL-4	XM52 DSL-1 XM54 DSL-2 XM51 DSL-3 XM53 DSL-4	XM42 DSL-1/2 XM50 DSL-3/4	XM47 DSL-1/2 XM48 DSL-3/4	XM55 DSL-1 XM58 DSL-2 XM56 DSL-3 XM57 DSL-4	

Table 3.3 Possible remote power and wetting current supply modes

WARNING
IN CENTRAL EUROPE IT IS STRICTLY PROHIBITED TO SETUP THE REMOTE POWER TO MORE THAN 120VDC. EXCEPTIONS WITH MORE THAN 120VDC MUST BE INSTALLED ACCORDING THE SAFETY STANDARD EN 60950.

When a dual/quad DSL channel LTU is connected to NTU/RR and LTU and the remote power feature is used, a DCL alarm may appear. In this case we recommend to remove the jumpers for the corresponding remote power channel to the LTU (XM60, XM38, XM65 or XM35).

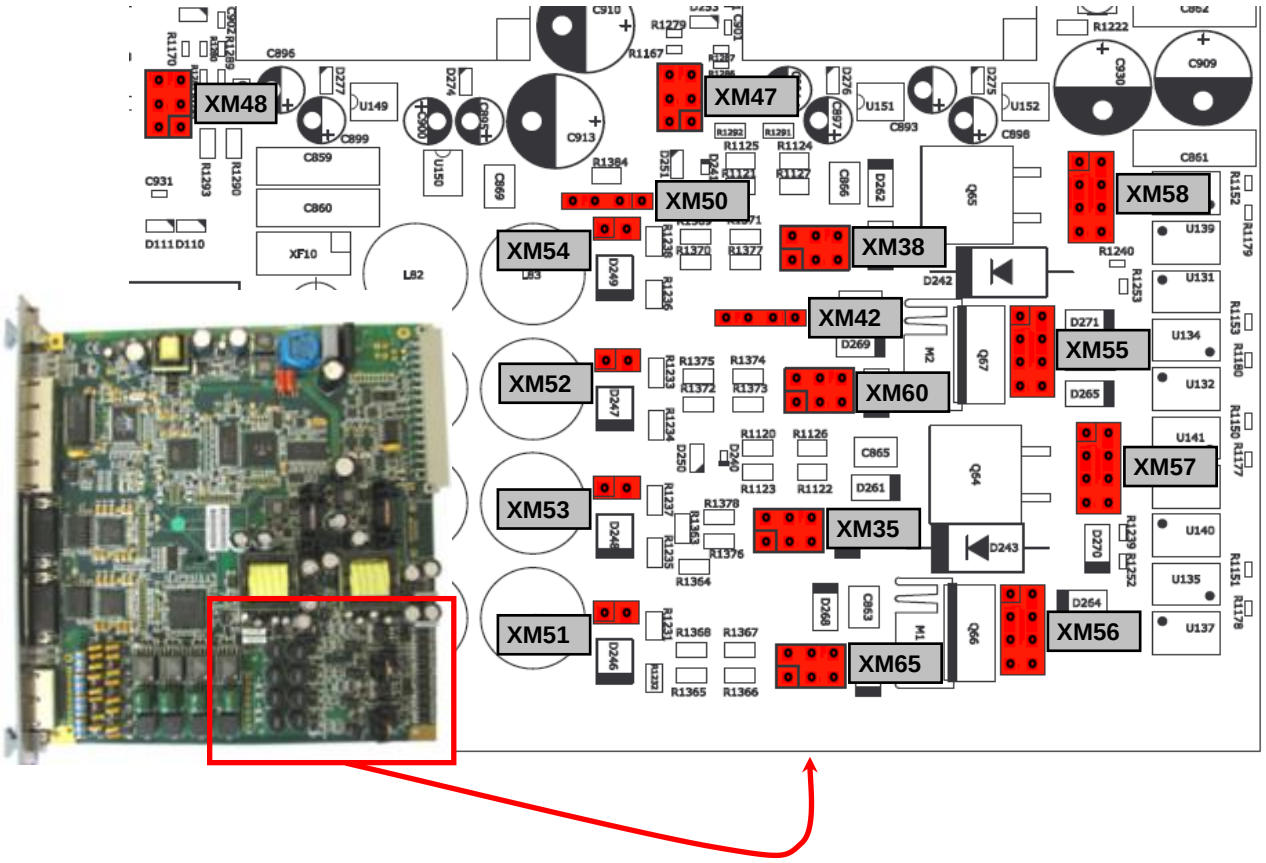


Figure 3.1 Remote power jumper location

In the following two figures two main applications are showed for clarifying the description about remote power modes.

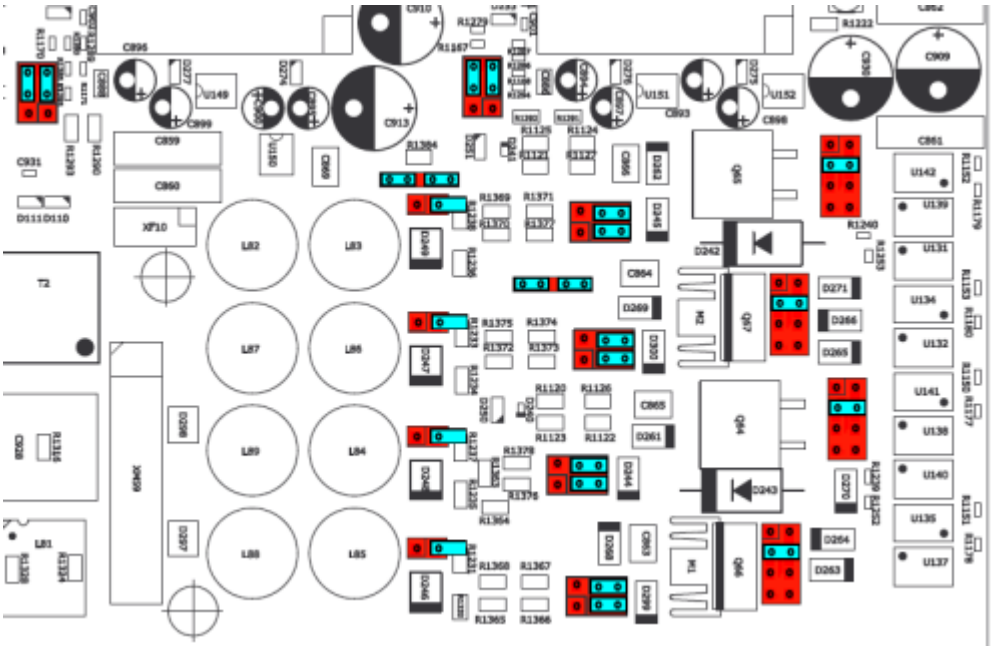


Figure 3.2 Example 120Volts, 60mA

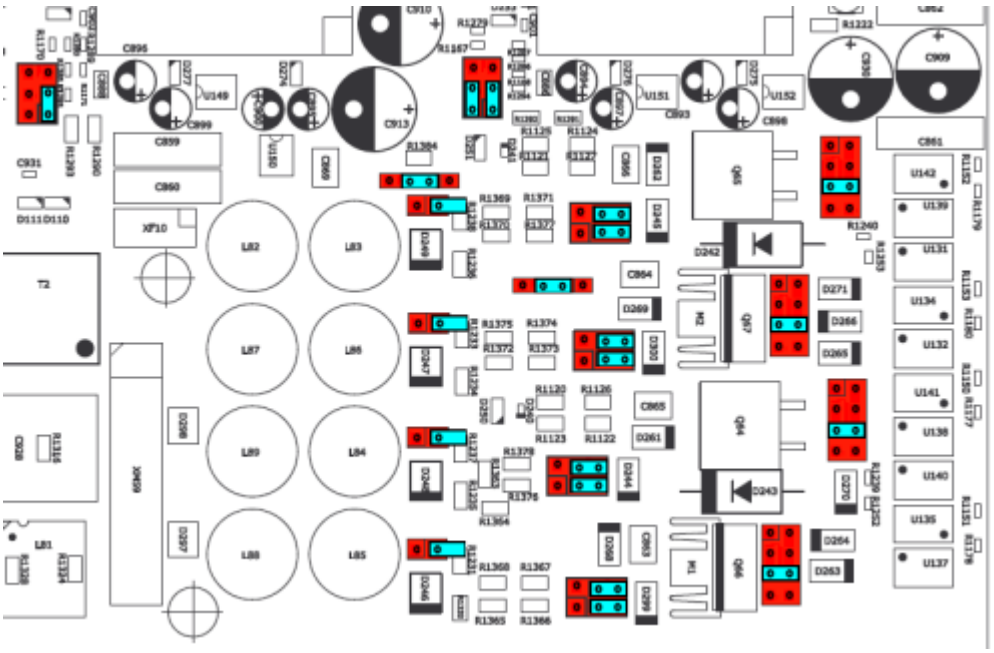


Figure 3.3 Example 200 Volts, 90mA

3.2.2 Description of Etherlink IV Interfaces

3.2.2.1 SHDSL Interface

The Etherlink IV devices are available with 1, 2 or 4 SHDSL interfaces. The interfaces can operate fully independent of each other as well as they can be combined to operate in multipair mode. Therefore all independent SHDSL interfaces and groups of SHDSL interfaces (multipair mode) can

be configured separately from each other. The multipair mode, the reservation mode and the automatic configuration detection mode naturally limit the independent working.
All SHDSL interfaces support plesiochronous data transmission. It means that reference clock frequencies, which are used to clock data transmission, are transmitted together with the data in different directions of one SHDSL link. The clock frequencies of different SHDSL channels are completely independent if they do not operate in the multipair mode.
An SHDSL channel working in the independent mode can simultaneously transmit one or several E1 streams and one WAN stream. This transmission is plesiochronous. All E1 streams received by one SHDSL interface should use the same clock frequency in one direction.

Mode	Coding Type	Baserate	Transmission Data Rate	Standard
Master/Slave Fix Configuration	PAM16	3..60	Baserate* 64 Kbit/s	Annex A, Annex B, Annex AB (autodetection)
	PAM32	12..89		
Master Autodetection	PAM16	Auto (3..60)		Annex AB (autodetection)
	PAM32	Auto (12..89)		
Slave Autodetection	Auto (PAM16/32)	Auto (3..89)		Annex AB (autodetection)

Table 3.4 Line settings per SHDSL interface, single pair

3.2.2.1.1 Master/Slave

To establish a connection, it is necessary that one transceiver side is configured as Master and the other as Slave. In this case, the connection is controlled by the Master device.

3.2.2.1.2 Multipair Mode

If 2, 3 or 4 SHDSL channels are configured to operate in the multipair mode, they work at the same clock frequency and line rate like one SHDSL channel with doubled, tripled or quadrupled transmission capacity. Similarly to the independent channel, such a combined channel can simultaneously transmit one or several E1 streams and one WAN stream. This transmission is also plesiochronous. All E1 streams that are transmitted over one SHDSL interface should use the same clock frequency per direction.
In multipair mode, one SHDSL channel serves as a “master” channel, while the other SHDSL channels serve as “slave” channels. If the link in one channel fails, links in all other channels break too and the procedure of connection/activation restarts.
The four-channel modems provide a possibility to organize pair-wise channels, i.e., these two two-pair links will operate independently from each other.
The main application for the multipair mode is the increasing of the transmission range. In this case, some channels operate at low transmission rates. In multipair mode some limitations are imposed on the Baserate parameter.

Mode	Coding Type	Baserate	Transmission Data Rate	Standard
2-pair, Master/Slave Fix Configuration	PAM16	3..60	2*Baserate* 64 Kbit/s	Annex A, Annex B, Annex AB (autodetection)
	PAM32	12..89		
2-pair, Master Autodetection	PAM16	Auto (3..60)		Annex AB (autodetection)
	PAM32	Auto (12..89)		
2-pair, Slave Autodetection	Auto (PAM16/32)	Auto (3..89)		Annex AB (autodetection)
3-pair, Master/Slave	PAM16	3..60		Annex A, Annex B,

Fix Configuration	PAM32	12..85	3*Baserate* 64 Kbit/s	Annex AB (autodetection)
3-pair, Master Autodetection	PAM16	Auto (3..60)		Annex AB (autodetection)
	PAM32	Auto (12..85)		
3-pair, Slave Autodetection	Auto (PAM16/32)	Auto (3..85)		Annex AB (autodetection)
4-pair, Master/Slave Fix Configuration	PAM16	3..60	4*Baserate* 64 Kbit/s	Annex A, Annex B, Annex AB (autodetection)
	PAM32	12..64		
4-pair, Master Autodetection	PAM16	Auto (3..60)		Annex AB (autodetection)
	PAM32	Auto (12..64)		
4-pair, Slave Autodetection	Auto (PAM16/32)	Auto (3..64)		Annex AB (autodetection)

Table 3.5 Line settings per SHDSL interface, multipair mode.

The next figure shows an example of an Etherlink IV device working in four-pair operation mode (the <MULTIPAIR> command is used to configure multipair operation mode). Four SHDSL channels are combined into one group. Through this multipair channel one E1 stream and Ethernet packets are transmitted. This mode allows increasing the transmission range, compared to the use of only one single SHDSL channel, because the data rate of each SHDSL channel is lower (the advantage in the transmission range will depend on the cable parameters and noise immunity).

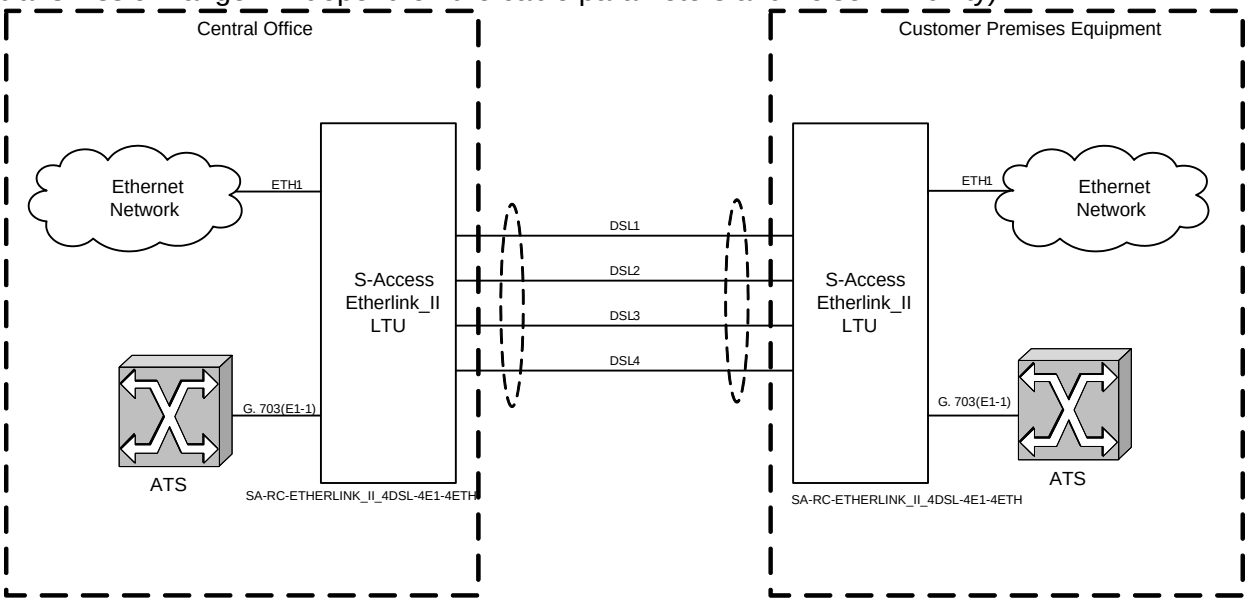


Figure 3.4 Example of four-pair multipair data transmission

3.2.2.1.3 Reservation Mode

Reservation is provisioned for 2- and 4-channel BlackBox Etherlink IV devices. The main task of reservation is to transmit the most important data even in the case of the failure of one or several SHDSL connections. Reservation also takes care about an efficient bandwidth usage over all SHDSL channels like the normal transmission modes.
Reservation will not guarantee a continuous transmission of important data in the case of a failure. When one or several DSL connections fail, a sort-term loss of Ethernet packet and E1 data can occur.
SHDSL channels with successive numbers (example: DSL-1, DSL-2 or DSL-2, DSL-3, DSL-4) are merged into a group of channels with reservation. For these merged channels, the traffic in the SHDSL channels with the lowest numbers has higher priority than the traffic with higher numbers.

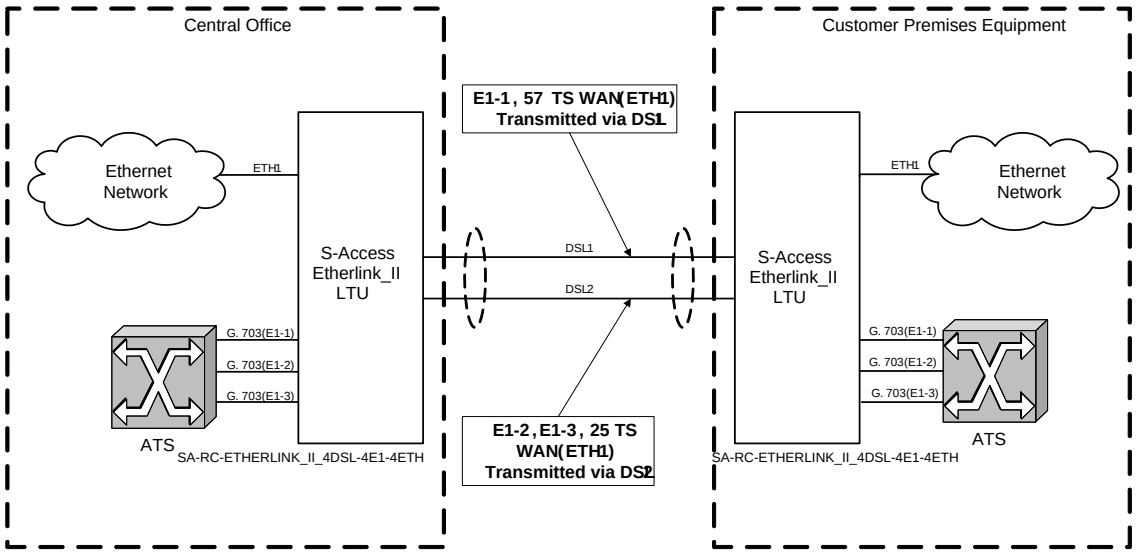
For example, DSL-1 has a higher priority than DSL-2, and DSL-2 has a higher priority than DSL-3. If the communication in one or several SHDSL channels inside the reservation group is broken, remaining working channels transmit the data of the failed high-priority channels. At any failure the system always operates as if the low-priority channels failed.
Consider the reservation with two channels: DSL-1 and DSL-2 (DSL-1 has a higher priority compared to DSL-2). If the DSL-2 channel fails, the DSL-1 channel continues to operate without any changes. If the DSL-1 channel fails, the DSL- 2 channel transmits the data of the DSL- 1 channel. Hence, the DSL-1 channel should transmit the high-priority data.
If the substitute channel has a lower transmission capacity than the main channel, the transmitted data will be decreased. First, the volume of WAN data will be decreased up to 1 timeslot (TS, 64kbit/s), and then, the number of transmitted E1 timeslots will be decreased. If multiple E1 streams are transmitted, the streams at the end of the list will be decreased (if E1-1, E1-2 are in the list, the E1-2 stream will be deleted). First, timeslots with large numbers are deleted. However, there is an exception for TS 16, which, if transmitted, will be deleted before or after TS 0.

Mode	Normal Mode		Reserve Mode DSL-2 down		Reserve Mode DSL-1 down	
	DSL-1	DSL-2	DSL-1	DSL-2	DSL-1	DSL-2
DSL-1: Baserate 72 DSL-2: Baserate 61 Total	E1-1 40 TS WAN E1-1, E1-2 69 TS WAN	E1-2 29 TS WAN	E1-1 40 TS WAN E1-1 40 TS WAN	Failure	Failure E1-1 29 TS WAN	E1-1 29 TS WAN
DSL-1: Baserate 72 DSL-2: Baserate 61 Total	E1-1, E1-2 8 TS WAN E1-1, E1-2 69 TS WAN	61 TS WAN	E1-1, E1-2 8 TS WAN E1-1, E1-2 8 TS WAN	Failure	Failure E1-1, 28 TS E-12 1 TS WAN	E1-1 28 TS E1-2 1 TS WAN
DSL-1: Baserate 72 DSL-2: Baserate 61 Total	72 TS WAN E1-1 101 TS WAN	E1-1 29 TS WAN	72 TS WAN 72 TS WAN	Failure	Failure 61 TS WAN	61 TS WAN
DSL-1: Baserate 89 DSL-2: Baserate 89 Total	E1-1 57 TS WAN E1-1, E1-2, E1-3 82 TS WAN	E1-2, E1-3 25 TS WAN	E1-1 57 TS WAN E1-1 57 TS WAN	Failure	Failure E1-1 57 TS WAN	E1-1 57 TS WAN

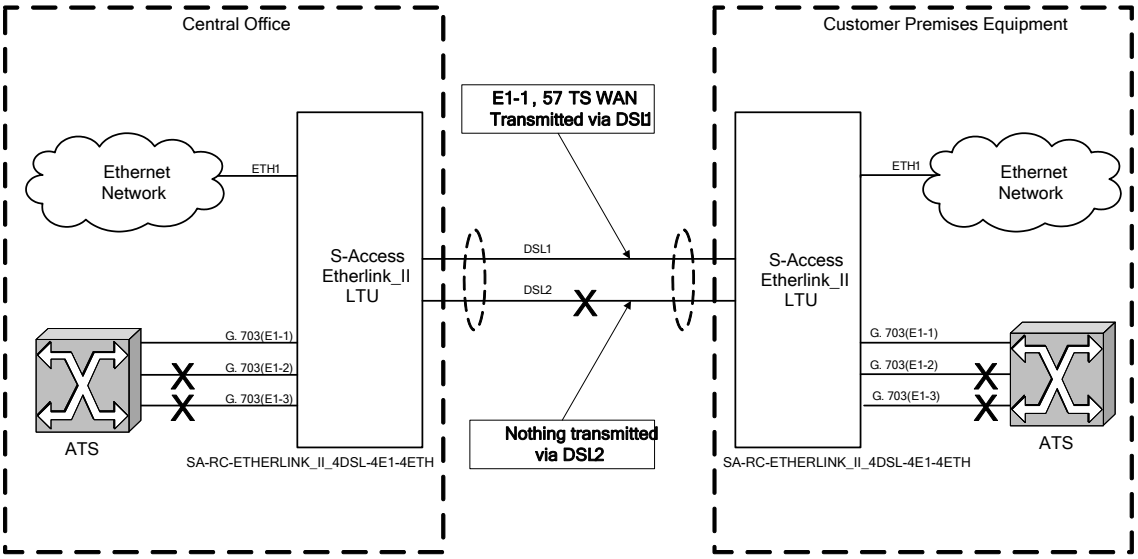
Table 3.6 Examples of reservation with two channels

The following pictures illustrate the last example in the previous table with reservation of two channels (The <RESERVE> command is used to configure reservation).

Normal Mode



DSL1 Up, DSL2 Down



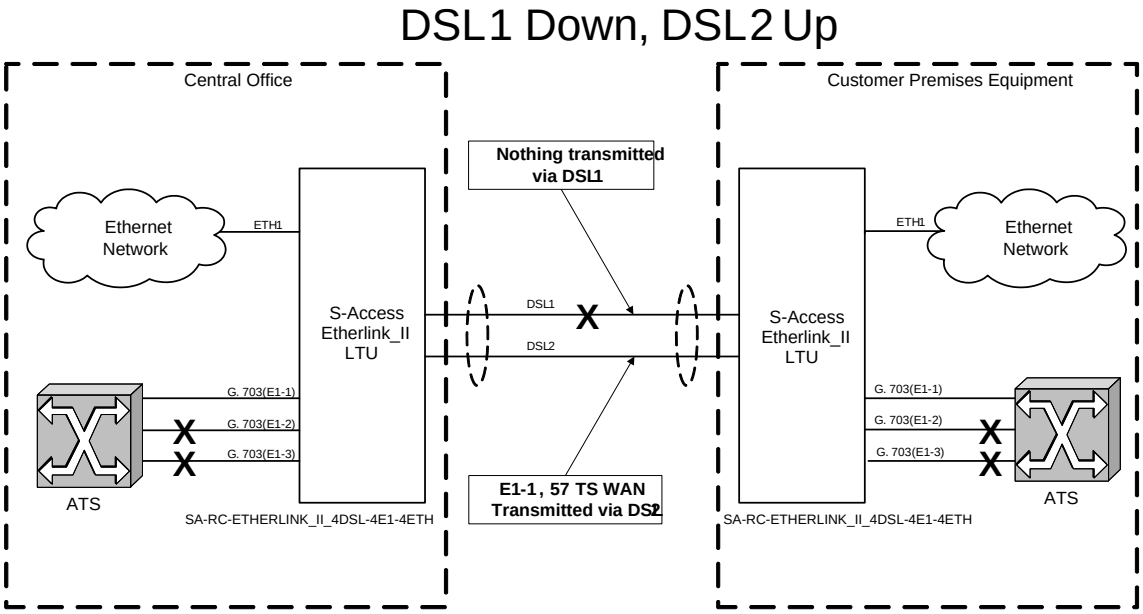


Figure 3.5 Example of reservation

While for a two SHDSL channels system in case of a failure the substitution of channels is “trivial”, in three and four SHDSL channels system different variants are possible. However, any system using the reservation mode follows a strict logic in channel substitution. The next table illustrates the logic of channel reservation with 2/3/4 SHDSL interfaces.
The table for four DSL channels is constructed based on the assumption that communication in one channel is lost frequently, while communication in two channels occurs less frequently. Usually a loss of communication occurs successively, i.e., the first channel fails and then the next channel fails. The logic and rules for channel substitution are made to minimize the number of channel switching (especially high-priority channels) to minimize the data losses.

DSL1	DSL2	DSL1	DSL2	DSL3	DSL1	DSL2	DSL3	DSL4
1	2	1	2	3	1	2	3	4
1	Down	1	2	Down	1	2	3	Down
Down	1	1	Down	2	1	2	Down	3
		1	Down	Down	Down	2	Down	Down
		Down	2	1	1	Down	3	2
		Down	1	Down	1	Down	2	Down
		Down	Down	1	1	Down	Down	2
					1	Down	Down	Down
					Down	2	3	1
					Down	2	1	Down
					Down	2	Down	1
					Down	1	Down	Down
					Down	Down	2	1
					Down	Down	1	Down
					Down	Down	Down	1

Table 3.7 Examples of reservation of systems with two, three and four SHDSL channels

3.2.2.1.4 Automatic Configuration of a Link

BlackBox Etherlink IV devices support to configure the complete link in accordance with the Master-Modem configuration. This mode is available for the following links:

- Point-to-Point single-channel or multipair links
- Point-to-Point multi-channel links with independent channels
- Star-topology multichannel links
- Point-to-Point two-channel two-pair links
- Star-topology two-pair links
- Links with regenerators

Note: Automatic configuration of link reservation is not supported.

When the automatic configuration is used, the Slave-Modems and Regenerators receive nearly all configuration parameters for DSL and all other interfaces (like E1) through the link from the Master-Modem. In a majority of cases they require just a minimum configuration, what helps not to duplicate manually the configurations to all other devices in the link. Configurations like the number of transmitted E1 timeslots over DSL, CRC4 and E1 (G703/4) modes do not have to be configured on all devices because they are received automatically through the link.
The system of automatic configuration operates the following way:

- The CP side (Slave) automatically adjusts configuration according to the stream structure received from the CO side (Master), not to cause permanent losses of user data.
- If the CP side (Slave) cannot adjust correspondingly, it displays a RCONF alarm and sends a message to the remote terminal device (Master). If configurations of terminal devices (Master and Slave) do not coincide, the RCONF alarm is displayed. RCONF means a remote urgent alarm.

The link is adjusted in the channel structure in the direction from the Master- to the Slave-Modem:

- The stream structure is configured on the Master-Modem device.
- If there is any Regenerator in the link, it receives this structure and configures itself according to it.

- Also a next Regenerator receives the structure from the previous Regenerator and performs configuration according to it.
- The Slave-Modem receives the stream structure from the last Regenerator in the link and also performs configuration
- When the Slave-Modem receives configuration, it distributes the received E1 streams information to its E1 ports. If the number of ports is not enough, it displays the RCONF alarm and does not change the configuration of the E1 streams. Also if the E1 streams are not distributed, the Slave-Modem receives the configurations of WAN. Therefore, the integrity of the Ethernet link is supported.

The RCONF alarm (displayed by the <ALARM> command) means that the local and remote equipment have incompatible configurations.

- The RCONF alarm is automatically not displayed if a DSL link, in which it was detected, fails.
- If the device operates in the CA mode (automatic configuration of a link), the alarm is not displayed when the device finally adjusts to the CO side (Master).

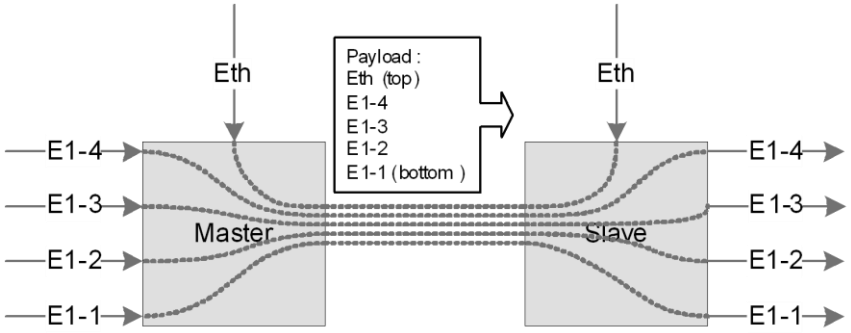


Figure. 3.6 Automatic configuration, 4x E1 and Ethernet are transmitted over one SHDSL link

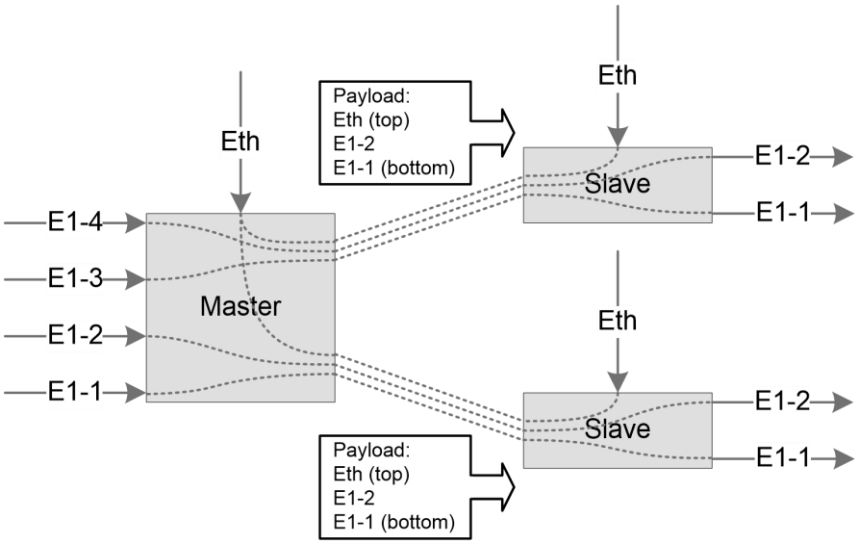


Figure 3.7 Automatic configuration Star-topology

A more complex case is the independent two-channel connection: two E1 streams and Ethernet packets are transmitted in the first channel and the second channel. The Slave-Modem determines the order of E1 interfaces for the streams from each DSL link only when the communication in both links is established.

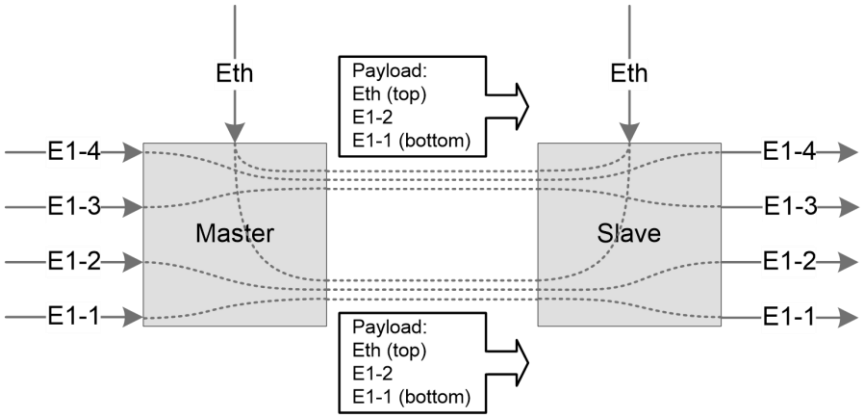


Figure. 3.8 Automatic configuration 2x E1 and Ethernet are transmitted over two SHDSL link.

3.2.2.2 E1 Interface (G.703/704)

3.2.2.2.1 Framed and Unframed E1

The Etherlink IV product family supports transmission of framed and unframed E1 interfaces.
In unframed (transparent) mode, the E1 data is transmitted over the SHDSL without any changes.
In framed mode (framing according to ITU-T G.704), the E1 data is processed by the onboard E1 framer. In this case, 1-32 timeslots per E1 stream can be transmitted over the SHDSL line.

3.2.2.2.2 CRC4 (Cyclic Redundancy Check)

The CRC4 mode enables the error performance monitoring of the E1 network interface with the help of a cyclic redundancy check.
If the mode is enabled, the modem synchronizes with CRC4 sub-multiframes at the E1 output and displays information about CRC errors. In this case the modem regenerates E1 CRC4 sub-multiframes and checksum words in the outgoing E1 stream.
If the mode is disabled, the modem transmits transparently CRC4 sub-multiframes and checksum words if the generation of the zero time slot is not activated. If the TS0GEN mode is activated, the zero time slot is generated without CRC4 sub-multiframes and checksum words.

3.2.2.2.3 AIS Generation (Alarm Indication Signal)

If this mode is enabled, AIS will be transmitted to the E1 side under the following conditions:

- the loss of the line signal from the remote device or loss of frame alignment on the DSL side
- the remote device receives an AIS over E1 interface, which is configured to transmit data from E1 to DSL. This mode is enabled only if the AIS detection mode is enabled on the remote device (see below). If multiple E1 streams are transmitted the AIS generation and detection are independent per E1 stream.

WARNING
IF THE AIS GENERATION MODE IS DISABLED, THE SIGNAL AT THE OUTPUT OF THE E1 INTERFACE WILL BE ABSENT WHEN LOSING COMMUNICATION IN THE DSL LINE (EXCEPT FOR TIME SLOTS OF THIS INTERFACE DEDICATED TO CARRY ETHERNET DATA)
IF SOME TIMESLOTS OF AN E1 INTERFACE ARE USED TO TRANSMIT ETHERNET DATA, AIS WILL NOT BE GENERATED FOR THIS INTERFACE.

3.2.2.2.4 AIS Detection

If this mode is enabled, the reception of an AIS through the E1 interface will cause the following:

- a non-urgent alarm will appear
- AIS will be transmitted to the remote device of the DSL

WARNING
IT IS RECOMMENDED TO ENABLE THE AIS DETECTION AND AIS GENERATION MODES FOR ALL E1 NETWORK INTERFACES.

3.2.2.2.5 E1 Clock Modes

The Etherlink IV product family has different possibilities to synchronize E1 interfaces. Usually the E1 interface takes the E1-clock from the E1-input and transmits it through the SHDSL link to the E1-output (plesiochronous). But we also support external clocking, internal clocking and clocking priorities.

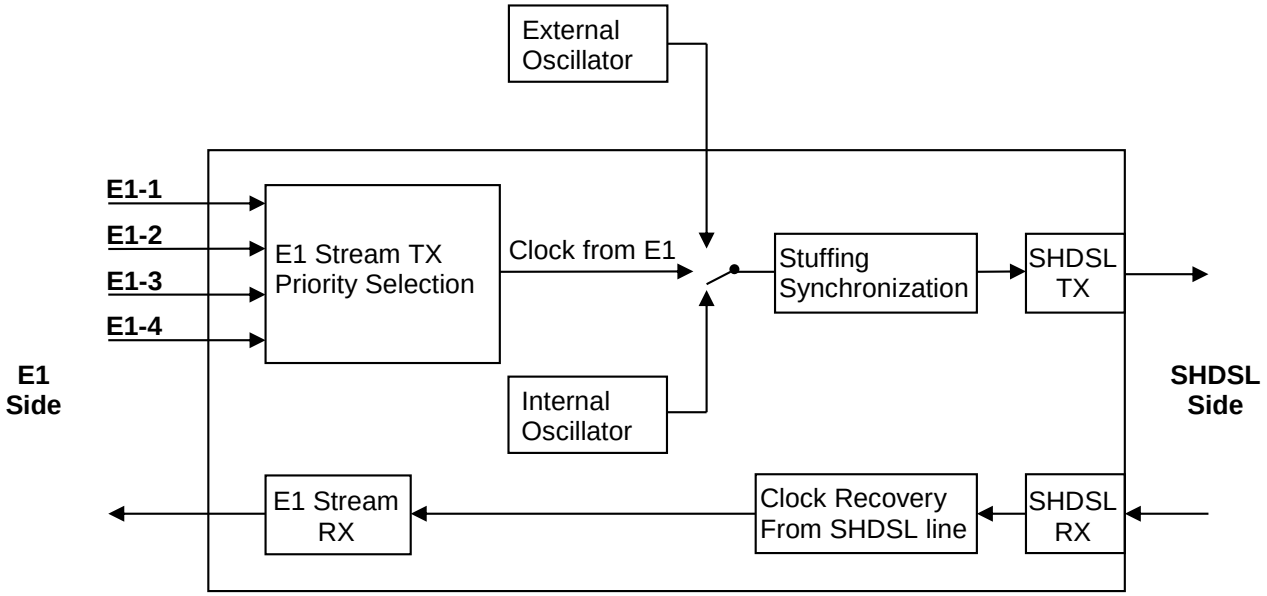


Figure 3.9. E1 clock modes

From E1 network interface side to SHDSL line side the following clock sources can serve as reference timing signals:

1. External clock generator (**EXTERNAL**) (inside subrack/minirack/SA-DESKTOP-4).
2. Clocking from the first E1 input stream (**E1-1**) (if available).
3. Clocking from the second E1 input stream (**E1-2**) (if available).
4. Clocking from the third E1 input stream (**E1-3**) (if available).
5. Clocking from the forth E1 input stream (**E1-4**) (if available).
6. Clocking from the internal generator (**INTERNAL**).

With the **SETCLOCK** command, the user can configure the priority levels for the clock sources. The device automatically switches to the clock source with the highest priority under conditions that synchronization in this mode is possible.
EXTERNAL means a synchronization from an external clock generator corresponding to the recommendation ITU-T G.703.10. If the input signal of the external clock is lost, the device switches to another clock source according the priority level. Using the external clock in synchronization

priorities, this external clock should have the highest priority. If the external clock generator is absent, it should not be included in the priority list.
E1-1, E1-2, E1-3 and E1-4 mean synchronization from one of the input E1 stream. If the E1 stream, which serves as a clock, is lost, the device switches to another clock according to the priority level.
INTERNAL means synchronization from an internal clock source. This clock source should be the last one in the priority list (but in the absence of any other clock source, for example, when only Ethernet data are transmitted, this source can be the primary and the only one).
Switching between clock sources occurs within 100 ms, after loosing synchronization.

3.2.2.3 Nx64, RS-232/RS-485 and G.703/E0 Interfaces

The Etherlink IV product family can be equipped with a wide range of modular and exchangeable daughtercards with different interfaces. In this manual we describe the most important three cards. The first card supports Nx64 interfaces (V.35, V.36, X.21, V.28), the second card supports asynchronous RS-232 interfaces, the third supports asynchronous RS-485 and the fourth supports a codirectional G.703/E0 (64 kbps) interface.
Nx64 interfaces:

- V.35, Speed 64…8192 kbps
- V.36 (with termination), Speed 64…8192 kbps
- X.21 (with termination), Speed 64…8192 kbps
- V.28 (synchronous), Speed 64…192 kbps

Interface type is cable selected. You can use the command EXTRATE [N] (N=1…128) to set the data rate (N*64 kbps).
RS-232 interface:

- RS-232, Speed 75, 1200-230400 bps
- number of data bits: 5…8
- number of stop bits:1, 1.5 or 2
- parity: odd/even/odd/mark/space

You can use the command EXTRATE [N] to set the baud rate (N is baud rate, for instance 9600). The command RSFORMAT [format] is used to set the data format (example of format: 8N1).
RS-485 interface:

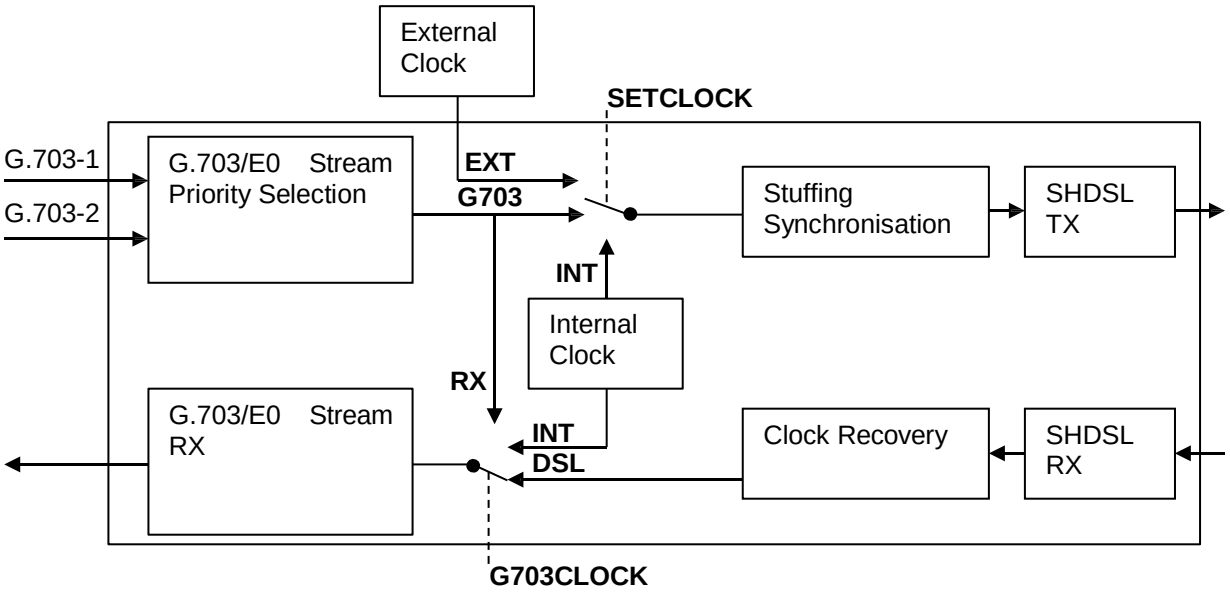
- RS485, Speed 75, 1200-230400 bps
- number of data bits: 5…8
- number of stop bits:1, 1.5 or 2
- parity: odd/even/odd/mark/space

You can use the command EXTRATE [N] to set the baud rate (N is baud rate, for instance 9600). The command RSFORMAT [format] is used to set the data format (example of format: 8N1). The RS485 interface supports half- and full-duplex operation configurable by the command RSDUPLEX [F/H].
G3/E0 codirectional 64 kbps interface:

- G.703/E0, Speed 64 kbps
- Range 500 m

There are different possibilities to synchronize the G.703/E0 64 kbps codirectional interface. Usually this interface takes the clock from the G.703/E0 input signal and transmits it through the SHDSL link

to the G.703/E0 output signal. For that reason you can use the command SETCLOCK to select the G.703/E0 clock as SHDSL clock source. But we also support external clocking, internal clocking and clocking priorities. With the command G703CLOCK you select the reference clock for the outgoing data



.
Figure 3.10. G.703/E0 clock modes

3.2.2.3.1 Nx64 Clocking Modes

Nx64 clocking modes can be selected by using the command EXTCLOCK [SRC] [DIR]. The SRC argument sets one of 3 possible clock modes for the transmit and receive clocks (signal number 114 (TX clock) and 115 (RX Clock)):

- NORMAL (DSL) both clocks are derived from the receiving DSL stream
- INT (internal) both clocks are generated from the internal generator signal
- TTC (external) clock for signal number 115 is derived from the terminal transmit clock input (signal number 113)

The DIR argument sets the transmit clock direction:

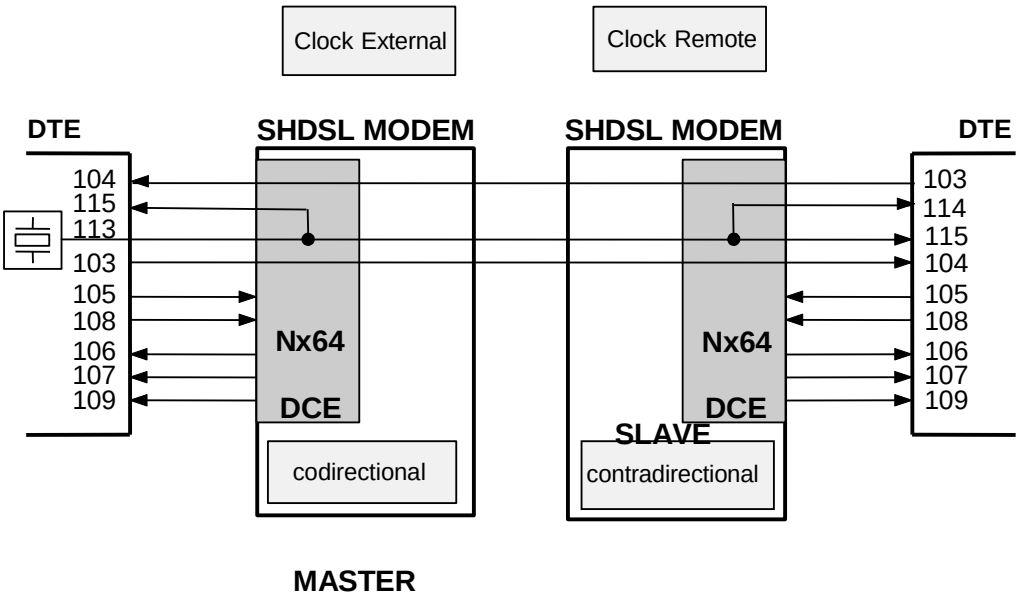
- CO (codirectional): Transmit clock and transmit data have same directions, i.e. both are inputs to the modem at signal number 113 (clock) and 103 (data). In case of RX mode (see above) the whole TX path is clocked by this clock, while in other modes data coming to TX input (signal number 103) is put into FIFO using the clock from line 113 and get out from FIFO by clock defined by SRC.
- CONTRA (contra directional): Transmit clock and transmit data have opposite directions, i.e. transmit clock is an output from the modem at signal number 114 and transmit data is an input to the modem at signal number 103.

In combination with the command SETCLOCK (units with Nx64 interface have the possibility to set the clock source to the SHDSL line side as Nx64 clock (parameter “V35” of SETCLOCK command)), it is possible to realise different clock schemes. The following table shows different valid combinations of clock modes for the Master modem:

	Command:		EXTCLOCK		SETCLOCK
	Argument:		SRC	DIR	
	Modes:	DTE Clock Mode	DCE Clock Mode	DCE Clock Direction	xDSL Clock Mode
DSL payload	Nx64 only, Nx64 * & WAN	Slave	internal	don't care	internal
		Master	external	codirectional	Nx64
	E1 & Nx64 E1 & Nx64 & WAN	Slave	DSL	don't care	E1

The following table shows different valid combinations of clock modes for Slave modem:

	Command:		EXTCLOCK		SETCLOCK
	Argument:		SRC	DIR	
	Modes:	DTE Clock Mode	DCE Clock Mode	DCE Clock Direction	xDSL Clock Mode
DSL payload	Nx64 only, Nx64 * & WAN	Slave	DSL	don't care	E1
	E1 & Nx64 E1 & Nx64 & WAN	Slave	DSL	don't care	E1



```
Interface  V35-1:V35       Interface    V35-1:V35
Extrate  : 128             Extrate  :      128
Autoloop : ON              Autoloop :      OFF
Extclock : TTC/CO          Extclock :      NORMAL/CONTRA
```

Figure 3.11. Application Example V.35 with external clock master

3.2.2.3.2 Automatic V.54 Loops

The system supports only a local V.54 loop managed by the line 141. The support of the V.54 loops is software programmable. You can use the command AUTOLOOP to adjust automatic loop reaction: Lines 140 and 142 are not supported by the system.

3.2.2.4 Input Sensor and Output Relay

BLACKBOX Etherlink IV devices can be equipped with IO module containing 4 Inputs and 4 Outputs. Input is a pair of contacts connected to current detector; if the current is present in the electric circuit the Input switches its state to "Closed". Input changes its state into "Open" if no current detected in the electric circuit.
Output is a pair of contacts (normally-open and normally-closed) and common wire connected to relay. Relay may stay either on "Active" or in "Inactive" state. Active state means that the current passes through relay coil and common contact is connected to the normally-open contact. Inactive state means that no current passes through relay coil and common contact is connected to normally-closed one.
Two Etherlink IV units with IO daughter-modules create communication channel that transfers Input status to corresponding Output relay over DSL, Ethernet or E1 link.
Input sensors can also be configured to trigger internal Minor or Major alarm of the Etherlink IV device while Output relays can be triggered by the modem Alarm status.
4I4O daughter-card of Etherlink IV creates IP-based channel and uses either UDP or TCP messages for operation.

3.2.2.5 Ethernet Interface

The Ethernet interfaces of all BlackBox Etherlink IV devices fulfil the standard IEEE 802.3 and support the Port (PBVLAN command) and Tag (VLAN command) based VLAN protocol (Virtual Local Area Network – IEEE 802.1Q). A virtual network represents a group of network nodes, whose traffic, including the broadcast traffic, is completely isolated from other network nodes. The organization of virtual networks usually decreases the load in the network, because the broadcast traffic will be transmitted not to the entire network but to members of the VLAN sender. Due to the fact that the members of different VLANs can exchange information via a router, which allows a controlled traffic, the use of VLAN technology provides a high level of security. In addition, any changes in the network structure are simplified because instead of configuring the work station to which the modem is connected you only have to configure the modem port.
To construct VLAN networks and to provide the priority in the data transmission, an extended Ethernet frame is used, which contains an additional VLAN tag of 2 bytes length. The tag includes the number of the VLAN to which the packet belongs and its priority level.

Some types of traffic (real-time video, voice or IP traffic) should be sent inside the network without any delays. To provide the necessary quality of this traffic, the Etherlink IV devices support Ethernet traffic priority according to the standard protocol IEEE 802.1P (so-called QoS, Quality of Service). It means to analyse the header content of each Ethernet frame to get information about the necessary priority of this application. The internal switch places this data to the corresponding queue of the output port. The Etherlink IV equipment supports two priority queues when sending packets – a high and low priority queue. According to it, all Ethernet traffic can be divided into high priority groups (for example VoIP traffic or control and management channels) and low priority groups (for example LAN1 and LAN2).

The Ethernet traffic between all network interfaces of the device is distributed by the internal Ethernet switch (see next figure). In Etherlink IV devices four types of network interfaces exist:

- Ethernet interfaces (external connector on the front panel, and backplane connector)
- SHDSL interfaces (when the device is properly configured)
- E1 interfaces (when the device is properly configured)
- Virtual management port (Telnet session)

The number of E1 and SHDSL interfaces depends on the model of the Etherlink IV family. The choice of the interface (DSL or E1), which will be mapped to the corresponding WAN interface is performed by the <PAYLOAD> and <WANTS> command.

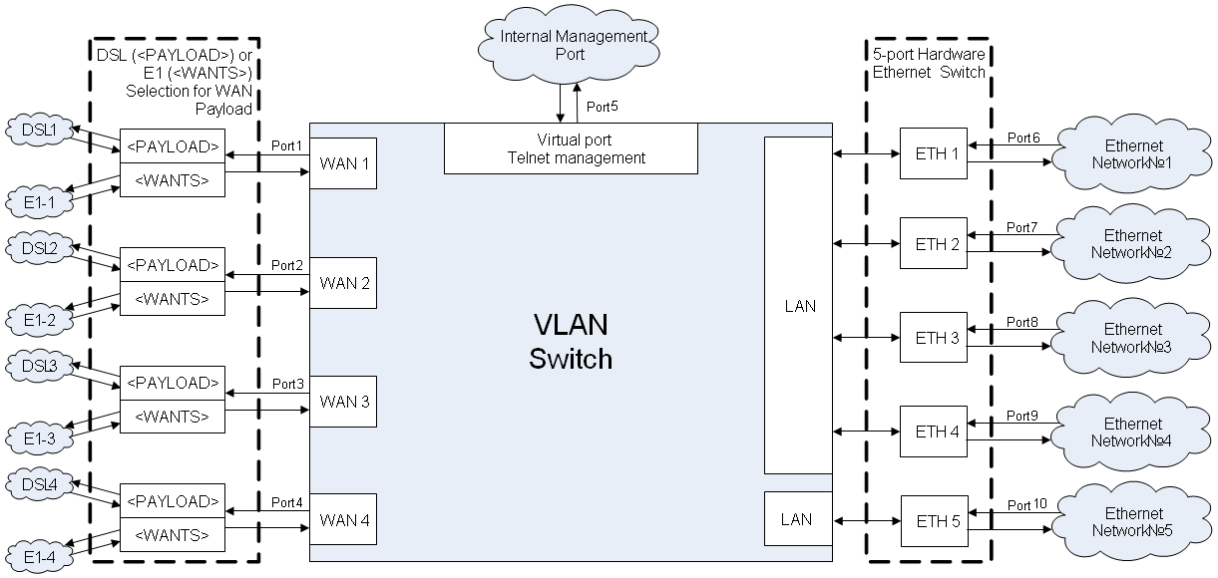


Figure 3.10 Internal Switch

For single-channel modems the DSL channel is strictly mapped to WAN1, while the E1 interface is strictly mapped on WAN2.

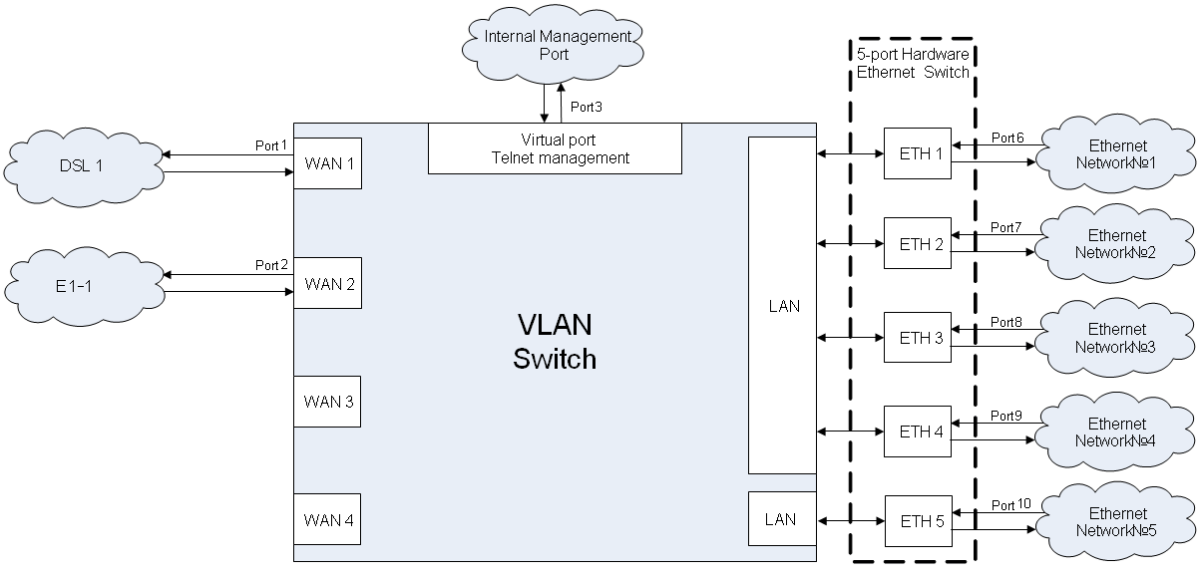


Figure 3.11 Internal Switch for single-channel devices (SA-RC-ETHERLINK_IVL-2E1B/4Eth-RP,V90)

A group of LANx Ports (Ethernet interface) means the LAN port connector on the front panel or backplane that can serve as a **Trunk port**, **Access port** or **Mixed port**.
The **Trunk port** is a port where all present packets have the VLAN format, namely, the Ethernet frame with a header, determining the number of the VLAN and QoS. In Trunk mode, only tagged frames pass into and out of LANx port, frames are allowed to pass on per-VLAN basis. This means that special equipment supporting VLAN is connected to the Trunk port. A PC with a standard network interface card cannot be connected to the Trunk port.
The **Access port** is a port where all present packets have a standard Ethernet format (without the additional two bytes for the header). It means that only untagged frames pass into (ingress) and out of (egress) any LANx port. On ingress, frames are assigned with a default VLAN tag (configured by VID and QoS commands). On egress, only frames with VLAN equal to the default VLAN of the port are allowed, and this tag is removed. A PC with a standard network interface card can be connected to the Access port.
The **Mixed port** is a port where tagged and untagged traffic is allowed. However, on ingress, a default VLAN tag is assigned to untagged traffic (configured by QOS and VLAN commands), so that all frames in the system are actually tagged. On egress frames with VLAN equal to the default VLAN (configured with VLAN command), exit the port untagged, while to all other VLANs apply pass/block rules set by the ALLOW command.

Mode	Default VLAN (set with VLAN command)	VLAN1-VLAN8, OTHER (set with ALLOW command)
ACCESS	Untagged traffic outside of the modem. VLAN tag is added on ingress, removed on egress.	Not taken into account
TRUNK	Not taken into account	Tagged traffic outside of the modem. VLAN tag is not modified on egress and ingress.
MIXED	Untagged traffic outside of the modem. VLAN tag is added on ingress, removed on egress.	Tagged traffic outside of the modem for VLANs not equal to default VLAN. VLAN tag is not modified on egress and ingress.

Table 3.8 Access, Trunk and Mixed Mode

Etherlink IV devices always transmit Ethernet packets over DSL or E1 interfaces with the VLAN format. It means that data packets coming from Access ports are first transformed into Ethernet packets with VLAN format (adding standard VLAN number and QoS priority level) and after this transmitted over any line interface.

There is a special case when having the same MAC address on different VLANs and PBVLANs. Normally, there should not be two devices on the network sharing the same VLAN. But IEEE 802.1Q VLANs as well as port-based VLANs allow creating separate logical networks on one physical network. Thus, in different VLANs or PBVLANs there could be devices sharing the same MAC address. On Etherlink IV, however, there is a hardware limitation preventing all VLAN+PBVLAN combinations from having different address databases, and therefore, allowing same MAC address to be used on all VLAN&PBVLAN combinations is possible in the modem configuration. But, knowing which configurations are valid will allow using modems in all really vital configurations. There are two rules.

1. For separately managed VLANs 1-8. Each VLAN has its own MAC address table, and thus device with MAC address ABC in each of these 8 VLANs will not conflict with any device with MAC address ABC in any other VLAN. But the limitation here is the use of port-based VLANs. MAC address database is shared among all PBVLANs for VLAN1-8. Therefore a device with MAC address XYZ, VLAN1, PBVLAN A, will conflict with device with MAC address XYZ, VLAN1, PBVLAN B.
2. For all other VLANs. Here, every PBVLAN has its own MAC address table, but different VLANs on one PBVLAN share the same database. A device with the MAC address XYZ, VLAN(any other), PBVLAN A, will not conflict with a device having the MAC address XYZ, VLAN(any other), PBVLAN B. But the device with the MAC address ABC, VLAN(any other), PBVLAN A, will conflict with the device having the MAC address ABC, VLAN(any other+1), PBVLAN A.

Same MAC address	VLAN1, VID=1 PBVLAN A	VLAN other, VID=100 PBVLAN A	VLAN other, VID=200 PBVLAN A	VLAN1, VID=1 PBVLAN B	VLAN other, VID=100 PBVLAN B	VLAN other, VID=200 PBVLAN B
VLAN1, VID=1 PBVLAN A	N/A	OK	OK	NOK Same MAC on same VLAN for VLAN=1..8	OK	OK
VLAN other, VID=100 PBVLAN A		N/A	NOK Same MAC on same PBVLAN for VLAN≠1..8	OK	OK	OK
VLAN other, VID=200 PBVLAN A			N/A	OK	OK	OK
VLAN1,VID=1 PBVLAN B				N/A	OK	OK
VLAN other, VID=100 PBVLAN B					N/A	NOK Same MAC on same PBVLAN for VLAN≠1..8
VLAN other, VID=200 PBVLAN B						N/A

Table 3.9 Same MAC address on different VLANs and PBVLANs

In addition, every unit has a table of static MAC addresses (up to 8 addresses) for connected devices, so that each device can have a VLAN number and a QoS priority level (this is a table of special MAC addresses). If a packet is received from the Access port and the MAC address of the packet sender is inside this table, a header with the necessary VLAN number and the QoS priority will be assigned to this packet before transmitting it to the Trunk port. Otherwise, a default VLAN number and QoS priority will be assigned to the packet.

A group of DSL ports (WAN1–WAN4) (SHDSL interface) means that Ethernet data can be mapped onto specified timeslots (64kbit/s) on the SHDSL interface by using the internal switch. In this case, this port always serves as a **Trunk port**. Any data received from **Access/Mixed ports** are first transformed into Ethernet packets with VLAN format and then transmitted over the SHDSL interface.

A group of E1 ports (WAN1–WAN4) (E1 interface) means that Ethernet data can be mapped onto specified timeslots (64kbit/s) on the E1 interface by using the internal switch. In this case, this port always serves as a **Trunk port**.

A virtual management port (INT) (Virtual management port) is an internal device management program. The IP-address of this device is the logical address of the management program. For example, to open a session for managing a remote device, the IP-address of this device should be specified in the Telnet program. At the physical layer, the MAC address of the device is also the management program address, which is inside the Ethernet frame.

Note: As a rule the data of the management port have the highest priority (example, QoS = 7).

3.2.2.6 MAC Filter

The system supports MAC filtering feature. If enabled the device will filter MAC addresses and acts according to the defined MAC filtering rule. If disabled, the system will store and forward correct Ethernet packets according to the configuration of Ethernet subsystem.

White List

White List contains a list of MAC addresses. The fact of MAC address presence in the list means that the data exchange between the modem device and the node with selected MAC is allowed.

The data exchange between the modem device and the node with non-listed MAC address is prohibited.

Interfaces

The White List is applicable per LAN Interface. Therefore the number of lists is equal to the number of physical Ethernet ports of the device.

Note: White List can't be enabled on WAN interfaces.

Number of Entries

Every White List stores up to 10 MAC addresses. A same MAC address can be stored in several White Lists.

3.2.2.6.1 MAC Filter Rules

MAC Address Filtering

If ingress packet has a MAC address that is not listed in the White List the LAN interface belongs to, this packet will be dropped. No information will be recorded and no message will be generated by the device. It is default mode and it will be enabled automatically as soon as the MAC filtering feature will be enabled.

MAC Address Filtering and Intruder Alarm

It is possible to enable Intruder Alarm indication on the device. If enabled, the SNMP Trap will be generated by the device if the unlisted MAC will arrive to the port. The Trap from the same non-listed MAC address will be generated approximately once in 3 minutes. Trap contains the information about the Intruder MAC address.

Port Blocking and Intruder Alarm

It is possible to enable Port Blocking Mode in case if unlisted MAC has been arrived. Upon receiving the wrong MAC the Port will go to Down State equal to ETHSD OFF X command where X is an interface number. The Intruder Alarm Trap and Link Down Traps will be generated in this case.

> **NOTE:** Port will keep the blocked Down State even after reset of the device. To restore port operation the command ETHSD 10H/10F/100H/100F/AUTO X or WEB GUI shall be used.

3.2.2.7 IEEE 802.1x Access Control

The IEEE 802.1x protocol nowadays commonly used in LAN environment that generally was developed as "multipoint to multipoint" media for simple and secure point-to-point authorization. It works on MAC level and provides Authentication and Authorization for a terminal device connected to a port of active network equipment, i.e. Ethernet Switch or Wireless Access Point. The IEEE 802.1x protocol divides network elements into three parts:

The Supplicant

The supplicant is a client device (laptop, PC) that supports IEEE 802.1x protocol as a client. The supplicant is connected to the Authenticator over Ethernet or wireless link.

The Authenticator

The Authenticator is a network device like Switch or Wireless Access Point which acts as an aggregator of user traffic in a network. It is connected to the Authentication Server and acts as an intermediate agent between supplicant and network. Etherlink IV/MaxiMiniLink devices operate as Authenticator.

The Authentication Server

The Authentication Server is, for example RADIUS server. It is responsible for security policy of the network. Upon receiving of authentication messages from the Authenticator it grants or blocks network access for the Supplicant.

The Supplicant is connected to the Authenticator via Ethernet patch-cord or through wireless link. In case of Etherlink IV/MaxiMiniLink devices the wired access is used. If it is not allowed by the Authentication Server, the Authenticator's port the Supplicant is connected to, stays in blocking condition and transmits only EAPOL (Extensible Authentication Protocol Over LAN) frames. These frames carry authentication and authorization messages and are encrypted. As soon as Authentication Server grants network access to the Supplicant, the Authenticator changes the port status, so all frames can pass through the port.

3.2.2.7.1 IEEE 802.1x Device Settings

The following IEEE 802.1x parameters can be changed on Etherlink IV/MaxiMiniLink device:

IEEE 802.1x Enable / Disable

Enables or Disables IEEE 802.1x protocol on a LAN port

IEEE 802.1x SHOST/MHOST/MAUTH

If IEEE 802.1x is enabled on a LAN port the port may work in these three modes:

- Single-host (mode option SHOST): only one host (MAC-address) can be authenticated on the port, others hosts will be blocked.
- Multi-host (mode option MHOST): once one host has been authenticated, port is allowed to pass traffic from any other hosts.
- Multi-auth (mode option MAUTH): multiple hosts can be authenticated on a port, but only authenticated hosts are allowed to pass traffic.

> **NOTE:** As IEEE 802.1x mode conflicts with MAC Filter a LAN port may operate either in 802.1x or in MAC Filter modes or both modes must be deactivated.

As IEEE 802.1x protocol relays on RADIUS protocol and use encrypted messages the RADIUS and SNTP clients must be configured first.

3.2.2.8 Rapid Spanning Tree Protocol

The system supports Rapid Spanning Tree Protocol (RSTP) according to IEEE 801.1d 2004 recommendation. All available Ethernet ports as well as all available WAN interfaces could participate in RSTP construction. A WAN interface could be configured to carry Ethernet data over DSL line or over E1 interface. If several DSL links or E1 interfaces are combined into MULTIWAN, this MWAN will participate in RSTP construction too.

The RSTP itself is a protocol used for dynamic link switching in networks with ring topology. The ring topology improves reliability of data networks; nevertheless Ethernet networks must have only one active path between any of two nodes to prevent packet loop. Ethernet switches with enabled RSTP detect paths availability in a ring and quickly select active path, discarding other paths. All RSTP-enabled devices exchange information about topology change in so-called BPDU packets.

Root Bridge

One switch in a RSTP-enabled network must acts as Root Bridge. Root Bridge selection will be done automatically according to Bridge ID – a unique ID that each member of RSTP network has. Bridge ID is a combination of Switch MAC address and Bridge Priority. Switch with smallest Bridge Priority will act as Root Bridge. If two or more switches have same priority, Switch with less MAC address will become Root Bridge.

Port Roles

After Root Bridge has been selected, other switches define their ports role. The port that has the shortest path to Root Bridge will become Root Port. The opposite port on the other switch will become Designated Port. The Root Bridge has Designated Ports only, while other switches have one Root port and could have Designated Port connected to other switches

A Root and Designated ports are active, they learn and forward packets. Other ports have blocking state. They could act as Alternate port or as Backup port. Please take a look to a picture below:

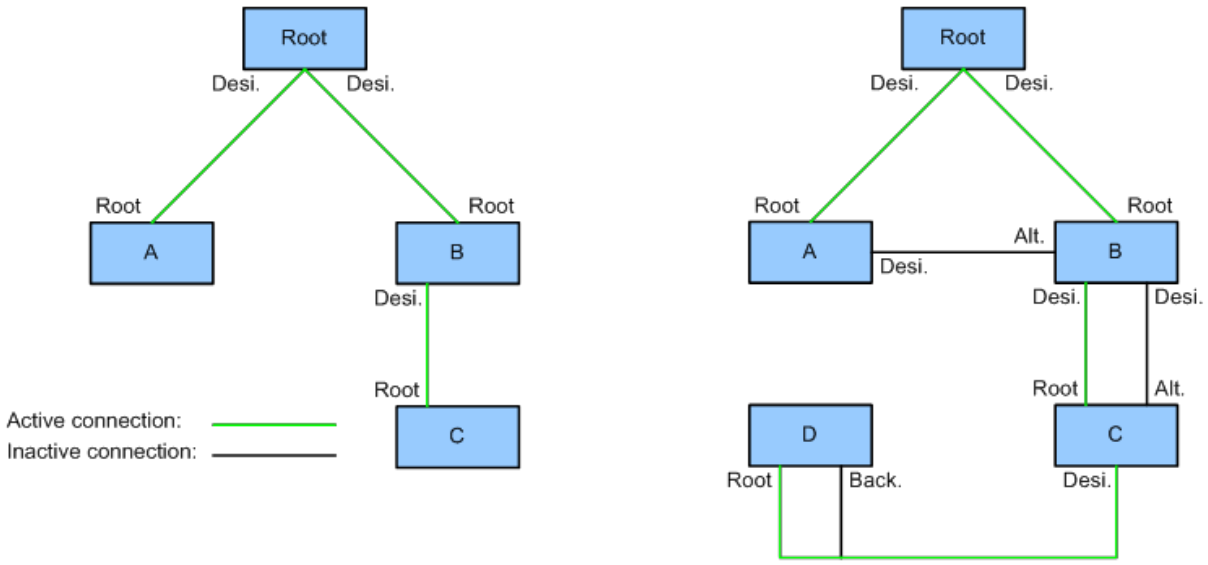


Figure 3.14 Port role definition in RSTP.

When a failure appears on a network, an alternative path will be selected and port roles will be changed. Please take a look to a picture below:

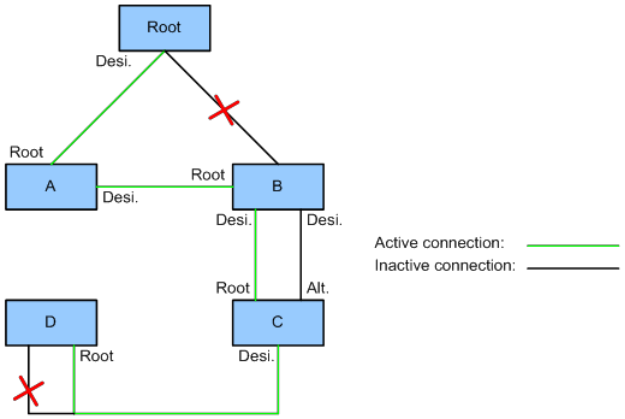


Figure 3.15 Change of Port role upon network failure.

ONLY PORTS WITH ROOT AND DESIGNATED ROLES WILL FORWARD DATA PACKETS. PORTS WITH ALTERNATIVE ROLE WILL BE IN BLOCKED STATE

3.2.2.9 RADIUS

The RADIUS (Remote Authentication in Dial-In User Service) is used to authenticate and authorise remote devices from the single place. Unlike the local authentication and authorisation, where USERNAME/PASSWORD/ACCESS_RIGHTS have to be created for every single unit in the network, the RADIUS authentication and authorisation means that user credentials must be created and stored only once on the RADIUS server. The remote RADIUS clients will connect to the RADIUS server and request user authentication and authorisation.

NOTE: RADIUS subsystem depends on Advanced Security settings. SECURE ON command has to be enabled before activating the RADIUS service

The Etherlink IV modem acts as RADIUS client. It will request user authentication and authorisation from RADIUS server if operator will access command line or WEB interface of the device.

NOTE: The current realisation of RADIUS protocol is designed for authentication and authorisation of the device operator. It is not intended for granting or disallowing an access from LAN ports to the network.

Etherlink IV RADIUS client supports one or two RADIUS servers. The following options are configurable:

Parameter	Value	Description

Server IP	IP Address	IP address of primary and secondary RADIUS Server.
Server port	0-65535	UDP Port, the RADIUS server is listen on for incoming connections. Default port is 1812.
Shared key	String (64 symbols)	A passphrase. It must be the same for RADIUS server and all clients. If two RADIUS servers are used, the passphrase can be unique for each server.
Retries	0-10	Number of retries, the client will use to authenticate the user on both RADIUS servers. 0 means no attempts. Default value is 2.
Timeout, seconds	1-5	Time interval between authentication attempts. Default value is 2 seconds.

The authentication and authorisation process has the following scenario: as soon as operator opens console session through Telnet, SSH or Serial interface, or if he opens WEB session and connects to the HTTP server of the device, the LOGIN prompt appears. Operator enters the USERNAME/PASSWORD pair and the RADIUS client (modem) sends authentication request to the first RADIUS server. If the USERNAME/PASSWORD pair match the server database, the operator will be authorized and access to CLI or WEB interface will be granted. If either USERNAME/PASSWORD pair, or shared key doesn't match the server database record, the access will be disallowed. Operator has 3 attempts per session to authenticate himself.

If first RADIUS server didn't reply during a defined timeout, the build-in modem RADIUS client tries to authenticate the user at the second RADIUS server. If the second server didn't reply, the client tries the first server again. This sequence keeps running until the number of retries counter expires. The number of retries is user defined.

If the whole authentication sequence fails, the build-in modem RADIUS client tries to authenticate and authorise the operator using the local user record.

NOTE: It is not possible to authenticate user with local user record, if at least one RADIUS server is running and accessible from the build-in client.

3.2.2.9.1 RADIUS Server Setup with Defined Vendor Specific Attributes

As an example we will configure Freeradius server running on Linux Debian/Ubuntu platform. Server will use Vendor Specific Attributes field during message exchange.

Freeradius server can store its configuration in SQL database or in plain text files. We will select second way because of simplicity.

Vendor configuration. File dictionary.BLACKBOX

First of all, we need to tell Freeradius server to use Vendor Specific Attribute for the access to BLACKBOX equipment. We need to create the following text file:

File is located at /usr/share/freeradius/dictionary.BLACKBOX

```
#
#
# Radius settings for BLACKBOX units
#
#
VENDOR          BLACKBOX        4249

BEGIN-VENDOR    BLACKBOX
ATTRIBUTE       BLACKBOX-Rights 0       string
END-VENDOR      BLACKBOX
```

AS a second step we need to connect newly created Vendor Specific file to the Freeradius dictionary file:

File is located at /usr/share/freeradius/dictionary String to add:

```
$INCLUDE dictionary.BLACKBOX
```

If Vendor Specific Attributes are used, the server will send the message containing two fields:

<Vendor-Specific> <4249 0 ACCESS_RIGHTS_STRING>. Here 4249 is Vendor ID of BLACKBOX. ACCESS_RIGHTS_STRING contains the user privileges.

Client configuration. File clients.conf. We need to define RADIUS clients

Client configuration file contains the IP addresses of the modems with build-in RADIUS clients and shared secret passphrase. File is located at /etc/freeradius/clients.conf

```
# BLACKBOX Etherlink IV Clients
# Modems from network 192.168.1.0/24 will be authenticated using secret
# phrase. Don't forget to add "sharing secret" to Etherlink IV modem using
# RADIUS SECRET command
client 192.168.1.0/24 {
   secret   =   My1stSecretCode4Radius
   require_message_authenticator = no
   nastype = other
}
```

User configuration. File users

We need to create USERS with appropriate rights

User records are located at /etc/freeradius/users

```
# Etherlink IV User with Administration rights
ETHERLINK   IVADMIN   Cleartext-Password   :=
"AdminPass"
  BLACKBOX-Rights = ALL,
  Framed-IP-Address = 192.168.169.0,
  Framed-IP-Netmask = 255.255.255.0

#  Etherlink  IV  User  with  User  rights.  Basic  change  of
configuration   ETHERLINK   IVUSER   Cleartext-Password   :=
"UserPass"
  BLACKBOX-Rights         =
  CONTROL,  BLACKBOX-Rights
  +=  TEST,  BLACKBOX-Rights
  +=   STATUS,   BLACKBOX-
  Rights += CONFIG,
  Framed-IP-Address = 192.168.169.0,
  Framed-IP-Netmask = 255.255.255.0

# Etherlink IV User with Read-only rights
ETHERLINK    IVOPERATOR    Cleartext-Password    :=
  "OperatorPass" BLACKBOX-Rights = TEST,
```

NOTE: Don`t forget to restart freeradius server after changing configuration using `sudo service freeradius restart` command.

3.2.2.9.2 Simplified RADIUS Server Setup

Alternatively, we can setup the Freeradius server without Vendor Specific dictionary file and declare Vendor-Specific field in user configuration file instead

User configuration. File users

We need to create USERS with appropriate rights

User records are located at /etc/freeradius/users

```
# Etherlink IV User with Administration rights
ETHERLINK   IVADMIN   Cleartext-Password   :=
"AdminPass"
  Vendor-Specific = ALL,
  Framed-IP-Address = 192.168.1.0,
  Framed-IP-Netmask = 255.255.255.0

#  Etherlink  IV  User  with  User  rights.  Basic  change  of
configuration   ETHERLINK   IVUSER   Cleartext-Password   :=
"UserPass"
  Vendor-Specific = CONTROL,
  Vendor-Specific  +=  TEST,
  Vendor-Specific += STATUS,
  Vendor-Specific += CONFIG,
  Framed-IP-Address = 192.168.1.0,
  Framed-IP-Netmask = 255.255.255.0

# Etherlink IV User with Read-only rights
ETHERLINK    IVOPERATOR    Cleartext-Password    :=
  "OperatorPass" Vendor-Specific = TEST,
  Vendor-Specific    +=    STATUS,
```

Without Vendor Specific Attributes defined, the server will send the message containing two fields:

<Vendor-Specific> <ACCESS_RIGHTS_STRING>. No vendor ID will be attached to the message.

Client configuration file contains the same information as in the previous example.

Client configuration. File clients.conf.

We need to define RADIUS clients

Client configuration file contains the IP addresses of the modems with build-in RADIUS clients and shared secret passphrase. File is located at /etc/freeradius/clients.conf

```
# BLACKBOX Etherlink IV Clients
# Modems from network 192.168.1.0/24 will be authenticated using secret
# phrase. Don't forget to add "sharing secret" to Etherlink IV modem using
# RADIUS SECRET command
client 192.168.1.0/24 {
   secret   =   My1stSecretCode4Radius
   require_message_authenticator = no
   nastype = other
}
```

NOTE: Don`t forget to restart freeradius server after changing configuration using `sudo service freeradius restart` command.

3.2.2.9.3 RADIUS Server setup with defined Service-Type Attribute

Alternatively, we can setup the freeradius server with Service-Type Attribute. Currently the following Service-types are supported:

- Type 6: Administrative; modem grants access equal to BLACKBOX-Rights = ALL
- Type 7: NAS Prompt; modem grants access equal to BLACKBOX-Rights += TEST, += STATUS

User configuration. File users

User records are in /etc/freeradius/users

```
# Etherlink IV User with Administration rights
ETHERLINK   IVADMIN   Cleartext-Password   :=
"AdminPass"
  Framed-IP-Address = 192.168.169.0,
  Framed-IP-Netmask = 255.255.255.0,
  Service-Type = Administrative-user

# Etherlink IV User with Read-only rights
ETHERLINK    IVOPERATOR    Cleartext-Password    :=
  "OperatorPass" Framed-IP-Address = 192.168.169.0,
  Framed-IP-Netmask = 255.255.255.0,
```

NOTE: Don`t forget to restart freeradius server after changing configuration using `sudo service freeradius restart` command.

3.2.2.9.4 Configuring User Access Rights

The <Vendor-Specific> or <BLACKBOX-Rights> or <Service-Type> field in RADIUS configuration tells the client what access rights the user has. It is possible to grant or discard access to various commands and menu items of the modem device. All commands of the CLI are divided into 3 levels. Selection of upper level means that the commands from low levels will be selected too. Some commands are available for every user, they can't be revoked.

Privileges

Hierarchy Levels			Description	Related commands
Top Level	Group	Subgroup		

ALL		Commands of this level are available for everyone. No additional authorization is required	ALARM ALARM T DISCONNECT LINKCLEAR	TLM SENSOR ACO SOFTINFO
	CONTROL [CTRL]	Operation of remote devices	CONNECT	LINK
	TEST [T]	Test of the device	LOOP1 LOOP2 STARTAL RESTART	PING MACTABLE MACTABLE C BERT Submenu
	ADMIN [A]	Administration of the device	DIFF DUMP SERNUM LICENSE ACO change RESET	SOFTUPDATE SOFTCONFIRM ID RESPONSE PASSWORD NMTHR

				BACKUP RESTORE LOAD TLM D TLM S TLM C SENSOR [N] [O/C] TFTP	LATHR LICENSE ADD DEFAULT EVERYTHING SECURE LOG USERS USER APPLY CONFIRM
	STATUS [S]	:LINK	Link status	G826 G826 C G826 E1 G826 E1 C ALLG826 LINKSTAT LINKALARM ALARMLOG	NM LINKNM STATUS STATUS T STATUS L STATUS EXT POWER DIAG
		:LINKC	All commands from LINK + reset of the counters	RESETG826 RESETALLG826	ALARMLOG C
		:LAN	Ethernet status	NETSTAT NETERR	STATUS ETH MACTABLE
		:LANC	All commands from LAN + reset of Ethernet counters and MAC table	RESETNETSTAT MACTABLE C	

ALL	CONFIG [C]	:VIEW	Displaying of device configuration	CONFIG NETCONFIG	COSCONFIG RSTP CONF
		:LINK	All commands from VIEW +line, E1 and Nx64 interface configuration	DEFAULT AUTO MASTER EXT BASERATE PAM PAYLOAD ANNEX SETCLOCK MULTIPAIR RESERVE G704 CRC4 AISDET AISGEN DSLTS WANTS	E1CLOCK E1MODE POWER GSCOMPAT PTMP MODE N RSRATE RSFORMAT RSDUPLEX AUTOLOOP EXTCLOCK N64RATE WAN WANIDLE APPLY CONFIRM

		:LAN	All commands from VIEW + LAN configuration	NETDEFAULT RSTP DEFAULT RSTP STATE RSTP ... PBVLAN MODE [IF] VLAN QOS ALLOW VID	ETHSD FC IRATE ERATE CRATE COS PING APPLY CONFIRM

	:SNMP	All commands from VIEW + SNMP configuration	TRAPIP COMMUNITY SNMPSET SNMPACL	RMONALARM RMONEVENT APPLY CONFIRM
	:NET	All commands from VIEW + IP configuration	SETIP GATEWAY NETMASK MTU SYSLOG	SNTP APPLY CONFIRM PING

NOTE: The abridgements in braces "[ ]" can be entered instead of complete name.
If group has been entered without subgroup definitions, all subgroups will become available.
To define subgroup, type it after group name with ":" in the beginning of a subgroup.
The WEB interface will follow the rights of CLI interface.

In the RADIUS Server configuration example three different users have been defined in the users file.

User ETHERLINK IVADMIN has full access to the device, because <Vendor-Specific> or <BLACKBOX- Rights> field is set to ALL.

ETHERLINK IVUSER has partial access, because <Vendor-Specific> or <BLACKBOX-Rights> filed is set to CONTROL + TEST + STATUS + CONFIG.

ETHERLINK IVOPERATOR can only perform tests and check device status, because <Vendor-Specific> or <BLACKBOX-Rights> field is set to TEST + STATUS.

3.2.2.10 LLDP

LLDP is an abbreviation of Link layer discovery protocol defined in IEEE 802.1AB. The LLDP protocol is used by network devices to identify themselves and to advertise their capabilities to their peers over IEEE 802 (Ethernet) networks or over WAN (MWAN) channels formed via DSL/E1 links. LLDP protocol is vendor neutral, so various devices can interoperate and introduce their capabilities to remote peers even if they were produced by other vendors. The LLDP implementation in BLACKBOX Etherlink IV / MaxiMiniLink devices can read and display the following parameters received from remote peer:

Parameter	Value	Description
Chassis ID	String	Manually assigned chassis ID or an chassis MAC address
Port ID	String	Remote port ID
TTL	Timer	Time To Live Value in seconds shows the validity of remote system information
Port Description	String	Manually assigned port description
System Description	String	Manually assigned system description
System Capabilities:	Digit	Capabilities of remote system (Bridge, Router, Phone, etc.)
Management address:	IP Address	Management IP address of remote system
Management VID:	VLAN ID	A VLAN ID assigned for management port
Maximal Frame Size	Digit	Maximal size of frame in bytes the remote system can accept

MED capabilities	Array	Shows if the remote peer is Endpoint or Network Connectivity Device and its Media Endpoint Device capabilities
Hardware Revision	String	Remote system hardware version
Software Revision	String	Remote system software version
Serial Number	String	Remote system serial number
Model Name	String	Remote system model name

Local system advertises the same own parameters to its neighbours.

3.2.3 An Integrated Switch of 64-kbit/s Time Slots

3.2.3.1 E1 Transmission Mode (only E1 Time Slots)

In this mode, only time slots of E1 data streams are transmitted over SHDSL lines according to ITU-T Rec. G.991.2.

Time slots of E1 data streams (first E1 / second E1)	Total number of transmitted time slots	Minimal required SHDSL data rate transmitting this number of time slots (Kbit/s)
0,1,16 / 0,1,2,3	7	456
0,1,2,3,31 / none	5	328
0-29,31 / none	31	1992
0-31 / 0-31	64	4104

Table 3.10 Comparison of SHDSL data rate and number of possible time slots of one E1 stream

3.2.3.2 E1 and Ethernet Simultaneous Transmission Mode

The system supports simultaneous transmission of E1 time slots and Ethernet data (from the ports WAN1, WAN2, WAN3, WAN4, and the internal Ethernet switch) into an SHDSL line. This mode means time slot multiplexing from E1 and Ethernet network interface into the SHDSL line. The distribution of SHDSL time slots is performed as follows:

- time slots of the first E1, chosen for transmission in the SHDSL line interface in the ascending order, are transmitted in time slots from 0 to m1-1
- time slots of the second E1, chosen for transmission in the SHDSL line interface in the ascending order, are transmitted in time slots from m1 to m1+m2-1
- Nx64/RS-232/RS-485 data is transmitted in time slots from m1+m2 to m1+m2+m3-1
- Ethernet data is transmitted in time slots from m1+m2 to n-1

Here

- n is the total number of transmitted SHDSL time slots
- m1 is the number of time slots from the first E1 selected for transmission into SHDSL
- m2 is the number of time slots from the second E1 selected for transmission into SHDSL
- m3 is the numer of time slots required for Nx64/RS-232/RS-485 data
-

Note: A part of time slots of an E1 interface can be used to transmit data from the WAN2 port of the internal Ethernet switch.

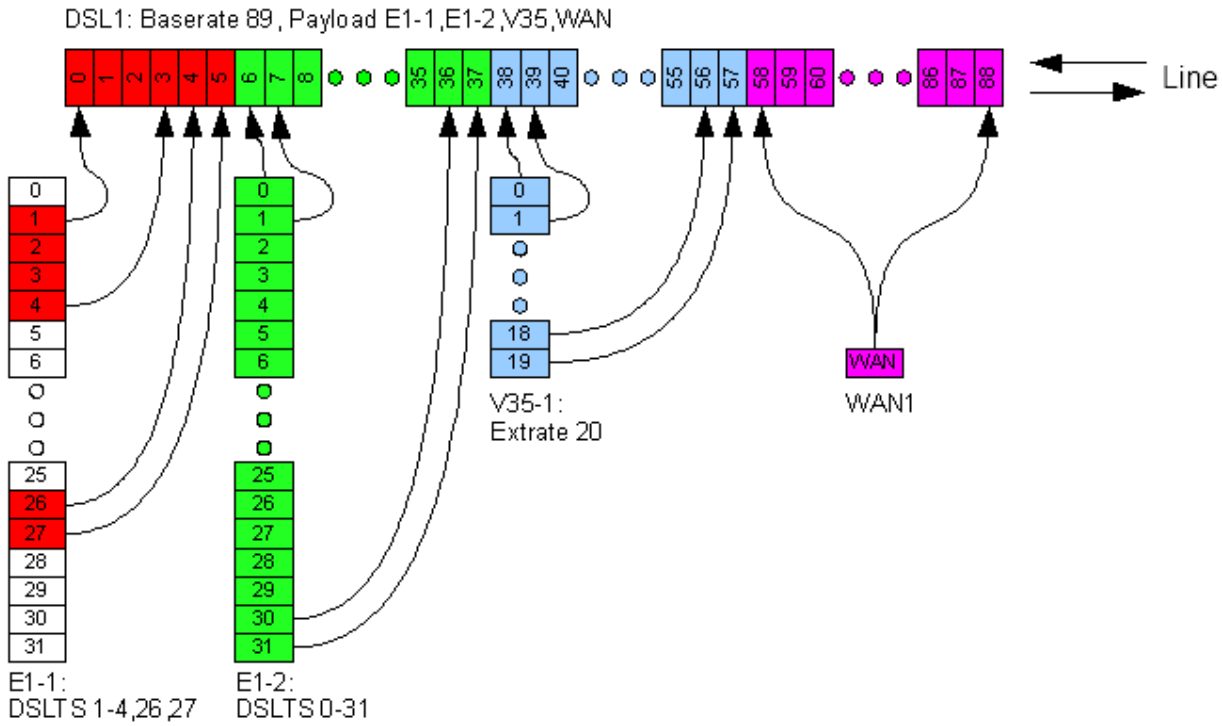


Figure 3.12 Example of distribution of time slots in an SHDSL frame at a line rate of 89x64 Kbit/s in the mode when both E1 interfaces and both internal WAN1 and WAN2 ports are used for the termination device.

3.2.4 Test Loops

The possibility to activate test loops on E1 or SHDSL line interface simplifies the device start-and-adjustment.

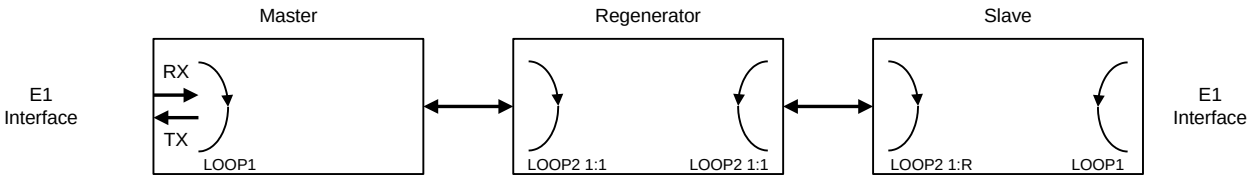


Figure 3.13. Test loops

Test loops can be activated for the Master and Slave devices as well as for the Regenerator.
The **LOOP1 ON/OFF N** command is used to activate/deactivate LOOP1, where **N** is the number of the network interface.
LOOP2 M:N, where **M** is the number of the line interface and **N** is the number of the Regenerator, can be activated **only remotely**. This command allows activating remotely a loop back to the device, from which the command was sent. It means that if LOOP2 is activated remotely by the Master device, the data will be looped back by the Slave device to the Master device side, and vice versa.

WARNING
WHEN ACTIVATING LOOP2 UNDER CONDITIONS THAT SHDSL IS USED TO TRANSMIT ETHERNET DATA, IT IS NECESSARY THAT THE DEVICE IS DISCONNECTED FROM THE ETHERNET NETWORK!

3.2.4.1 Analogue Loop back

During the analogue loop back test, the SHDSL transceiver receives the transmitted signal from its own transmitter. The analogue loop back function (the **STARTAL** command is used to activate the analogue loop back) is used to test the equipment itself.
The analogue loop back causes a non-urgent alarm of the local unit and an urgent alarm of the remote unit.

WARNING
TO PERFORM THE ANALOG LOOPBACK, THE CABLE SHOULD BE DISCONNECTED FROM THE UNIT!

3.2.4.2 Performance Monitoring

The transmission performance of a link can be monitored in two different ways. The signal quality is typically used during installation and maintenance procedures, whereas the G.826 error performance parameters are used for long term evaluation of operating links and during acceptance testing.
The Noise Margin (NM) provides qualitative performance information of a specific link. The NM command is used to activate this test. This parameter is calculated according to ITU-T G.991.2 and is an efficient tool for determining the qualitative performance of an SHDSL link.
During acceptance testing, it is recommended to set the line rate or choose cable pairs (at a fixed line rate) so that the NM value is no less than 6 dB.
An NM of 0dB in the presence of a Gaussian noise would yield an expected Bit-Error-Ratio of 10-7.

3.2.4.3 G.826 Performance Monitoring

The error performance monitoring of a SHDSL link is performed according to ITU-T Rec. G.704. The evaluation of the G.826 error performance parameters is based on CRC (Cyclic Redundancy Check) error detection. CRC generation and detection are performed separately for the E1 interfaces and SHDSL interfaces.

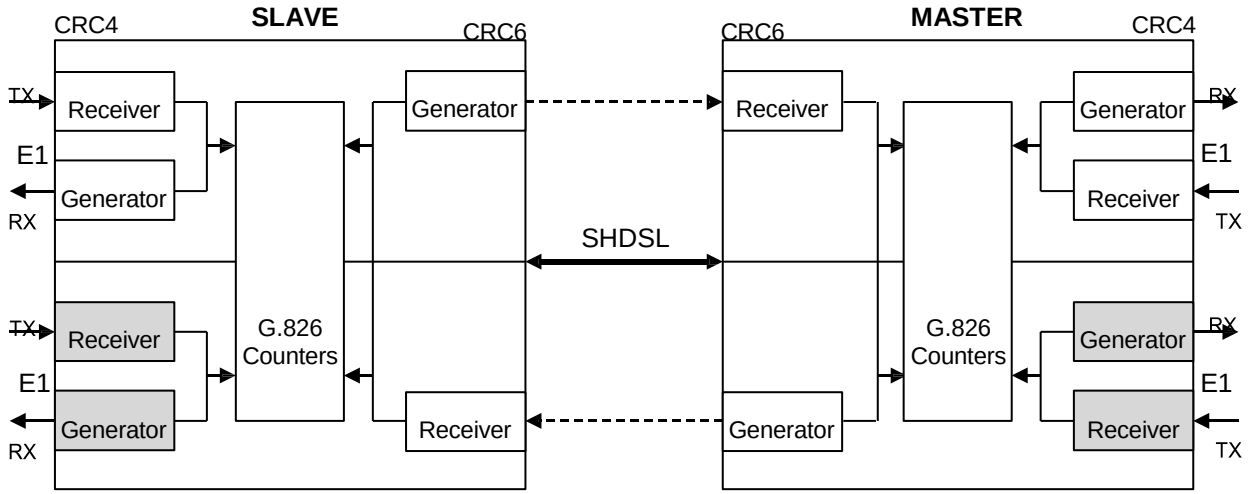


Figure 3.14 G.826 performance evaluation

On the E1 side, four CRC4 check bits are generated per sub-multiframe (SMF) and compared with the corresponding bits of the next SMF. If they do not match, the CRC4 error counter is incremented. On the SHDSL side, six CRC6 check bits are generated per SHDSL frame. CRC6 errors are used by the software to count the block errors of the SHDSL channel and to evaluate its error performance according to ITU-T Rec. G.826.
For the E1 interface, calculations according to G.826 are only possible in the framed mode according to G.704 with the CRC4 option enabled. In the framed mode with the CRC4 option disabled, only FAS errors are detected.
The estimation of a bit error rate is not within the scope of G.826 calculations.

3.2.5 BERT Test

We suggest BERT testing in the following way: Switch on Loop2 on the remote unit (slave) and setup the BERT on the master unit.

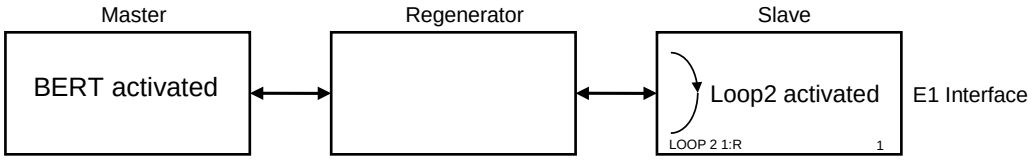


Figure 3.15. BERT setup Example

Configuration Example:

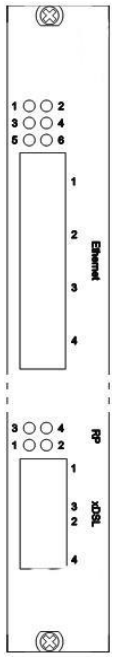
```
CO_BERT>CONF
--------------------------------------------------------------------------------
        Current BERT configuration:
--------------------------------------------------------------------------------
Interface   : E1-1, Internal (to SHDSL1)
Pattern     : 2E7

TX Slots    : [00-15] PG PG PG PG PG PG PG PG PG PG PG PG PG PG PG PG
            : [16-31] PG PG PG PG PG PG PG PG PG PG PG PG PG PG PG PG

RX Slots    : [00-15] BT BT BT BT BT BT BT BT BT BT BT BT BT BT BT BT
            : [16-31] BT BT BT BT BT BT BT BT BT BT BT BT BT BT BT BT
--------------------------------------------------------------------------------
CO_BERT>
```

3.3 Alarm Indication

When managing the device via the local craft terminal (RS-232) or via Telnet, all LEDs, except the Ethernet LEDs will blink with a frequency of 1 Hz.

3.3.1 LEDs

The LEDs display the normal operation conditions and alarm conditions of a device.



Element			Description	
1	**2**		LED: status local device	LED: status remote device
3	**4**		LED: status 1st E1 port	LED: status 2nd E1 port
5	**6**		LED: status 3rd E1 port	LED: status 4th E1 port
	1	**Ethernet**	Status 1st Ethernet Interface	
	2		Status 2nd Ethernet Interface	
	3		Status 3rd Ethernet Interface	
	4		Status 4th Ethernet Interface	
3	**4**	**RP**	LED: Status RP (remote power) 3rd DSL	LED: Status RP 4th DSL
1	**2**		LED: Status RP (remote power) 1st DSL	LED: Status RP 2nd DSL
	1 **3**	**SHDSL**	Status 1st DSL line Status 3rd DSL line	
	2 **4**		Status 2nd DSL line Status 4th DSL line	

Device Status	**LED local/remote Status**		**LED E1 port**	**LED DSL line**
	«1»	**«2»**	**«3», «4»** **«5», «6»**	**«1», «3»** **«2», «4»**
Power failure or power is off	Off	Off	Off	Off
Hardware or software failure	Red blinking	Off	Off	Off
Normal operation	Green	Green	Green	Green

Non-urgent alarm	Amber	Amber	-	-
Urgent alarm	Red	Red	-	-
Non-urgent alarm at E1 interface	-	-	Amber	-
E1 interface data is not used for transmission into SHDSL line interface nor for Ethernet data transmission	-	-	Off	
Urgent alarm at the line interface	-	-	-	Red

Table 3.11 LED behaviour according the device status

LED	LED Status	Device Status
Ethernet left LED	Green	Connection is active
	Off	Connection is not active
	Green blinking	Data receive and/or transmit
Ethernet right LED	Amber	100 Mbit/s receive/transmit rate
	Off	10 Mbit/s receive/transmit rate

Table 3.12 Ethernet LED behaviour according the device status

RP LED	LED Status	Device Status
«3», «4» **«1», «2»**	Off	Remote power source is off
	Green	Remote power is on, normal operation
	Yellow	Detecting over current
	Red blinking	Remote power is off due to an alarm state

Table 3.13 The device statuses corresponding to statuses of RP LEDs

3.3.2 Alarm LEDs

The alarm LED's on any Etherlink IV device (Master/Slave) light with red or amber if any alarm appears.

Name	Group	Alarm status	LD «1»	RD «2»	E1 «3», «4» «5», «6»	DSL «1», «3» «2», «4»	Description
LOS	DSL	Urgent	R	R		R	Loss of signal in an SHDSL link
LOSW			R			R	Loss of frame alignment in an SHDSL link
LOSD				R		R	Loss of signal at the remote SHDSL side
BER-H			R			R	Block-error-rate in an SHDSL line according to G.826 ≥ 30%
SEGD				R		R	Loss of signal or an alarm on a regeneration segment (segment degradation)
ALB		Urgent & Non-urgent	A	R		R	SHDSL analogue loop back is activated
SEGA		Non-urgent		A		R	Data errors or loss of frame alignment on a regeneration segment (segment alarm)
NM			A			R	Noise Margin < setup NMTHR value

LA			A			R	Line Attenuation > setup LATHR value
LOOP2				A		R	Loop is activated from the remote device to the local device
RCONF			R				Configuration of the remote device is not compatible with the configuration of the local device (for example, the local device is configured to transmit Ethernet data, while the remote device is configured to transmit two E1 streams)
LOS-S	E1-1, E1-2,E1-3,E1-4				A		Loss of signal on the E1 side
LFA-S					A		Loss of frame alignment on the E1 side
AIS-S					A		Receiving AIS on the E1 side
BER-S					A		Excessive block error rate on the E1 side
LOOP1					A		Loop is activated towards the E1 equipment
AIS-R				A			Receiving AIS on the E1 side of a remote device
HW-F	Maintenance		RB				Hardware failure
DSL-F			RB				DSL signal processor initialization failure

Table 3.14 Alarm LEDs of an Etherlink IV device

“A” – amber LED
“R” – red LED
“RB” – red LED blinking
To display an urgent alarm has the highest priority (overwrite a non-urgent alarm).

3.4 Management of Etherlink IV Devices

Etherlink IV devices have integrated management and diagnostic functionality. The access to this functionality is done by:

- Connecting the local craft terminal (LCT) or MONITOR interface (RS-232 interface) to any management terminal (PC with VT100 terminal, for example the application Hyper-Terminal).
- Connecting the local Ethernet interface to any management terminal (PC with Ethernet network card). In this case you access with a Telnet session or you use the WEB interface to display some statistics. Also the SNMP (Simple Network Management Protocol) is integrated.

The management and diagnostic functionality is used to configure the devices and to receive additional information like G.826 parameters or any G.SHDSL link quality.

3.4.1 Management by Local Craft Terminal or MONITOR Interface (RS-232 Interface)

Etherlink IV LTU devices have at the backplane connector a TTL-voltage-level management bus that is organized according to the point-multipoint scheme. If the LTU is inserted in any subrack (with ACU/TCU), minirack or SA-DESKTOP-x, these housings convert the TTL signals to a usual standard based RS-232 interface. The corresponding connector can be found either on the front or the rear panel of the devices.

To access the unit in any housing, you have to choose the slot number in which the unit is connected:

- subrack has slot numbers 1..14
- SA-DESK-TOP-4 has slot number 1..4
- minirack and SA-DESK-TOP-1 have slot number 1

To select the necessary device, you have to type **<%SN↵>,** where SN is the slot number.
For example to access the unit mounted in slot 3 type: **%03↵**
The unit in any housing displays the slot number after entering the ECHO command
After typing **<ECHO↵>**, the operator will receive a response from the LTU devices:

```
ECHO↵
01 02 08 10 11 12
```

3.4.2 Management by Ethernet Interface

3.4.2.1 Telnet

The **TELNET** (TELecommunication NETwork) access is made through the Ethernet network. With any computer and a program with the Telnet protocol Etherlink IV devices (they always have an Ethernet interface) can be fully managed. After opening the Telnet session, there is a user authentication: “admin” users, who can change configurations and “user” users who can only view parameters and statistics. Initially passwords are empty. In this case the authentication is not performed and users automatically have the administrator rights. Only “admin” users can set passwords for both types of users. If authentication is successful, the modem main menu is displayed. If authentication fails, it can be repeated up to three times, and after it the connection breaks.
Example: The management through a Telnet session can be activated by a standard command on any Windows computer: **telnet <IP-address>**
If no symbols are received by the modem over the telnet connection within 5 minutes, this session breaks. And with correct configuration, every DSL modem with an IP address can be reached; it does not matter if near end, far end or repeater.

At any time (except for the moment when the password is entered in the Telnet session) Etherlink IV subrack devices (LTU) can choose the command <%NNN> to manage other devices (NNN are digits and symbols of the Latin alphabet in the range from 0 to 80). This command is used to configure Etherlink IV subrack devices as well as other devices connected to the same MONITOR bus (installed in the same subrack). To clear the screen and to establish a connection to the MONITOR bus, the <↵%1↵> command is used. This command sends the “ECHO command”.
First the MONITOR bus is checked whether it is occupied by another device (for example by the second Etherlink IV modem). If the bus is busy by another device, the following message is displayed: “ERROR: Console is busy.” If this message is not displayed, enter the next command % to choose the device. To clear the screen and to connect the device to the MONITOR bus and then to configure the unit, which is in this subrack, enter the command <↵%1XXXX↵>.In this case, the <?↵%XXXX↵> command is sent to the Monitor bus (symbols “?↵” are necessary to complete the command, which probably was already entered over the MONITOR bus). Here, xxxx are digits or letters with the length of up to 79 symbols. (The modem does not check the correctness of xxxx). While configuring any device connected to the MONITOR bus, enter the ↵%↵ command to return to the device management for which the Telnet session is open.

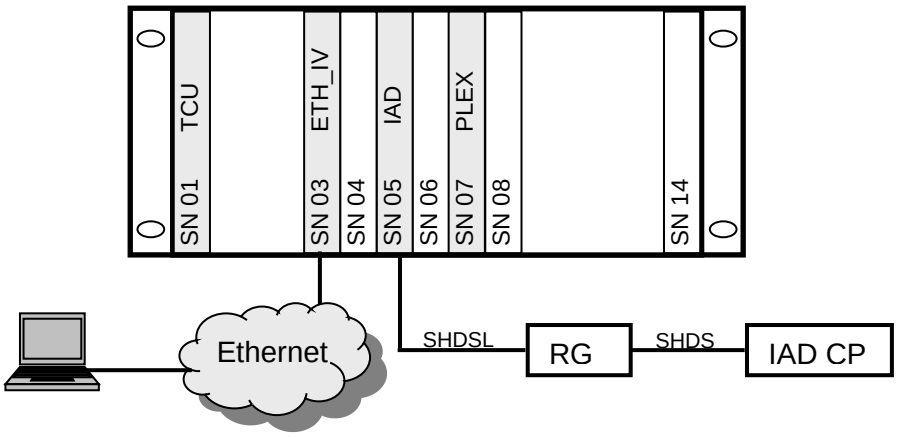


Figure 3.20 Example of Telnet access through Etherlink IV LTU in subrack

To manage devices via TELNET, it is necessary:

- open the Telnet session for the ETHERLINK IV LTU device. Perform authentication (enter the unit with the admin rights)
- to access the IAD unit, enter <%105>
- to access the PLEX unit, enter <%107>
- to access the RGN unit (IAD and RGN are units of the Etherlink family), enter <%10510>
- to access the IAD CP unit, enter <%105120>

3.4.2.2 WEB

The WEB interface is used to display statistics when the Etherlink IV SHDSL modems are connected to the management computer via the Ethernet interface. Any WEB browser can be used to access the WEB interface. To display the statistics you should enter the command: **http://X.X.X.X/** on the WEB browser. (X.X.X.X is the IP-address of the modem). After the connection is established, the active window of the WEB browser displays the following alarms and statistics (there are several pages available):

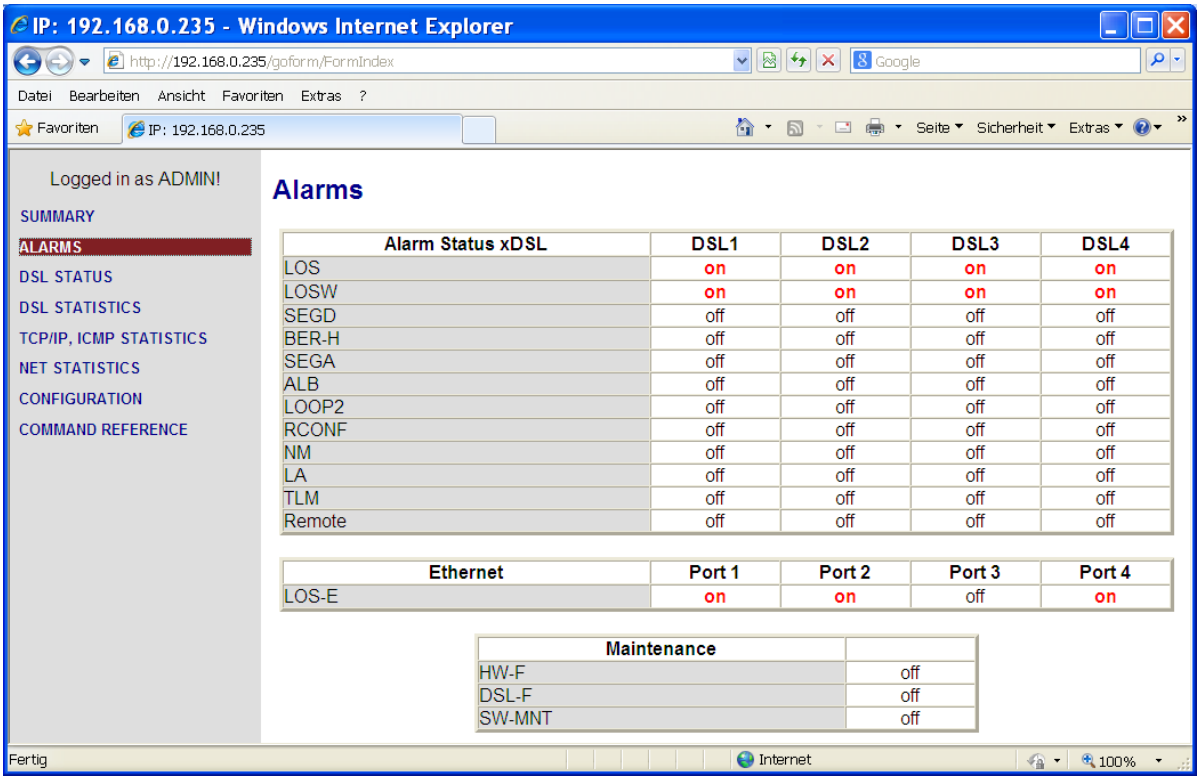


Figure 3.21 WEB interface – “Etherlink IV Alarms”

If you chose the configuration menu you have some tabs for the configuration. Please check under the command description if you need some explanation about any setting. If you have changed the configuration you have to press the “Save” button. The configuration gets active after pressing the “Apply All” button and if you like to have the configuration stored you have to press the “Confirm” button.

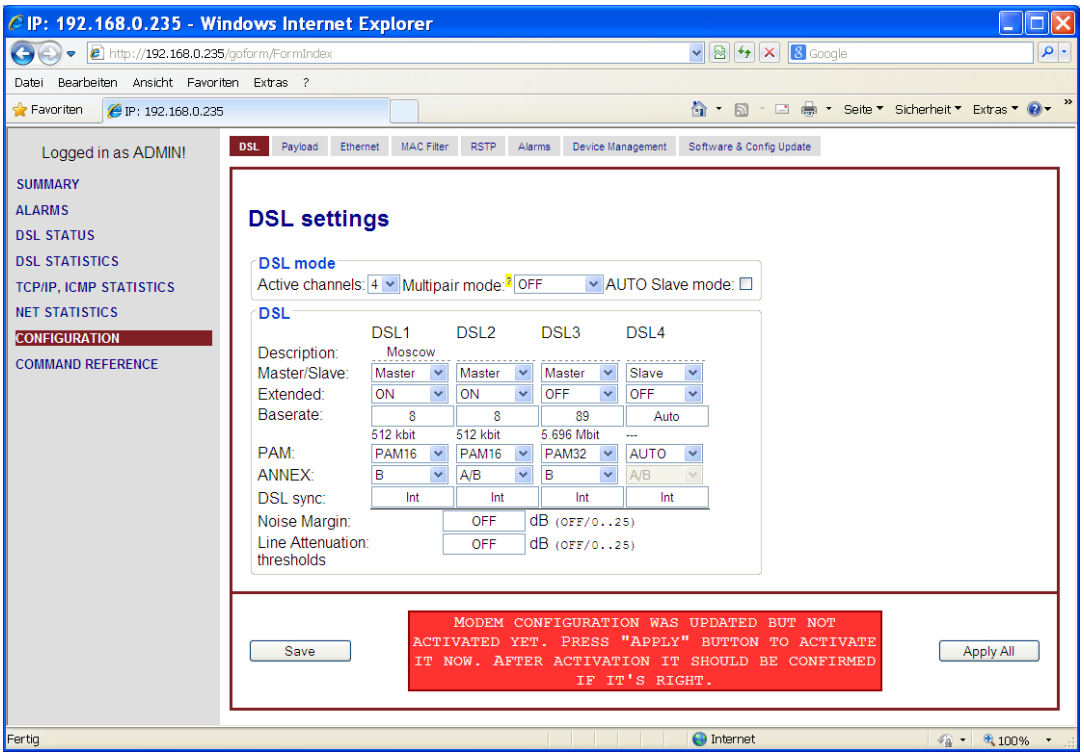


Figure 3.22 WEB interface – “Etherlink IV Configuration”

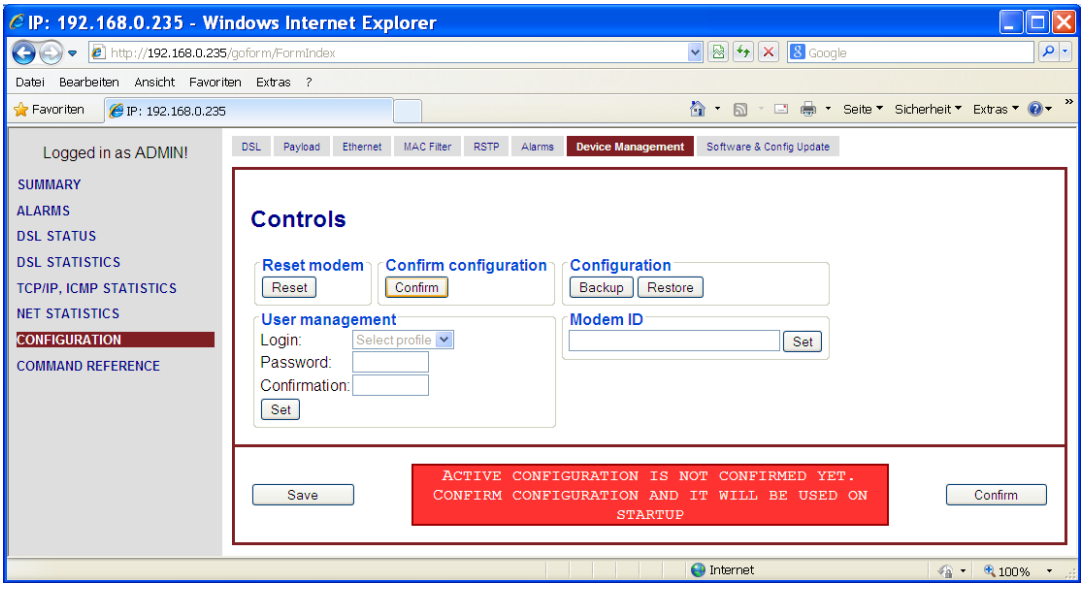


Figure 3.23 WEB interface – “Etherlink IV Configuration-Device Management”

All tables are displayed dynamically. The parameters in the tables are refreshed every 5 seconds. Click the button in the left part of the window of the WEB browser to display the necessary table. The software version is also displayed in the left part of the window. The WEB interface of the SHDSL line card has following windows: Alarms, DSL Status, DSL Statistics (G.826), TCP/IP & ICMP Statistics, Net (WAN) Statistics, Command Reference.

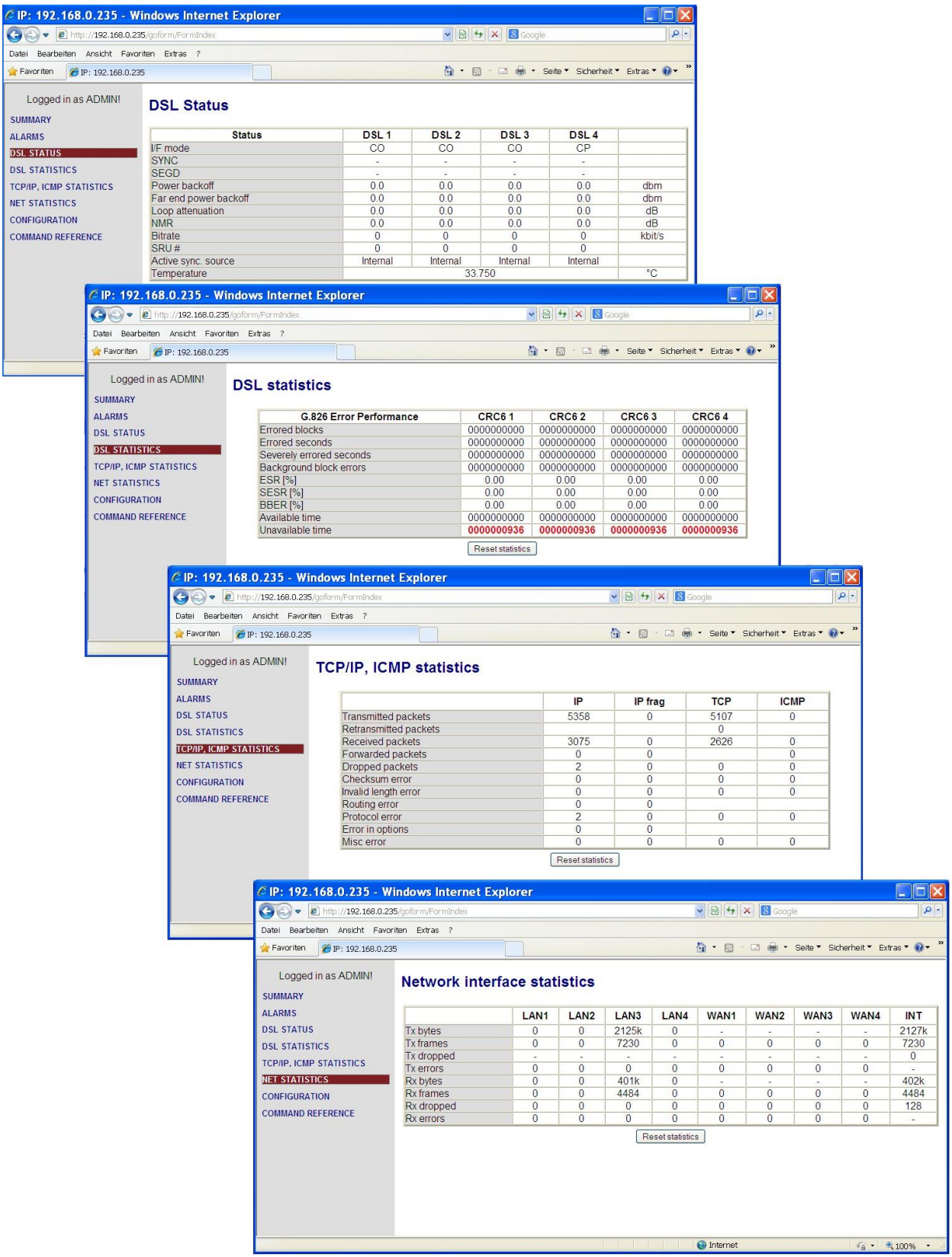

IP: 192.168.0.235 - Windows Internet Explorer
Logged in as ADMIN!
SUMMARY
ALARMS
DSL STATUS
DSL STATISTICS
TCP/IP, ICMP STATISTICS
NET STATISTICS
CONFIGURATION
COMMAND REFERENCE
DSL Status
Status DSL 1 DSL 2 DSL 3 DSL 4
I/F mode CO CO CO CP
SYNC - - - -
SEGD - - - -
Power backoff 0.0 0.0 0.0 0.0 dbm
Far end power backoff 0.0 0.0 0.0 0.0 dbm
Loop attenuation 0.0 0.0 0.0 0.0 dB
NMR 0.0 0.0 0.0 0.0 dB
Bitrate 0 0 0 0 kbit/s
SRU # 0 0 0 0
Active sync. source Internal Internal Internal Internal
Temperature 33.750 °C
DSL statistics
G.826 Error Performance CRC6 1 CRC6 2 CRC6 3 CRC6 4
Errored blocks 0000000000 0000000000 0000000000 0000000000
Errored seconds 0000000000 0000000000 0000000000 0000000000
Severely errored seconds 0000000000 0000000000 0000000000 0000000000
Background block errors 0000000000 0000000000 0000000000 0000000000
ESR [%] 0.00 0.00 0.00 0.00
SESR [%] 0.00 0.00 0.00 0.00
BBER [%] 0.00 0.00 0.00 0.00
Available time 0000000000 0000000000 0000000000 0000000000
Unavailable time 0000000936 0000000936 0000000936 0000000936
Reset statistics
TCP/IP, ICMP statistics
IP IP frag TCP ICMP
Transmitted packets 5358 0 5107 0
Retransmitted packets 0
Received packets 3075 0 2626 0
Forwarded packets 0 0 0
Dropped packets 2 0 0 0
Checksum error 0 0 0 0
Invalid length error 0 0 0 0
Routing error 0 0
Protocol error 2 0 0 0
Error in options 0 0
Misc error 0 0 0 0
Reset statistics
Network interface statistics
LAN1 LAN2 LAN3 LAN4 WAN1 WAN2 WAN3 WAN4 INT
Tx bytes 0 0 2125k 0 - - - - 2127k
Tx frames 0 0 7230 0 0 0 0 0 7230
Tx dropped - - - - - - - - 0
Tx errors 0 0 0 0 0 0 0 0 -
Rx bytes 0 0 401k 0 - - - - 402k
Rx frames 0 0 4484 0 0 0 0 0 4484
Rx dropped 0 0 0 0 0 0 0 0 128
Rx errors 0 0 0 0 0 0 0 0 -
Reset statistics

Figure 3.24 WEB interface – “Etherlink IV DSL Status, Statistics G.826, WAN (Net) Statistics, E1 Statistics, TCP/IP, ICMP Statistics”

3.4.2.3 SNMP

The SNMP (Simple Network Management Protocol) is used to monitor the status and to manage network devices. Unlike other management protocols such as Telnet, SSH and HTTP, the SNMP protocol not only allows an operator to manage the unit, but also informs him about the changes in the device status when management session was inactive.

The SNMP protocol has a client-server background. The modems act as SNMP-Agents, they communicate with the SNMP-Server that is actually a software and available free or commercially from various vendors for different platforms. The AccessView Network Management System (NMS) from Blackbox is available too.

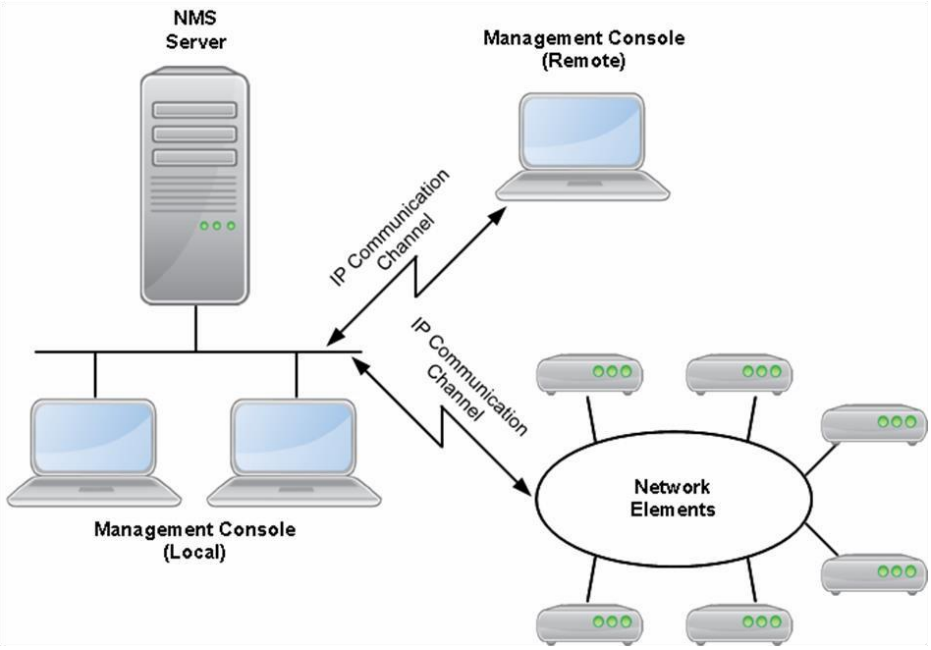


Figure 3.25 The structure of SNMP-based NMS.

The NMS Server authenticates local and remote Management Consoles, interact with other NMS Servers, sends and receives SNMP messages and stores various databases including the MIB database. The Management Information Base (MIB) is a plain text file that has to be imported into the SNMP Server for the purpose of translation the Object Identification (OID) numbers and their content to the human readable format. For example, it is requested to check the status of LAN port. The network administrator can check the SNMP variable with the OID 1.3.6.1.2.2.1.2.2.1.8 path, or, if using MIB file, the same variable can be reachable at the RFC1213-MIB|ifOperStatus address. Its content can be "2" in the first example, or "down" if MIB file is used.

The following MIB files are supported:

- MIB II RFC1213-MIB, a standard MIB for all devices is fully supported
- IF-MIB, RFC-2863, MIB descriptions of interfaces is fully supported
- NATEKS-MIB, MIB for the Nateks/Blackbox equipment is fully supported

- DS1-MIB, RFC-2495, MIB describing E1 streams is partially supported
- RMON-MIB, RFC-2819 remote monitoring for statistics is fully supported
- RS-232-MIB, RFC-1659 for serial interfaces is partially supported
- BRIDGE-MIB, RFC-4188, a standard MIB for Ethernet Bridges is fully supported
- Q-BRIDGE-MIB, RFC-4363, an extended MIB for Ethernet Bridges is partially supported
- RSTP-MIB, RFC-4318, an extended MIB for RSTP protocol is fully supported
- RFC-4133 Entity-MIB partially supported

Local and Remote Management Console are intended for the graphical representation of network map, device icons and device views. It accepts the user actions such as mouse clicks, zooming, key pressings, etc. The Management Console interacts with the SNMP Server via the Remote Procedure Call (RPC) data in TCP/IP envelope. The Management Console can coexist with the SNMP-Server on the same PC or work on a separate computer.

Network Elements are copper and fiber modems, converters and other network devices. Network Elements support the following versions of SNMP protocol:

- V1, is initial version of SNMP protocol
- V2c, is the updated version of SNMP protocol featured bulk requests and long counters
- V3, is the latest version featured authentication and message encryption. Two users are actually supported.

Depending on the SNMP protocol version, the following SNMP messages are supported:

- for the SNMP V1: GET, GET NEXT, SET, TRAP
- for the SNMP V2c: GET, GET NEXT, GET BULK, SET, TRAP
- for the SNMP V3: READ, WRITE, TRAP

GET and READ messages initialized by the SNMP Server and intended for getting information from the Network Element.

SET or WRITE message initialized by the SNMP Server and intended for changing the SNMP variable of the Network Element.

TRAP messages initiated by the Network Element. These messages carry information about status change of the Network Element. For example, if port goes Down or Up, if the device have been restarted, or if the alarm appeared, the TRAP message will be send to the direction of the SNMP Server. Two destinations are supported for TRAP messages.

The following TRAP messages are supported:

- cold Start (RFC-1215)
- authentication Failure (RFC-1215)
- linkUp (RFC-1213-MIB, IF-MIB)
- linkDown (RFC-1213-MIB, IF-MIB)
- dsx1LineStatusChange (DS1-MIB)
- device specific traps (nateks.mib)
- newRoot and topologyChange (RFC-4188, BRIDGE-MIB)
- RMON Event (RMON-MIB)

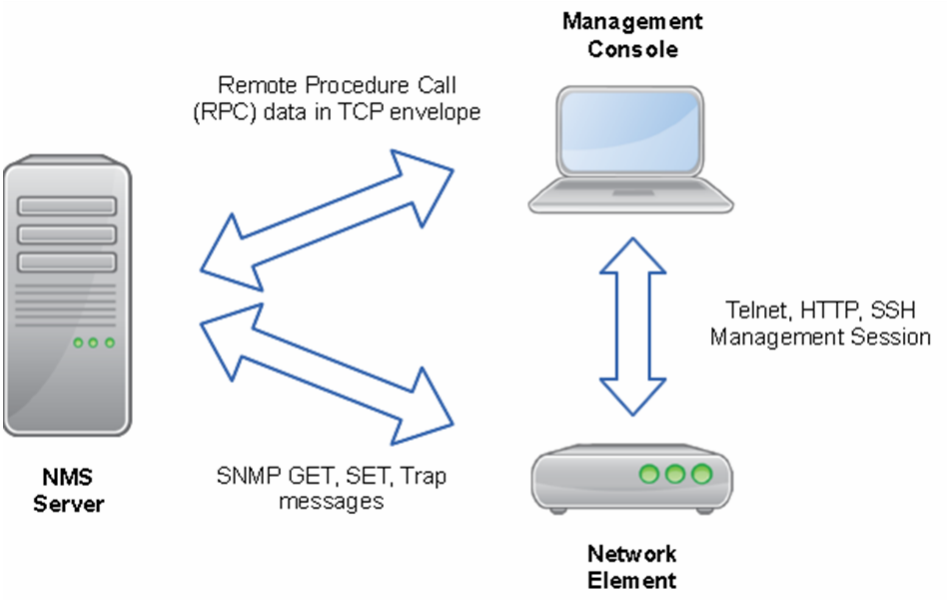


Figure 3.26 Message exchange in SNMP-based networks.

NOTE: The NMS Server is not involved into the message exchange for management protocols such as Telnet, SSH and HTTP. These sessions are initiated between Management Console and Network Element directly.

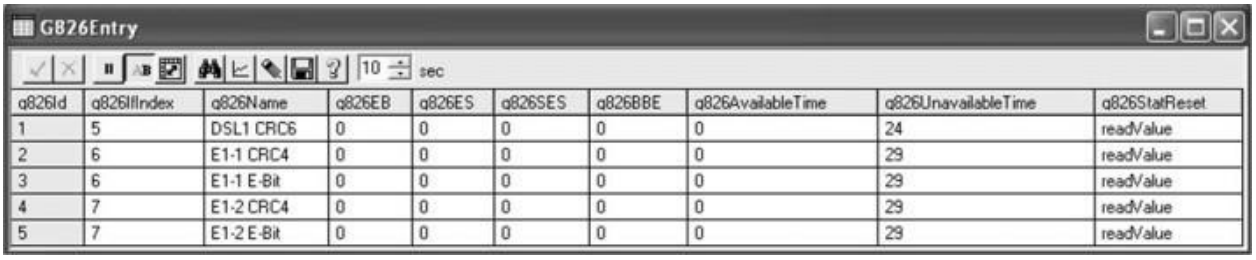
AlarmEntry

10 sec

alarmId	alarmIfIndex	alarmName	alarmValue	alarmCutoff	alarmType
1	2	LOS-E	off	on	local-minor
2	5	LOS	on	off	local-major, remote-major
3	5	LOSW	on	off	local-major
4	5	BER-H	off	off	local-major
5	5	SEGD	off	off	remote-major
6	5	SEGA	off	off	remote-minor
7	5	LOOP2	off	off	local-minor
8	5	ALB	off	off	local-minor, remote-major
9	6	LOS-S	on	off	local-minor
10	6	LFA-S	on	off	local-minor
11	6	BER-S	off	off	local-minor
12	6	AIS-S	off	off	local-minor
13	6	AIS-R	off	off	remote-minor
14	6	LOOP1	off	off	local-minor
15	7	LOS-S	on	off	local-minor
16	7	LFA-S	on	off	local-minor
17	7	BER-S	off	off	local-minor
18	7	AIS-S	off	off	local-minor
19	7	AIS-R	off	off	remote-minor
20	7	LOOP1	off	off	local-minor
21	0	S1-F	off	off	local-major, maintenance
22	0	HW-F	off	off	local-major, maintenance

commonInfo

model	SA-PAM-SA2N-2E1B/Eth
id	NTU MASTER
hardwareVersion	1.0
softwareVersion	1.1.4
softwareDate	26.7.2006
moduleType	standalone-small
subrackAddress	0
errorCode	0



g826Id	g826IfIndex	g826Name	g826EB	g826ES	g826SES	g826BBE	g826AvailableTime	g826UnavailableTime	g826StatReset
1	5	DSL1 CRC6	0	0	0	0	0	24	readValue
2	6	E1-1 CRC4	0	0	0	0	0	29	readValue
3	6	E1-1 E-Bit	0	0	0	0	0	29	readValue
4	7	E1-2 CRC4	0	0	0	0	0	29	readValue
5	7	E1-2 E-Bit	0	0	0	0	0	29	readValue

Figure 3.27 SNMP– “Alarm statistics”, “Information about the device”, “G.826 statistics”

3.4.2.4 SSH

The SSH (Secure SHell) protocol is used to access Etherlink IV devices over IP networks. Unlike Telnet, the SSH packets are encrypted with a key and can't be read if intercepted by an intruder. Therefore User data such as login and password credentials can be safely transmitted over public networks.

The Etherlink IV modem acts as SSH server. It listens default TCP Port 22 for incoming connections from remote clients and initialises Login/Password sequence if connection appears. Default Port 22 can be changed for the security reasons.

User will have an access to the CLI after successful login.

The SSH client is a software for PC. We suggest to use PuTTY for the Microsoft (c) Windows and build-in ssh client for Linux/Unix/MACOS X systems.

NOTE: On Linux/UNIX/MACOS X systems run ssh command with -l parameter to specify the device login name if it is differs from the name of a user who initialise the SSH session.

4 PROGRAMMING GUIDE

4.1 Command Structure

Main Menu		
PM Performance management	**FMM** Fault and maintenance management	**CM** Configuration management
G826	NM	SECURE [ON/OFF]
G826 C	LINKNM	USERS
G826 E1	LINKALARM	USER [name]
G826 E1 C	ALARMLOG [N]	USER [name] DEL
ALLG826 N	ALARMLOG C	USER [name] [+|-] [PRIV]
RESETG826	LINKDIAG	USER [name] [IP] [subnet]
RESETALLG826 N	STATUS	USER [name] [LOCAL/ALL]
NETSTAT [LAN/WAN]	STATUS T	PASSWORD {user}
NETERR [LAN/WAN]	STATUS L	AUTO [ON/OFF]
RESETNETSTAT	STATUS ETH	CONFIG
LINKSTAT	STATUS EXT	CONFIG [N/R/S/B]
LINKALARM	STATUS LLDP	MASTER [ON/OFF] [N]
ALARMLOG [N]	STATUS DOT1X	EXT [ON/OFF] [N]
ALARMLOG C	STATUS RADIUS	BASERATE [N/AUTO] [M]
CONNECT [N:[1-13/R]]	LOOP1 [ON/OFF] [N]	PAM [16/32] [N]
APPLY [ALL/GROUP]	LOOP2 [N:[A/R]] [ON/OFF]	PAYLOAD [list] [N]
LINK [NN]	ALARM	ANNEX [A,B,A/B] [N]
LINKDIAG	ALARM T	SETCLOCK [list] [N]
LINKCLEAR	ACO	MULTIPAIR [2/3/4/2+2/OFF]
M(AIN)	ACO [GROUP] [ON/OFF]	RESERVE [list1] {list2}
H(ELP)	MACTABLE C	G704 [ON/OFF] [N]
	MACTABLE [1-8/OTHER/Port]	CRC4 [ON/OFF] [N]
	MACTABLE	AISDET [ON/OFF] [N]
	LLDP STAT [IF/ALL]	AISGEN [ON/OFF] [N]
	STARTAL [N]	DSLTS [list] [N]
	RESTART [N]	WANTS [list] [N]
	RESET	E1CLOCK {source} [N]
	CONFIRM	E1MODE {mode} [N]
	BACKUP	ID string
	RESTORE	RESPONSE [NN/OFF]
	DIFF [N/R/S/B] [N/R/S/B]	DEFAULT [0-4]
	DUMP [N/R/S/B]	DEFAULT EVERYTHING
	LOAD	DEFAULT DESC
	TLM	SERNUM
	TLM D	GSCOMPAT [ON/OFF]
	TLM S [N:Rnn-Rkk] [ABC]	NMTHR [N/OFF]
	TLM C	LATHR [N/OFF]
	LOG	PTMP [ADD|DEL] [IF]
	LOG C	PTMP SHOW
	SOFTUPDATE	G703CLOCK [DSL/INT/RX]
	TFTP [CMD] [ARG1][ARG2]	MODE [N]
	SOFTCONFIRM	LICENSE
	SOFTINFO	LICENSE ADD [key]
	PING x.x.x.x	RSIP {option} [IF]
	LINKSTAT	RSRATE [N]
	RSTP [CONF/STATE]	RSFORMAT [Format]
	MODEMVIEW	RSDUPLEX [F/H]
	SD SNAPSHOT	AUTOLOOP OFF/ALL/DATA
	SD DIR	EXTCLOCK [SRC] [DIR]
	SD DEL [NAME]	IOIP {option} [IF]

- SD SAVE [N=0..9]
- SD LOAD [N=0..9]
- SD BOOT [ON/OFF]
- SD STATUS
- APPLY [ALL/GROUP]
- CONNECT [N:[1-13/R]]
- LINK [NN]
- LINKCLEAR
- BERT ➡
  - START
  - STOP
  - TRACE
  - SHOW
  - RES
  - SET [E11-E12] [IN/EXT]
  - PATD [2En/bitsring]
  - TS [TX/RX] [list/NONE]
  - CONF
  - APPLY [ALL/GROUP]
  - CONNECT [N:[1-13/R]]
  - LINK [NN]
  - LINKCLEAR
  - M(AIN)
  - H(ELP)
- M(AIN)
- H(ELP)

- APPLY [ALL/GROUP]
- CONNECT [N:[1-13/R]]
- LINK [NN]
- LINKCLEAR
- NET ➡
  - NETCONFIG
  - NETCONFIG [N/R/S/B]
  - COSCONFIG
  - COSCONFIG [N/R/S/B]
  - RSTP DEFAULT
  - RSTP [CONF/STATE/DIAG]
  - RSTP [BR/IF] [OPT] [N]
  - RSTP [A..E] [ON/OFF]
  - PBVLAN [IF] [A..E]
  - MODE [IF] [ACC/TRUNK/MIX]
  - VLAN [IF] [1..8]
  - QOS [IF] [0..7]
  - ALLOW [IF] [VLAN list]
  - VID [1-8] ID
  - MACLIST SHOW
  - MACLIST SHOW [N/R/S/B]
  - MACLIST [IF] ADD [MAC]
  - MACLIST [IF] DEL [MAC/N]
  - MACFILTER [LAN1-5] [ON/OFF]
  - MACRULE [LAN1-5] [rule]
  - DOT1X [LAN1-5] {OPTION}
  - SETIP x.x.x.x
  - GATEWAY x.x.x.x
  - NETMASK x.x.x.x
  - MTU [68..1500]
  - WANIDLE [1/7E]
  - ETHSD [MODE] [N=1-4]
  - FC [ON/OFF] [N=1-4]
  - IRATE [speed/OFF] [N=1-4]
  - ERATE [speed/OFF]
  - CRATE [speed] [CoS] [WAN]
  - COS [QOS/VLAN] [N] [0..3/OFF]
  - SNMP [V1|V2C|V3] [ON|OFF]
  - SNMPACL [1/2] [IP/OFF]
  - TRAPIP [1/2] [IP/OFF]
  - TRAP [1/2] [V1/V2C]
  - TRAP [1/2] V3 [RO/RW]
  - COMMUNITY
  - COMMUNITY [GET/SET/TRAP]
  - SNMPSET [ON/OFF]
  - SNMP [RO|RW] NAME
  - SNMP [RO|RW] AUTH [MODE]
  - SNMP [RO|RW] PRIV [MODE]
  - RMONALARM N [ON/OFF]
  - RMONEVENT N [ON/OFF]
  - LLDP [ON/OFF]
  - LLDP DEFAULT
  - LLDP [PARAM] [VALUE]
  - LLDP [TX|RX] [ON/OFF]
  - LLDP INT VLAN [ON/OFF]
  - LLDP CONFIG
  - SNTP [1/2] [IP/OFF]
  - SNTP TZ [+/-]HH:MM
  - DST [SUMMER|WINTER]
  - DST [OFF/INFO/NAME]
  - SYSLOG [1/2] [IP/OFF]
- M(AIN)
- H(ELP)

[SSH|TELNET|HTTP] [ON/OFF]
SSH PORT [N]
RADIUS [1/2] [IP:P/OFF]
RADIUS [1/2] SECRET
RADIUS RETRIES [0..10]
RADIUS TIMEOUT [1..5]
RADIUS [1/2] TEST
STATUS RADIUS [N/R/S/B]
NETDEFAULT
APPLY [ALL/GROUP]
CONNECT [N:[1-13/R]]
LINK [NN]
LINKCLEAR
M(AIN)

Table 4.1 Command structure according to ITU-T Rec. M.3400

4.2 Etherlink IV Software

Every Etherlink IV device stores up to two software versions in the memory (EEPROM): one unchangeable software (standby software No.1) and one upgradeable software (software No.2). Two versions are necessary to prevent any device failure due to downloading of faulty or damaged software or due to hardware failure during downloading of the new software.
During downloading, the new software overwrites the upgradeable software. If the new software downloading via X-modem is successful, a message appears that the modem should be restarted to start operating under the new software. After the restart, i.e., when the new version of the upgraded software is started for the first time, the operator should confirm the downloaded software. After confirmation, this software becomes unchangeable. If downloading was interrupted or there was a failure in the data transmission, a message is displayed. In this case, if the data has already been partially downloaded into the modem and the upgradeable software is damaged, the unchangeable software will be used to start the modem (please repeat the downloading of the software).
By default, the upgradeable software is the basic one, if it was confirmed. If the upgradeable software was not confirmed after the first start or it was damaged (invalid data format, incorrect checksum), the standby software is loaded.

4.3 Configuration and Application Storage

The whole the system stores four configurations: running configuration, start-up configuration, new configuration and backup configuration.
The **running configuration** contains all configuration values guarantee the current operation of the device. If two modems have the same version of the software and the same running configuration they should operate equally. The running configuration is stored in the RAM of the device. The current parameters determine the operation until the next restart or any actions on the running configuration (storage and etc.). During initialization, the initial parameters of the running configuration are loaded from the start-up configuration.
The **start-up configuration** contains all configuration values which will be used to configure the device after its restart. The start-up configuration is stored in EEPROM and is used to initialize the running configuration during the system start-up.
The **new configuration** stores changes in configuration parameters combined into groups of parameters that require a confirmation of changes (i.e., this configuration stores setting, which should be confirmed after being changed, for example, IP-address of the device). The new

configuration is stored in the device RAM. After setting all necessary changes from the group, the system administrator confirms changes in the group, and values belonging to this group are written from the new configuration into the running one. In this case, the simultaneous application of all setting in the group is guaranteed.
The **backup configuration** is a backup of the current configuration. The backup configuration is stored in the EEPROM. During the configuration restoration, values from the backup configuration are copied to the start-up configuration.

All configuration parameters are divided into three groups according to their application:

- configuration parameters applied after the restart
- configuration parameters applied instantly
- configuration parameters requiring a confirmation

Configuration changes, which are used after the restart, are written into the start-up configuration, but before doing the restart the device continues working according to its “old” configuration. During the device restart, the values of these configurations are copied from the start-up configuration into the running one and thus become valid.

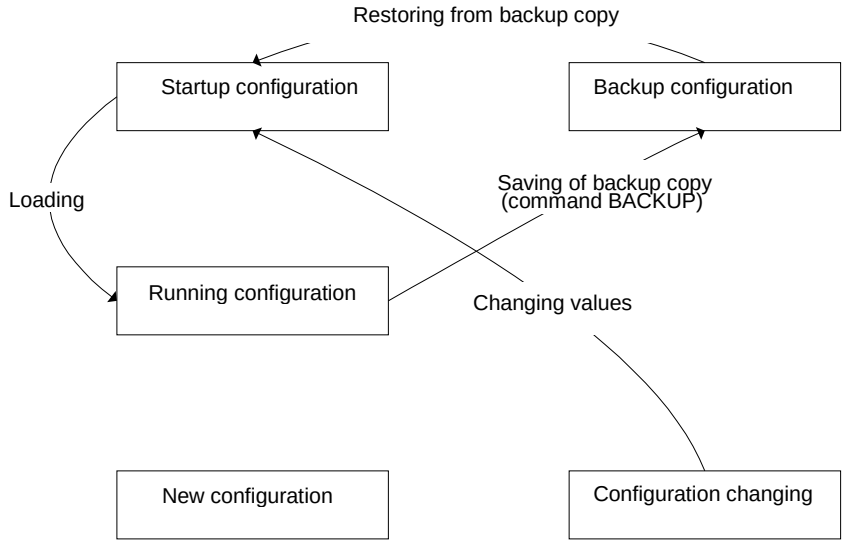


Figure 4.1 Operations of the configuration parameters after the restart

Configuration changes, which are used instantly, are written into the running, start-up and new configuration, and the device continues working according to these configurations.

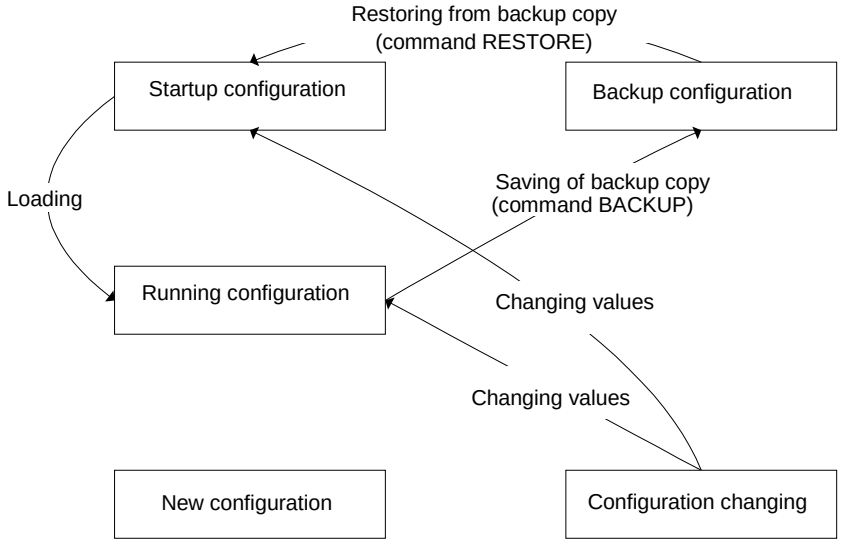


Figure 4.2 Operations of the configuration parameters with the instant application

Changes in configurations, which are part of a group of configurations that require a confirmation, are initially written into the new configuration. After the administrator confirms changes in the group of configurations, this group is copied from the new configuration into the running configuration and the device starts working according to these configurations. The administrator also can confirm changes in all groups. After the received running configuration is checked, the administrator can confirm this configuration. In this case, changes in all groups are copied from the running configuration into the start-up configuration.

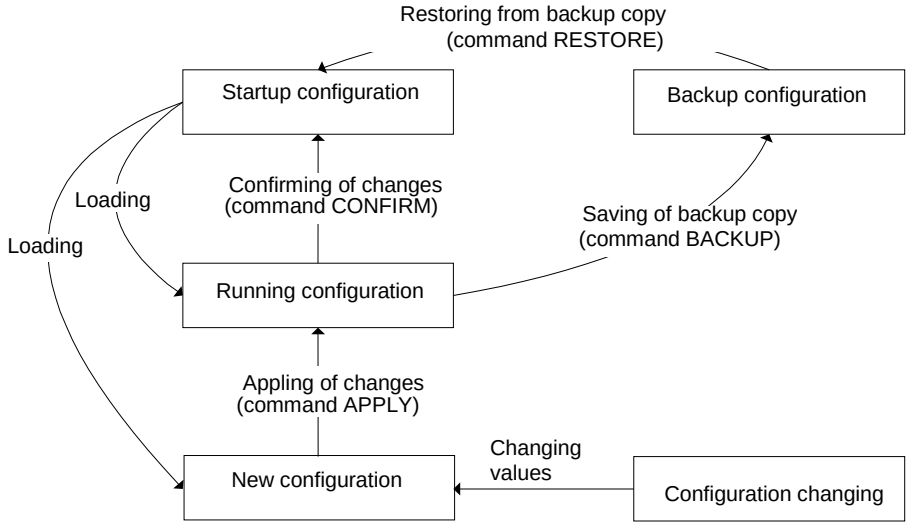


Figure 4.3 Operations of configuration parameters that should be confirmed

4.4 Groups of Commands Requiring Confirmation

In Etherlink IV devices the following four groups of parameters require a confirmation: LINE, NET, VLAN and SNMP. Changing configurations of each group use some special commands. The APPLY

<name of the group> command is used to apply changes in configurations performed in a group. After this, the unit applies changes in configurations. If groups LINE, NET, VLAN were changed not in the local management session via the RS-232 interface but via Telnet the management session breaks and the unit waits for the second connection within 5 minutes (for the LINE group – 30 minutes). If the LINE group was changed remotely (using the CONNECT command), the unit waits for the second connection within 30 minutes. If within this time the operator did not enter the modem menu, the changed parameters are read from the start-up configuration of the unit. Therefore, it is possible to restore the configurations of the unit. A “successful” configuration can become the start-up configuration by using the CONFIRM command.

4.5 Command Syntax

The following rules are used to describe commands:

- parameters in angular brackets **< >** are obligatory
- parameters in direct brackets **[ ]** are not obligatory
- the symbol (***|***) between parameters requires to enter one of the listed parameters
- in real commands brackets and vertical line are not entered, they are used for description
- after the command is typed, press **<enter>**

4.6 Commands

4.6.1 Main Menu

The main menu is presented as shown below:

```
MODEL SA-RC-ETHERLINK_IV4L-4E1B/4Eth-RP, V96
HW 1.6
SW 1.0.0
DATE 10-11-2009
ID
RUNS 0d 00:45:59
ALARM URGENT
STATUS LINK DOWN
MODEL_DESC Subrack Quad xDSL/Quad E1/Quad Ethernet 120 Ohm
IP 192.168.0.235



------------- Main Menu -----------------
1. Performance management (PM)
2. Fault and maintenance management (FMM)
3. Configuration management (CM)

5. Exit
-----------------------------------------
Select [1..5]
CO_01_MM>
```

To select the desired sub-menu, type the appropriate number from “1” to “5” and press <enter>.

4.6.1.1 System Invitation

The following format of the system invitation is used in all menus:

<**cc**>_<**addr**>_<**sf**>>

cc is the device mode:

- RR - Regenerator
- CO – Master
- CP – Slave
- CX – Modem with both types of modes (MASTER and SLAVE)
- CA – Device with automatic selection of the DSL line parameters (MASTER, BASERATE, PAM and ANNEX)

addr is the address of:

- Regenerator in the system (only for Regenerators)
- LTU device in the subrack (slot number, only for subrack LTU devices)

sf is the short form of the current menu:

- MM – Main Menu
- PM – Performance Management
- FMM – Fault and Maintenance Management
- CM – Configuration Management).

For example: CO_PM>
means the device is in the Master mode and we are in the Performance Management menu.

4.6.2 General Commands

4.6.2.1 <H> Command

After the <H> command is entered the device displays the help menu.

4.6.2.2 <APPLY [ALL/GROUP]> Command

This command is used to apply changes in all groups or to apply changes in one of these groups: LINE, VLAN, NET, and SNMP. As a result, changed in the group are written from the new configuration into the running one. Examples:

```
CO_FMM>APPLY
Applying all configuration changes to running configuration

CO_01_PM>APPLY LINE
Applying configuration changes in group LINE to running configuration
```

4.6.2.3 <CONNECT N:1..13/R> Command

The <CONNECT N:1..13/R> commands initialize the management of the remote device. The parameter N sets the number of the SHDSL channel, over which the connection is initialized. In single-channel systems the parameter N can be absent.

Notes:
1. The <CONNECT R> command in the Slave mode is only available if the Master device can be configured locally at this instant.
2. The <CONNECT N> (N=1..13) command initializes the management of the remote regenerator. The <CONNECT N> command is only available in the Master mode.
3. This command is not provisioned for regenerators.
4. If the channel of remote management is blocked (for example, a message or a table are not displayed completely), press Enter.

4.6.2.4 <LINK [SN/00/FE]> Command

The < LINK [SN/00/FE]> command establishes connection to specified unit over the backplane.

- SN - Specifies the slot number of a subrack unit to connect with. If the backplane is busy or if the specified subrack slot is free (or no response in 1.5 first seconds) the "LINK ERROR" message will be issued by the unit. For subrack units SN should not be 00.
- 00 - (double zero) Switches on the Monitor (Local Craft Terminal) connector control mode for Minirack and standalone units. In this mode all typed characters will be translated to the Monitor connector.
- FE - (for ever) Switches on Monitor connector control mode for common CLI RS232 units. In this mode all typed characters will be translated to Monitor connector. The connection will be established until a terminal timeout appears.

Example:
- LINK 10 - Establish connection to subrack unit with slot number 10.
- LINK 00 - Establish monitor control node.
- LINK FE - Establish monitor control node.

Notes: To refuse link connection just exit from controllable unit.
To refuse link connection urgently use CTRL+Z keystroke.

4.6.2.5 <LINKCLEAR> Command

The < LINKCLEAR > command closes current virtual link connections.

4.6.3 Performance Management Menu

After typing “1” in the main menu and pressing <enter>, the following message is displayed:

```
Performance management activated
Enter 'M' to return to MAIN, or 'H' for HELP information

CO_01_PM>
```

4.6.3.1 <H> Command

Type <H> and the monitor list all available commands in the performance sub-menu. If you type H [command] you will get additional help on [command].

```
CO_01_PM>H
------------------------------------------------------------------------------
Type  'H  [command]'  to  get  additional  help  on
[command] G826           Display     xDSL     G.826
statistics
G826 C                   Display xDSL G.826 statistics continuously
G826 E1                  Display E1 G.826 statistics
G826 E1 C                Display E1 G.826 statistics continuously
G826 G703                Display G703 card statistics
G826 G703 C              Display G703 card statistics continuously
ALLG826 N                Display xDSL G.826 statistics for all link
RESETG826                Reset G.826 statistics
RESETALLG826 N           Reset  xDSL  G.826  statistics  for  the  whole
link NETSTAT [LAN/WAN]   Show network statistics counters
NETERR [LAN/WAN]         Show    network    error
counters RESETNETSTAT    Reset network counters
LINKSTAT                 Display link status of all xDSL channels
LINKALARM                Display link alarms of all xDSL channels
ALARMLOG [N]             Display the link alarm log
ALARMLOG C               Clear the link alarm log
LINKNM                   Trace xDSL noise margin of all accessible units
LINKDIAG                 Trace  xDSL  status  of  all  accessible
units APPLY [ALL/GROUP]  Apply changes to running configuration
CONNECT [N:[1-13/R]]     Establish connection to remote unit
LINK [NN]                Establish local connection
LINKCLEAR                Exit all local connections
M                        Return to Main Menu
H                        Show available commands
------------------------------------------------------------------------------
CO_01_PM>
```

4.6.3.2 <G826> Command

The <G826> command displays the ITU-T G.826 performance parameters of the SHDSL line. Depending on the number of SHDSL channels in the system, a table is displayed containing 1, 2 or 4 columns of data.

```
CO_PM>G826
------------------------------------------------------------------------------
G.826 Error Performance  :   CRC6 1     CRC6 2     CRC6 3     CRC6 4
------------------------------------------------------------------------------
Errored blocks           : 0000000000 0000000000 0000000000 0000000000
Errored seconds          : 0000000000 0000000000 0000000000 0000000000
Severely errored seconds : 0000000000 0000000000 0000000000 0000000000
```

```
Background block errors  : 0000000000 0000000000 0000000000 0000000000
ESR  [%]                 :       0.00       0.00       0.00       0.00
SESR [%]                 :       0.00       0.00       0.00       0.00
BBER [%]                 :       0.00       0.00       0.00       0.00
Available time           : 0000005360 0000005360 0000005359 0000005359
Unavailable time         : 0000000031 0000000031 0000000032 0000000032
--------------------------------------------------------------------------------
CO_PM>
```

Option: C – update the table continuously.

CRC6 – Cyclic redundancy check indicating errored blocks received on the SHDSL side.
Errored Block (EB) – A block (transmission duration 6ms) in which one or more bits have errors.
Errored Seconds (ES) – A second period with one or more errored blocks or at least one defect.
Severely Errored Seconds (SES) – A one-second period, which contains more than 30% of errored blocks per second from the total number of all received blocks. SES is a subset of ES.
Background Block Error (BBE) – An errored block not occurring as a part of SES.
Errored Second Ratio (ESR) – The ratio of ES to total seconds in available time during a fixed measurement interval.
Severely Errored Seconds Ratio (SESR) – The ratio of SES to the total number of error-free seconds in available time during a fixed measurement interval.
Background Block Error ratio (BBER) – The ratio of BBE to the total number of error-free seconds in available time during a fixed measurement interval.
Available time – The period when measurements of the parameters are possible.
Unavailable time – The period when the measurements of the parameters are impossible.

4.6.3.3 <G826 E1> Command

This command displays the ITU-T G.826 error performance parameters on the E1 side.

If for the E1 interfaces the CRC4 mode is on the following parameters are shown:

```
CO_PM>G826 E1
--------------------------------------------------------------------------------
G.826  :  1-CRC4   1-E-Bit  2-CRC4   2-E-Bit  3-CRC4   3-E-Bit  4-CRC4   4-E-Bit
--------------------------------------------------------------------------------
EB     : 00000000 00000000 00000000 00000000 00000000 00000000 00000003 00000002
ES     : 00000000 00000000 00000000 00000000 00000000 00000000 00000001 00000001
SES    : 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
BBE    : 00000000 00000000 00000000 00000000 00000000 00000000 00000003 00000002
ESR [%]:     0.00     0.00     0.00     0.00     0.00     0.00     0.01     0.01
SESR[%]:     0.00     0.00     0.00     0.00     0.00     0.00     0.00     0.00
BBER[%]:     0.00     0.00     0.00     0.00     0.00     0.00     0.00     0.00
AT     : 00000000 00000000 00005412 00005412 00000000 00000000 00005411 00005411
UAT    : 00005452 00005452 00000040 00000040 00005452 00005452 00000041 00000041
--------------------------------------------------------------------------------
CO_01_PM>
```

If for the E1 interfaces the CRC4 mode is off the following parameters are shown:

```
CO_PM>G826 E1
--------------------------------------------------------------------------------
G.826  :  1-FAS             2-FAS             3-FAS             4-FAS
--------------------------------------------------------------------------------
EB     : 00000000          00000000          00000000          00000003
ES     : 00000000          00000000          00000000          00000001
SES    : 00000000          00000000          00000000          00000000
BBE    : 00000000          00000000          00000000          00000003
ESR [%]:     0.00              0.00              0.00              0.01
SESR[%]:     0.00              0.00              0.00              0.00
BBER[%]:     0.00              0.00              0.00              0.00
AT     : 00000000          00005557          00000000          00005556
UAT    : 00005609          00000052          00005609          00000053
--------------------------------------------------------------------------------
CO_01_PM>
```

If for the E1 interfaces the ITU-T G.704 framed mode is off, the following parameters are shown:

```
CO_01_PM>G826 E1
-------------------------------------------------------------------------------
G.826  :    1                2                3                4
-------------------------------------------------------------------------------
EB     :
ES     :
SES    :
BBE    :
ESR [%]:
SESR[%]:
BBER[%]:
AT     : 00000000          00005557          00000000          00005556
UAT    : 00005681          00000124          00005681          00000125
-------------------------------------------------------------------------------
CO_01_PM>
```

Option: C – update the table continuously.

Digits 1, 2, 3 and 4 in the first row of the table indicate 1st, 2nd, 3rd and 4th E1 interfaces.
CRC4 – Cyclic redundancy check indicate errored submultiframes received on the E1 side.
E-Bit – CRC4-indication bit denoting received errored submultiframes received on the E1 side.
FAS – Errored frame alignment signal received on the E1 side.
Errored Block (EB) – A block in which one or more bits are in error.
Errored Second (ES) – A second period with one or more errored blocks or at least one defect.
Severely Errored Second (SES) – A second period, which contains more than 805 errored blocks per second (if CRC4 options are enabled) or the number of errored framed alignment is more than 28 per second. SES is a subset of ES.
Background Block Error (BBE) – An errored block not occurring as a part of SES.
Errored Second Ratio (ESR) – The ratio of ES to total seconds in available time during a fixed measurement interval.
Severely Errored Seconds Ratio (SESR) – The ratio of SES to the total number of error-free seconds in available time during a fixed measurement interval.
Background Block Error Ratio (BBER) – The ratio of BBE to the total number of error-free seconds in available time during a fixed measurement interval.
Available time – The period when measurements of the parameters are possible.
Unavailable time – The period when the measurements of the parameters are impossible.

4.6.3.4 <ALLG826 N> Command

This command displays the ITU-T G.826 performance parameters of the specified SHDSL line for the local and remote devices as well as for Regenerators.

```
CO_PM>ALLG826 1
-------------------------------------------------------------------------------
G.826 Error Performance  :  MASTER     N <-- RR1 --> C     SLAVE
-------------------------------------------------------------------------------
Errored blocks           : 000000006 000000001 000000014 000000001
Errored seconds          : 000000002 000000001 000000014 000000001
Severely errored seconds : 000000000 000000000 000000000 000000000
Background block errors  : 000000006 000000001 000000014 000000001
ESR  [%]                 :      0.14      0.14      4.54      4.54
SESR [%]                 :      0.00      0.00      0.00      0.00
BBER [%]                 :      0.00      0.00      0.02      0.02
Available time           : 000001344 000000684 000000308 000000022
Unavailable time         : 000000242 000000421 000000797 000000043
-------------------------------------------------------------------------------
CO_PM>
```

Please see the previous commands for the explanation of the different parameters.

4.6.3.5 <RESETG826> Command

This command clears the ITU-T G.826 error performance counters of the local SHDSL interfaces.

4.6.3.6 <RESETALLG826 N> Command

This command clears the ITU-T G.826 error performance counters of the specified SHDSL interface of the local device, all Regenerators connected to it and on the remote device.

4.6.3.7 <NETSTAT [LAN/WAN]> Command

This command shows the main network (LAN or WAN & MWAN) interface counters.

```
CO_PM>NETSTAT LAN
--------------------------------------------------------------------------------
Interface           LAN1       LAN2        INT
--------------------------------------------------------------------------------
Mode         :      DOWN       DOWN
In
  Octets     :         0          0          0
  Packets    :         0          0          0
  B/mcast    :         0          0          0
  Speed, Kbit:         0          0          0
Size
  64         :         0          0          0
  65-128     :         0          0          0
  129-256    :         0          0          0
  257-512    :         0          0          0
  513-1024   :         0          0          0
  >1024      :         0          0          0
Out
  Octets     :         0          0          0
  Packets    :         0          0          0
  B/mcast    :         0          0          0
  Speed, Kbit:         0          0          0
--------------------------------------------------------------------------------
CO_PM>
```

Parameter	Value	Description
Mode	LAN WAN	LAN status and speed is shown (DOWN, 100F, 10H, etc.) WAN status and working mode is shown (DOWN, WAN1, MWAN1, etc.)
IN	Octets Packets B/mcast Speed,	Total number of octets (bytes) received by this interface incl. erroneous octets. Total number of packets received by this interface incl. erroneous packets. Total number of received broadcast and multicast packets. Average received layer 2 data rate through interface during last second.
Size	64 65-128 129-256 257-512 513-1024 >1024	A histogram of the received packets. It shows the frame size distribution.
OUT	Octets Packets B/mcast Speed,	Total number of octets (bytes) sent by this interface. Total number of packets sent by this interface. Total number of sent broadcast and multicast packets. Average sent layer 2 data rate through interface during last second.

The INT interface (internal) counters are a special case. It's in and out directions are reversed in comparison to any other interface. For example, if frame enters LAN1 and leaves modem through WAN1, it will be counted as in for LAN1 and out for WAN1. But if frame enters LAN1 and is forwarded to INT, it will be counted as in by both LAN1 and INT.
Counters displayed by the NETSTAT command is a subset of the RMON group 1 counters. More interface counters may be seen in SNMP tables defined by RFC1213-MIB, IF-MIB and RMON- MIB.

4.6.3.8 <NETERR [LAN/WAN]> Command

This command shows the main network (LAN or WAN & MWAN) interface error counters.

```
CO_PM>NETERR WAN
--------------------------------------------------------------------------------

Interface           WAN1       WAN2       WAN3       WAN4      MWAN1      MWAN2


--------------------------------------------------------------------------------

In
  Bad octets:          0          0          0          0          0          0
  Discards  :          0          0          0          0          0          0
  Undersize :          0          0          0          0          0          0
  Oversize  :          0          0          0          0          0          0
  Fragments :          0          0          0          0          0          0
  Jabber    :          0          0          0          0          0          0
  MAC error :          0          0          0          0          0          0
  Bad FCS   :          0          0          0          0          0          0
Out
  FCS error :          0          0          0          0          0          0
  Deferred  :          0          0          0          0          0          0
  Collisions:          0          0          0          0          0          0
  .Late     :          0          0          0          0          0          0
  .Excessive:          0          0          0          0          0          0
  .Single   :          0          0          0          0          0          0
  .Multiple :          0          0          0          0          0          0
Pause
  In pause  :          0          0          0          0          0          0
  Out pause :          0          0          0          0          0          0
--------------------------------------------------------------------------------

CO_PM>
```

Parameter	Value	Description
IN	Bad octets	Total number of octets (bytes) received with error.
	Discards	Total number of discarded packets even when no error.
	Undersize	Total number of received packets with size <64 bytes (68 when tagged).
	Oversize	Total number of received packets with size >2040 bytes (2044 when tagged).
	Fragments	Received packets that were undersized and had either FCS or alignment Error.
	Jabber	Received packets that were oversized and had either FCS or alignment Error.
	MAC error	Total number of packets that were dropped due to hardware errors in receiver
	Bad FCS	Total number of received frames that had bad FCS (Frame Check Sequence).
OUT	FCS error	Total number of transmittet octets (bytes) with error.
	Deferred	Total number of discarded packets even when no error.
	Collisions	Total number of collisions:
	Late	Number of late collisions.
	Excessive	LAN half-duplex, number of dropped frames due to excessive number of coll..
	Single	LAN half-duplex, number of successfully transmitted frames due to single coll..
	Multiple	LAN half-duplex, number of successfully transmitted frames due to multiple collisions.
Pause	In pause	LAN links, Number of received MAC pause frames (Flow control).
	Out pause	LAN links, Number of sent MAC pause frames.

4.6.3.9 <RESETNETSTAT> Command

This command resets the statistics from the commands NETSTAT and NETERR.

4.6.3.10 <LINKSTAT> Command

This command shows an actual quick status of the whole link.

```
--------------------------------------------------------------------------------
        DSL 1
--------------------------------------------------------------------------------
          CO link up
     RR1 (N) link up
     RR1 (C) link up
          CP link up
--------------------------------------------------------------------------------
CO_PM>
```

4.6.3.11 <LINKALARM> Command

This command shows the actual alarm status for all units connected over SHDSL.

```
 ------------------------------------------------------------------------------
  Local Alarm: Major
 ------------------------------------------------------------------------------
  DSL 1               DSL 2
 ------------------------------------------------------------------------------
                      RR01 Major
                      CO   Major
 ------------------------------------------------------------------------------
CO_PM>CO_PM>
```

4.6.3.12 <ALARMLOG [N]> Command

This command displays the alarm log (list of all alarms that were detected) for the specified SHDSL interface.

```
--------------------------------------------------------------------------------
      Time ago | Unit  | Event  | Description
--------------------------------------------------------------------------------
        04:45s | LOCAL | E1-2   | LOS-S ----- BER-S ----- -----
        04:18s | RR 1  | N-SIDE | LOS   ----- ----- ----- ----- LOOP2  ------
        04:16s | CO    | E1-1   | ----- ----- ----- ----- -----
--------------------------------------------------------------------------------
CO_PM>
```

Option: C – clears the Alarm log

Time ago - Time since the alarm was detected.
Unit - Unit in link, that reported about the alarm.
Event - Interface of the unit, that detected the alarm.

4.6.3.13 <LINKDIAG> Command

The <LINKDIAG> command displays important parameters of DSL link for local unit, remote unit and for connected repeaters.

```
CO_06_FMM>LINKDIAG
Querying link data: DSL1(.) DSL3(.)
-------------------------------------------------------------------------------
 DSL  Unit        NM    G.826(ES)  Status  Alarms      Description
-------------------------------------------------------------------------------
1     local (CO)  19.0 000000001  up      None        DSL1
      RR1-N       18.0 000000000  up      None        DSL2
      RR1-C       18.0 000000001  up                  DSL1
      remote(CP)  18.0 000000000  up      Minor       DSL1
-------------------------------------------------------------------------------
2     local (CO) ---.- 000000000  pre act LOSW        DSL2
-------------------------------------------------------------------------------
3     local (CO)  18.0 000000001  up      None        DSL3
      RR1-N       19.0 000000000  up      None        DSL4
      RR1-C       18.0 000000001  up                  DSL3
      remote(CP)  17.0 000000000  up      Minor       DSL2
-------------------------------------------------------------------------------
4     local (CO) ---.- 000000000  pre act LOSW        DSL4
-------------------------------------------------------------------------------
CO_06_FMM>
```

Parameter	Value	Description
DSL	1 ... 4	Number of DSL channel counted on local unit
Unit	local remote RRx-N RRx-C	The unit on which the LINKDIAG command executed Remote unit "N" and "C" side of Repeater with number x. X always counted from the Master side. "N" side is connected to Master, while "C" side is connected to Slave
Master / Slave	CO CP	Unit acts as Master modem Unit acts as Slave modem
NM	dB	Noise Margin
G.826(ES)	ES	Number of seconds with errors. According to G.826
Status	up down pre act act	Link is UP Link is Down Link is preparing for activation Link is activating
Alarm	None Minor Major LOSW	No Alarm present on the unit Unit has minor alarm Unit has major alarm Loss of Word on DSL link
Description	ifAlias	Interface Description

4.6.3.14 <M> Command

After this command is entered the device jump to and displays the main menu.

4.6.4 Fault and Maintenance Management Menu

After typing “2” in the main menu and pressing <enter>, the following message is displayed:

```
Fault and maintenance management activated
Enter 'M' to return to MAIN, or 'H' for HELP information

CO_01_PM>
```

4.6.4.1 <H> Command

Type <H> and the monitor lists all available commands in the fault and maintenance sub-menu. If you type H [command] you will get additional help on [command].

```
CX_06_FMM>H
------------------------------------------------------------------------------
Type  'H  [command]'  to  get  additional  help  on
[command] NM              Trace xDSL noise margin
LINKNM                    Trace xDSL noise margin of all accessible units
LINKALARM                 Display link alarms of all xDSL channels
ALARMLOG [N]              Display the link alarm log
ALARMLOG C                Clear the link alarm log
LINKDIAG                  Trace xDSL status of all accessible units
STATUS                    Show current DSL working parameters
STATUS T                  Show current DSL working parameters continuously
STATUS L                  Show current DSL and LINK payload parameters
STATUS ETH                Show Ethernet status
STATUS LLDP               Show LLDP neighbours
STATUS RADIUS [NRSB]      Show RADIUS server status and parameters
LOOP1 [ON/OFF] [N]        Start/stop  local  loopback  at  Nth  E1
interface
LOOP2  [N:[A/R]]  [ON/OFF]  Starts/stops  the  remote  loopback  at  Nth  xDSL
interface ALARM           Display alarms
ALARM T                   Display alarms continuously
ACO                       Show alarm cutoff configuration
ACO [GROUP] [ON/OFF]      Change alarm indication for alarm group
GROUP MACTABLE C          Clear MAC table
MACTABLE  [1-8/OTHER/Port]Print  MAC  table  for
VLAN/port MACTABLE        Print   all   MAC   table
entries
LLDP STAT [IF/ALL]        Show LLDP status per port/for all ports
STARTAL [N]               Toggles  Nth  xDSL  channel  the  analog  loopback
ON/OFF RESTART [N]        Restart Nth xDSL channel
RESET                     Reset modem
CONFIRM                   Confirm running configuration
BACKUP                    Backup running configuration
RESTORE                   Restore  start-up  configuration  from
backup  DIFF  [N/R/S/B]  [N/R/S/B]  Show  difference  between
configurations DUMP [N/R/S/B]      Dump              selected
configuration
LOAD                      Load configuration via XModem
TLM                       Show external alarm status
TLM D                     Show    external    alarm
reaction TLM S [N:Rnn-Rkk] [ABC]  Set up external
alarm reaction TLM C      Clear external alarm table
POWER DIAG                Remote power diagnostics
LOG                       Show non-volatile log messages
LOG C                     Clear non-volatile log
SOFTUPDATE                Update software
TFTP [CMD] [ARG1][ARG2]   Perform maintenance over
TFTP SOFTCONFIRM          Confirm uploaded software
SOFTINFO                  List loaded software
PING x.x.x.x              PING host
LINKSTAT                  Display  link  status  of  all  xDSL
channels RSTP [CONF/STATE]  Show RSTP state/configuration
MODEMVIEW                 Collect modem configuration
SD BOOT [ON/OFF]          Enable/Disable SD card boot
mode SD STATUS            SD card status
```

```
BERT                        BERT configuration menu
APPLY [ALL/GROUP]           Apply    changes    to    running
configuration CONNECT [N:[1-13/R]] Establish connection to
remote unit LINK [NN]       Establish local connection
LINKCLEAR                   Exit all local connections
M                           Return to Main Menu
H                           Show available commands
--------------------------------------------------------------------------------
```

4.6.4.2 <NM> & <LINKNM> Command

The <NM> command displays the ITU-T G.991.2 Noise Margin. It means the maximum possible increase in the Noise Margin for which the BER is expected to be not less than 10^{-7} [dB].

```
CO_FMM>NM
Channel:    DSL1      DSL2      DSL3      DSL4
SHDSL NM:    10.5      11.5      10.5      10.0 dB
```

The number of columns is equal to the number of SHDSL channels of the device.
The <LINKNM> command displays the noise margin of a complete link (CO, RR and CP).

A normal quality of a SHDSL data transmission is possible for NM ≥ 6 dB.

4.6.4.3 <STATUS> Command

The <STATUS> command displays the actual status of the SHDSL transceiver.

```
CO_01_FMM>STATUS
--------------------------------------------------------------------------------
Status                 :       DSL1       DSL2       DSL3       DSL4
--------------------------------------------------------------------------------
I/F mode               :         CO         CO         CO         CO
SYNC                   :          -          -          -          -
SEGD                   :          -          -          -          -
Power backoff          :        0.0        0.0        0.0        0.0 dbm
Far end power backoff  :        0.0        0.0        0.0        0.0 dbm
Loop attenuation       :        0.0        0.0        0.0        0.0 dB
NMR                    :        0.0        0.0        0.0        0.0 dB
Bitrate                :          0          0          0          0 Kbit/s
SRU #                  :          0          0          0          0
Active sync. source    :   Internal   Internal   Internal   Internal
Remote power state     :    120V,ON        OFF    120V,ON        OFF
--------------------------------------------------------------------------------
Temperature            :   42.875 C
--------------------------------------------------------------------------------

CO_01_FMM>
```

Option: T – update the table continuously.
Option: L – show the DSL and Link parameters. For the STATUS L explanation please see the CONFIG command explanations.

Parameter	Value	Description
I/F mode	CO CP	The interface is in the Master mode The interface is in the Slave mode
SYNC	1 - (0)	Synchronization in the SHDSL line is established Synchronization in the SHDSL line is absent

SEGD	1 0 -	Transmitted data over the SHDSL line are valid Transmitted data over the SHDSL line are not valid Data are not received
Power backoff	N	Output signal power [dBm]
Far end power backoff	N	Output signal power [dBm] remote side
Loop attenuation	N	Attenuation in the loop [dB]
NMR	N	Maximum possible increase in the noise margin for which the BER is expected to be not less than 10^{-7} [dB]
Bitrate	N	Data transmission rate of the SHDSL line [Kbit/s]
SRU #	N	Number of regenerators in the system
Active sync. source	External E1-1 E1-2 E1-3 E1-4 Internal	External sync E1-1 network interface E1-2 network interface E1-3 network interface E1-4 network interface Internal sync source
Remote Power State	120V,ON OFF	Remote Power Source switched on Remote Power Source switched off
Temperature	N	Unit temperature [C°]

Table 4.1 <STATUS> definitions

4.6.4.4 <STATUS ETH> Command

This command displays parameters of the Ethernet ports (ETH1 – ETH4), namely the rate and the operation mode.

```
CO_01_FMM>STATUS ETH
Ethernet port 1 speed/duplex: ---
Ethernet port 2 speed/duplex: 100 FULL
Ethernet port 3 speed/duplex: ---
Ethernet port 4 speed/duplex: ---
CO_01_FMM>
```

4.6.4.5 <STATUS EXT> Command

This command displays status of daughter card or cards.

```
CP_FMM>STATUS EXT
-------------------------------------------------
 Card     Cable    RTS  CTS  DCD  DTR  DSR  LL
-------------------------------------------------
 1. RS232 RS-232  OFF  OFF  OFF  OFF  OFF  ---
-------------------------------------------------
CP_FMM>
```

4.6.4.6 <STATUS LLDP> Command

The <STATUS LLDP> command shows LLDP neighbourhood.

```
CX_06_FMM>STATUS LLDP
MWAN1 neighbour:
```

```
     Port      description:      MWAN2
   Management address: 192.168.1.26
           Chassis   ID:   00:0f:d9:05:5e:61
              Port ID: MWAN2
   System  description:  SA-PAM-SA4N-2Eth,  V84    LABOR  (SW:  1.6.17  HW:  1.4)
CX_06_FMM>
```

Parameter	Value	Description
Port description	String	Remote port description
Management address	IP Address	IP address of remote unit
Chassis ID	ID	MAC address or ID of remote unit
Port ID	ID	Remote port identification
System description	String	Remote system description

4.6.4.7 <STATUS RADIUS> Command

The <STATUS RADIUS> command displays the actual status of RADIUS servers

```
CO_FMM>STATUS RADIUS
------------------------------------------------------------------------------
Status                :       Server 1             Server 2
------------------------------------------------------------------------------
Status                :       Connected            Not connected
Server IP             :       255.255.255.255      255.255.255.255
Server port           :       1812                 1812
Shared key            :       entered              empty
Retries               : 2
Timeout, seconds      : 2
------------------------------------------------------------------------------
CO_FMM>
```

Parameter	Value	Description
Status	Connected Not connected	Client has a connection with RADIUS server Radius server is not configured or not responding
Server IP	IP Address	IP address of RADIUS Server
Server port	0-65535	UDP Port, the RADIUS server is listen on for incoming connections
Shared key	Entered Empty	Shared key is present in the client Shared key is not present in the client
Retries	0-10	Number of retries, the client will use to authenticate the user on both RADIUS servers. 0 means no attempts.
Timeout, seconds	1-5	Time interval between authentication attempts.

4.6.4.8 <STATUS DOT1X> Command

The <STATUS DOT1X> command shows IEEE 802.1x status per LAN interface.

```
CP_FMM>STATUS DOT1X
====================================
Port  802.1x mode        Authorized
====================================
LAN1  Multi-host         Yes
      00:1b:24:a6:38:b6  Pass
      08:00:27:c8:0c:b8  Auth
LAN2  Multi-host         No
====================================
CP_FMM>
```

Parameter	Description
Authorized (Port)	Displays if LAN port received permission from server to pass traffic
Authorised (MAC)	Displays if device with MAC address either passed authentication (Auth), or transmits traffic (Pass) or in blocking state (Block)
802.1x mode	Ether MAUTH, MHOST or SHOST

4.6.4.9 <LOOP1 ON/OFF [N=1..4]> Command

This command activates/deactivates the local loop back on the network interface (E1 interface).

```
CO_FMM>LOOP1 ON 1
Local loopback on E1-1 interface has been set
CO_FMM>LOOP1 OFF 1
Local loopback on E1-1 interface has been cleared
CO_FMM>
```

4.6.4.10 <LOOP2 [N:A/R] [ON/OFF]> Command

This command activates/deactivates the remote loop back on the line interface.

The parameter N:A sets the number N of the DSL interface and the device address (as in the CONNECT command). In single-channel systems, the parameter N is not obligatory.
The parameters N=1..13 activates the loop back on the Regenerator, whose number is specified by the value of N. The regenerators are numbered, starting from the Master device.
The parameter N=R activated the remote loop back on the remote device.

```
CO_01_FMM>LOOP2 1:R ON
Loop2 set is initiated.
Loop2 is successfully set.
CO_01_FMM>LOOP2 1:R OFF
Loop2 reset is initiated.
Loop2 is successfully cleared.
CO_01_FMM>
```

4.6.4.11 <ALARM> Command

The <ALARM> command displays the actual alarm status of the local device. For devices with different numbers of E1 and SHDSL channels, the number of displayed columns is different too.

```
CO_01_FMM>ALARM
-------------------------------------------------------------------------------
Alarm status  : E1-1 E1-2 E1-3 E1-4     SHDSL  :  DSL1  DSL2  DSL3  DSL4
-------------------------------------------------------------------------------
LOS-S         :   on   on   on   on     LOS    :    on    on    on    on
LFA-S         :  off  off  off  off     LOSW   :    on    on    on    on
AIS-S         :  off  off  off  off     SEGD   :   off   off   off   off
AIS-R         :  off  off  off  off     BER-H  :   off   off   off   off
LOOP1         :  off  off  off  off     ALB    :   off   off   off   off
BER-S         :  off  off  off  off     SEGA   :   off   off   off   off
              :                         NM     :   off   off   off   off
              :                         LA     :   off   off   off   off
                                        LOOP2  :   off   off   off   off
                                        RCONF  :   off   off   off   off
-------------------------------------------------------------------------------
Ethernet      :    1    2    3    4     Maintenance
-------------------------------------------------------------------------------
LOS-E         :   on   on   on   on     HW-F   :   off
                                        DSL-F  :   off
-------------------------------------------------------------------------------
CO_01_FMM>
```

Option: T – enable the continuous updating of the table with actual alarm status.

Definitions (E1 interface)	
LOS-S	Loss of signal on the E1 side
LFA-S	Loss of frame alignment on the E1 side
AIS-S	Receiving AIS on the E1 side
AIS-R	Receiving AIS on the E1 side by a remote device
BER-S	The block error rate on the E1 side exceeded the admissible value
LOOP1	A loop is activated on the network interface in the direction of the E1 equipment
Definitions (Ethernet)	
LOS-E	Loss of signal on the Ethernet interface
Definitions (SHDSL)	
LOS	Loss of signal in SHDSL
LOSW	Loss of signal or frame alignment in SHDSL (loss wire)
SEGD	A failure in the line (segment degradation)
BER-H	The block error rate in the line is according to G.826 ≥ 30%
ALB	Analogue loop back is active
SEGA	Errored data or errored frame alignment (segment alarm)
NM	Noise Margin < NM threshold
LA	Loop Attenuation > LA threshold
LOOP2	A loop is activated on the line interface of a remote device in the direction of the local device
RCONF	Configuration of the remote device is not compatible with the configuration of the local device (for example, the local device is configured to transmit Ethernet data, while the remote device is configured to transmit two E1 streams)
Definitions (Maintenance):	
HW-F	Hardware failure
DSL-F	DSL failure

Table 4.2 <ALARM> definitions

4.6.4.12 <ACO [GROUP ON/OFF])> Command

The <ACO> command (Alarm Cut Off) without additional parameter shows deactivated alarm indications (LED and relays).

```
CO_FMM>ACO
ETH1, ETH2, ETH3, ETH4
CO_01_FMM>
```

The <ACO [GROUP ON/OFF]> command activates/deactivates a GROUP for alarm indications.

```
CO_01_FMM>ACO E1-1 OFF
ETHERNET
CO_FMM>
```

Available alarm groups:

GROUP	Description
E1-1 or E11	1st E1 channel
E1-2 or E12	2nd E1 channel
E1-3 or E13	3rd E1 channel
E1-4 or E14	4th E1 channel
E1	All E1 channels
ETH1 or ETHERNET1	1st Ethernet port

GROUP	Description
ETH2 or ETHERNET2	2nd Ethernet port
ETH3 or ETHERNET3	3rd Ethernet port
ETH4 or ETHERNET4	4th Ethernet port
ETH or ETHERNET	All Ethernet ports
DSL1 or SHDSL1	1st DSL channel
DSL2 or SHDSL2	2nd DSL channel
DSL3 or SHDSL3	3rd DSL channel
DSL4 or SHDSL4	4th DSL channel
DSL or SHDSL	All DSL channels
RCONF	RCONF alarm

The deactivated alarms do not generate any urgent or non-urgent alarms (i.e. does not affect the colour of LEDs on the front panel and alarm relay status).

Note: By default the Ethernet alarm LEDs are blocked in all configurations.

By typing this command, the GROUP parameter cannot contain several alarm groups. Example: if it is necessary to deactivate the alarm status of the group E1-1 and DSL, enter the ACO command twice: first, with the parameter E1-1, and second, with the parameter DSL.

```
CP_FMM>ACO E1-1 ON
E1-1, ETHERNET
CP_FMM>ACO DSL ON
E1-1, SHDSL, ETHERNET
CP_FMM>
```

4.6.4.13 <MACTABLE> Command

This command shows the MAC address table of every interface. If MAC address is blocked by the MAC Filter Rule, it will be marked as "BLOCKED"

The command MACTABLE C clears the MAC table.

The command MACTABLE [Port] shows the entries only for a [Port], where Port represents any network interface according to NETCONFIG command. For example: LAN1, WAN2, MWAN1, INT.

The command MACTABLE [1-8] shows the entries only for any selected VLAN number. VLANs are according to the NETCONFIG command.

The command MACTABLE OTHER shows the entries for OTHER VLANs (with VID not matching one of VLAN 1..8.

First column is the MAC address. The second column is the originating interface where this MAC is learned from. Third column is VLAN number. Forth column indicates if MAC address is blocked.

```
CX_05_FMM>MACTABLE
00:0f:d9:10:45:84  MWAN1  VLAN1
00:0f:d9:06:83:20  MWAN2  VLAN1
00:e0:4c:69:23:41  MWAN2  VLAN1
00:0f:d9:05:3f:8d  MWAN1  VLAN1
00:0f:d9:06:77:91  INT    VLAN1
00:0f:d9:04:d3:95  MWAN1  VLAN1
00:0f:d9:10:21:77  MWAN1  VLAN1
00:90:f5:3e:7a:0b         VLAN1 BLOCKED
CX_05_FMM>
```

4.6.4.14 <LLDP STAT [IF/ALL]>

The <LLDP STAT [IF/ALL]> command shows detailed LLDP status for selected port or for all ports.

```
CX_06_FMM>LLDP STAT ALL
IfIndex 11 neighbors
00:0f:d9:05:5e:61  age: 1 ttl: 121
           Chassis  ID:  MAC  address  00:0f:d9:05:5e:61
              Port ID: Interface name MWAN2
                  TTL: 121
     Port description: MWAN2
   System description: SA-PAM-SA4N-2Eth, V84  LABOR (SW: 1.6.17 HW: 1.4) System
  capabilities: system: 0x4 enabled: 0x4
   Management address: IPv4 192.168.1.26 ifIndex(2): 5

       Management    VID:    1
   Maximum frame size: 2048
     MED  capabilities:  device  type:  1,  capabilities:  0x21
    Hardware Revision: 1.4
    Software   Revision:   1.6.17
        Serial            Number:
        CCS110412309
           Model Name: SA-PAM-SA4N-2Eth, V84  LABOR
CX_06_FMM>
```

Parameter	Value	Description
Chassis ID	ID	MAC address or ID of remote unit
Port ID	ID	Remote port identification
TTL	Integer	Remote table actualization time in seconds
Port description	String	Remote port description
System Description	String	System name
System Capabilities	HEX	System capabilities according to IEEE 802.1AB
Management Address	IP Address	IP address of remote unit
Maximum frame size	Integer	Maximal frame size the unit can accept. Note it reflects only the LAN switch side of the modem. Maximal Frame size is 2044 for data transmission over DSL
MED Capabilities	HEX	System capabilities according to MED extension
Hardware Revision	String	Hardware version
Software Revision	String	Software version
Serial Number	String	System serial number
Model Name	String	Remote system name

4.6.4.15 <STARTAL [N]> Command

This command starts/stops (toggles) the analogue loop back at the SHDSL line interface on the device with the number N. For single-channel devices this command is entered without the parameter N.

```
CO_09_FMM>STARTAL 1
Analog loopback started
CO_09_FMM>STARTAL 1
Analog loopback stopped
CO_09_FMM>
```

Note: This command is used in the Master mode. Detach the cable from the SHDSL connector before starting the analogue loop back.

4.6.4.16 <RESTART [N=1..4]> Command

This command restarts the corresponding SHDSL channel. First it causes the loss of sync between modems which later will be restored. For single-channel devices the command is used without any additional parameters.

```
RR_FMM>RESTART 1
Restarting channel 1
RR_FMM>
```

4.6.4.17 <RESET> Command

The <RESET> command restarts the device.

```
CP_FMM>RESET
```

4.6.4.18 <CONFIRM> Command

This command confirms the running configuration and writes it to the start-up configuration. As a result, after confirmation of the configuration variables changes in all groups, they will be written from the running configuration into the start-up configuration.

```
CO_FMM>CONFIRM
Current running configuration is confirmed and written to
startup configuration in EEPROM
```

4.6.4.19 <BACKUP> Command

This command is used to create a backup of the running configuration of the device in the EEPROM. As a result, the running configuration is written to the backup configuration.

```
CO_FMM>BACKUP
Current running configuration is written to
backup configuration in EEPROM
CO_FMM>
```

4.6.4.20 <RESTORE> Command

This command restores the start-up configuration from the backup configuration, which was stored in the EEPROM. The modem should be restarted that restored values become valid.

```
CO_FMM>RESTORE
Restored startup configuration from backup configuration.
Reset modem for all changes to take effect
CO_FMM>
```

4.6.4.21 <DIFF N/R/S/B N/R/S/B> Command

This command displays differences between up to four configurations: New, Running, Start-up, or Backup.

```
CO_FMM>DIFF R B
--------------------------------------------------------------------------
Running configuration     Backup configuration
--------------------------------------------------------------------------
VLAN.VLANMASK.3
```

```
00 01                    | 00 07
------------------------------------------------------------------------
CO_FMM>
```

The command displays the name of the difference parameter and data from two configurations. In the above example one can see that the VLANMASK parameter of interface 3 (WAN2) of the VLAN group in the running configuration differs from the backup configuration. If there are no differences, the result is presented as follows:

```
CO_FMM>DIFF N R
------------------------------------------------------------------------
New configuration         Running configuration
------------------------------------------------------------------------
--- No differences ---    --- No differences ---
------------------------------------------------------------------------
CO_FMM>
```

4.6.4.22 <DUMP N/R/S/B> Command

This command displays the dump of the corresponding configuration: New. Running, Start-up or Backup.

```
CO_FMM>DUMP R
------------------------------------------------------------------------
Dump of running configuration
------------------------------------------------------------------------
NET.MAC_ADDRESS
00 0F D9 00 10 03
M.DEVICE_ID
00 00 00 00 00 00 00 00 00 43 4F 4D 4D 4F 4E 00\
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00\
00
NET.MAC_SPEED
5A
SNMP.TRAPIP.0
00 00 00 00
SNMP.TRAPIP.1
00 00 00 00
SNMP.COMMUNITY
43 4F 4D 4D 4F 4E 00 20 60 00 00 13 00 02 B2 3C\
00 18 65 44 00 05 5E 2C FF FF FF FF 00 17 59 F8\
00
M.ALARM_CUTOFF
02
NET.IP
C0 A8 5A 14
NET.NETMASK
FF FF FF 00
NET.GATEWAY
C0 A8 5A 64
NET.PPPREMIP
C0 A8 5A 5A
PE1.G704.0
01
SE1.G704.1
01
PE1.CRC4DET.0
00
SE1.CRC4DET.1
00
  ...

------------------------------------------------------------------------
CO_FMM>
```

The results of the command show the coded configuration of the device and can be copied from the terminal window into the notepad as well as saved on any data carrier. This txt file can be

downloaded into a similar device with the help of the LOAD command via the XModem or 1K XModem protocols.

4.6.4.23 <LOAD> Command

The <LOAD> command downloads the configuration file obtained with the help of the DUMP command into a device via the XModem or 1K XModem protocols. For Windows 95 or above, this procedure can be performed with the help of the HyperTerminal program. By typing LOAD, the following text will be displayed in the terminal window:

```
CO_FMM>LOAD
Now upload configuration via XModem or 1K XModem
C
```

Select "Send File" in the Transfer menu. Select the protocol XModem or 1K XModem in the window which appears. Select the downloading configuration file and click the Send button.

If downloading is successful, a message will appear to reset the modem:

```
Configuration was loaded successfully.
For all configuration options to apply, type RESET to reset modem.
CO_FMM>
```

If the configuration file contained errors, a message with the line number in which the error was detected will be displayed. The configuration of the device in this case will not change.

4.6.4.24 <TLM> Command

The < TLM > command shows the external alarm status of Regenerators.

```
CO_01_FMM>TLM
Distant external alarms status
---------- Line 1 -------- Line 2 -------- Line 3 -------- Line 4 ----
     | ALM1 ALM2 ALM3| ALM1 ALM2 ALM3| ALM1 ALM2 ALM3| ALM1 ALM2 ALM3|
-------------------------------------------------------------------------
RR01 | off  off  off | off  off  off | off  off  off | off  off  off |
RR02 | off  off  off | off  off  off | off  off  off | off  off  off |
RR03 | off  off  off | off  off  off | off  off  off | off  off  off |
RR04 | off  off  off | off  off  off | off  off  off | off  off  off |
RR05 | off  off  off | off  off  off | off  off  off | off  off  off |
RR06 | off  off  off | off  off  off | off  off  off | off  off  off |
RR07 | off  off  off | off  off  off | off  off  off | off  off  off |
RR08 | off  off  off | off  off  off | off  off  off | off  off  off |
RR09 | off  off  off | off  off  off | off  off  off | off  off  off |
RR10 | off  off  off | off  off  off | off  off  off | off  off  off |
RR11 | off  off  off | off  off  off | off  off  off | off  off  off |
RR12 | off  off  off | off  off  off | off  off  off | off  off  off |
RR13 | off  off  off | off  off  off | off  off  off | off  off  off |
-------------------------------------------------------------------------
CO_01_FMM>
```

Option: D – shows the reaction of the external alarms of Regenerators.

```
CO_01_FMM>TLM D
Reactions on external alarms
---------- Line 1 -------- Line 2 -------- Line 3 -------- Line 4 ----
     | ALM1 ALM2 ALM3| ALM1 ALM2 ALM3| ALM1 ALM2 ALM3| ALM1 ALM2 ALM3|
-------------------------------------------------------------------------
RR01 | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ |
RR02 | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ |
RR03 | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ |
RR04 | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ |
RR05 | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ |
RR06 | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ |
```

```
RR07 | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ |
RR08 | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ |
RR09 | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ |
RR10 | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ |
RR11 | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ |
RR12 | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ |
RR13 | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ |
-------------------------------------------------------------------
CO_01_FMM>
```

Option C - Clears the status of the TLM table.

4.6.4.25 <TLM S [N:[Rnn-Rkk]] [ABC]> Command

This command sets some LTU reaction on external alarms of Regenerators.

N: Selected line

Rnn - Rkk: Regenerator or the range of regenerators to set reaction for.
Example: 'R1', 'R9', 'R04', 'R1-R4', 'R07-R09'.

ABC: List of reactions. Must be a string of three digits, each from 0 to 3. First digit corresponds to the first alarm, second - to second, third - to third.
Possible Values:
0 - no reaction.
1 - LTU will show this alarm by 'TLM' command.
2 - LTU will indicate minor remote alarm and show this alarm by 'TLM' command.
3 - LTU will indicate major remote alarm and show this alarm by 'TLM' command.

```
CO_01_FMM>TLM S 1:R1 213
Reactions on external alarms
---------- Line 1 -------- Line 2 -------- Line 3 -------- Line 4 ----
     | ALM1 ALM2 ALM3| ALM1 ALM2 ALM3| ALM1 ALM2 ALM3| ALM1 ALM2 ALM3|
-------------------------------------------------------------------
RR01 | MIN  RES  MAJ | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ |
RR02 | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ |
RR03 | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ |
RR04 | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ |
RR05 | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ |
RR06 | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ |
RR07 | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ |
RR08 | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ |
RR09 | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ |
RR10 | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ |
RR11 | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ |
RR12 | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ |
RR13 | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ | MAJ  MAJ  MAJ |
-------------------------------------------------------------------
CO_01_FMM>
```

4.6.4.26 <POWER DIAG> Command

This command shows the diagnostic information for the remote power. It shows each remote power source configuration, voltage, whether it is turned ON in configuration or actually now. It also shows detailed remote power alarms and leakage current. The alarms are:

- CUR - remote power CURrrent limit is exceeded.
- DCL - 'DC leakage' current value is beyond normal limits (300uA max).
- ACL - 'AC leakage' current value is beyond normal limits (700uA rms max).
- ACM - 'AC Mains'-leakage current with industrial frequency value (50Hz, 60Hz, 16.67Hz) is present and is above 500uA rms.

Leakage currents are measured on a per-remote power supply basis, so for 2x120VDC mode it may be required to unplug one DSL channel to find the channel with leakage current or source of industrial noise.
The DC leakage alarm is the sign that somewhere the wire line insulation is broken and there is conducting path between the wire and ground or any other potential. The AC leakage and especially the AC Mains alarm indicates that there is some longitudinal AC noise, probably from industrial facility, train passing by, bad grounding or direct power contacting.
To track down the AC noise source and frequency, press '1' to show spectrum analysis of the common-mode noise. Further on, from the screen displayed, detailed analysis in 5 different bands from 0-85Hz to 0-12800Hz can be called.
Please, note that DC leakage values can be offset from 0-point by up to 150uA even with DSL line plugged off. This is normal error offset specific to the unit and should not be taken into account.

```
RP overview

RP source 1
  Mode: 2x120V
  Leakage: DC    -3uA  AC:    10uA
    DSL1: Config:  ON, Status:  ON
          Alarms:  --- --- --- ---
    DSL3: Config: OFF, Status: OFF
          Alarms:  --- --- --- ---

RP source 2
  Mode: 2x120V
  Leakage: DC   215uA  AC:     8uA
    DSL2: Config: OFF, Status: OFF
          Alarms:  --- --- --- ---
    DSL4: Config: OFF, Status: OFF
          Alarms:  --- --- --- ---

(1) Leakage analysis    (M) Exit
```

Pressing “1”

```
AC analysis
RP source 1
                    uA ^
                     1k|
                    500|
DC       :   -5uA   100|
AC(RMS)  :    8uA    50|
                     10|
                       `+--+--+--+--+--+--+--+--+--+--+-->
                        0  10 20 30 40 50 60 70 80 90 100Hz
RP source 2
                    uA ^
                     1k|
                    500|
DC       :  214uA   100|
AC(RMS)  :    9uA    50|
                     10|
                       `+--+--+--+--+--+--+--+--+--+--+-->
                        0  10 20 30 40 50 60 70 80 90 100Hz

(1) Detailed RP1    (2) Detailed RP2    (M) Exit
```

4.6.4.27 <LOG> and [LOG C] Command

The command <LOG> shows a record about all commands and events that are stored in non-volatile memory. The command <LOG C> clears the record (log).

4.6.4.28 <SOFTUPDATE> Command

This command downloads the new software into the device memory by using the XMODEM or 1K XMODEM protocol. The SOFTUPDATE command downloads only the second version of the software into the flash memory. During the new software downloading the analysis of the % symbols is not performed.

```
CP_FMM>SOFTUPDATE
Flash manufacturer: Spansion
      Flash device: S29AL016D(02)
     Start address: 0x1000000
        Flash size: 2048 KB
Now upload program via XModem or 1K XModem
CCC
```

After the new software is successfully downloaded a message is displayed to restart the modem. If the downloading failed, a message is displayed too and the modem returns to the usual operation mode. (The operator can try again to download the software.) If the downloading was interrupted, the software is most likely damaged. In this case the restart will result in the loading the first version of the software, that is correct in the memory.

4.6.4.29 <TFTP [CMD] [ARG1][ARG2]> Command

This command allows to perform some maintenance operations over TFTP. CMD operations can be:

- SOFTUPDATE: Update software from TFTP server. In this case ARG1 should contain the IP address of the TFTP server and ARG2 should contain the path to the file on server.
- DUMP: Sends the startup configuration to the TFTP server. In this case ARG1 should contain the IP address of the TFTP server and ARG2 should contain the path to file where the configuration should be stored.
- LOAD: Download the startup configuration from the TFTP server. In this case ARG1 should contain the IP address of the TFTP server and ARG2 should contain the path to file with the configuration.
- SET: Set the TFTP protocol options. ARG1 specifies the option name and ARG2 the new value for this option. Following options are supported: TIMEOUT (the time the device will wait for a reply from the TFTP server) and RETRY (the number of times the device will retry the operation).
- SHOW: Show the current TFTP settings (timeout and retry)

Examples:

- TFTP SHOW
- TFTP SOFTUPDATE 172.16.53.1 APP.BIN
- TFTP LOAD 172.16.53.1 ltu/backup_cfg.txt
- TFTP DUMP 172.16.53.1 ltu/current_cfg.txt
- TFTP SET TIMEOUT 10
- TFTP SET RETRY 1

4.6.4.30 <SOFTCONFIRM> Command

This command confirms the new version of the software. After downloading the new software, a counter is switched on and starts of the running software. If this software is not confirmed with the help of the <SOFTCONFIRM> command after the restart, it will not be valid.

```
CO_FMM>SOFTCONFIRM
Software confirmed
CO_FMM>SOFTCONFIRM
Software already confirmed
CO_FMM>
```

4.6.4.31 <SOFTINFO> Command

This command displays some information about the software, which are stored in the current device. Any device can have two stored software copies (different versions are possible). One copy of the software is started after switching power on, while the other is a backup software.

```
CP_FMM>SOFTINFO
1:   ver.: 1.1.3, date: 2.6.2006, length:  328k, CRC OK, fixed
2: * ver.: 1.1.4, date: 3.7.2006, length:  330k, CRC OK, confirmed
CP_FMM>
```

The asterisk shows the running downloaded version (starts after power on).
ver – The number of the software version.
date – The date of the software creation.
length – The size in bytes.
CRC OK/FAIL – A label showing if the software is damaged or not.
The software status is displayed at the end of the corresponding line:
fixed – First basic software. Cannot be downloaded, does not require confirmation.
just loaded – Downloaded second software.
not confirmed – Non-confirmed second software.
confirmed – Confirmed second software.

4.6.4.32 <PING x.x.x.x> Command

This command will PING any remote IP address. It sends an ICMP ECHO request message and wait for the corresponding ICMP ECHO reply message. This command will not ping the own device IP address.

```
CO_FMM>PING 192.168.1.11
```

4.6.4.33 <MODEMVIEW> Command

This is a single command that collects and displays the modem configuration and status in a readable format. It is helpful to get an overview of the modem with just one command.

4.6.4.34 <SD SNAPSHOT> Command

This command generates the SNAPSHOT DAT, APP.BIN, LDR_xTU.BIN and STARTUP.CFG files in the O3MF directory on the SD card. This cmd is only available if the SD card is inserted.

4.6.4.35 <SD DIR> Command

This command shows the content of the SD card. This cmd is only available if the SD card is inserted.

4.6.4.36 <SD DEL [NAME]> Command

This command allows to delete files from the SD card. This cmd is only available if the SD card is inserted.

Example:

```
CO_01_FMM>SD     DEL     /O3MF/APP.BIN
CO_01_FMM>
```

4.6.4.37 <SD SAVE [N=0..9]> Command

The <SD SAVE> command generates a configuration file and saves it to the SD card. The SD SAVE <CR> generates the STARTUP.CFG file while SD SAVE x<CR> generates the desired PROFILEx.CFG file. This cmd is only available if the SD card is inserted.

4.6.4.38 <SD LOAD [N=0..9]> Command

The <SD LOAD> command downloads the configuration file from the SD card to the unit. The <SD LOAD> selects the STARTUP.CFG file while <SD LOAD x> selects the desired PROFILEx.CFG file.

4.6.4.39 <SD BOOT [ON/OFF]> Command

The <SD BOOT> command enables/disables the automatically SD card Software Upgrade feature during the boot sequence. If this feature is activated (SD BOOT ON) the software will compare the SNAPSHOT.DAT, APP.BIN, LDR_xTU.BIN and STARTUP.CFG files with the software and configuration files from the unit during the boot sequence. If any differences will be detected the corresponding software / configuration file from the SD card will be downloaded to the unit.

4.6.4.40 <SD STATUS> Command

The <SD status> command shows if the SD BOOT is enabled and the SD card information

```
CO_01_FMM>SD STATUS
SD Boot   :     OFF
Card  type  :  SDHC
Capacity   :  3781M
Blocks    : 7744512
Read err  : 0
Write err : 0
FAT       : FAT32
Partition size : 3768M
Free  space   :  3766M
Snapshot files
        /APP.BIN, correct
```

```
        /LDR_LTU.BIN, correct
        /STARTUP.CFG,          correct
CO_01_FMM>
```

SD STATUS	
SD BOOTs	Status of the automatically SD card Software Upgrade feature
Card type	Type of the inserted SD card
Capacity	Capacity of the SD card

Blocks	Number of the usable blocks on the SD card
Read err	Number of read errors
Write err	Number of write errors
FAT	Fileformat used on the SD card
Partition size	Partition size on the SD card
Free space	Usable Space on the SD card
Snapshot files	Status of every file that is checked during the boot sequence in case <BOOT ON> is activated. Correct indicates that the actual software / configuration file from the unit is equal to the file on the SD card.

4.6.4.41 <BERT> Command

The <BERT> command allows to enter into the submenu for BERT settings. Please also read the description in the chapter “TECHNICAL DESCRIPTION / 3.2.5 BERT Test”.

4.6.4.42 <H> Command

Type <H> and the monitor lists all available commands in the BERT sub-menu. If you type H [command] you will get additional help on [command].

```
CX_BERT>H
-------------------------------------------------------------------------------
Type 'H [command]' to get additional help on [command]
START                    Start BERT
STOP                     Stop BERT
TRACE                    Trace BERT statistics
SHOW                     Show BERT statistics once
RES                      Reset BERT statistics
SET  [E11-E12]  [INT/EXT]   Set  BERT  interface
PATD [2En/bitstring]     Set BERT pattern
TS [TX/RX] [list/NONE]   Set controlled slot list
CONF                     Display  current  BERT  configuration
APPLY [ALL/GROUP]        Apply changes to running configuration
CONNECT [N:[1-13/R]]     Establish  connection  to  remote  unit
LINK [NN]                Establish local connection
LINKCLEAR                Exit all local connections
M                        Return to Fault and Maintenance Menu
H                        Show available commands
```

4.6.5 Configuration Management Menu

After typing “3” in the main menu and pressing <enter>, the following message is displayed:

```
Configuration management activated
Enter 'M' to return to MAIN, or 'H' for HELP information

CO_01_CM>
```

The content of the configuration management menu mainly depends on the operation mode of the device. There are four possible modes of the device operation:

CO – All channels are in the Master mode, manual configuration.
CP – All channels are in the Slave mode, manual configuration.
CX – Some Channels are in Master, some channels are in Slave mode, manual configuration.
CA - Configuration of E1 and WAN streams is received from the SHDSL line, automatic config.

In the CA mode, it is impossible to configure the channel reservation, to arbitrarily assign E1 streams to DSL channels and to arbitrarily set clock sources. Nevertheless, this mode satisfies 90% of users, because it does not require many efforts to configure the device.

4.6.5.1 <H> Command

Type <H> and the monitor lists all available commands in the configuration management sub-menu. If you type H [command] you will get additional help on [command].

```
CO_01_CM>H
--------------------------------------------------------------------------------
Type 'H [command]' to get additional help on [command]
SECURE [ON/OFF]          Change security mode
USERS                    List user accounts
USER [name]              Add user account
USER [name] DEL          Delete user account
USER [name] [+|-] [PRIV] Assign user access rights
USER [name] [IP] [subnet]Set IP access list for user
USER [name] [LOCAL/ALL]  Set all IP/ or local only user access
PASSWORD [user]          Set user password
AUTO [ON/OFF]            Set CA mode
CONFIG                   Display local configuration
CONFIG [N/R/S/B]         Display new/running/startup/backup configuration
MASTER [ON/OFF] [N]      Select Nth xDSL channel master/slave
EXT [ON/OFF] [N]         Turn Nth DSL channel Extended mode ON or OFF
BASERATE [M/AUTO] [N]    Set Nth DSL channel baserate to M*64k + 8k
PAM [4-128] [N]          Set Nth xDSL channel line coding
PAYLOAD [list] [N]       Set Nth xDSL channel payload
ANNEX [A,B,A/B] [N]      Set Nth xDSL channel Annex A or Annex B or Annex A/B
SETCLOCK [list] [N]      Set Nth xDSL channel clock source priorities MULTIPAIR
[2/3/4/2+2/OFF]Select or turn off multipair mode
RESERVE [list1] {list2}  Set lists of channels for the reserve groups
G704 [ON/OFF] [N]        Set Nth E1 framer G704 mode
CRC4 [ON/OFF] [N]        Set Nth E1 framer CRC4 mode
AISDET [ON/OFF] [N]      Set Nth E1 framer AIS detection mode
AISGEN [ON/OFF] [N]      Set Nth E1 framer AIS generation mode
DSLTS [list] [N]         Select Nth E1 channel timeslots, transmitted via DSL
WANTS [list] [N]         Select Nth E1 channel timeslots for WAN payload
E1CLOCK {source} [N]     Set Nth E1 channel clock source
E1MODE {mode} [N]        Set Nth E1 channel coding or loop mode
POWER [ON/OFF] [N]       Turn the remote power on/off over the N-th DSL channel
ID [string]              Set/Clear device ID
RESPONSE [NN/OFF]        Set response ID
DEFAULT [0-4]            Set default configuration
DEFAULT EVERYTHING       Set everything to default configuration
DEFAULT DESC             Set default Description (ifAlias)
SERNUM                   Show serial number
GSCOMPAT [ON/OFF]        Set GS compatibility mode on and off
NMTHR [N/OFF]            Set Noise Margin alarm threshold
```

```
LATHR [N/OFF]             Set Loop Attenuation alarm threshold
PTMP [ADD|DEL] [IF]       Add/delete interface to PTMP network
PTMP SHOW                 Show interfaces of PTMP network
MODE [N]                  Switches number of DSL channels to N

LICENSE                   Show         active
licenses LICENSE ADD [key]  Add     software
options
NET                       Network configuration menu
APPLY [ALL/GROUP]         Apply     changes     to     running
configuration CONNECT [N:[1-13/R]] Establish   connection   to
remote unit LINK [NN]     Establish local connection
LINKCLEAR                 Exit all local connections
M                         Return to Main Menu
H                         Show available commands
--------------------------------------------------------------------------------
CO_01_CM>
```

4.6.5.2 <SECURE ON/OFF> Command

This command activates/deactivates the advanced security. The basic security allows 2 users, ADMIN and USER. The Advanced Security software license allows up to eight users. Each user can have different access rights to command line interface (CLI) and SNMP commands. The optional access control list (ACL) is possible to set for every user additionally. The user will be able to access the WEB interface and the CLI only if source IP address belongs to the defined domain.

Starting from the software version 1.5.1, the Advanced Security option activates SSH and Radius protocol support.

Note: The SECURE ON feature needs a special LICENSE KEY that has to be ordered together with the unit.

Starting from the software version 1.5.2 no additional LICENSE KEY is required for activation of Advanced Security feature.

4.6.5.3 <USERS> Command

This command shows the list of users of the device with their control and access rights.

```
CO_CM>USERS
--------------------------------------------------------------------------------
Username Controls IP ACL
--------------------------------------------------------------------------------
ROOT ALL Local access only
WHEEL  CONTROL,TEST,STATUS,CONFIG  192.168.1.64/30
NET C{SNMP,NET} 192.168.1.16/30
LAN S{LANC},C{LAN} 192.168.20.16/30
LINK   CONTROL,TEST,S{LINKC},C{LINK}   192.168.20.24/30
WATCH S{LINK,LAN} Any IP
GUESTLINK S{LINKC},C{LINK} 192.168.2.16/30
--------------------------------------------------------------------------------
CO_CM>
```

4.6.5.4 <USER> Command

This command allows the control of various user parameters. You must have ADMIN rights to use this command.

Command	Description
USER [username]	Creates a user USERNAME and asks for a password
USER [username] DEL	Deletes user USERNAME
USER [username] [+/-] [PRIV]	Modify privileges for user USERNAME
USER [username] [IP] [net]	Set the IP range for user USERNAME. Net should be in range from 0 to 32. If no IP is set, no restrictions are applicable.
USER [username] LOCAL	Disable remote access for user USERNAME. This command is equal to USER [username] 0.0.0.0 32.
USER [username] ALL	Allow access from any IP address for user USERNAME. This command is equal to USER [username] 0.0.0.0 0.

Every user in the list has rights to control some parts of the device through the command line interface. The list of control points is empty for the new user. To change (to add or to delete) control points (Controls) the USER [USERNAME] [+|-] [PRIV] command is used. If "+" is selected, the one of the following privileges will be added. In case if "-" is used, the one of the following privileges will be revoked.

All commands of the CLI are divided into 3 levels. Selection of upper level means that the commands from low levels will be selected too. Some commands are available for every user, they can't be revoked.

Privileges

Hierarchy Levels			Description	Related commands	
Top Level	**Group**	**Subgroup**			
ALL			Commands of this level are available for everyone. No additional authorization is required	ALARM ALARM T DISCONNECT LINKCLEAR	TLM SENSOR ACO SOFTINFO
	CONTROL [CTRL]		Operation of remote devices	CONNECT	LINK
	TEST [T]		Test of the device	LOOP1 LOOP2 STARTAL RESTART	PING MACTABLE MACTABLE C BERT Submenu

	ADMIN [A]		Administration of the device	DIFF DUMP SERNUM LICENSE ACO change RESET BACKUP RESTORE LOAD TLM D TLM S TLM C SENSOR [N] [O/C] TFTP	SOFTUPDATE SOFTCONFIRM ID RESPONSE PASSWORD NMTHR LATHR LICENSE ADD DEFAULT EVERYTHING SECURE LOG USERS USER APPLY CONFIRM
	STATUS [S]	:LINK	Link status	G826 G826 C G826 E1 G826 E1 C ALLG826 LINKSTAT LINKALARM ALARMLOG	NM LINKNM STATUS STATUS T STATUS L STATUS EXT POWER DIAG
		:LINKC	All commands from LINK + reset of the counters	RESETG826 RESETALLG826	ALARMLOG C
		:LAN	Ethernet status	NETSTAT NETERR	STATUS ETH MACTABLE
		:LANC	All commands from LAN + reset of Ethernet counters and MAC table	RESETNETSTAT MACTABLE C	

ALL	CONFIG [C]	:VIEW	Displaying of device configuration	CONFIG NETCONFIG	COSCONFIG RSTP CONF
		:LINK	All commands from VIEW +line, E1 and Nx64 interface configuration	DEFAULT AUTO MASTER EXT BASERATE PAM PAYLOAD ANNEX SETCLOCK MULTIPAIR RESERVE G704 CRC4 AISDET AISGEN DSLTS WANTS	E1CLOCK E1MODE POWER GSCOMPAT PTMP MODE N RSRATE RSFORMAT RSDUPLEX AUTOLOOP EXTCLOCK N64RATE WAN WANIDLE APPLY CONFIRM

	:LAN	All commands from VIEW + LAN configuration	NETDEFAULT RSTP DEFAULT RSTP STATE RSTP ... PBVLAN MODE [IF] VLAN QOS ALLOW VID	ETHSD FC IRATE ERATE CRATE COS PING APPLY CONFIRM
	:SNMP	All commands from VIEW + SNMP configuration	TRAPIP COMMUNITY SNMPSET SNMPACL	RMONALARM RMONEVENT APPLY CONFIRM
	:NET	All commands from VIEW + IP configuration	SETIP GATEWAY NETMASK MTU SYSLOG	SNTP APPLY CONFIRM PING

Note: The abridgements in braces "[ ]" can be entered instead of complete name. If group has been entered without subgroup definitions, all subgroups will become available. To define subgroup, type it after group name with ":" in the beginning of a subgroup. The WEB interface will follow the rights of CLI interface

Examples:

USER TESTUSER + S:LINK,LANC add privileges to show LINK status, LAN status and to clear LAN statistics for the TESTUSER (it should be created firstly)

USER TESTUSER - S:LANC remove privileges to clear LAN statistics for the TESTUSER

USER TESTUSER + CONFIG add privileges to change configuration for the TESTUSER

Access Control

All listed users have local access to CLI via RS232 interface. The remote access through Telnet and WEB can be granted from anywhere, from selected IP addresses, or canceled.

The USER [USERNAME] [IP] [netclass] command is used to define the IP domain.

The USER [USERNAME] ALL command is used to allow access from all IP addresses.

The USER [USERNAME] LOCAL command is used to disable access from all IP addresses.

4.6.5.5 <PASSWORD {users}> Command

This command sets the access password for users. With basic security, there are two users available: USER is a non-privileged, ADMIN is a privileged user. With advanced security, up to 8 users with arbitrary names are allowed.

PASSWORD ADMIN: sets password for the user ADMIN

PASSWORD USER: sets password for the user USER

```
CO_CM>PASSWORD USER
Enter   password:
Confirm password:
Ok
```

Only the administrator can perform this command. The password length is not more than 11 symbols (advanced security 63 symbols). The password can contain Latin letters and digits.

Note: It is also possible to set an empty password (in this case, the password is not requested while opening the telnet session). This command sets the password only to access the device over the telnet protocol. When managing the devices via the RS-232 interface, the password is not requested.

4.6.5.6 <CONFIG / N / R / S / B > Command

The <CONFIG> command always displays the running configuration of the device. If a new configuration differs from the running one a warning is displayed. Options:

- N - Display New line configuration
- R - Display Running line configuration
- S - Display Startup line configuration
- B - Display Backup line configuration

```
CO_01_CM>CONFIG
--------------------------------------------------------------------------------
Running Line Configuration
--------------------------------------------------------------------------------
xDSL               DSL1          DSL2          DSL3          DSL4
  Mode          :  Master(HTU-C) Master(HTU-C) Master(HTU-C) Master(HTU-C)
  Extended rates:  OFF           OFF           OFF           OFF
  Line coding   :  PAM32         PAM32         PAM32         PAM32
  Baserate      :  89            89            89            89
  Annex         :  B             B             B             B
  Payload       :  E1-1,WAN      E1-2,WAN      E1-3,WAN      E1-4,WAN
  Clock source  :  E1-1,Int      E1-2,Int      E1-3,Int      E1-4,Int
  Reserve       :  ---           ---           ---           ---
  Power         :  ON            OFF           OFF           OFF
  GS compatible :  OFF

E1                 E1-1          E1-2          E1-3          E1-4
  G.704 framing :  ON            ON            ON            ON
  CRC4          :  ON            ON            ON            ON
  AIS Detection :  ON            ON            ON            ON
  AIS Generation:  ON            ON            ON            ON
  E1 clock      :  DSL           DSL           DSL           DSL
  TS into DSL   :  0-31          0-31          0-31          0-31
  TS into WAN   :  NONE          NONE          NONE          NONE
--------------------------------------------------------------------------------
CO_01_CM>
```

Group of SHDSL parameters	
Mode	Master, Slave, Multipair All slave, configured by master All slave, MULTIPAIR xx, configured by master
Extended rates	Extended DSL feature ON/OFF
Line coding	Type of the line encoding (PAM128, PAM64, PAM32, PAM16, PAM8, PAM4)
Baserate	Data Transmission Rate on SHDSL line (BR*64kbit/s). Auto – adaptation mode
Annex	Transmission Mode (ANNEX A, ANNEX B, ANNEX AB)
Payload	Data Transmission interfaces: list of E1 and/or WAN streams
Clock source	Priority list of clock sources
Reserve	The reservation group to which the DSL channel belongs

GS compatible	Enables the Globespan (Conexant) compatibility
Group of E1 parameters	
G.704 framing	Framing mode
CRC4	CRC4 mode
AIS Detection	AIS detection mode
AIS Generation	AIS generation mode
E1 clock	Clock source
TS into DSL	List of E1 time slots transmitted/received over DSL
TS for WAN	List of E1 time slots used for WAN data (Ethernet over E1)

Table 4.3 All possible configurations of independent channels

The main operation modes of any device are:

- Independent channels (CO, CP, CX)
- Independent channels with reservation (CO, CP, CX)
- Multipair mode (CO, CP, CX)
- Two-pair mode with reservation (available only in the four-channel version) (CO, CP, CX)

The CONFIG table for the mode with independent channels is presented above. Typical configurations for other modes are presented below.

Presentation of CONFIG table in “independent channels with reservation” mode. In this configuration, channels 1, 2, 3 are combined for reservation (CO, CP, CX).

```
CO_09_CM>CONFIG
--------------------------------------------------------------------------
Running Line Configuration
--------------------------------------------------------------------------
SHDSL               DSL1          DSL2          DSL3          DSL4
  Mode          :  Slave(HTU-R)  Slave(HTU-R)  Slave(HTU-R)  Slave(HTU-R)
  Extended rates:  OFF           OFF           OFF           OFF
  Line coding   :  AUTO          AUTO          AUTO          AUTO
  Baserate      :  AUTO          AUTO          AUTO          AUTO
  Annex         :  A/B           A/B           A/B           A/B
  Payload       :  E1-1,WAN      E1-2,WAN      E1-3,WAN      E1-4,WAN
  Clock source  :  E1-1,Int      E1-2,Int      E1-3,Int      E1-4,Int
  Reserve       :  {========== Reserve group A ==========} ---
  Power         :  OFF           OFF           OFF           OFF
  GS compatible :  OFF

E1                  E1-1          E1-2          E1-3          E1-4
  G.704 framing :  OFF           OFF           OFF           OFF
  CRC4          :  N/A           N/A           N/A           N/A
  AIS Detection :  ON            ON            ON            ON
  AIS Generation:  ON            ON            ON            ON
  E1 clock      :  DSL           DSL           DSL           DSL
  TS into DSL   :  0-31          0-31          0-31          0-31
  TS into WAN   :  NONE          NONE          NONE          NONE
--------------------------------------------------------------------------------
CP_01_CM>
```

Presentation of CONFIG table in “independent channels with reservation” mode. In this configuration, channels 1, 2 and 3, 4 are combined for reservation (CO, CP, CX).

```
CO_09_CM>CONFIG
--------------------------------------------------------------------------
Running Line Configuration
--------------------------------------------------------------------------
SHDSL               DSL1          DSL2          DSL3          DSL4
  Mode          :  Master(HTU-C) Master(HTU-C) Master(HTU-R) Master(HTU-C)
  Extended rates:  OFF           OFF           OFF           OFF
  Line coding   :  PAM32         PAM32         PAM32         PAM32
  Annex         :  A/B           A/B           A/B           A/B
```

```
  Payload       :  E1-1,WAN      E1-2,WAN      E1-3,WAN      E1-4,WAN
  Clock source  :  E1-1,Int      E1-2,Int      E1-3,Int      E1-4,Int
  Reserve       :  {==== Reserve group A ====} {==== Reserve group B ====}
  Power         :  OFF           OFF           OFF           OFF
  GS compatible :  OFF

E1                 E1-1          E1-2          E1-3          E1-4
  G.704 framing :  OFF           OFF           OFF           OFF
  CRC4          :  N/A           N/A           N/A           N/A
  AIS Detection :  ON            ON            ON            ON
  AIS Generation:  ON            ON            ON            ON
  E1 clock      :  DSL           DSL           DSL           DSL
  TS into DSL   :  0-31          0-31          0-31          0-31
  TS into WAN   :  NONE          NONE          NONE          NONE
--------------------------------------------------------------------------------CO_09_CM>
```

4.6.5.7 <MASTER ON/OFF [N = 1..4]> Command

This command activates/deactivates the «MASTER» mode on the interface with the number N. For single-channel modems, the command is used without the number of the SHDSL channel.

```
CP_01_CM>MASTER ON 1
```

Note: In a data transmission systems one device should be configured as a Master device, while the other as a Slave device.

4.6.5.8 <AUTO ON/OFF> Command

This command This command activates the modem in CA mode. This means that all SHDSL channels are set to “SLAVE” mode and getting most settings from SHDSL line.

```
CP_01_CM>AUTO ON
```

4.6.5.9 <EXT ON/OFF [N = 1..4]> Command

This command activates/deactivates the standard and the extended G.SHDSL mode on the interface with the number N.

Note: The EXT ON feature needs a special LICENSE KEY that has to be ordered together with the unit.

In extended mode higher data rates and line codes (PAM4, PAM8, PAM16, PAM32, PAM64, PAM128) are available.

Standard mode **Command**	**Channel Coding**	**Min Baserate**	**Max Baserate**
PAM 16	PAM 16	3	60
PAM 32	PAM 32	12	89
Extended mode			
PAM 4	PAM 4	2	39
PAM 8	PAM 8	3	79
PAM 16	PAM 16	1	119
PAM 32	PAM 32	1	159
PAM 64	PAM 64	2	199
PAM 128	PAM 128	4	238

4.6.5.10 <BASERATE K/AUTO [N=1..4]> Command

This command sets the transmission rate K to the line SHDSL interface, where N is the number of the SHDSL interface. For modems with just one SHDSL channel, the command is entered without typing the number N. The data transmission is BASERATE * 64kbit/s.
For PAM16 the available rates (BASERATE) are the range from 3 to 60, and for PAM32 from 12 to 89.

Coding Type	Parameter	Values	Description
PAM16	N	3..60	Transmission rate over the line interface (N*64+8) Kbit/s.
PAM32		12..89	

Table 4.4 Available rates (BASERATE) for different coding types

WARNING
FOR LOW BASERATES YOU SHOULD USE THE LOWEST POSSIBLE NUMBER OF CODE LEVELS. FOR A STANARD BASED DEVICE USE PAM16 AND NOT PAM32.

On the Slave device, the <BASERATE AUTO> command adapts the rate of the Slave device to the rate of the Master device. In this case, PAM and Annex are automatically detected (opposite Annex in the <CONFIG> configuration AB appears, opposite PAM is Auto). The command does not change the Annex and PAM modes in the configuration. In the Slave mode, the <BASERATE AUTO> command automatically detects all configurations.

4.6.5.11 <PAM [16/32] [N]> or <PAM [4-128] [N]> Command

This command sets the number of levels in the line code. The following options are possible – 4,8,16, 32, 64 & 128 for EXT mode ON. For modems with just one SHDSL channel, the command is entered without typing the number N

```
CO_01_CM>PAM 16
```

4.6.5.12 <PAYLOAD list/NONE [N=1..4]> Command

This command sets the list of streams transmitted over the SHDSL channel. N is the number of the SHDSL channel. The parameter list displays the list of E1 and WAN interfaces (Ethernet), separated by comma. The E1 interface may be denoted both by a short-form (for example E1-1, E11), and by numbers (for example 1). Spaces in the list are not allowed. The parameter NONE deactivates transmission of E1 and WAN over this SHDSL interface. For modems with just one SHDSL channel, the command is entered without typing the number N

```
CO_CM>PAYLOAD WAN
CO_CM>PAYLOAD E11,WAN
CO_CM>PAYLOAD NONE
```

4.6.5.13 <ANNEX A/B/AB [N=1..4]> Command

This command enables the transmission standard G.991.2 ANNEX A or ANNEX B, where N is the number of the SHDSL interface. The ANNEX AB automatically selects the transmission standard.

Note: If devices use different transmission standards, synchronization will not be established between them.

4.6.5.14 <SETCLOCK list [N=1..4]> Command

This command sets the priority list of clock sources for the SHDSL channel, where N is the number of the SHDSL channel. The parameter N can be absent for single-channel modems. The possible clock sources are:

- External sync source: EXT, EXTERNAL
- first E1 channel: 1, E11, E1-1, E1_1
- second E1 channel: 2, E12, E1-2, E1_2
- third and fourth E1 channel
- internal sync source: INT, INTERNAL

The external clock source should be either the first one in the priority list or be not used at all. The next clock sources in the list should be E1 channels. The internal clock source should be the last one in the priority list. It is even not necessary to type it in the command.

Two rules: The list of priority clock sources should contain only those E1 channels, which are used to transmit data over the SHDSL channel. If the SHDSL channel does not transmit any E1 streams, it is possible to set any of the E1 channel as a reference clock source or to use the external clock.

Note: If the list of the E1 channels transmitted over DSL is changed by the PAYLOAD command, it can change the list so that it corresponds to the previous two criteria.

```
CO_09_CM>SETCLOCK EXT,E1-1,E1-2
CO_CM>SETCLOCK INT
```

4.6.5.15 <MULTIPAIR [2/3/4/2+2/OFF]> Command

This command activates the multipair mode, which allows to merge DSL channels.

Groups of 2, 3 and 4 channels can be merged into the multipair mode. The following variants are possible:

```
CO_01_CM>MULTIPAIR 2
CO_01_CM>MULTIPAIR 3
CO_01_CM>MULTIPAIR 4
CO_01_CM>MULTIPAIR 2+2
```

4.6.5.16 <RESERVE [list]>, <RESERVE [list] [list]> Command

This command allows combining SHDSL channels into groups in order to reserve them. Not more than 2 groups are possible in a system with 4 SHDSL channels. The reservation groups are called A and B groups. The parameter sets the list of channel numbers separated by a comma. To simplify configuration and maintenance of devices, any groups of successive channels can be reserved. To configure the reserve group, type the following command:

```
CO_01_CM>RESERVE 1,2
```

To configure two reserve groups type the command as follows. Note that groups should not use same channels.

```
CO_01_CM>RESERVE 1,2 3,4
```

The parameter NONE deactivates reservation.

```
CO_01_CM>RESERVE NONE
```

4.6.5.17 <G704 ON/OFF [N]> Command

This command activates/deactivates the ITU-T G.704 framed mode for the E1 interface with number N. The <G704 ON 1> activates the ITU-T G.704 framed mode. The <G704 OFF 1> deactivates the ITU-T G.704 framed mode, i.e., the devices starts operating in the so-called transparent mode.

```
CO_CM>G704 ON 1
```

4.6.5.18 <CRC4 ON/OFF [N]> Command

This command activates/deactivates the CRC4 mode for the E1 channels, where N is the number of the E1 channel.

```
CO_CM>CRC4 ON 1
```

4.6.5.19 <AISGEN ON/OFF [N]>, <AISDET ON/OFF [N]> Commands

The <AISGEN ON/OFF [N]> command activates/deactivates the AIS Generation mode for the E1 interface, where N is the number of the E1 interface.
The <AISDET ON/OFF [N]> command activates/deactivates the AIS Detection mode for the E1 interface, where N is the number of the E1 interface.

```
CO_CM>AISGEN ON 1
CO_CM>AISDET ON 1
```

4.6.5.20 <DSLTS list/NONE [N=1..4]> Command

This command sets transmitted/received time slots of the E1 channel with number N to be transmitted over the SHDSL interface. The list consist of numbers of separate time slots or their ranges, separated by comma. For example: 1,5,14-19. The empty list is set by typing NONE. Spaces in the list are not allowed. Use the “minus” sign or two dots “..” to set the range.

```
CO_CM>DSLTS 0-31 1
CO_CM>DSLTS 0-12,16 1
CO_CM>DSLTS 1..31 1
```

4.6.5.21 <WANTS [list] [N=1..4]> Command (Ethernet over E1)

This command sets the list of E1 time slots to be transmitted over the WAN interface (Ethernet). N is the number of the E1 interface.

```
CO_CM>WANTS 0-31 1
CO_CM>WANTS 12-18,19 1
CO_CM>WANTS 0-21,24 1
CO_CM>WANTS 1..21 1
```

4.6.5.22 <E1CLOCK [DSL/RX/EXT] [N]> Command

This command sets the E1 output clock source for the WANTS mode.

Examples:
E1CLOCK DSL: The Rx clock of the DSL channel connected to this E1 interface
E1CLOCK RX: E1 input clock
E1CLOCK EXT: External input clock.
E1CLOCK INT: Internal input clock.

4.6.5.23 <E1MODE [HDB3/AMI] [N]>, <E1MODE [SHORT/LONG] [N]> Commands

This command sets the E1 line coding to AMI or HDB3. And additionally it sets with short/long the receiver sensitivity. Long means high receiver sensitivity required by long haul. Short means lower sensitivity and signals below -12.5dB are considered as loss of signal.

4.6.5.24 <POWER ON/OFF [N=1..4]> Command

This command activates/deactivates the remote power source for the selected [N] SHDSL channel.

4.6.5.25 <ID string> Command

This command is used to enter an identification number on the device (text containing no more than 12 symbols). This ID will be displayed on top the main menu. If the parameter is not written, the device ID will be empty.

4.6.5.26 <DEFAULT [0-4]> Command

The <DEFAULT N> command sets the default operation mode, where N is the mode number (there are four default operation modes).

- The DEFAULT 0 command sets the following mode: SLAVE, PAM 32, BASERATE 89, ANNEX B, transmission of the E1 stream and Ethernet over SHDSL.
- The DEFAULT 1 command sets the following mode: MASTER, PAM 32, BASERATE 89, ANNEX B, transmission of the E1 stream and Ethernet over SHDSL.
- The DEFAULT 2 command sets the following mode: SLAVE, PAM 32, BASERATE AUTO, ANNEX A/B, transmission of the E1 stream and Ethernet over SHDSL.
- The DEFAULT 3 command sets the following mode: MASTER, PAM 32, BASERATE 89, ANNEX B, transmission of the 2xE1 stream and Ethernet over SHDSL.

4.6.5.27 <DEFAULT EVERYTHING> Command

This command sets default operation modes for line parameters (see the DEFAULT command) and for network parameters (see the <NETDEFAULT> command). The result of this command is similar to the result of two commands:

DEFAULT 0
NETDEFAULT

4.6.5.28 <DEFAULT DESC> Command

This command writes default Port Description (ifAlias)

```
CO_06_CM>DEFAULT   DESC
CO_06_CM>
```

4.6.5.29 <SERNUM> Command

This command shows the production serial number of the unit.

4.6.5.30 <GSCOMPAT ON/OFF> Command

This command sets the Globespan (Conexant) compatibility mode on/off. This feature will also limit the baserate to 36 (PAM16).

4.6.5.31 <NMTHR> Command

The <NMTHR> command allows to setup the desired Noise Margin alarm threshold in dB.
Syntax: NMTHR [value], where value is in the range from 0...25
NMTHR OFF disables the Noise Margin alarm threshold function

4.6.5.32 <LATHR> Command

The <LATHR> command allows to setup the desired Line Attenuation alarm threshold in dB. Syntax: LATHR [value], where value is in the range from 0...25
LATHR OFF disables the Line Attenuation alarm threshold function

4.6.5.33 <PTMP [ADD/DEL] [IF]> Command

This command helps to add or delete an interface to the Point-to-Multipoint group channel. [IF] is the name of interface to add or delete:

- RS-1: RS-232 or RS-485
- WAN1-WAN4: WAN interface to transmit PTMP data through
- DSL1-DSL4: DSL interface transmitting WAN

DSL and E1 interface names are automatically converted to corresponding WAN channels by this command.

4.6.5.34 <PTMP SHOW> Command

This command shows the members of the Point-to-Multipoint group channels.

4.6.5.35 <G703CLOCK [DSL/INT/RX]> Command

The <G703CLOCK> command selects the reference clock for the outgoing data. If you use 2 G.703/E0 interfaces the syntax is G703CLOCK {clock source} {G703 card index}
Following clock sources can be selected as a reference for outgoing data:

DSL	data clock is derived from carrier DSL channel
INT	data is clocked with internal clock source
RX	data is clocked with a clock derived from incoming data

G703 card index is 1 for the first G.703/E0 interface card and 2 for second. 1 can be omitted if just one interface card is installed.

```
CO_CM>G703CLOCK DSL 1
```

4.6.5.36 <MODE N> Command

The <MODE> command sets number of SHDSL interfaces system will operate with.

For example: The MODE 1 in a four-channel unit disables channels 2,3 & 4.

To setup this configuration parameter you should perform the following command sequence:
1. Apply and confirm all configuration changes
2. Issue MODE [N] command
3. RESET

After the reset unit will work with specified number of SHDSL channels.

4.6.5.37 <LICENSE> Command

This command shows the active licenses.

```
CP_01_CM>LICENSE
Current license status:
Extended PAM and baserates: Not activated
```

4.6.5.38 <LICENSE ADD> Command

This command activate a special functionality added by a license KEY, that you can get from the manufacturer.

4.6.5.39 <RSIP> Command

This command configures the RS<->IP (Serial to Ethernet) function of the modem.

Syntax: RSIP [I/O] [addr] [IF]
RSIP [{mode}/ON/OFF] [IF]
RSIP SIGNALING {sign} [IF]
RSIP RTS [CTS/DCD] [IF]
RSIP BREAK [ON/OFF] [IF]

[I/O]: Defines which parameter to configure. Input (IN: local IP port that receive serial data packets) or Output (OUT: remote IP address to forward serial data packets).

[addr]: IP port or IP address and port. For Input (IN) address [addr] is just a port number. For Output (OUT) address [addr] is an IP address and port number, separated by a colon (:). For TCP Server mode only an IP address should be specified. The port number should be in range from 1024 to 65535 inclusively. Port numbers below 1024 may be used as well as port numbers above 1024, but may conflict with another built-in services like SNMP or NTP. It's not recommended to use ports below 1024.

{mode}: Selects the IP protocol and mode. Possible values are: UDP (use UDP protocol), SERVER (work as TCP Server), CLIENT (work as TCP Client).

[ON/OFF]: Enables/Disables RS<->IP function

{sign}: Define the RTS/CTS signals operation mode and is only for RS-232 available. Possible values are: OFF (CTS & RTS signals are not used), LOCAL (TCP: When UP local RTS is looped to CTS), UDP (RTS is always looped to CTS), REMOTE (CTS input is transferred to the remote RTS output and vice versa). If communication is not established RTS is low. This mode works over both TCP and UDP protocols and should be enabled on both ends of connection simultaneously.

[IF]: Selects corresponding serial RS interface. Possible values are RS1 (for first RS interface). This parameter may be ommited when only one RS232/422/485 interface is available.

[RTS] Selects input/output pair for signalling. In normal conditions the RTS will trigger CTS and DTR will trigger DCD. This parameter allows to change default operation the way whre RTS will trigger DCD and DTR will trigger CTS.

NOTE: RSIP RTS [CTS/DCD] [IF] command available for 1xRS232 daughterboard only

BREAK: Allows to switch ON/OFF the transmission of the BREAK condition. ON means to ransmit BREAK conditions through RSIP, OFF ignore the BREAK conditions. In this case BREAK conditions will appear as zero bytes in data stream.

Examples:

RSIP ON RS: Enable RS<->IP

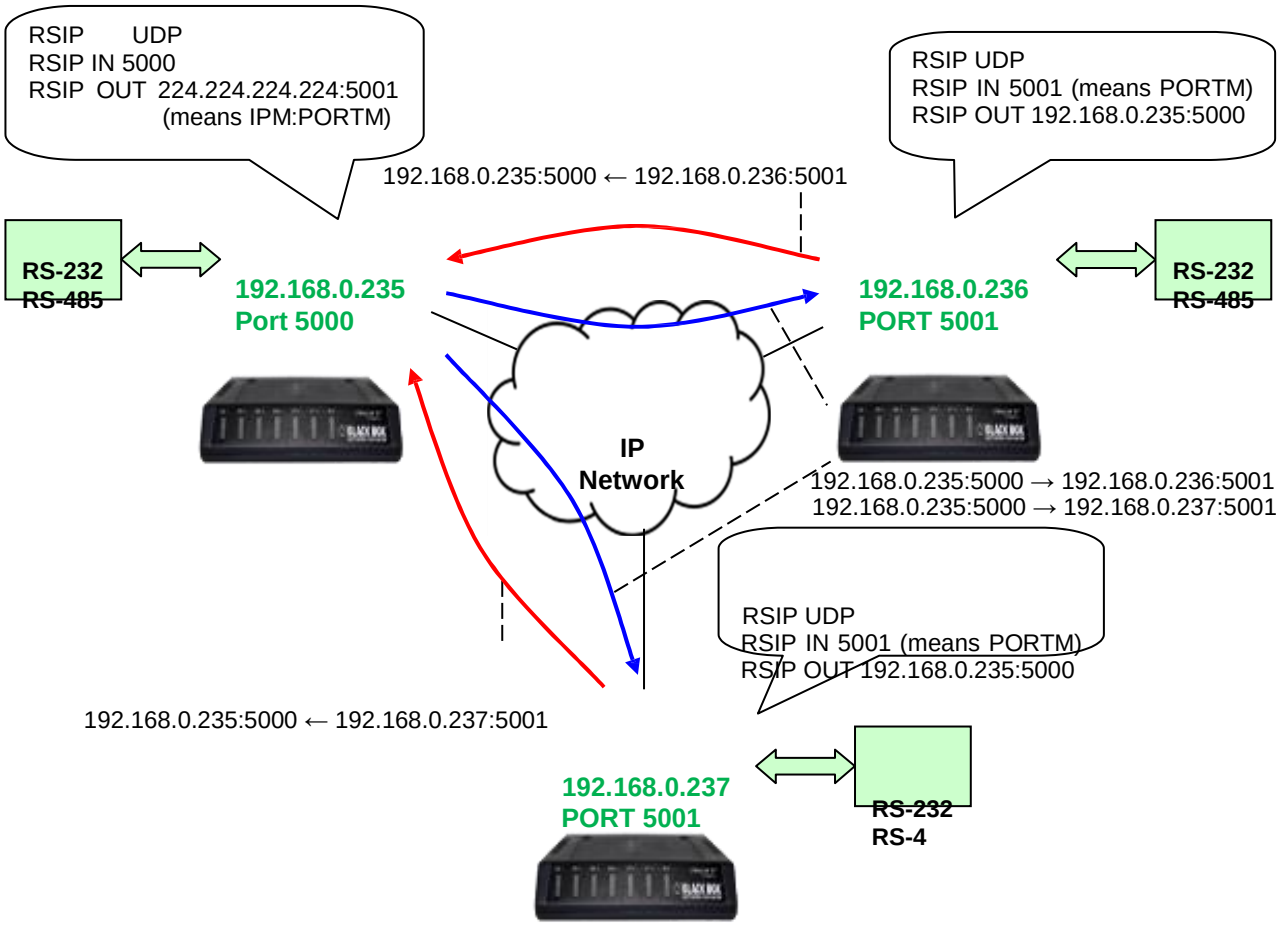
RSIP UDP RS: Select UDP mode

RSIP IN 5000 RS: Means to select port 5000 for the reception of serial data packets

RSIP OUT 172.16.53.1:5000 RS: Select IP address 172.16.53.1 and port 5000 as address of the remote system where serial data will be transferred to. Only packets from this address will be accepted when received on listen port.

UDP Point to Multipoint (Multicast addresses are IP addresses in the range from 224.0.0.0 to 239.255.255.255):

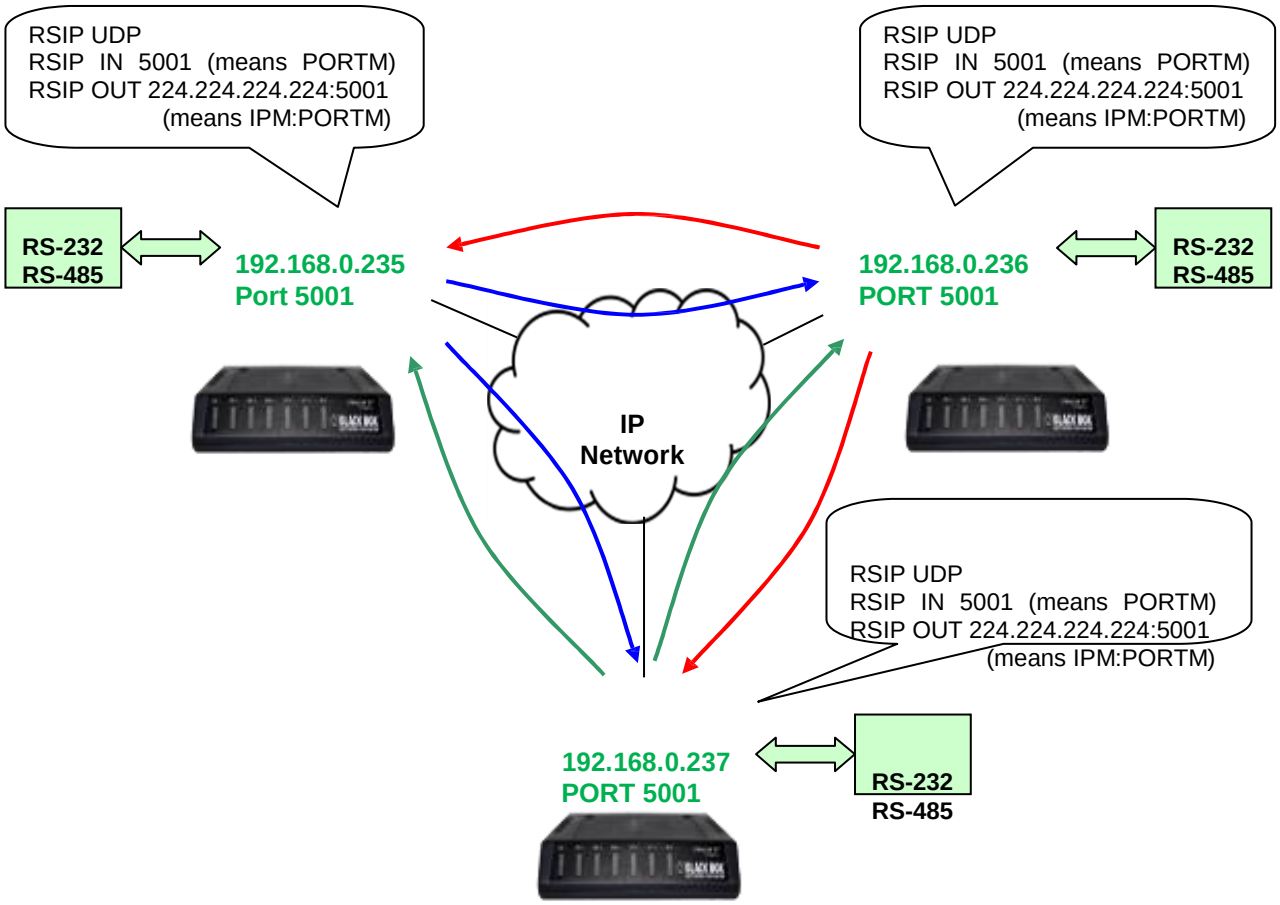
.



Picture 2.2. Serial Data Transmission with UDP Point-To-MultiPoint

UDP Broadcast Mode

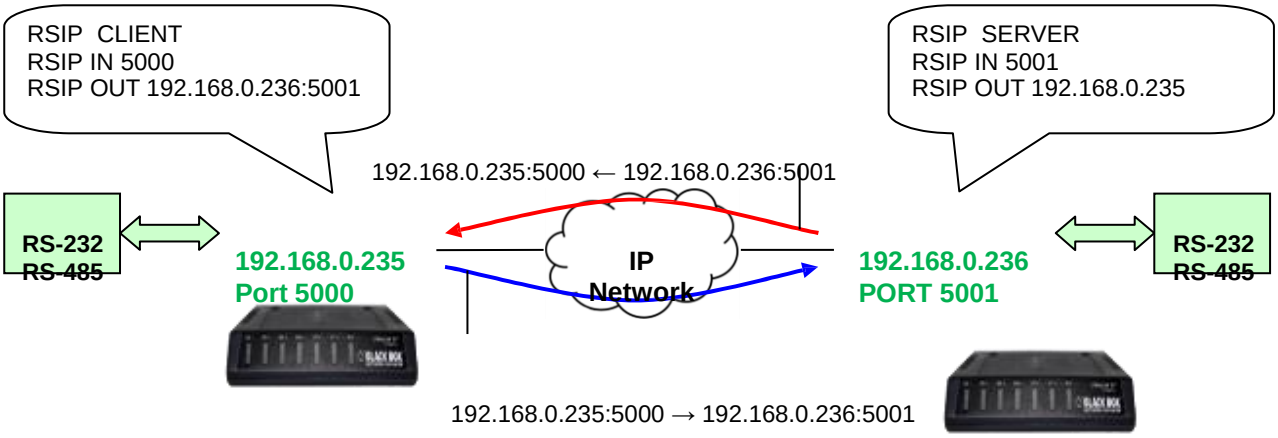
In this mode the endpoints should be configured to send their serial data to the multicast IP Address (IPM). Incoming and outgoing PORT Number (PORTM) should be the same for all endpoints to receive each other's serial data.



Picture 2.3. Serial Data Transmission with UDP Broadcast

TCP Point-To-Point

In this mode one serial data endpoint should be configured as Server and the other as Client. Client configuration is the same as UDP endpoint. On the Server endpoint the Client IP Address and incoming PORT Number should be specified.



Picture 2.4. Serial Data Transmission with TCP Point-To-Point

Configuration Commands for Serial Data Transmission over IP Networks

Following configurations are possible when programming serial data over an IP Network:

Mode (UDP/TCP Client/TCP Server)
Local IP PORT Number for incoming serial data
Remote IP Address and PORT Number for outgoing serial data
Operation over IP Network or not (RSIP ON/OFF)

To enable the serial data transmission over IP Network functionality on the specific interface, it should be removed from DSL Payload and from the PTMP group. The following commands allow configuring the interfaces:

RSIP [[MODE]/ON/OFF] [IF]
RSIP IN [PORT] [IF]
RSIP OUT [ADDR] [IF]

[MODE] define the protocol and mode, such as:

UDP (Switch to UDP protocol for serial data transmission
CLIENT (Switch to TCP protocol for serial data transmission, Client side)
SERVER (Switch to TCP protocol for serial data transmission, Server side)

[IF] is the name of interface, such as:

RS or RS1 (if one 1xRS-232 or 1xRS-485 interface card is installed)
4RS,[channel_number] or 4RS1,[channel_number] (if one 4xRS-232 interface card is installed)
4RS1,[channel_number] or 4RS2,[channel_number] (if two 4xRS-232 interface cards are installed)

[PORT] is the PORT_Number, decimal from 1024 to 65535 inclusively

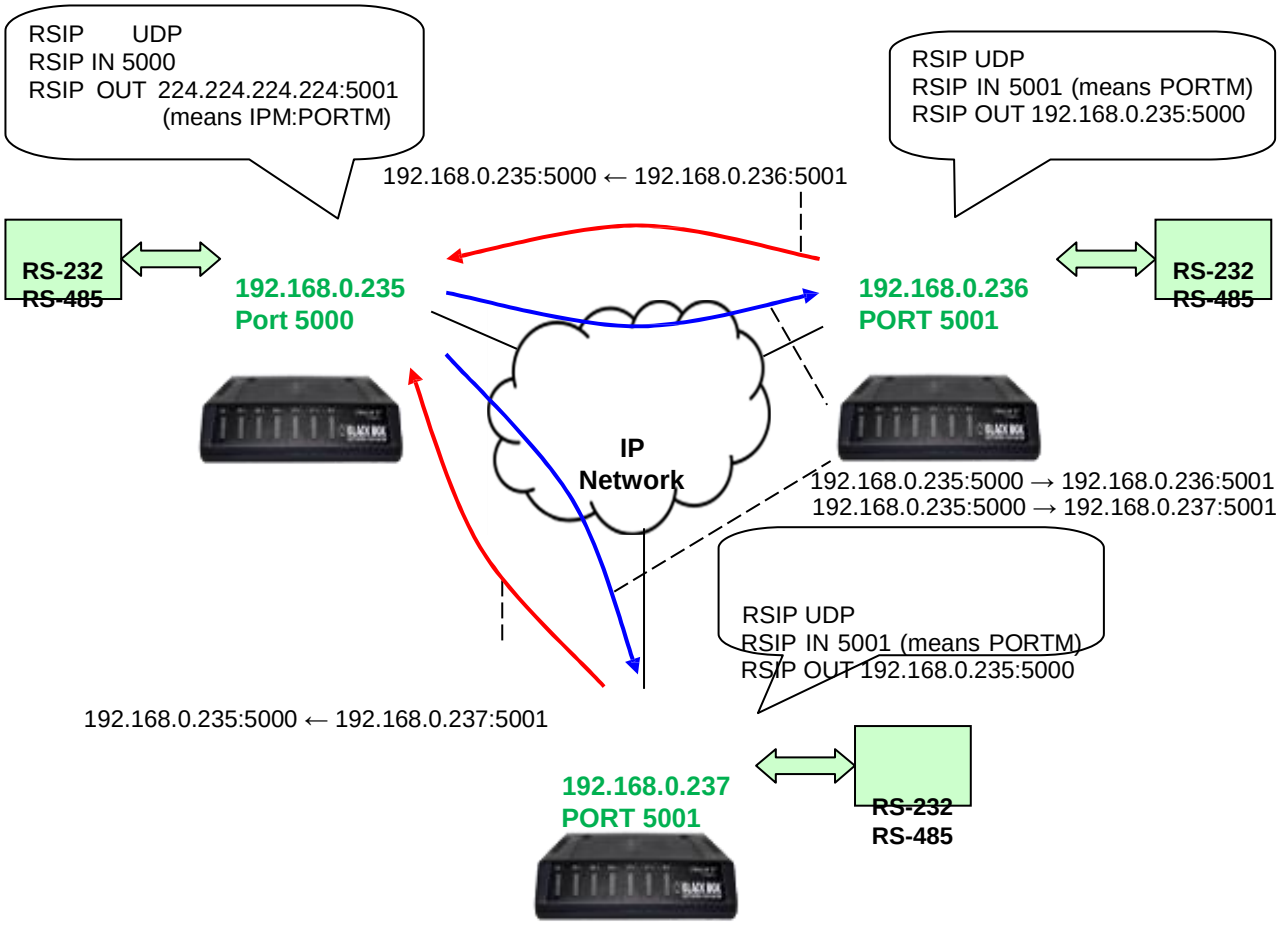
[ADDR] is [IP_Address:PORT_Number] for UDP and TCP Client, but [IP_Address] for TCP Server mode.

IN and OUT have following meaning: It means to configure - INput or OUTput Address. With IN the local IP port (listen port) will be configured that is used to receive serial data packets from the IP Network. With OUT the remote IP Address will be configured where serial data packets will be forwarded to.

Examples for possible commands:

RSIP UDP RS (Switch serial data to IP Network with UDP protocol)
RSIP CLIENT 4RS,2 (Switch second channel of 4xRS-232 card to TCP Client mode)
RSIP IN 5000 RS1 (Receive and send serial data with PORT Number 5000)
RSIP OUT 172.16.53.1:5000 RS1 (Select endpoint with IP Address 172.16.53.1 and PORT Number 5000 as remote side for serial data)

Serial Data Transmission UDP Point-To-MultiPoint



Please refer to picture 2.2 in paragraph 2.2 UDP Point-To-MultiPoint. You can perform on “Master” unit the following commands in menu 3 (CM):

RSIP UDP
RSIP IN 5000
RSIP OUT 224.224.224.224:5001

Please see the configuration on the unit with IP Address 192.168.0.235:

```
-------------------------------------------------------------------------------
Running Line Configuration
-------------------------------------------------------------------------------
xDSL                DSL1            DSL2
  Mode           :  Master(HTU-C)   Master(HTU-C)
  PAM, Baserate  :  PAM32,89        PAM32,89
  Annex          :  B               B
  Payload        :  WAN             WAN
  Clock source   :  Into            Int
  Reserve        :  ---             ---
  Power          :  OFF             OFF
  GS compatible  :  OFF
  NM/LA alarm    :  OFF/OFF

RS:RS-232
  Mode     :   RS<->IP
  Rate     :  9600
  Format   :  8N1
RS<->IP    (UDP,ON)
  Remote IP, port:
  224.224.224.224,
           5001
  Local port: 5000
-------------------------------------------------------------------------------
```

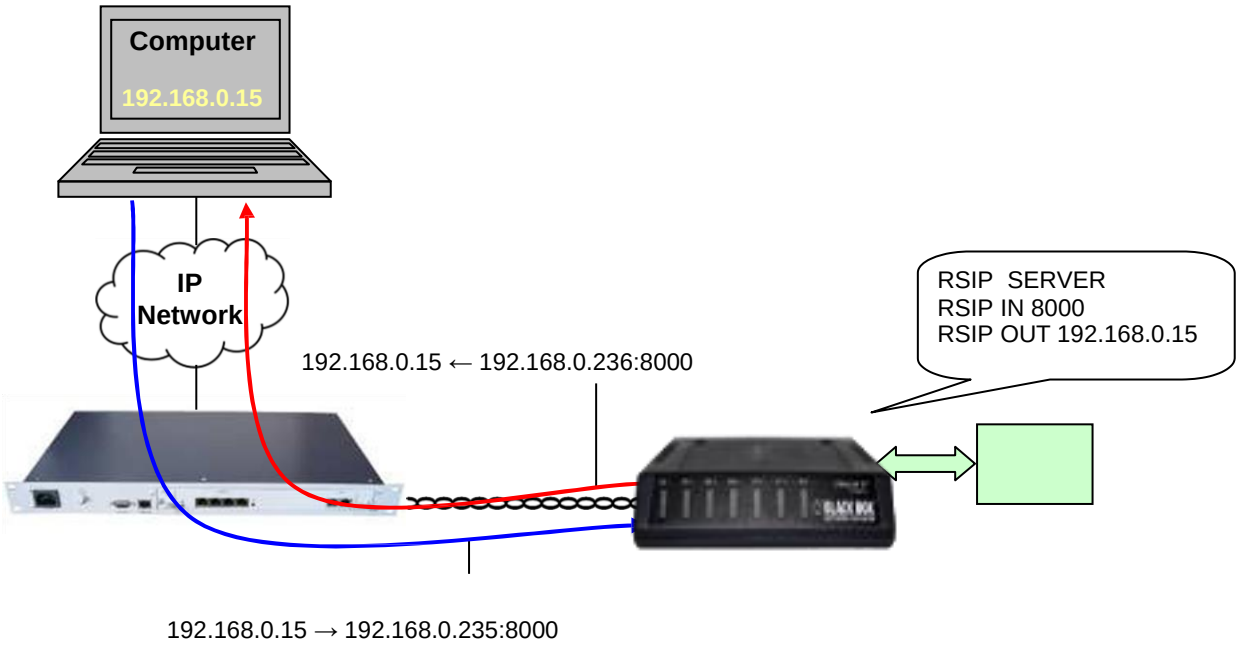
You can perform on other units the following commands in menu 3 (CM):

RSIP UDP
RSIP IN 5001
RSIP OUT 192.168.0.235:5000

Please see the configuration on the unit with IP Address 192.168.0.236 and 192.168.0.237:

```
-------------------------------------------------------------------------------
Running Line Configuration
-------------------------------------------------------------------------------
xDSL                DSL1            DSL2
  Mode           :  Slave(HTU-R)    Slave(HTU-R)
  PAM, Baserate  :  PAM32,89        PAM32,89
  Annex          :  B               B
  Payload        :  WAN             WAN
  Clock source   :  Int             Int
  Reserve        :  ---             ---
  GS compatible  :  OFF
  NM/LA alarm    :  OFF/OFF

RS:RS-232
  Mode     :   RS<->IP
  Rate     :  9600
  Format   :  8N1
RS<->IP (UDP,ON)
  Remote IP, port:
    192.168.0.235,
           5000
  Local port: 5001
-------------------------------------------------------------------------------
```

At the central side is a computer with the IP Address 192.168.0.15. At this computer any application program can work that needs the serial data of any equipment on the CPE side connected to the RS-232 card. The CPE side has the IP Address 192.168.0.235.



COM-Server application

4.6.5.40 <RSRATE [N]> Command

This command sets the bitrate of the serial interface.

```
CP_01_CM> RSRATE 115200
```

4.6.5.41 <RSFORMAT [Format]> Command

This command defines the RS-232/RS-485 data format. [Format] means:
Data bits: 5..8

Parity: N, E, O, M, S

- N - None
- E - Even
- O - Odd
- M - Mark
- S - Space Stop bits: 1, 1.5, 2

```
CP_01_CM> RSFORMAT 8N1
```

4.6.5.42 <RSDUPLEX [F/H] Command

This command sets the operating mode of the RS-485 interface:

- F means FULLDUPLEX
- H means HALFDUPLEX

4.6.5.43 <EXTRATE [N]> Command

This command sets the transmission rate N for Nx64/RS-232/RS-485 interfaces.

For the Nx64 interface: N=1…128 (V.35/V.36/X.21) or N=1…7 (V.28), in this case the Nx64 data rate will be Nx64 kbps.

For the RS232 and RS485 interfaces: N is the baudrate (9600 for instance). N=1200…256000.

4.6.5.44 <AUTOLOOP OFF/ALL/DATA> Command

This command sets the autoloop mode.

- OFF means line 141 is ignored
- ALL means a local loop forced by line 141 is allowed. Data from line 103 is looped to line 104 and clock from line113 is looped to line 115 (use in TTC clocking mode)
- DATA means local loop forced by line 141 is allowed. Data from line 103 is looped to line 104.

4.6.5.45 <EXTCLOCK [SRC] [DIR]> Command

This command defines the Nx64 clocking modes. SRC:

- NORMAL means clocked by DSL
- INT means clocked by internal oscillator
- TTC means clocked (Received Clock) by line 113 (Terminal Transmit Clock) DIR:
- CO means Codirectional mode
- CONTRA means Contradirectional mode

```
CO_01_CM>EXTCLOCK INT CO
```

4.6.5.46 <IOIP {OPTION} [IF]> Command

The IOIP command configures Input/Output (IO) signal transmission over IP-based networks running over DSL, Ethernet or E1 channels.

<IOIP INSENSITIVITY [TIME]> Command

This command defines the sensitivity of an Input signal in milliseconds. Signal shorter than INSENSITIVITY value will not be detected. Allowed settings are 100 ... 10000 ms.

<IOIP [UA/NUA/OFF] [NO/NC] [IF]> Command

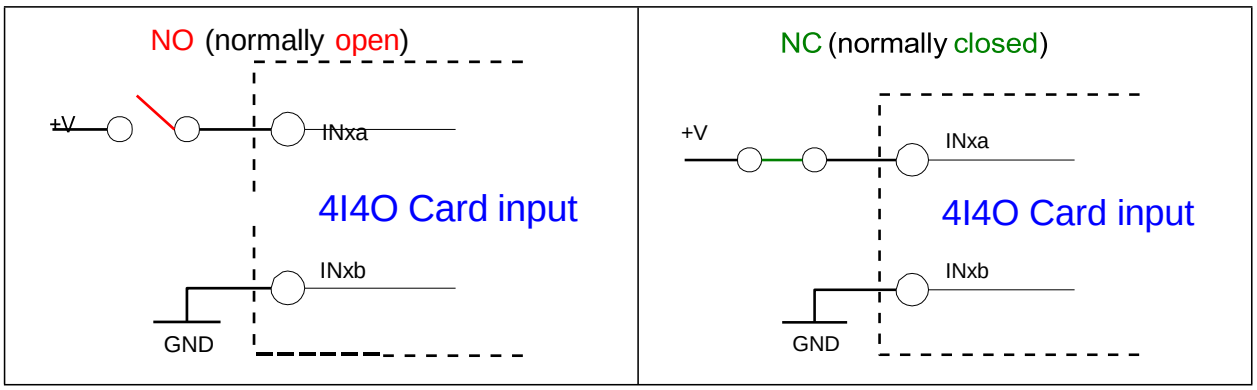
This command specifies operation mode of selected Input or Output interface.

UA/NUA Specifies that IN-x interface triggers ether Major (Urgent) or Minor (Non urgent) alarm of the unit or the OUT-x that should be triggered by Major (UA) or Minor (NUA) alarms.

OFF Shut down interface IN-x or OUT-x

NO Specifies that interface IN-x is normally opened (NO) or normally closed (NC). In NO state the current absence means no Alarm generation. Alarm will be generated if the current will be present on wire. NC defines the opposite state.

IF Interface: IN-1 ... IN-8 or OUT-1 ... OUT-8



<IOIP [CLIENT/SERVER/UDP] [IF]> Command
This command specifies operation mode of selected Input or Output interface.

CLIENT	Specifies TCP Client mode for interface IN-x.
SERVER	Specifies TCP Server mode for interface OUT-x.
UDP	Specifies UDP mode for interfaces IN-x or OUT-x.
IF	Interface: IN-1 ... IN-8 or OUT-1 ... OUT-8

<IOIP LOCAL [PORT] [IF]> Command
This command sets local IP port for an IF interface, an IF interfaces listens on.

PORT	Port can be in range from 1024 to 65535 and shouldn't be used by other services.
IF	Interface: IN-1 ... IN-8 or OUT-1 ... OUT-8

Local port always connected with management IP address of the device.

<IOIP REMOTE [IP:PORT] [IF]> Command
This command defines remote IP address and IP port number a local interface should be connected with.

IP:PORT	Specifies IP Address and Port number for pre-defined connection or "ANY" string. If ANY is specified, a TCP client with any IP address is allowed to connect the TCP server.

Examples:

IOIP LOCAL 5000 IN-1	Set local port for interface IN-1
IOIP LOCAL 5001 IN-2	Set local port for interface IN-2
IOP REMOTE 192.168.0.1:5000 IN-1	Set remote destination for interface IN-1
IOP REMOTE 192.168.0.1:5001 IN-2	Set remote destination for interface IN-2
IOP LOCAL 6000 OUT-1	Set local port for interface OUT-1
IOP REMOTE ANY OUT-1	Set any remote connection for interface OUT-1

4.6.5.47 <NET> Command

The <NET> command allows to enter into the submenu for NET settings.

4.6.5.48 <H> Command

Type <H> and the monitor lists all available commands in the NET sub-menu. If you type H [command] you will get additional help on [command].

```
CX_06_NET>H
------------------------------------------------------------------------------
Type 'H [command]' to get additional help on [command]
NETCONFIG                 Show network configuration
NETCONFIG [N/R/S/B]       Show       new/running/startup/backup       network
configuration COSCONFIG   Show CoS configuration
COSCONFIG [N/R/S/B]       Show       new/running/startup/backup       CoS
configuration RSTP DEFAULT  Set default RSTP configuration
RSTP [CONF/STATE/DIAG]    Show RSTP state/configuration/diagnostics
RSTP [BR/IF] [OPT] [N]    Set RSTP Bridge/Interface properties
RSTP [A..E] [ON/OFF]      Switch RSTP ON/OFF at PBVLAN A..E
PBVLAN [IF] [A..E/S]      Set port-based VLAN for the interface
MODE [IF] [ACC/TRUNK/MIX]Set mode of LANx interfaces: access, trunk, mixed
VLAN [IF] [1..8]          Set default VLAN index for access ports
QOS [IF] [0..7]           Set default QoS for access ports
ALLOW [IF] [VLAN list]    Set list of VLANS to allow on trunk interface
VID [1-8] ID              Assign VID to the VLAN specified
MACLIST SHOW              Show MAC filter settings
MACLIST SHOW [N/R/S/B]    Show new/running/startup/backup MAC list
MACLIST [IF] ADD [MAC]    Add MAC to the white list
MACLIST [IF] DEL [MAC/N] Delete MAC from the white list
MACFILTER [LAN1-5] [ON/OFF]Enable/disable MAC filtering
MACRULE [LAN1-5] [rule]   Set the MAC Filter behaviour
SETIP x.x.x.x             Set modem IP address
GATEWAY x.x.x.x           Set gateway IP address
NETMASK x.x.x.x           Set netmask
MTU [68..1500]            Set port INT MTU
WANIDLE [1/7E]            Select  WAN  idle  pattern
ETHSD [MODE] [N=1-5]      Set Nth Ethernet port speed
FC [ON/OFF] [N=1-5]       Set Ethernet port flow control
IRATE [speed/OFF] [N=1-5]Set LAN port ingress rate limit
ERATE [speed/OFF]         Set  modem  egress  rate  limit
CRATE [speed] [CoS] [WAN]Set COS egress rate limit
COS [QOS/VLAN] [N] [0..3/OFF]Set QoS/VLAN to COS mapping
SNMP [V1|V2C|V3] [ON|OFF]Activate support for SNMP v1, v2c, v3
TRAP [1/2] [IP/OFF]       Set trap IP address or disable
TRAP [1/2] [V1/V2C]       Select v1/v2c for trap
TRAP [1/2] V3 [RO/RW]     Select  v3  and  user  for  trap
COMMUNITY                 Set SNMP v1,v2c community name
SNMPSET [ON/OFF]          Enable/disable SNMP v1,v2c SET commands
SNMP [RO|RW] NAME         Set SNMPv3 user security name
SNMP [RO|RW] AUTH [MODE] Set SNMPv3 user authentication: MD5,SHA,NONE
SNMP [RO|RW] PRIV [MODE] Set SNMPv3 user privacy: DES,AES,NONE
RMONALARM N [ON/OFF]      Setup RMON alarm N
RMONEVENT N [ON/OFF]      Setup RMON event N
LLDP [ON/OFF]             Enable/disable LLDP
LLDP DEFAULT              Set default LLDP setup
LLDP [PARAM] [VALUE]      Set various LLDP transmission parameters
LLDP [TX|RX] [ON/OFF]     Enable/disable transmission or receiving of LLDPDU
LLDP INT VLAN [ON/OFF]    Enable/disable LLDP in management VLAN only
LLDP CONFIG               Show LLDP configuration
SNTP [1/2] [IP/OFF]       Set/delete SNTP server IP addresses
SNTP TZ [+/-]HH:MM        Set local time zone
DST SUMMER                Set Summer time rule
DST WINTER                Set winter time rule
DST [OFF/INFO/NAME]       Select Daylight Saving Time
SYSLOG [1/2] [IP/OFF]     Set/delete Syslog server IP addresses
NETDEFAULT                Set  default  network  configuration
SSH|TELNET|HTTP [ON/OFF] Enable/disable management servers
SSH PORT [N]              Set TCP port for SSH service
```

```
RADIUS [1/2] SECRET      Set shared key for Radius Server 1 or 2
RADIUS [1/2] SECRET OFF  Clear shared secret for Radius 1 or 2 RADIUS
[1/2] TEST               Test Radius server connection and User data
RADIUS [1/2] [IP:PORT/OFF]Set/delete IP address and port for Radius Server
RADIUS RETRIES [0..10]   Set number of retries for both Radius servers
RADIUS TIMEOUT [1..5]    Set Radius response timeout, seconds
SYSNAME [SET]            Show/Set   sysName   variable
SYSLOCATION [SET]        Show/Set sysLocation variable
SYSCONTACT [SET]         Show/Set sysContact variable
STATUS RADIUS [NRSB]     Show RADIUS server status and parameters
APPLY [ALL/GROUP]        Apply changes to running configuration
CONNECT [N:[1-13/R]]     Establish connection to remote unit LINK
[NN]                     Establish local connection
LINKCLEAR                Exit all local connections
M                        Return to Configuration Management Menu
H                        Show available commands
--------------------------------------------------------------------------------
CX_06_NET>
```

4.6.5.49 <NETCONFIG [N/R/S/B]> Command

Without parameters the <NETCONFIG> command displays the running configuration of the network subsystem and interfaces:

```
CO_06_NET>NETCONFIG
-------------------------------------------------------------------------------
Running Network Configuration
-------------------------------------------------------------------------------
Ethernet settings : LAN1  LAN2  LAN3  LAN4  LAN5  WAN1  WAN2  WAN3  WAN4   INT
  Description     : LAN1  LAN2  LAN3  LAN4  Backp WAN1  WAN2  WAN3  WAN4   INT
  Access/Trunk    :  ACC   ACC   ACC   ACC   ACC  Trunk Trunk Trunk Trunk  ACC
  Port-based VLAN :  [A]   [A]   [A]   [A]   [A]   [A]   [A]   [A]   [A]   [A]
  VLAN            :   1     1     1     1     1                             1
  QoS             :   2     2     2     2     2                             2
  VLAN1 VID=1     :                                 +     +     +     +
  VLAN2 VID=2     :                                 +     +     +     +
  VLAN3 VID=3     :                                 +     +     +     +
  VLAN4 VID=4     :                                 +     +     +     +
  VLAN5 VID=5     :                                 +     +     +     +
  VLAN6 VID=6     :                                 +     +     +     +
  VLAN7 VID=7     :                                 +     +     +     +
  VLAN8 VID=8     :                                 +     +     +     +
  OTHER VLANS     :                                 +     +     +     +
  Speed           : AUTO  AUTO  AUTO  AUTO  AUTO
  Flow control    :  OFF   OFF   OFF   OFF   OFF
System settings
  IP address      :  192.168.1.6      MAC address     :  00:0f:d9:04:a7:25
  Subnet mask     :  255.255.255.0    Management MTU  :  1500
  Default gateway :  192.168.1.254    WAN idle pattern:  All 1's
SNMP
  SNMP versions   :  v1 v2c
  v3 Allowed pollers :  All
  Trap IP/version :  192.168.169.12(v3, RO)
SNMP v1,v2c community
  GET/SET/TRAP    :
  public/public/public SET command :
  Enabled
SNMP v3 users     :  Read-only (RO)           Read-write
  (RW) Security name                          :    snmp_ro
                 snmp_rw
  Auth/Priv       :  none/none                not selected
  Auth Password   :  ---                      ---
  Priv Password   :  ---                      --- Services:  TELNET, SSH(22), HTTP
  Syslog servers  :
  SNTP   servers  :  192.168.1.254                                TZ: UTC+01:00
  Summer time     :   MAR  lastSUN   (30)  00:00w
  +60min Winter time:   OCT  lastSUN   (26)  00:00w
  +0min
  Radius servers  :  192.168.1.252:1812       192.168.1.254:1812
  Radius secret   :  entered                  entered
-------------------------------------------------------------------------------
CO_06_NET>
```

VLAN (VLANs & QoS) configurations	
Ethernet settings	Port identifier of the internal Ethernet switch
Description	Port Description (ifAlias)
Mode	Type of port (trunk, access or mixed)
Port based VLAN	Isolation of ports
VLAN	VLAN identifier for each of access ports
QoS	Priority for each of access ports
VLAN1 VID=xx : : VLAN8 VID=xx	Configurations and identifiers (xx=1..4094) for each of 8 VLANs which are configured separately. Pluses and minuses mark transmission/locking of VLAN for each of interfaces.
OTHER VLANS	Configurations for other VLANs, which are not configured separately. Pluses and minuses mark transmission/locking for each of interfaces.
Ethernet port configurations	
Speed/Duplex	Operation mode of the Ethernet interface
Flow control	Flow control mode of the Ethernet interface
General settings	
MAC address	MAC address of the device
IP address	IP address of the device
Subnet Mask	Network mask of the device
Default Gateway	Default gateway of the device
Management MTU	Maximal size of management packets, bytes
WAN idle pattern	Idle pattern for empty frames if transmitted over E1 links: all 1's or 7E
SNMP settings	
SNMP Version	Active SNMP versions
Allowed pollers	List of hosts allowed to perform SNMP poll
Trap IP/version	IP address of Trap receiver and Trap version. If SNMP v3 is selected, it is shown what user (RO or RW) will send trap messages.
GET/SET/TRAP	SNMP v1 and v2c community for GET, SET and TRAP messages
SET command	Enabled or Blocked SNMP V1 and V2c SET operation
SNMP v3 users	User with Read-Only (RO) and Read-Write (RW) access rights
Security name	User names for RO and RW user
Auth/Priv	User Authentication (MD5/SHA/NONE) and Privacy (DES/AES/NONE)
Auth password	Authentication password (SNMP v3)
Priv password	Privacy password (SNMP v3)
Service settings	
Services	List of running management servers
Syslog servers	First and Second Syslog server IP address
SNTP servers	First and Second SNTP server IP address
TZ	Time Zone settings
Summer Time	Summer Time change settings
Winter Time	Winter Time change settings
Radius servers	IP address and port used for first and second RADIUS servers
Radius secret	Shows if shared secret has been entered or not

The NETCONFIG command always displays the running configuration. If the new configuration differs from the running one, the NETCONFIG command displays the running configuration and a warning:

```
--------------------------------------------------------------------------------
Warning: New network configuration differs from running network configuration!
         To view new network configuration, type 'NETCONFIG N'
         To view running network configuration, type 'NETCONFIG R'
         To apply changes in configuration, type 'APPLY VLAN' or 'APPLY ALL'.
         Do not forget to 'CONFIRM' a good working configuration.
CP_NET>
```

The <NETCONFIG [N/R/S/B]> command displays one of four configurations: New, Running, Startup, or Backup, depending on the parameter.

After successful execution of a command that changes any parameter showed by NETCONFIG, the new configuration is shown. The warning message explaining that the new configuration differs from the running configuration is displayed as well.

4.6.5.50 <COSCONFIG [N/R/S/B]> Command

Without parameters the <COSCONFIG> command displays the running CoS configuration:

```
CO_NET>COSCONFIG
--------------------------------------------------------------------------------

Running QoS Configuration
--------------------------------------------------------------------------------

QoS to CoS mapping      Per-VLAN CoS override
------------------      --------------------
QoS : 0 1 2 3 4 5 6 7   VLAN: 1 2 3 4 5 6 7 8
CoS : 3 3 3 3 3 3 3 3   CoS : - - - - - - - -

---------------Rate limit--------------------
Egress  :   WAN1   WAN2   WAN3   WAN4
CoS 0   :    OFF    OFF    OFF    OFF
CoS 1   :    OFF    OFF    OFF    OFF
CoS 2   :    OFF    OFF    OFF    OFF

-------------------------------------------
Ingress :   LAN1    LAN2
Per port:    OFF     OFF
Total   :    OFF
--------------------------------------------------------------------------------

CO_NET>
```

It shows the QoS-to-CoS and VLAN-to-CoS mapping. CoS (Class of Service) as well as QoS (Quality of Service) have to be configured for a correct behaviour!
The rate limits for any interface is showed too.

The <COSCONFIG [N/R/S/B]> command displays one of four CoS configurations: New, Running, Startup, or Backup, depending on the parameter.

4.6.5.51 <RSTP DEFAULT> Command

RSTP DEFAULT command restores factory settings for RSTP subsystems:

- All RSTP instances are disabled; modem works like it has no RSTP system.
- Each system interface has priority 128 (0x80)
- Each system interface calculates PCOST automatically
- Each RSTP instance has priority 32768 (0x8000)
- Each RSTP instance works in VLAN# 1
- Hello time for each RSTP instance is 2 seconds
- Forward Delay for each RSTP instance is 15 seconds
- Maximum Age for each RSTP instance is 20

```
CO_NET>RSTP DEFAULT
 PB Status   Vlan/VID Prio  Hello FwdDelay MaxAge
-------------------------------------------------
 A  Disabled 1/1      32768 2     15       20
 B  Disabled 1/1      32768 2     15       20
 C  Disabled 1/1      32768 2     15       20
 D  Disabled 1/1      32768 2     15       20
 E  Disabled 1/1      32768 2     15       20
-------------------------------------------------
IFACE  Prio PathCost  Edge
-------------------------
LAN1   128  AUTO      Yes
LAN2   128  AUTO      Yes
LAN3   128  AUTO      Yes
```

```
LAN4   128  AUTO      Yes
LAN5   128  AUTO      Yes
WAN1   128  AUTO      Yes
WAN2   128  AUTO      Yes
WAN3   128  AUTO      Yes
WAN4   128  AUTO      Yes
MWAN1  128  AUTO      Yes
MWAN2  128  AUTO      Yes
-------------------------
```

4.6.5.52 <RSTP [A..E] [ON/OFF]> Command

RSTP system creates separate instance for each PBVLAN. Every instance will work only with ports included in specific PBVLAN. It means that up to 5 RSTP instances could be created on a device.

RSTP [A . . E] [ON/OFF] Command enables/disables RSTP for specific PBVLAN.

4.6.5.53 <RSTP [A..E] PRIO [value]> Command

This command allows to setup custom bridge priority for RSTP instance working at specific PBVLAN. This value represents priority and settable part of bridge id (802.1D - 2004, 9.2.5).

Smaller value denotes better priority. This option allows Root bridge selection for network and it's replacements in case of faults. Available interval is from 0 to 65535 inclusively. It is recommended to use values from 0 to 61440 while each value should be multiple of 4096.

Default RSTP bridge priority is 32768.

4.6.5.54 <RSTP [A..E] VLAN [1..8]> Command

This command allows selection of a VLAN that will be used for RSTP service data transmission (BPDU) for RSTP instance working at specific PBVLAN. Please note that RSTP will relay on network topology covered by selected VLAN, that’s why a VLAN that covers all network should be selected. Default VLAN is 1.

4.6.5.55 <RSTP [A..E] HELLO [2..10]> Command

This command selects time interval between two consecutive RSTP service messages in seconds. It means that BPDU packets will be send every HELLO time. Default value is 2 seconds.

4.6.5.56 <RSTP [IFACE] FWD [4..30]> Command

This command defines forwarding delay in seconds. Depending on the port role: Edge or Not- edge, designated port changes its status according to the following sequence:

<u>For Non-edge ports, i.e. for ports connected to other RSTP-enabled devices:</u>

- Discarding - port discards incoming traffic
    - Forwarding Delay (in seconds)
- Learning - port learns information about peer (MAC, RSTP priority, etc.)

  - Forwarding Delay (in seconds)
- Forwarding - port forwards traffic

Forwarding Delay implies delay between port status change in sequence. Device will be ensured that the link is valid and stable before enabling traffic forwarding on a port.

For Edge ports, i.e. for ports connected to PCs, servers and other terminal devices that don't support RSTP:

- Discarding - port discards incoming traffic
- Forwarding - port forwards traffic

Edge ports must be switched very fast to prevent traffic lost. Forwarding Delay is not applicable in this mode. Port switches its state from Discarding to Forwarding state without Learning phase.

4.6.5.57 <RSTP [IFACE] MA [6..40]

This parameter sets Maximum Age parameter. According to the IEEE 802.1D:2004 standard the Maximum Age parameter declares the node number in the chain, that will discard the BPDU packet that root-bridge sends. Every node in the chain will compare “Age” value in BPDU and will drop the packet if its “Age” will be greater than Maximum Age.

Message parameters	**Node Number, counted from Root / Message Age**							
	Root	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Output: Age = 0 Max Age = 6	**Age: 0 →**							
Input: Age = 0 Max Age = 6 Age < Max Age? Yes, forward packet Age = Age + 1		**Age: 1 →**						
Input: Age = 1 Max Age = 6 Age < Max Age? Yes, forward packet Age = Age + 1			**Age: 2 →**					
Input: Age = 2 Max Age = 6 Age < Max Age? Yes, forward packet Age = Age + 1				**Age: 3 →**				
Input: Age = 3 Max Age = 6 Age < Max Age? Yes, forward packet Age = Age + 1					**Age: 4 →**			
Input: Age = 4 Max Age = 6 Age < Max Age? Yes, forward packet Age = Age + 1						**Age: 5 →**		
Input: Age = 5 Max Age = 6 Age < Max Age? Yes, forward packet Age = Age + 1							**Age: 6**	
Input: Age = 6 Max Age = 6 Age < Max Age? No, discard packet								

4.6.5.58 RSTP [IFACE] PRIO [0..240]> Command

This command selects interface priority. The value should be multiple by 16. The port priority intended to resolve situation when several interfaces have the same root path cost. The port with lowest port priority will be selected then. Available interfaces are:

- LAN1 – LAN5
- WAN 1, 2, 3, 4
- MWAN 1, 2

4.6.5.59 <RSTP [IFACE] PCOST [AUTO/1..200000000]> Command

This command allows automatic path cost selection or allows manual settings. In automatic mode the value depends on the bit rate. The higher bit rate the lower path cost is. The port with lower path cost will be selected as root port. Available interfaces are:

- LAN1 – LAN5
- WAN 1, 2, 3, 4
- MWAN 1, 2

4.6.5.60 <RSTP [IFACE] EDGE [ON/OFF]> Command

This command configures how the unit will treat with the “Edge” attribute of an interface. Edge attribute tells the port how to trigger its states from Discarding to Forwarding phases. The general rule is:

- If port connected to the Spanning Tree network, it is “Non-Edge” and it changes its state slow, going through Learning phase.
- If port connected to terminal devices (PCs, Servers), it is “Edge” and it changes its status fast, escaping the Learning phase.

<RSTP [IFACE] EDGE OFF> command means that the port will never become “Edge”. It will change all its phases and always will send RSTP BPDUs in egress direction.

<RSTP [IFACE] EDGE ON> command tells the interface to set the “Edge” attribute automatically. Port will keep its “Edge” status and will change its status fast until it will receive first BPDU

Default settings is EDGE = ON. It is recommended to keep default value. Available interfaces are:

- LAN1 – LAN5
- WAN 1, 2, 3, 4
- MWAN 1, 2

4.6.5.61 <RSTP CONF> Command

This command shows actual RSTP configuration for all instances.

```
PB Status   Vlan/VID Prio  Hello FwdDelay MaxAge
-------------------------------------------------
 A  Enabled  1/1      32768 2     15       20
 B  Disabled 1/1      32768 2     15       20
 C  Disabled 1/1      32768 2     15       20
 D  Disabled 1/1      32768 2     15       20
 E  Disabled 1/1      32768 2     15       20
```

```
IFACE  Prio PathCost  Edge
-------------------------
LAN1   128  AUTO      Yes
LAN2   128  AUTO      Yes
LAN3   128  AUTO      Yes
LAN4   128  AUTO      Yes
LAN5   128  AUTO      Yes
WAN1   128  AUTO      Yes
WAN2   128  AUTO      Yes
WAN3   128  AUTO      Yes
WAN4   128  AUTO      Yes
MWAN1  128  AUTO      Yes
MWAN2  128  AUTO      Yes
-------------------------
CX_03_NET>
```

RSTP configurations for whole device	
PB	Port Base VLAN letter. Could be from A to E
Status	RSTP status for an instance.
VLAN/VID	Displays service VLAN number and VID for RSTP service messages
Prio	RSTP bridge priority
Hello	Hello time in seconds
FwdDelay	Forwarding Delay
MaxAge	Maximal Age
RSTP configuration for an interface	
IFACE	Interface name
Prio	Interface priority
PathCost	Interface Path Cost
Edge	Port Edge behaviour: Yes: means port can become “Edge” No: means port will never be “Edge”

4.6.5.62 <RSTP STATE> Command

Command shows RSTP actual status.

```
CX_03_NET>RSTP STATE

 PV PortID IFACE Status State Role Bitrate   PCost          Edge
-------------------------------------------------------------  A
 8001      LAN1  UP     Fwd   Desi 100.0Mbit AUTO/200000    Yes
    8002   LAN2  DOWN    ---   ---    ---     AUTO/   ---     ---
    8003   LAN3  DOWN    ---   ---    ---     AUTO/   ---     ---
    8004   LAN4  DOWN    ---   ---    ---     AUTO/   ---     ---
    8005   LAN5  DOWN    ---   ---    ---     AUTO/   ---     ---
    8006   WAN1  UP     Disc  Alt  5.696Mbit AUTO/3511235   No
    8007 R WAN2  UP     Fwd   Root 5.696Mbit AUTO/3511235   No
    8008   WAN3  DOWN    ---   ---    ---     AUTO/   ---     ---
    8009   WAN4  DOWN    ---   ---    ---     AUTO/   ---     ---
    800A   MWAN1 DOWN    ---   ---    ---     AUTO/   ---     ---
    800B   MWAN2 DOWN    ---   ---    ---     AUTO/   ---     ---
 B  8001   MWAN1 DOWN    ---   ---    ---     AUTO/   ---     ---
    8002   MWAN2 DOWN    ---   ---    ---     AUTO/   ---     ---
```

```
 C  8001   MWAN1 DOWN    ---   ---    ---    AUTO/   ---     ---
    8002   MWAN2 DOWN    ---   ---    ---    AUTO/   ---     ---
 D  8001   MWAN1 DOWN    ---   ---    ---    AUTO/   ---     ---
    8002   MWAN2 DOWN    ---   ---    ---    AUTO/   ---     ---
 E  8001   MWAN1 DOWN    ---   ---    ---    AUTO/   ---     ---
    8002   MWAN2 DOWN    ---   ---    ---    AUTO/   ---     ---
-------------------------------------------------------------------
CX_03_NET>
```

RSTP Status	
PV	Port Base VLAN letter
PortID	Port identification
IFACE	Interface name
Status	Status of a port: Up or Down
State	State of a port: Forwarding or Discarding
Role	Port role: Designating, Root or Alternative
Bitrate	Port bitrate
PCost	Actual interface Path Cost.
Edge	Actual Edge status of a port. Yes: means that port is “Edge” and switches own phases fast No: means that port is “Non-edge” and participates in spanning tree construction.

4.6.5.63 <RSTP DIAG> Command

The <RSTP DIAG> command shows RSTP diagnostics per interface. It displays what RSTP priority and what MAC address switch receives and what MAC address / RSTP priority it advertises to its neighbours.

```
CX_06_NET>RSTP DIAG
RSTP A 36864:00-0F-D9-04-A7-25 :
        1. LAN1   32768:00-0F-D9-05-F5-BC
        2. LAN2   36864:00-0F-D9-04-A7-25
        3. LAN3   36864:00-0F-D9-04-A7-25
        4. LAN4   36864:00-0F-D9-04-A7-25
        5. LAN5   36864:00-0F-D9-04-A7-25
        6. INT    36864:00-0F-D9-04-A7-25
        7. WAN1   36864:00-0F-D9-04-A7-25
        8. WAN2   36864:00-0F-D9-04-A7-25
        9. WAN3   36864:00-0F-D9-04-A7-25
        10. WAN4   36864:00-0F-D9-04-A7-25
        11. MWAN1  36864:00-0F-D9-04-A7-25
        12.  MWAN2   36864:00-0F-D9-04-A7-25
RSTP B 32768:00-0F-D9-04-A7-25 :
        1. MWAN1  32768:00-0F-D9-04-A7-25
        2.  MWAN2   32768:00-0F-D9-04-A7-25
RSTP C 32768:00-0F-D9-04-A7-25 :
        1. MWAN1      0:00-00-00-00-00-00
        2. MWAN2      0:00-00-00-00-00-00
RSTP D 32768:00-0F-D9-04-A7-25 :
        1. MWAN1      0:00-00-00-00-00-00
        2. MWAN2      0:00-00-00-00-00-00
RSTP E 32768:00-0F-D9-04-A7-25 :
        1. MWAN1      0:00-00-00-00-00-00
        2. MWAN2      0:00-00-00-00-00-00
CX_06_NET>
```

4.6.5.64 <PBVLAN [IF] [A..E]> Command

This command assigns the network interface (LANx, WANx, INT) to one of 5 port-based VLANS (PBVLAN A..E).

```
CP_01_NET>PBVLAN LAN1 B
CP_01_NET>PBVLAN INT A
-------------------------------------------------------------------------------
New Network Configuration
```

```
--------------------------------------------------------------------------------
Ethernet settings : LAN1  LAN2  LAN3  LAN4  LAN5  WAN1  WAN2  WAN3  WAN4   INT
  Access/Trunk    :  ACC   ACC   ACC   ACC   ACC  Trunk Trunk Trunk Trunk  ACC
  Port-based VLAN :  [B]   [A]   [A]   [A]   [A]   [A]   [A]   [A]   [A]   [A]
  VLAN            :   1     1     1     1     1                              1
  QoS             :   2     2     2     2     2                              2
  VLAN1 VID=1     :                                 +     +     +     +
  VLAN2 VID=2     :                                 +     +     +     +
  VLAN3 VID=3     :                                 +     +     +     +
  VLAN4 VID=4     :                                 +     +     +     +
  VLAN5 VID=5     :                                 +     +     +     +
  VLAN6 VID=6     :                                 +     +     +     +
  VLAN7 VID=7     :                                 +     +     +     +
  VLAN8 VID=8     :                                 +     +     +     +
  OTHER VLANS     :                                 +     +     +     +
  Speed           : AUTO  AUTO  AUTO  AUTO  AUTO
System settings   :
  MAC address     :  00:0f:d9:00:00:00
  IP address      :  192.168.0.254
  Subnet mask     :  255.255.255.0
  Default gateway :  192.168.0.254
--------------------------------------------------------------------------------
Warning: New network configuration is shown, because it differs from running.
         To view new network configuration, type 'NETCONFIG N'.
         To view running network configuration, type 'NETCONFIG R'.
         To apply changes in configuration, type 'APPLY VLAN' or 'APPLY ALL'.
         Do not forget to 'CONFIRM' a good working configuration.
CP_01_NET>
```

PBVLANs are used as a way to isolate groups of network interfaces from each other. No frames from interface LAN2 connected to PBVLAN A will ever be forwarded to interface INT, which is connected to PBVLAN E. And vice versa.

Each PBVLAN is a separate switching fabric. As there are 5 PBVLAN and no more than 10 network interfaces in the modem, one can connect any WAN interface to any LAN interface exclusively, as well as create isolated LAN-LAN or LAN-INT connections. Each PBVLAN can include from none to all interfaces. To populate PBVLAN with interfaces, just set the appropriate PBVLAN letter for selected interfaces.

PBVLAN isolation works only in the limits of one modem. Outside the modem, there is no information about the PBVLAN letter the frame had inside. This is the major difference with VLANs, where the VLAN information is carried in the VLAN tag. So, it does not hurt if WAN1, PBLAN A on one modem is connected to WAN1, PBVLAN C on another.

PBVLAN isolation also affects aggregation of WANs in MWAN (multi-WAN). Only WAN channels from the same PBVLAN will aggregate with each other. For example, if WAN1 and WAN3 are in PBVLAN A, and WAN2 and WAN4 are in PBVLAN B, and all WANs go in one direction, two MWANs will be created each consisting of 2 WANs instead of 1 MWAN with 4 WANs.

Creating a PBVLAN with only LAN ports and one WAN port will allow the modem to eliminate most software processing of frames, creating bridge connection and thus reducing frame propagation delay. The same applies to the case when there are several WAN ports in the PBVLAN, but they all go in the same direction. Assigning INT port to the PBVLAN with LAN and WAN will turn on the internal Layer2 switch. This will, however, not be sensible in most of the applications.

Most setups where LAN traffic separation is needed can be made with PBVLANs only or VLANs only. In some setups PBVLANs way has benefits, in some the VLAN way. Mix of VLANs and PBVLANs is also convenient in some applications. The user can select the approach.

4.6.5.65 <MODE [IF] [ACC/TRUNK/MIX]> Command

This command selects the 802.1Q VLAN mode for any LAN interface. Along with the full words ACCESS, TRUNK and MIXED, also abbreviations can be used, for example A or ACC for ACCESS, MIX or M for MIXED.

In ACCESS mode only untagged frames pass into (ingress) and out of (egress) the LANx port. On ingress, frames are assigned to default VLAN tag with VID and QoS defined by QOS, VLAN and VID commands. On egress, only frames with VLAN equal to the default VLAN of the port (set with VLAN command) are allowed, and the VLAN tag is removed.

In TRUNK mode only tagged frames pass into and out of the LANx port. Frames are allowed to pass on per-VLAN basis. VLANs allowed to pass are those selected with the ALLOW command (any combination of VLAN1-8 and OTHER can be selected).
In MIXED mode tagged and untagged traffic is allowed on the port. However, on ingress, a default VLAN tag (selected with QOS, VLAN and VID commands) is added to untagged frames so that all frames in the system are actually tagged. On egress frames with VLAN equal to the default VLAN (set with VLAN command) exit the port untagged, while to all other VLANs apply pass/block rules are set by the ALLOW command.

4.6.5.66 <VLAN [IF] [1..8]> Command

This command sets default VLAN number for interfaces in ACCESS or MIXED mode ([IF] is LANx, INT). Default VLAN is used to assign VLAN information for untagged traffic.

In ACCESS mode, only frames with VLAN equal to port's default VLAN are allowed to egress.
In MIXED mode, frames with VLAN equal to port's default VLAN egress untagged. Frames of all other VLANs are blocked or are allowed to egress tagged according to rules set by ALLOW command.
In both ACCESS and MIXED modes ingressing untagged frames are assigned to default VLAN.
There are 8 separately managed VLANs in the modem. For each managed VLAN the VID (VLAN ID) can be selected with the VID command.

4.6.5.67 <QOS [IF] [0..7]> Command

This command sets default QoS for interfaces in ACCESS or MIXED mode ([IF] is LANx, INT). The Lowest priority is 0, the highest is 7. Default QoS is used to assign quality of service information for ingressing untagged traffic.
The INT interface is always considered in ACCESS mode and all frames coming from the INT interface will have default QoS assigned.

4.6.5.68 <ALLOW [IF] [VLAN list]> Command

This command selects which VLANs are allowed on interfaces in TRUNK or MIXED mode ([IF] is LANx, WANx).
The VLAN list is a comma-separated list of allowed VLANS from 1 to 8, and the word OTHER (allows all other VLANs except 1-8). Spaces in the list are not allowed. To allow all VLANS on the interface, write ALL in the list.

```
CP_01_NET>ALLOW LAN1 1,2,3
CP_01_NET>ALLOW WAN2 5,3,OTHER
CP_01_NET>ALLOW WAN4 ALL
```

4.6.5.69 <VID [1-8] ID> Command

The <VID [1...8] ID> command sets VID for the VLAN with the number 1..8 equal to the ID parameter. ID=1...4094. 8 VLANs are supported by the device, and available VID numbers assigned to the VLAN are in the range from 1 to 4094. VID as well as QoS are an attribute of the VLAN packet.

4.6.5.70 <MACLIST SHOW> Command

Without parameters the <MACLIST SHOW> command displays the whole MAC Filter table for all available interfaces:

```
CX_05_NET>MACLIST SHOW
------------------------------------------------------------------------------
Running MAC Filter Configuration
------------------------------------------------------------------------------
```

```
Port      LAN1           LAN2           LAN3           LAN4           LAN5
Mode    ON/FILTER      ON/INDICATE     ON/BLOCK       ON/BLOCK      OFF/FILTER
White list
  1  0090f5-3e7a0b  0090f5-bb7a0b  0090f5-bb7a0b  0090f5-bb7a0b       ---
  2  0090f5-bb7a0b  0090cc-3e7a0b  0090cc-3e7a0b  0090cc-3e7a0b       ---
  3  0090cc-3e7a0b       ---            ---            ---            ---
  4       ---            ---            ---            ---            ---
  5       ---            ---            ---            ---            ---
  6       ---            ---            ---            ---            ---
  7       ---            ---            ---            ---            ---
  8       ---            ---            ---            ---            ---
  9       ---            ---            ---            ---            ---
 10       ---            ---            ---            ---            ---
--------------------------------------------------------------------------------
```

MAC Filter configuration	
Port	Port identifier of the internal Ethernet switch
Mode	ON: MACFILTER is enabled OFF: MACFILTER is disabled FILTER: non-listed ingress packets will be filtered INDICATE: non-listed ingress packets will be filtered and SNMP Trap will be generated
	BLOCK: port will be blocked upon receiving of non-listed packet and SNMP Trap will be generated
White list	List of allowed MAC addresses per interface

The <MACLIST SHOW [N/R/S/B]> command displays, depending on the parameter, one of four configurations: New, Running, Startup, or Backup.

4.6.5.71 <MACLIST [IF] ADD [MAC]> Command

The <MACLIST [IF] ADD [MAC]> command adds [MAC] address to the White List of the specified [IF] interface:

```
CX_05_NET>MACLIST 1 ADD 00-90-F5-3E-7F-AC
--------------------------------------------------------------------------------
New  MAC Filter Configuration
--------------------------------------------------------------------------------
Port      LAN1           LAN2           LAN3           LAN4           LAN5
Mode    ON/FILTER      ON/INDICATE     ON/BLOCK       ON/BLOCK      OFF/FILTER
White list
  1  0090f5-3e7a0b  0090f5-bb7a0b  0090f5-bb7a0b  0090f5-bb7a0b       ---
  2  0090f5-bb7a0b  0090cc-3e7a0b  0090cc-3e7a0b  0090cc-3e7a0b       ---
  3  0090cc-3e7a0b       ---            ---            ---            ---
  4  0090f5-3e7fac       ---            ---            ---            ---
  5       ---            ---            ---            ---            ---
  6       ---            ---            ---            ---            ---
  7       ---            ---            ---            ---            ---
  8       ---            ---            ---            ---            ---
  9       ---            ---            ---            ---            ---
 10       ---            ---            ---            ---            ---
--------------------------------------------------------------------------------
```

It is allowed to use interface number or interface name, for example LAN1 as [IF] parameter. System accepts ":" or "-" symbols as MAC address separator. It is possible to enter MAC address without separator at all.

4.6.5.72 <MACLIST [IF] DEL [MAC/N]> Command

The < MACLIST [IF] DEL [MAC/N]> command deletes [MAC] address or entry number [N] from the White List of [IF] interface:

```
CX_05_NET>MACLIST LAN1 DEL 5
-------------------------------------------------------------------------------
New  MAC Filter Configuration
-------------------------------------------------------------------------------
Port     LAN1           LAN2           LAN3           LAN4           LAN5
Mode   ON/FILTER     ON/INDICATE     ON/BLOCK       ON/BLOCK      OFF/FILTER
White list
  1  0090f5-3e7a0b  0090f5-bb7a0b  0090f5-bb7a0b  0090f5-bb7a0b       ---
  2  0090f5-bb7a0b  0090cc-3e7a0b  0090cc-3e7a0b  0090cc-3e7a0b       ---
  3  0090cc-3e7a0b       ---            ---            ---            ---
  4  0090f5-3e7fac       ---            ---            ---            ---
  5       ---            ---            ---            ---            ---
  6       ---            ---            ---            ---            ---
  7       ---            ---            ---            ---            ---
  8       ---            ---            ---            ---            ---
  9       ---            ---            ---            ---            ---
 10       ---            ---            ---            ---            ---
-------------------------------------------------------------------------------
```

It is allowed to use interface number or interface name, for example LAN1 as [IF] parameter. System accepts ":" or "-" symbols as MAC address separator. It is possible to enter MAC address without separator at all.

4.6.5.73 <MACFILTER [LAN1-5] [ON/OFF]> Command

The <MACFILTER [LAN1-5] [ON/OFF]> command enables or disables MAC Filter option on selected LAN interface.

```
CX_05_NET>MACFILTER 4 OFF
-------------------------------------------------------------------------------
New  MAC Filter Configuration
-------------------------------------------------------------------------------
Port     LAN1           LAN2           LAN3           LAN4           LAN5
Mode   ON/FILTER     ON/INDICATE     ON/BLOCK       OFF/BLOCK     OFF/FILTER
White list
  1  0090f5-3e7a0b  0090f5-bb7a0b  0090f5-bb7a0b  0090f5-bb7a0b       ---
  2  0090f5-bb7a0b  0090cc-3e7a0b  0090cc-3e7a0b  0090cc-3e7a0b       ---
  3  0090cc-3e7a0b       ---            ---            ---            ---
  4  0090f5-3e7fac       ---            ---            ---            ---
  5       ---            ---            ---            ---            ---
  6       ---            ---            ---            ---            ---
  7       ---            ---            ---            ---            ---
  8       ---            ---            ---            ---            ---
  9       ---            ---            ---            ---            ---
 10       ---            ---            ---            ---            ---
-------------------------------------------------------------------------------
```

It is allowed to use interface number or interface name, for example LAN1 as [IF] parameter.

4.6.5.74 <MACRULE [LAN1-5] [RULE]> Command

The <MACRULE [LAN1-5] [rule]> command changes MAC Filter [RULE] for selected interface:

```
CX_05_NET>MACRULE 4 INDICATE
-------------------------------------------------------------------------------
New  MAC Filter Configuration
-------------------------------------------------------------------------------
Port     LAN1           LAN2           LAN3           LAN4           LAN5
Mode   ON/FILTER     ON/INDICATE     ON/BLOCK     OFF/INDICATE    OFF/FILTER
White list
  1  0090f5-3e7a0b  0090f5-bb7a0b  0090f5-bb7a0b  0090f5-bb7a0b       ---
  2  0090f5-bb7a0b  0090cc-3e7a0b  0090cc-3e7a0b  0090cc-3e7a0b       ---
  3  0090cc-3e7a0b       ---            ---            ---            ---
  4  0090f5-3e7fac       ---            ---            ---            ---
  5       ---            ---            ---            ---            ---
  6       ---            ---            ---            ---            ---
  7       ---            ---            ---            ---            ---
  8       ---            ---            ---            ---            ---
  9       ---            ---            ---            ---            ---
 10       ---            ---            ---            ---            ---
```

It is allowed to use interface number or interface name, for example LAN1 as [IF] parameter.

MACRULE parameter	
Parameter	Description
FILTER	Default rule. Unlisted MAC will be filtered.
INDICATE	Equal to Filter Rule, but the SNMP message will be generated. Extended Traps must be activated.
BLOCK	If unlisted MAC will arrive the Port will be blocked and the SNMP message will be generated. Type ETHSD 10H/10F/100H/100F/AUTO X to restore port back.

4.6.5.75 <DOT1X [LAN1-5] {OPTION}> Command

The <DOT1X> Command configures IEEE 802.1x access control option on selected LAN interface.

Syntax:

DOT1X [LAN1-5] [ON/OFF] Enables or disables 802.1x option on selected port

DOT1X [LAN1-5] [SHOST/MHOST/MAUTH] Sep 802.1X working mode

DOT1X parameter	
Parameter	Description
SHOST	Default parameter. Only one host (MAC address) can be authenticated on a port. If one host passed authentication, requests from other hosts will be ignored.
MHOST	If one host passed authentication other hosts allowed traffic exchange through the port without authentication.
MAUTH	Multiple hosts can be authenticated on a port. Only authenticated hosts allow traffic exchange through the port.

4.6.5.76 <SETIP X.X.X.X> Command

The <SETIP A.B.C.D> command sets the IP-address of the modem. The parameter A, B, C and D can take values from 0 to 255 (note that neither address of the network nor the address of the node can be equal to 0, or to 255).

4.6.5.77 <NETMASK X.X.X.X> Command

The <NETMASK A.B.C.D> command sets the subnet mask of the modem.

4.6.5.78 <GATEWAY X.X.X.X> Command

The <GATEWAY X.X.X.X> sets the default IP address of the router.

4.6.5.79 <MTU> Command

This command sets the MTU size (Maximum Transmission Unit) for the port INT and is used just for management. Standard MTU size is 1500 Bytes.

4.6.5.80 <WANIDLE [1/7E]> Command

This command sets the idle pattern for a WAN interface. Sometimes, when the unit transmits Ethernet over E1, then an idle pattern of 1 is not convenient because the some E1 equipment will detect a Loss of Signal. In this case, the change of the idle pattern to 7E can help.

4.6.5.81 <ETHSD [10H/10F/100H/100F/AUTO] [N=1..5]> Command

The <ETHSD [10H/10F/100H/100F/AUTO] [N=1..5]> command sets the operating mode of the Ethernet port, where N is the number of the Ethernet port, 10/100 is the rate of 10 or 100 Mbit/s, F is full duplex and H is half duplex.

The <ETHSD AUTO> command activates the rate and duplex auto detection.

```
CO_09_CM>ETHSD 10H 1
CO_09_CM>ETHSD AUTO 2
```

4.6.5.82 <FC [ON/OFF] [N1-4]> Command

This command enables and disables IEEE 802.3x flow control on LAN ports.

4.6.5.83 <IRATE [speed/OFF] [N1-4]> Command

The command IRATE is an abridgement of the Ingress Rate. It limits the incoming data stream that reaches the internal Hardware Ethernet Switch. The IRATE can be set up for every LAN port separately.

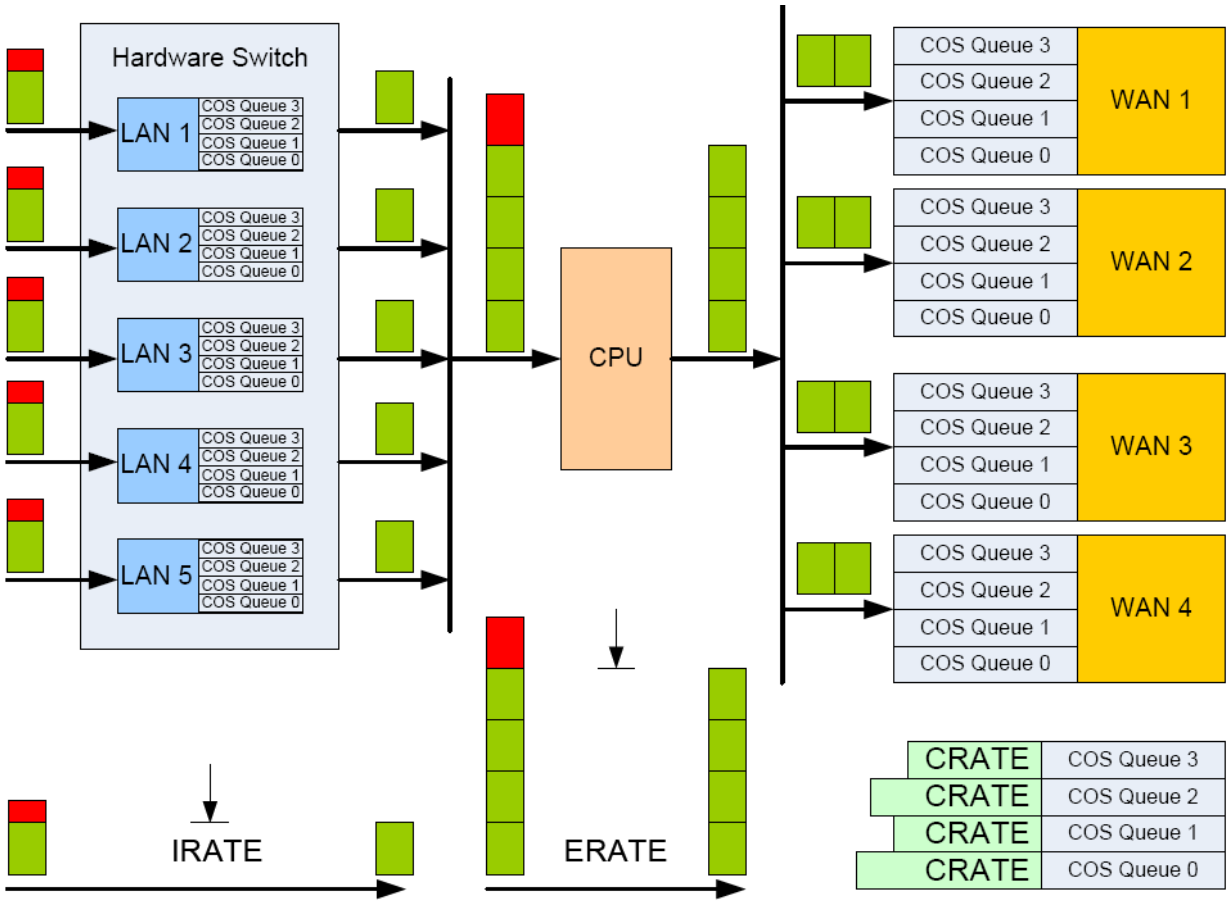
IRATE command counts all arriving traffic without discrimination between ingress VLAN numbers and QoS settings. It means that IRATE command should be used when the LAN port is set to ACCESS mode, so all traffic will be processed by the internal switch with selectable VLAN and QoS settings. If incoming traffic has bigger bandwidth then selected by IRATE command, the excess will be dropped if Flow Control is disabled on the port, or the switch will send so called “MAC Pause Frame” if the Flow Control is enabled.

In general it is possible to use IRATE command if LAN port is set to TRUNK or to MIXED mode. IRATE command will limit the whole incoming bandwidth without taking into account VLAN tags and priorities inside incoming traffic. In that case a network will work without QoS support but with bandwidth control.

- IRATE [rate] [N]: Sets the desired rate limit.
- IRATE OFF [N]: Disable rate limiting.

The parameter [rate] is expressed in Kbits or Mbits, for example:

IRATE 128K 1	- will set 128 kbps limit on LAN1
IRATE 256 2	- will set 256 kbps limit on LAN2
IRATE 1M 3	- will set 1000 kbps limit on LAN3



4.6.5.84 <ERATE [speed/OFF]> Command

The command ERATE is an abridgement of Egress Rate. It limits the traffic heading to CPU of the device.

ERATE command counts all traffic, but unlike IRATE command the QoS settings make sense for traffic drop. In case if traffic has bigger bandwidth then the ERATE settings the device will drop traffic starting from packets with low priority tag.

Network administrator can configure QoS with IRATE and ERATE commands if LAN ports of the device works in ACCESS mode. He has to be sure that those LAN ports of the device have different default QoS or VLAN settings.

- ERATE [rate]: Sets the desired rate limit.
- ERATE OFF: Disable rate limiting.

The parameter [rate] is expressed in Kbits or Mbits, for example:
128K means 128 kbps
256 means 256 kbps
1M means 1000kbps
30M means 30000kbps

4.6.5.85 <CRATE [speed] [CoS] [WAN]> Command

The command CRATE is an abridgement of CoS Rate. It limits the egress bandwidth of selected CoS queue for specified WAN interface. Starting from the 1.3.0 firmware BlackBox Etherlink_IV and MaxiMiniLink devices have 4 CoS queues with numbers from 0 to 3. The queue with “0” number has the lowest priority while the queue with “3” number has highest priority. Command CRATE is not

intended to define QoS [0…7] to CoS; or VLAN ID to CoS mapping. On the contrary, it is designed for assigning bandwidth each CoS queue can occupy.

Only CRATE command can be used if incoming traffic has VLANs, IRATE command is useless because the hardware Ethernet switch can’t check the QoS filed on its entry point. CRATE can be used too if the traffic is not intended for LAN interface, for example repeater applications or interface converter mode when traffic is transmitted between two or several WAN interfaces.

If the sum of all CRATE settings and their load is bigger than the working bandwidth of WAN or MWAN interfaces, queues with high priority will be served firstly, while other queues will be hold in buffer and will wait for an opportunity to be transmitted.

- CRATE [rate] [CoS:0..3] [WAN:1..4]: Sets the desired rate limit.
- CRATE OFF [CoS:0..3] [WAN:1..4]: Disable rate limiting.

Examples: CRATE 128 2 1 – Sets rate limit to 128kbps for CoS2 on WAN1.

The parameter [rate] is expressed in Kbits or Mbits, for example:

128K means 128 kbps
256 means 256 kbps
1M means 1000kbps
30M means 30000kbps

4.6.5.86 <COS [QOS/VLAN] [N] [0..3/OFF]> Command

This command sets the VLAN to CoS and QoS to CoS mapping.

COS [VLAN/QOS] [V=1..8/Q=0..7] [CoS=0..3/OFF]
VLAN: Change VLAN-to-CoS mapping
QOS: Change QoS-to-CoS mapping
V: VLAN number (1..8) according to NETCONFIG table
Q: IEEE 802.1p QoS (0..7)
CoS: Resulting CoS (0..3)
OFF: Turns off VLAN-to-CoS mapping for selected VLAN.
Examples: COS VLAN 1 3 - All frames in VLAN 1 will have CoS 3.

4.6.5.87 <SNMPACL> Command

This command is used to create SNMP ACL. If enabled, the SNMP SET and Poll messages will be accepted only from IP addresses inside this list.

SNMPACL [1/2] x.x.x.x - set 1st or 2nd IP address in x.x.x.x format.
SNMPACL [1/2] OFF - remove 1st or 2nd IP address.

4.6.5.88 <SNMP [V1|V2C|V3] [ON|OFF]> Command

This command activates or deactivates various SNMP versions.
<SNMP V3 ON>. This command enables SNMP v3.
<SNMP V1 OFF>. This command disables SNMP v1.

4.6.5.89 <TRAPIP [ADD/DEL] X.X.X.X> Command

This command lets you specify IP addresses to send SNMP traps to.
The <TRAPIP ADD X.X.X.X> command adds the IP-address X.X.X.X to the SNMP-trap list.
The <TRAPIP DEL X.X.X.X> command deletes the IP-address X.X.X.X from the SNMP trap list.
The list should not contain more than two IP addresses.

4.6.5.90 <TRAP [1/2] [V1/V2C]> Command

This command defines SNMP version of Trap messages for 1-s or 2-nd Trap receiver.
<TRAP 1 V1>. This command set SNMP version to v1 for 1-st Trap receiver.
<TRAP 2 V2C>. This command set SNMP version to V2c for 2-nd Trap receiver.

4.6.5.91 <TRAP [1/2] V3 [RO/RW]> Command

This command activates SNMP v3 for 1-st or 2-nd Trap receiver and assign the SNMP user (RO or RW) from whom the Trap messages will be send.
<TRAP 1 V3 RO>. This command assign RO SNMP user as "author" of Trap messages headed to 1-st Trap receiver.
<TRAP 2 V3 RW>. This command assign RW SNMP user as "author" of Trap messages headed to 2-nd Trap receiver.

4.6.5.92 <COMMUNITY> Command

With this command you can specify the SNMP community name to authenticate incoming and outgoing SNMP traps. After entering the command, you will be asked to enter the community name. Please note, that the SNMP community name is case sensitive.

4.6.5.93 <SNMPSET [ON/OFF]> Command

The <SNMPSET ON> command enables processing SNMP SET requests, which allow to configure and manage the device, however, this command makes the device sensitive to attacks over SNMP in unprotected PC networks.
The <SNMPSET OFF> command disables processing SNMP SET requests, what protects the device from network attacks, but does not allow to configure and manage it.
Use this command to process SNMP SET requests only in protected networks. If the network is not protected, use this command during configuration and administration only.

4.6.5.94 <SNMP [RO|RW] NAME> Command

This command set SNMPv3 user name for user with Read-Only (RO) or Read-Write (RW) access rights.
<SNMP RO NAME>. This command set SNMP user with Read-Only access rights.
<SNMP RW NAME>. This command set SNMP user with Read-Write access rights.

4.6.5.95 <SNMP [RO|RW] AUTH [MODE]> Command

This command set SNMPv3 user authentication type for RO or RW user. The following authentication types are supported: MD5,SHA,NONE.

<SNMP RO AUTH SHA>. This command set SHA authentication type for SNMP user with Read-Only access rights.

<SNMP RW AUTH MD5>. This command set MD5 authentication type for SNMP user with Read- Write access rights.

<SNMP RO AUTH NONE>. This command disables authentication for SNMP user with Read-Only access rights.

4.6.5.96 <SNMP [RO|RW] PRIV [MODE]> Command

This command set SNMPv3 user encryption type for RO or RW user. The following encryption types are supported: DES,AES,NONE.

<SNMP RO PRIV DES>. This command set DES encryption type for SNMP user with Read-Only access rights.

<SNMP RW PRIV AES>. This command set AES encryption type for SNMP user with Read-Write access rights.

<SNMP RO PRIV NONE>. This command disables encryption for SNMP user with Read-Only access rights.

4.6.5.97 <SYSLOG [1/2] [IP/OFF]> Command

There is a build-in system Log (SYSLOG) client according to Syslog protocol (RFC-3164). It sends every message in a single UDP packet to the Syslog server. Message includes:

- Alarm status
- User login
- User actions

It is possible to add up to 2 Syslog severs. The SYSLOG command is used for that purpose.
SYSLOG [1/2] x.x.x.x - set 1st or 2nd IP address in x.x.x.x format.

SYSLOG [1/2] OFF - remove 1st or 2nd IP address.

4.6.5.98 <LLDP [ON/OFF]> Command

The <LLDP [ON/OFF]> command enables or disables LLDP messages exchange with all peers through all interfaces. It is global setting.

```
CX_06_NET>LLDP ON
-------------------------------------------------------------------------------
LLDP                                    : Enabled
-------------------------------------------------------------------------------
Retransmission Interval                 : 30
Transmission Multiplier                 : 4
Reinitialize Delay                      : 2
Transmission Delay                      : 2
Notification Interval                   : 5
MED Fast Start Counter                  : 3
LLDPU Transmission                      : Enabled
LLDPU Reception                         : Enabled
LLDP INT VLAN                           : Disabled
-------------------------------------------------------------------------------
CX_06_NET>
```

4.6.5.99 <LLDP DEFAULT> Command

The <LLDP DEFAULT> command restores factory LLDP parameters.

Parameter	Value
Retransmission Interval	30 seconds
Transmission Multiplier	4
Reinitialize Delay	2 seconds
Transmission Delay	2 seconds
Notification Interval	5 seconds
MED Fast Start Counter	3
LLDPU Transmission	Enabled
LLDPU Reception	Enabled
LLDP internal VLAN	Enabled

4.6.5.100 <LLDP [PARAM] [VALUE]> Command

This command allows [VALUE] setup for selected LLDP parameter [PARAM]

Parameter	Value	Description
TXINT	5..32768	Sets Retransmission Interval in seconds
TXMULT	2..10	Sets Transmission Multiplier
REDEL	1..10	Sets Reinitialize Delay in seconds
TXDEL	1..8192	Sets Transmission Delay in seconds
NOTINT	6..3600	Sets Notification Interval in seconds
MFS	1..10	Sets MED Fast Start Counter

All LLDP configuration parameters are related with SNMP MIB. They can be set either from CLI or WEB or via SNMP.

Retransmission Interval: The interval at which LLDP frames are transmitted on behalf of this LLDP agent.

Transmission Multiplier: The actual time-to-live value used in LLDP frames, transmitted on behalf of this LLDP agent, can be expressed by the following formula: TTL = min(65535, (Retransmission_Interval * Transmission_Multiplier)). For example, if the value of Retransmission_Interval is "30", and the value of Transmission_Multiplier is "4", then the value "120" is encoded in the TTL field in the LLDP header.

The TTL value inside LLDP packet indicates time this packet should be stored and processed by remote system. It will be forgotten after TTL count-back timer will be equal to "0".

Reinitialize Delay: The Reinitialize_Delay indicates the delay in seconds from when LLDP-MIB|lldpPortConfigAdminStatus (1.0.8802.1.1.2.1.1.6.1.2) object of a particular port becomes "disabled" until re-initialization will be attempted.

Transmission Delay: The Transmission Delay indicates the delay in seconds between successive LLDP frame transmissions initiated by value/status changes in the local LLDP subsystem. The recommended Transmission Delay value is represented by the following formula: 1 <= Transmission_Delay <= (0.25 * Retransmission_Interval).

Notification Interval: This parameter indicates how often the lldpRemTableChange notification events should be sent**.**

MED Fast Start Counter: Sets the number of successive LLDP transmissions for one complete "Fast Start" interval. The LDP-MED Fast Start Protocol Behaviour used to advertise only few capabilities of the device designed for as fast as possible call processing after device start-up.

4.6.5.101 <LLDP [RX/TX] [ON/OFF]> Command

The <LLDP [RX/TX] [ON/OFF]> command enables or disables LLDP messages transmission and reception.

4.6.5.102 <LLDP INT VLAN [ON/OFF]> Command

The <LLDP INT VLAN [ON/OFF]> command enables or disables LLDP messages exchange in management VLAN only. This feature is disabled by default, so all interfaces (LAN and WAN) participate into the LLDP table construction. It means that, in case if two units are connected through the service-provider equipment, the border service provider switches or routers participate in LLDP network construction. For example, the service-provider switch will "see" the customer modem and the modem will "see" the service-provider switch. Despite the fact that such behaviour fulfils the standard, it may conflict with some network construction principles like security. Moreover the customer will not see own remote equipment as it is not connected directly, on the contrary through the service-provider cloud.

The <LLDP INT VLAN ON> command changes standard behaviour. If enabled, the LLDP messages will be transmitted only in the VLAN, the management port INT is connected too. It makes possible for the customer to "see" remote location as it is connected directly, but not through the service-provider network.

4.6.5.103 <LLDP CONFIG> Command

The <LLDP CONFIG> command shows actual LLDP configuration.

```
CX_06_NET>LLDP CONFIG
-------------------------------------------------------------------------------
LLDP                                  : Enabled
-------------------------------------------------------------------------------
Retransmission Interval               : 30
Transmission Multiplier               : 4
Reinitialize Delay                    : 2
Transmission Delay                    : 2
Notification Interval                 : 5
MED Fast Start Counter                : 3
LLDPU Transmission                    : Enabled
LLDPU Reception                       : Enabled
LLDP INT VLAN                         : Disabled
-------------------------------------------------------------------------------
CX_06_NET>
```

4.6.5.104 <SNTP [1/2] [IP/OFF]> Command

The Syslog protocol should carry the real time stamp in every message. For this reason the SNTP protocol (RFC-2030) has been implemented. The SNTP protocol uses a part of NTP protocol features and it is compatible with SNTP or NTP servers. As soon as SNTP servers were added, the SNTP client tries to connect with the server every 10 seconds. After successful connection, the polling interval will become 1024 seconds

It is possible to add up to 2 SNTP servers. The SNTP command is used for that purpose.

SNTP [1/2] x.x.x.x - set 1st or 2nd IP address in x.x.x.x format.

SNTP [1/2] OFF - remove 1st or 2nd IP address

4.6.5.105 <SNTP TZ [+/-]HH:MM> Command

The SNTP servers provide UTC time. To change time zone use SNTP TZ command. Note that SNTP protocol doesn't check the summer/winter time offset.

SNTP TZ +4:00 - Set Moscow time

SNTP TZ +1:00 - Set CET (Central European time) SNTP TZ -8:00 - Set PST (Pacific Standard time)

4.6.5.106 <DST> Command

This command configures Daylight Saving Time (DST) adjustable rules.

<DST [OFF/INFO/NAME]> Command

Parameter	Description
OFF	Disables Daylight Saving Time
INFO	List pre-defined time change rules
NAME	Select pre-defined time change rules

Pre-defined time change rules are:

Name	Rules	Description
Canada	MAR SUN>=8 (9) 02:00w +60min NOV firstSUN (2) 02:00w +0min	
Brazil	OCT SUN>=15 (19) 00:00w +60min FEB SUN>=15 (16) 00:00w +0min	
WS	SEP lastSUN (28) 03:00w +60min APR firstSUN (6) 04:00w +0min	Western Samoa
Syria	MAR lastFRI (28) 00:00w +60min OCT lastFRI (31) 00:00w +0min	
Palestine	MAR lastTHU (27) 24:00w +60min SEP FRI>=21 (26) 00:00w +0min	
Azer	MAR lastSUN (30) 04:00w +60min OCT lastSUN (26) 05:00w +0min	Azerbaijan
C-Eur	MAR lastSUN (30) 02:00s +60min OCT lastSUN (26) 02:00s +0min	Central Europe
ChileAQ	SEP SUN>=2 (7) 04:00u +60min APR SUN>=23 (27) 03:00u +0min	Chile Antarctic
Iran	MAR 22 00:00w +60min SEP 22 00:00w +0min	
Paraguay	OCT firstSUN (5) 00:00w +60min MAR SUN>=22 (23) 00:00w +0min	
Cuba	MAR SUN>=8 (9) 00:00s +60min NOV firstSUN (2) 00:00s +0min	
E-Eurasia	MAR lastSUN (30) 00:00w +60min OCT lastSUN (26) 00:00w +0min	Eastern EurAsia
LH	OCT firstSUN (5) 02:00w +30min APR firstSUN (6) 02:00w +0min	Lord Howe Island
W-Eur	MAR lastSUN (30) 01:00s +60min OCT lastSUN (26) 01:00s +0min	Western Europe
NZ	SEP lastSUN (28) 02:00s +60min APR firstSUN (6) 02:00s +0min	New Zeland
Jordan	MAR lastTHU (27) 24:00w +60min OCT lastFRI (31) 00:00s +0min	
Chile	SEP SUN>=2 (7) 04:00u +60min APR SUN>=23 (27) 03:00u +0min	
Haiti	MAR SUN>=8 (9) 02:00w +60min NOV firstSUN (2) 02:00w +0min	
Chatham	SEP lastSUN (28) 02:45s +60min APR firstSUN (6) 02:45s +0min	
TC	MAR SUN>=8 (9) 02:00w +60min NOV firstSUN (2) 02:00w +0min	Turks and Caicos
Thule	MAR SUN>=8 (9) 02:00w +60min NOV firstSUN (2) 02:00w +0min	
Name	**Rules**	**Description**
RussiaAsia	MAR lastSUN (30) 02:00s +60min OCT lastSUN (26) 02:00s +0min	
AN	OCT firstSUN (5) 02:00s +60min APR firstSUN (6) 02:00s +0min	New South Wales
Morocco	MAR lastSUN (30) 02:00w +60min OCT lastSUN (26) 03:00w +0min	
AS	OCT firstSUN (5) 02:00s +60min APR firstSUN (6) 02:00s +0min	South Australia
Namibia	SEP firstSUN (7) 02:00w +60min APR firstSUN (6) 02:00w +0min	
AT	OCT firstSUN (5) 02:00s +60min APR firstSUN (6) 02:00s +0min	Tasmania
AV	OCT firstSUN (5) 02:00s +60min	State Victoria

	APR firstSUN (6) 02:00s +0min	
EU	MAR lastSUN (30) 01:00u +60min OCT lastSUN (26) 01:00u +0min	European Union
Zion	MAR FRI>=23 (28) 02:00w +60min OCT lastSUN (26) 02:00w +0min	
E-Eur	MAR lastSUN (30) 00:00w +60min OCT lastSUN (26) 00:00w +0min	Eastern Europe
NZAQ	SEP lastSUN (28) 02:00s +60min APR firstSUN (6) 02:00s +0min	New Zeland Antarctic
Mexico	APR firstSUN (6) 02:00w +60min OCT lastSUN (26) 02:00w +0min	
Uruguay	OCT firstSUN (5) 02:00w +60min MAR SUN>=8 (9) 02:00w +0min	
US	MAR SUN>=8 (9) 02:00w +60min NOV firstSUN (2) 02:00w +0min	United States
Fiji	OCT SUN>=21 (26) 02:00w +60min JAN SUN>=18 (19) 03:00w +0min	
EUAsia	MAR lastSUN (30) 01:00u +60min OCT lastSUN (26) 01:00u +0min	Nicosia

<DST [WINTER/SUMMER]> Command allows manually definition for winter and summer daylight saving time change. The following parameters must be entered in the dialog:

Parameter	Description
MONTH	JAN FEB MAR APR MAY JUN JUL AUG SEP OCT NOV DEC
DAY	Day when you change time. NN Particular month day number like 5 or 30 firstDDD First week day in the month with name DDD. DDD is three-letter abbreviation of day name: MON TUE WED THU FRI SAT SUN lastDDD Last week day in the month with name DDD. DDD>=NN A week day DDD when month day number is >= than NN.
TIME	A moment to adjust clock. Has format HH:MM[W|S|U] HH Hour MM Minutes [W|S|U] Defines Type of specified time (W if omitted) W Time change happens according your wall clock, taking in account time zone offset and current season time. S Time change happens according with Standard time, taking in account only time zone offset. U UTC time. Time change happens when UTC clock shows specified time.
OFFSET	Amount of time we add to Standard zone time when switch to specified season time. Format is either HH:MM or MM. Typical values are: 0 Local time will be UTC time + TZ offset(selected with SNTP TZ command) + 0 This is so called Standard time. 1:00 Local time will be UTC time + TZ offset + 01:00 60 Same as above (60 minutes == 01:00) In the summer time it is usually 60 and in the winter it's 0 min.

Example:

```
CO_06_NET>DST    SUMMER
Month [MAR] : MAY
```

```
Day [lastSUN] : FIRSTMON
Time to advance the clock [00:00] : 02:00
Offset (relative to Standard zone time) [60 min] : 1:00
```

4.6.5.107 <[SSH|TELNET|HTTP] [ON/OFF]>

Command allows enabling or disabling of defined service.

```
CO_04_NET> SSH ON
--------------------------------------------------------------------------------
Running Network Configuration

<----------------------------------- cut ----------------------------------->

Service settings  :
  Running/Port     : TELNET, SSH(22), HTTP
  Syslog servers   : 255.255.255.255   255.255.255.255
  SNTP   servers   : 255.255.255.255   255.255.255.255
  RADIUS servers   : 255.255.255.255:1812      255.255.255.255:1812
  RADIUS secret    : entered                   entered
--------------------------------------------------------------------------------
CO_04_NET> TELNET OFF
--------------------------------------------------------------------------------
Running Network Configuration

<----------------------------------- cut ----------------------------------->

Service settings  :
  Running/Port     : SSH(22), HTTP
  Syslog servers   : 255.255.255.255   255.255.255.255
  SNTP   servers   : 255.255.255.255   255.255.255.255
  RADIUS servers   : 255.255.255.255:1812      255.255.255.255:1812
  RADIUS secret    : entered                   entered
--------------------------------------------------------------------------------
CO_04_NET>
```

Note: Default running management servers are TELNET and HTTP

4.6.5.108 <SSH PORT [N]>

Command changes port, the SSH server listens for incoming connections.

```
CO_04_NET> SSH PORT 2022
--------------------------------------------------------------------------------
Running Network Configuration

<----------------------------------- cut ----------------------------------->

Service settings  :
  Running/Port     : TELNET, SSH(2022), HTTP
  Syslog servers   : 255.255.255.255   255.255.255.255
  SNTP   servers   : 255.255.255.255   255.255.255.255
  RADIUS servers   : 255.255.255.255:1812      255.255.255.255:1812
  RADIUS secret    : entered                   entered
--------------------------------------------------------------------------------
CO_04_NET>
```

4.6.5.109 <RADIUS [1/2] SECRET>

Command defines common sharing secret for RADIUS server and client

```
CO_04_NET> RADIUS 1 SECRET
Enter     shared    secret:
Repeat shared secret:
--------------------------------------------------------------------------------
Running Network Configuration

<----------------------------------- cut ----------------------------------->
```

```
Service settings  :
  Running/Port     : TELNET, SSH(22), HTTP
   Syslog servers  : 255.255.255.255         255.255.255.255
  SNTP   servers   : 255.255.255.255         255.255.255.255
  RADIUS servers   : 192.168.1.1:1812        255.255.255.255:1812
  RADIUS secret    : entered
-------------------------------------------------------------------------------
CO_04_NET>
```

4.6.5.110 <RADIUS [1/2] TEST>

The command test connection with defined RADIUS server and returns access rights or Non-authorised for selected user.

```
CO_FMM>RADIUS   1   TEST
Login: ETHERLINK_IVUSER
Password:
Authorised;    CONTROL+TEST+STATUS+CONFIG
CO_FMM>
```

4.6.5.111 <RADIUS [1/2] [IP:P/OFF]>

Command adds or removes the IP address of primary or secondary RADIUS server. It is possible to specify port, the client will try to connect to. If port is not defined the default UDP port 1812 will be used.

```
CO_04_NET> RADIUS 1 192.168.1.1
-------------------------------------------------------------------------------
Running Network Configuration

<---------------------------------- cut ---------------------------------->

Service settings  :
  Running/Port     : TELNET, SSH(2022), HTTP
  Syslog servers   : 255.255.255.255   255.255.255.255
  SNTP   servers   : 255.255.255.255   255.255.255.255
  RADIUS servers   : 192.168.1.1:1812         255.255.255.255:1812
  RADIUS secret    : entered                   entered
-------------------------------------------------------------------------------
CO_04_NET>RADIUS 2 192.168.2.253:21812
-------------------------------------------------------------------------------
Running Network Configuration

<---------------------------------- cut ---------------------------------->

Service settings  :
  Running/Port     : TELNET, SSH(2022), HTTP
  Syslog servers   : 255.255.255.255   255.255.255.255
  SNTP   servers   : 255.255.255.255   255.255.255.255
  RADIUS servers   : 192.168.1.1:1812        192.168.1.2:21812
  RADIUS secret    : entered                   entered
-------------------------------------------------------------------------------
CO_04_NET>
```

4.6.5.112 <RADIUS RETRIES [0..10]>

Command defines the number of retries, the RADIUS client will try to authenticate at first and second RADIUS server. If the first RADIUS server fail to give a reply within a defined timeout, the client sends request to the second RADIUS server. The requests keep going until the number exceeds the number of retries, then the client will use local record for authentication. Default parameter is 2 retries.

```
CO_FMM>RADIUS RETRIES 5
```

```
-------------------------------------------------------------------------------
Status                :       Server 1             Server 2
-------------------------------------------------------------------------------
Status                :       Connected            Not connected
Server IP             :       255.255.255.255      255.255.255.255
Server port           :       1812                 1812
Shared key            :       entered              empty
Retries               : 5

Timeout, seconds      : 2
-------------------------------------------------------------------------------
CO_FMM>
```

4.6.5.113 <RADIUS TIMEOUT [1..5]>

Command defines the timeout is seconds. If RADIUS server gives no answer within defined period, the RADIUS client initialises next attempt. Default parameter is 2 seconds.

```
CO_FMM>RADIUS TIMEOUT 3
-------------------------------------------------------------------------------
Status                :       Server 1             Server 2
-------------------------------------------------------------------------------
Status                :       Connected            Not connected
Server IP             :       255.255.255.255      255.255.255.255
Server port           :       1812                 1812
Shared key            :       entered              empty
Retries               : 5
Timeout, seconds      : 3
-------------------------------------------------------------------------------
CO_FMM>
```

4.6.5.114 <STATUS RADIUS [N/R/S/B]> Command

This command Show 1-st and 2-nd RADIUS server status and parameters.

```
CO_06_FMM>STATUS RADIUS
-------------------------------------------------------------------------------
Status              :     Server 1             Server 2
-------------------------------------------------------------------------------
Status              :     Not connected        Connected
Server IP           :     192.168.1.252        192.168.1.254
Server port         :     1812                 1812
Server key          :     entered              entered
Retries             : 2
Timeout, seconds    : 2
-------------------------------------------------------------------------------
CO_06_FMM>
```

Parameter	Description
Status	Status of 1-st and 2-nd RADIUS Server
Server IP	IP address of 1-st and 2-nd RADIUS Server
Server port	Port, a server is listening on
Server key	Shows if shared secret has been entered or not

The <STATUS RADIUS [N/R/S/B]> command displays one of four RADIUS Server Status: New, Running, Startup, or Backup, depending on the parameter.

4.6.5.115 <NETDEFAULT> Command

The <NETDEFAULT> command sets the following configuration The MAC address of the modems takes the manufacturer value. The default IP address, sub-network masks and gateway are not changed.

```
CP_01_NET>NETCONFIG
-------------------------------------------------------------------------------
Running Network Configuration
```

```
--------------------------------------------------------------------------------
Ethernet settings : LAN1  LAN2  LAN3  LAN4  LAN5  WAN1  WAN2  WAN3  WAN4   INT
  Access/Trunk    :  ACC   ACC   ACC   ACC   ACC  Trunk Trunk Trunk Trunk  ACC
  Port-based VLAN :  [A]   [A]   [A]   [A]   [A]   [A]   [A]   [A]   [A]   [A]
  VLAN            :   1     1     1     1     1                              1
  QoS             :   2     2     2     2     2                              2
  VLAN1 VID=1     :                                 +     +     +     +
  VLAN2 VID=2     :                                 +     +     +     +
  VLAN3 VID=3     :                                 +     +     +     +
  VLAN4 VID=4     :                                 +     +     +     +
  VLAN5 VID=5     :                                 +     +     +     +
  VLAN6 VID=6     :                                 +     +     +     +
  VLAN7 VID=7     :                                 +     +     +     +
  VLAN8 VID=8     :                                 +     +     +     +
  OTHER VLANS     :                                 +     +     +     +
  Speed           : AUTO  AUTO  AUTO  AUTO  AUTO
System settings   :
  MAC address     :  00:0f:d9:00:00:00
  IP address      :  192.168.0.254
  Subnet mask     :  255.255.255.0
  Default gateway :  192.168.0.254
--------------------------------------------------------------------------------
CP_01_NET>
```

5 SOFTWARE DOWNLOAD

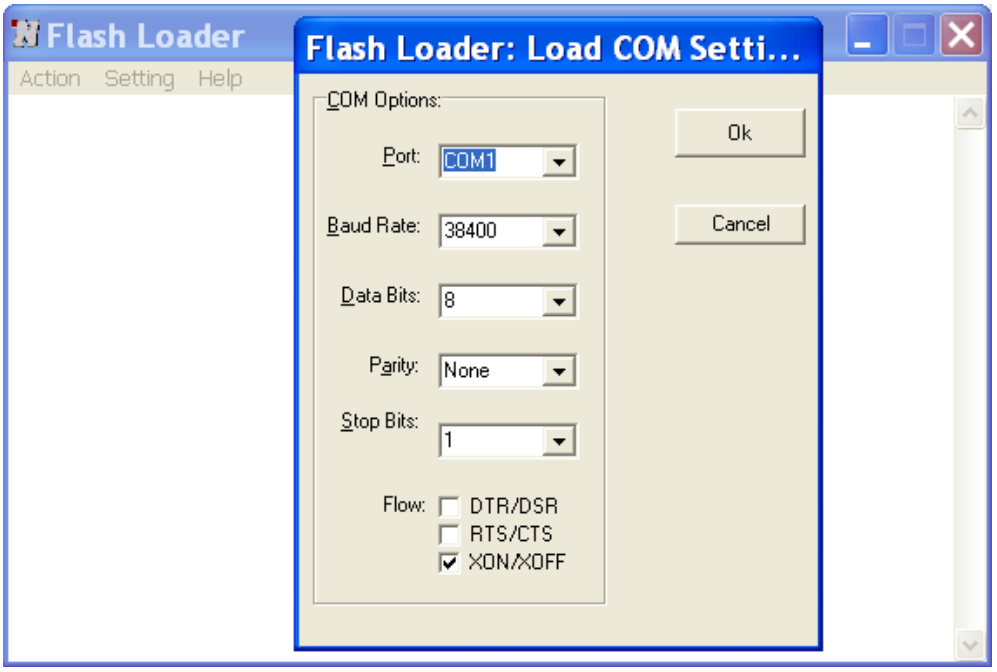
Etherlink IV devices support downloading new/old software versions to get some additional features or to protect the devices with a released only software version. The download of the software can be performed in following ways:

- via the RS-232 port (LCT) by using the “Flash Loader” program
- via the RS-232 port (LCT) by using the X-modem protocol
- via Ethernet (the X-modem protocol)

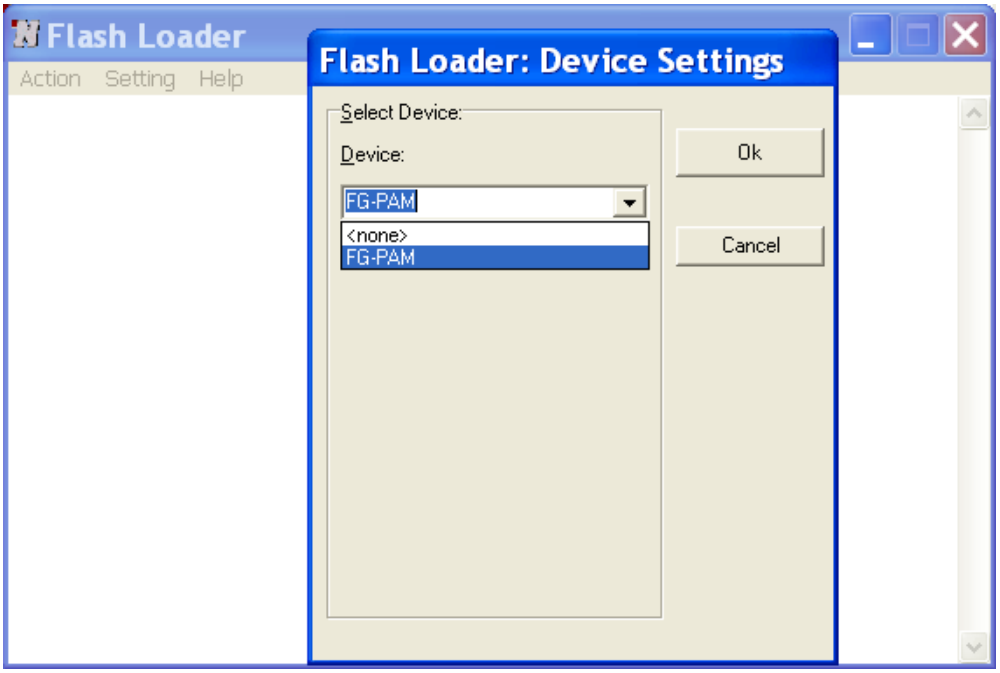
5.1 Software Download via RS-232 Port (LCT) Using the Flash Loader Program

To download the software on any Etherlink IV device, do the following steps:

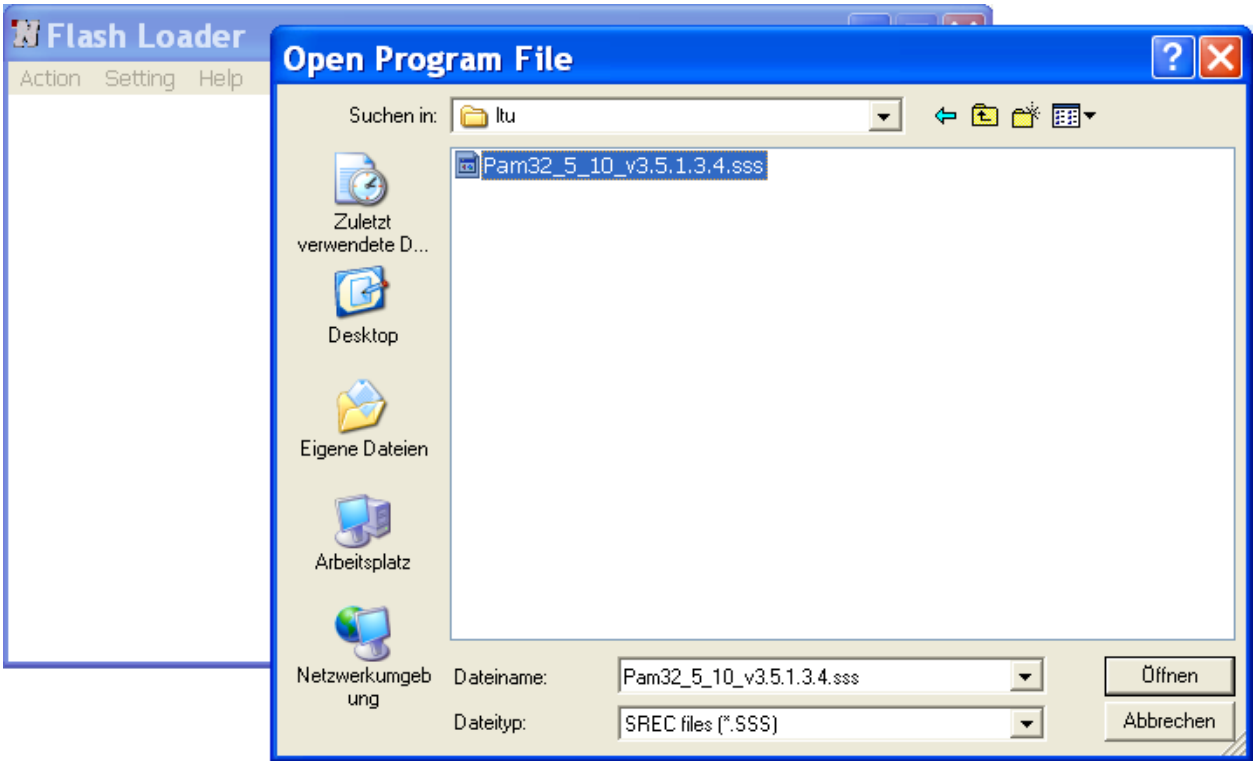
1. Power off the device. You may extract the unit a little from the subrack, minirack or SA-DESKTOP-x housing.
2. Connect the RS-232 connector of the device (Monitor, LCT) with the Com port (RS-232) of the Personal Computer.
3. Start the program “flashloader.exe” on your Personal Computer (Double-click on the icon). You can download the software on the following link: http://www.BlackBox.ch/extranetfiles/Software/FlashLoader_V12.zip
4. Select “Set Loader Communication” in the “Setting” menu and perform the settings as shown in the Figure below and click “Ok”.



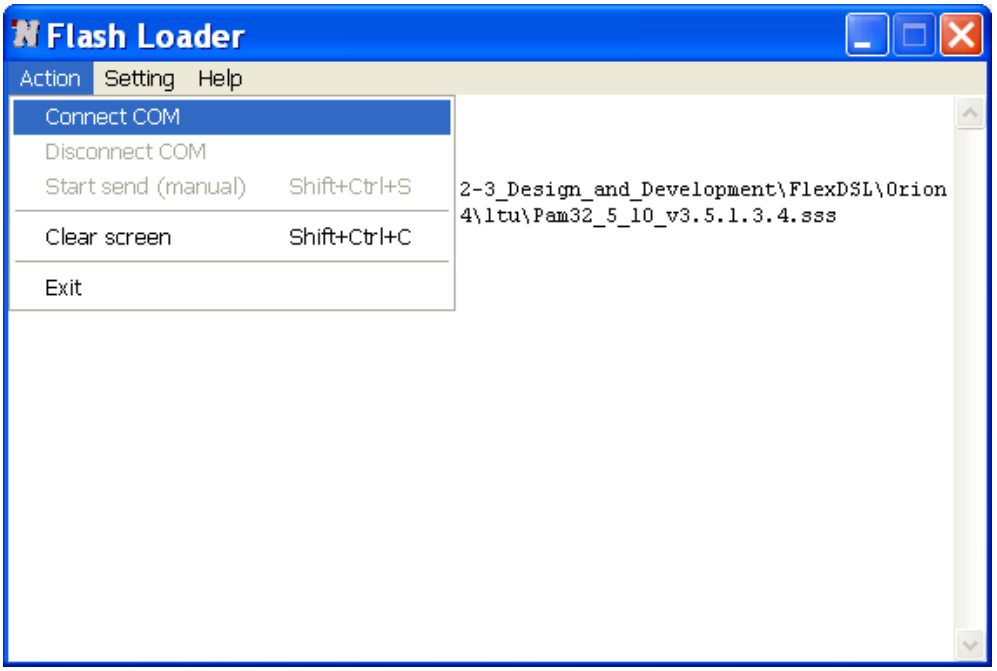
5. Select “Select Device” in the “Setting” menu, then select “SA-RC” and click “Ok”.



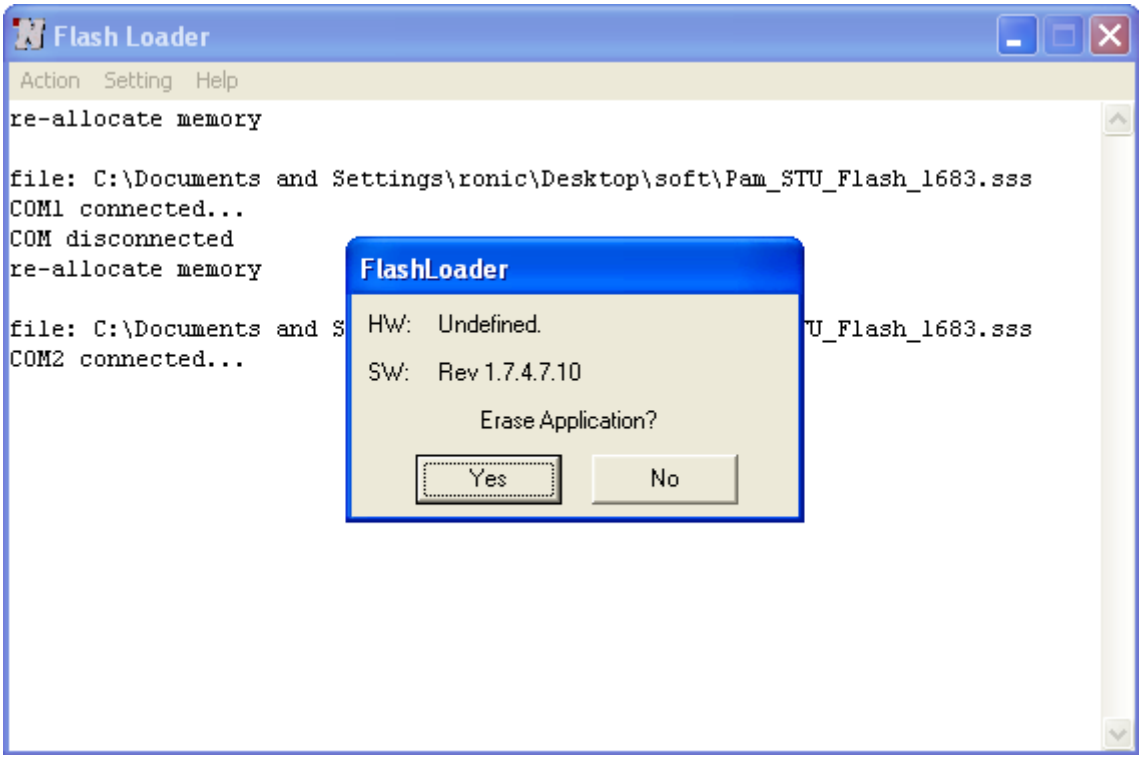
6. Select the “xxx.SSS” file and click “Open”.



7. Select “Connect COM” in the “Action” menu.

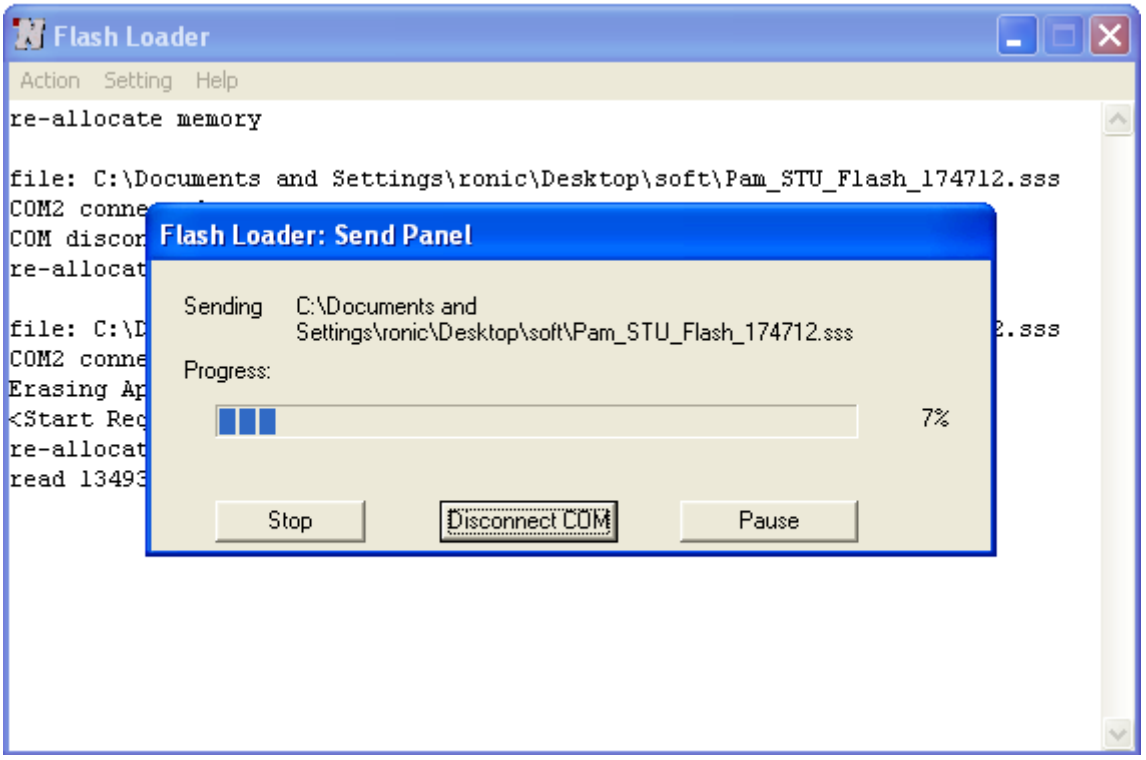


8. Power on the device (activate). You may insert the unit to the subrack, minirack or SA-DESKTOP-x housing.

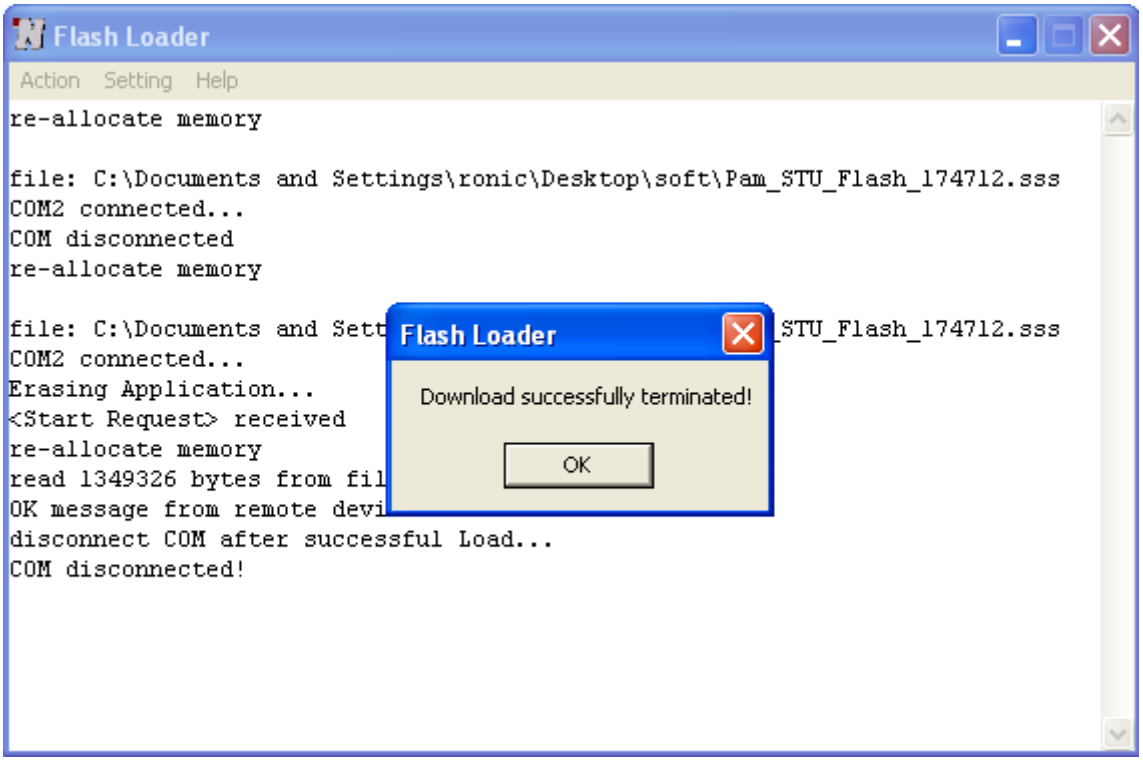


9. Click “Yes” in the “Flashloader” window.

10. The loading progress will be displayed in the window “Flash Loader: Send Panel”.



11. If the downloading was successful, the following window will be displayed.

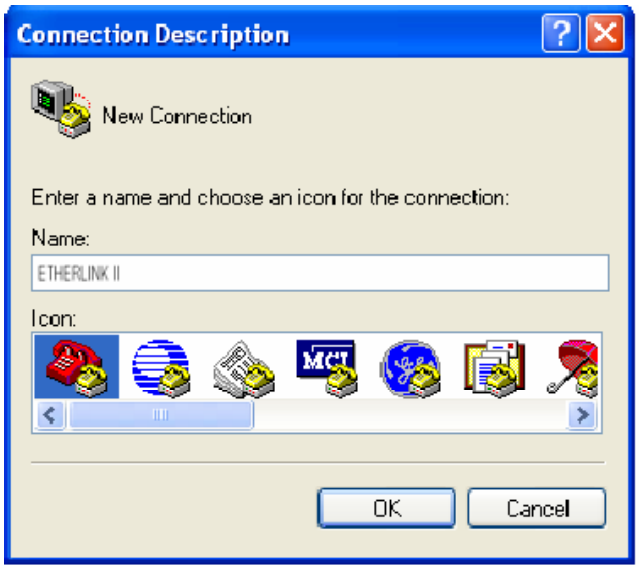


12. Click “Ok”.
13. Select “Disconnect COM” in the “Action” menu.
14. Power off the device being loaded and disconnect it from the Personal Computer.
15. Follow steps 1, 2, 7 – 15 to download the software into other devices.

5.2 Software Download via RS-232 COM Port (LCT) Using Xmodem Protocol

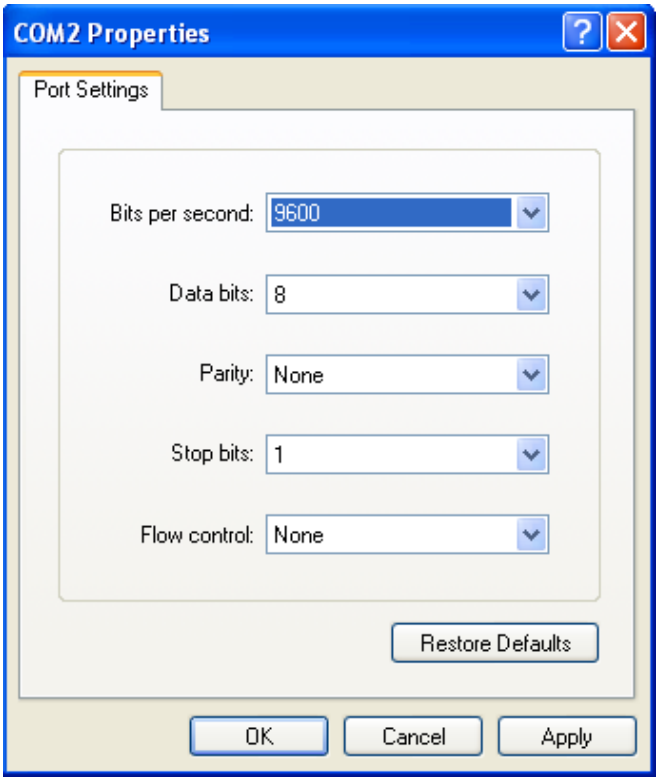
To download the software on any Etherlink IV device, do the following steps:

1. Power on the device.
2. Connect the RS-232 connector of the device (Monitor, LCT) with the Com port (RS-232) of the Personal Computer.
3. Run the Hyper Terminal program (hypertrm.exe).
4. Create a new connection in the “Connection Description” window. Input the name of the connection in the “Name” field. Click “Ok”.

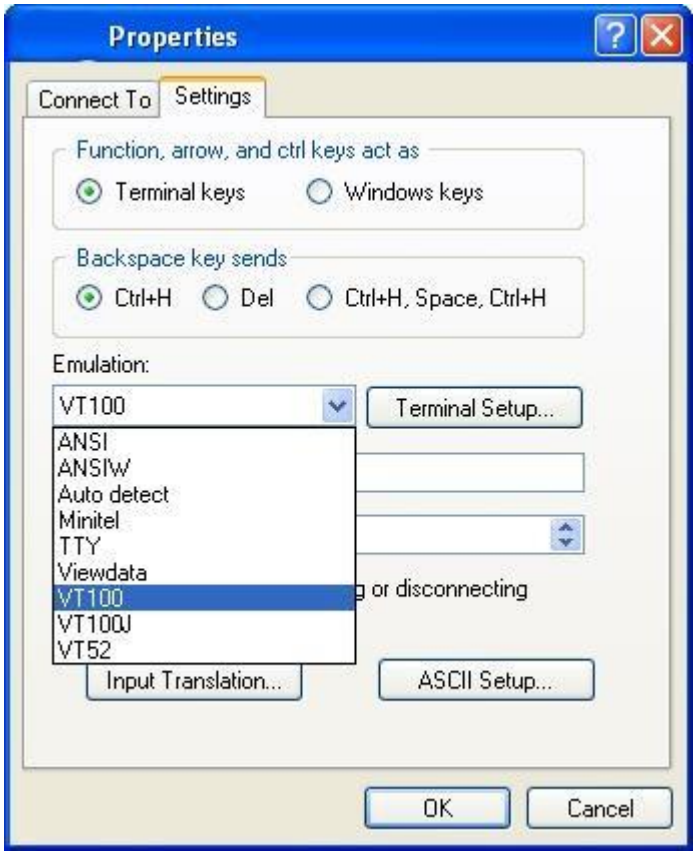


5. Then the “Connect To” window is displayed. Select the COM port connected to the subrack, minirack or SA-DESKTOP-x in the “Connect Using” drop-down menu. Click “Ok”.
6.

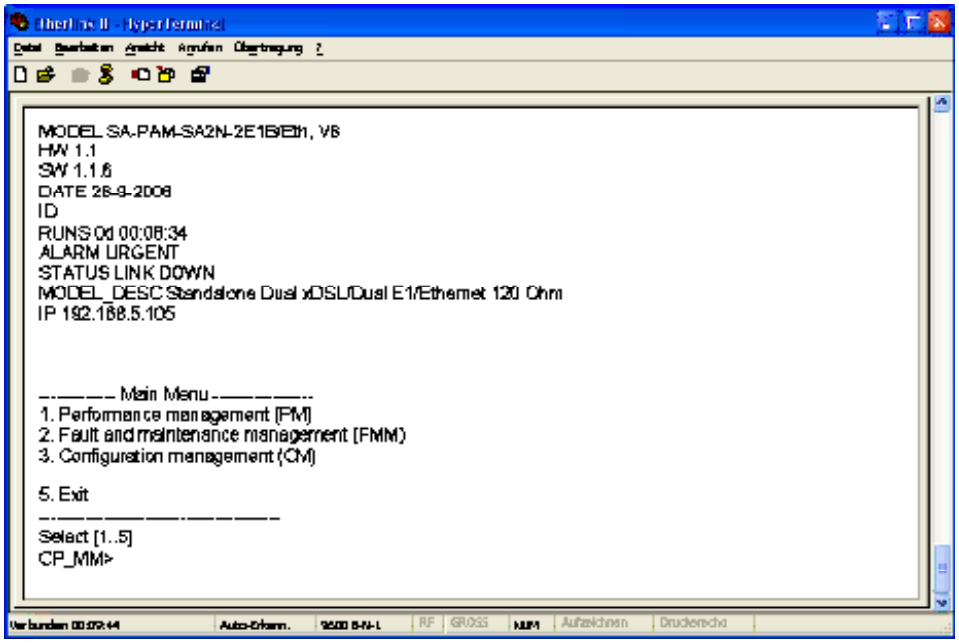
Configure the parameters of the COM port (COM properties). Click “Ok”.
Bits per second:9600, Data bits: 8, Parity: None, Stop bits: 1, Flow control: None



7. Select Properties in the “File” menu of the HyperTerminal program.
8. Select the “Setting” tab. Select the VT100 emulation in the “Emulation” menu. Click “Ok”.



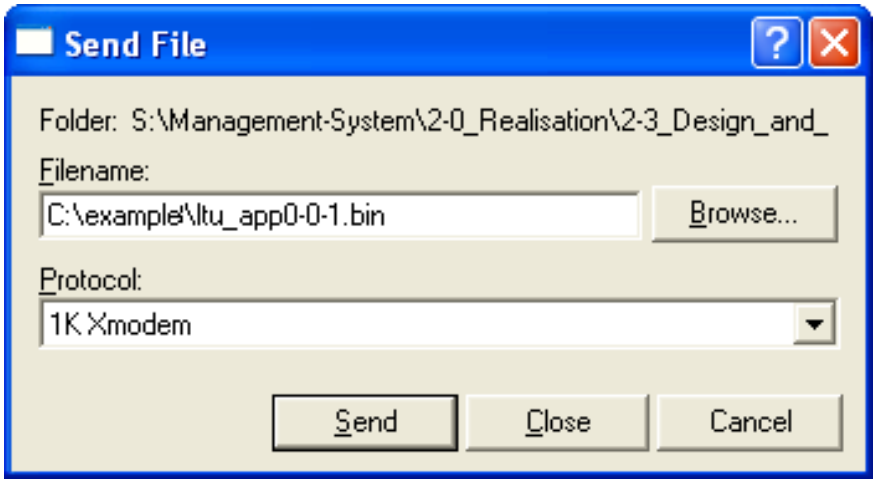
9. Select Call in the “Call” menu. (If the menu is not available, the connection is established automatically. Go to item 10.)
10. Enter %SN, where SN is the slot number in the Subrack. For SA-DESK-TOP-1 and Minirack enter %01. The main menu of the device will be displayed.



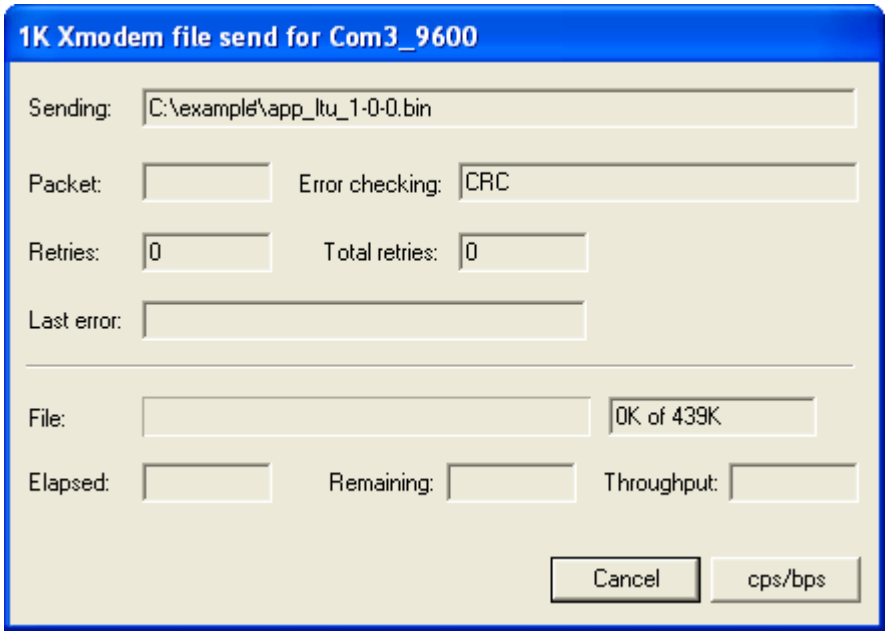
11. Go to the “Fault and maintenance management” menu, means to enter number 2. Enter the <SOFTUPDATE> command. After typing SOFTUPDATE, the device tries to establish connection over the X-modem protocol within 60 seconds.

```
CO_09_FMM>SOFTUPDATE
Flash manufacturer: Silicon Storage Technology(SST)
      Flash device: SST39LF/VF016
     Start address: 0x1000000
        Flash size: 2048 KB
Now upload program via XModem or 1K XModem
C
```

12. The time counter is started. Select Send File in the “Transfer” menu.



13. Select 1K-Xmodem in the “Protocol” drop-down menu of the “Send File” window. Browse the app.bin file in the “Filename” field (the name of the file depends on the software version). Click “Send”. The Hyper Terminal starts downloading the file. After the download is fully completed, the device stores the downloaded file into the memory. After the Send button is clicked, the “1K-Xmodem file send for…” window pops up.



The window displays the software downloading statistics (the name of the file, the number of transmitted packets, the error checking method, the last error, the downloading progress, time, etc.). To cancel downloading, click Cancel.

14. If the software is downloaded, the “1K Xmodem file send for...” window closes automatically.
15. After the software is downloaded completely, enter the <RESET> command in the “Fault and maintenance management” menu. After this, enter the main menu again with %SN, where SN is the slot number in the subrack into which the device is installed.
16. Enter the “Fault and maintenance management” menu and input the <SOFTCONFIRM> command.
17. The software downloading is now completed.

5.3 Software Download via Ethernet (1K-Xmodem and Telnet)

This method of the software downloading is similar to the “Software Downloading via the RS-232 COM Port (LCT) Using Xmodem Protocol” described in chapter 5.2. The only difference is that instead of selecting the number of the COM port, select TCP/IP Socket. Select 23 for the port number (TELNET). This method is the fastest one, because of the high data rate for downloading.

6 SERVICE INSTRUCTIONS

6.1 General Requirements

- Before unpacking, check if the packing box is intact and if the equipment model is equal to that specified in the purchase order/contract.
- Before running the device, read carefully the present technical description and service instructions. Take care about all Warnings inside this manual! Remember that the guarantee and the free-of-charge repair will not be granted under the following conditions:
  a) If the device or any of its parts fails due to improper installation, testing or operation.
  b) damages resulting from:
  1) Misuse and improper installation, including but not limited to:
  - to use the product for its normal purpose or in accordance with the all the instructions for the proper use and maintenance,
  - installation and use of the product in a conflicting way with the actual technical or safety standards in the country where it is installed, as well as the connection of the device to any other power supply source, that fulfil the required technical or safety standards.
  2) Maintenance or repair performed by unauthorized service centers and dealers.
  3) Operation of a malfunctioning device.
  4) Accidents, lightning strokes, flooding, water, fire, improper ventilation, voltage drops, ingress of moisture and insects inside the equipment as well as other reasons, for example, electromagnetic and other interferences which are beyond the supplier control and do not correspond to specified technical conditions.
  5) Transportation except when the shipping is performed by an authorized dealer or a service center.
  7) Defects of the system into which this product is included.
- If the equipment should be powered from a primary DC source (38 … 72 V), please us it with the grounded "+".
- Environment requirements: Temperature: from -5 to +45 °C; Relative air humidity: from 5% to 85% at +25 °C. Exceptions are units that are specified from the manufacturer to differ from these requirements, because there is a special application.
- It is strictly prohibited:
  a) to alter, delete, remove or make illegible the serial number of the device.
  b) to adapt, adjust and change the equipment in order to improve it or extend its applications without the prior written consent of the manufacturer.
  c) to alter or to adjust the equipment without the consent of the manufacturer.

6.2 Evaluation of the Digital Channel Quality and Operation Parameters

The digital channel quality is evaluated by:

- The ITU-T Rec. G.826 error performance (G826) monitoring of a SHDSL link is performed according to ITU-T Rec. G.704, based on CRC (Cyclic Redundancy Check) error detection. Six CRC6 check bits are generated per SHDSL frame. CRC6 errors are used by the software to count the block errors of the SHDSL channel.
- The Noise Margin (NM) performance monitoring.

The Noise Margin (NM) provides qualitative performance information of a specific SHDSL link according the ITU-T Rec. G.991.2. The <NM> command is used to show the noise margin. The recommended NM values should be no less than 6 dB. This value provides the necessary reserve of the signal/noise margin. It is recommended to perform the Noise Margin performance monitoring during acceptance tests and in case the system operates not stable. The test is also used to locate any damaged cable segment.
In addition, it is also recommended to monitor regularly the quality of data transmission over E1 interfaces. On the E1 side, four CRC4 check bits are generated per sub-multiframe (SMF) and

compared with the corresponding bits of the next SMF. If they do not match, the CRC4 error counter is incremented.
The G826 command is used to display the G.826 statistics.
The correctness of operation and configurations of network interfaces can be checked by using loop back tests (LOOP1) and G.826 statistics of E1 interfaces. If LOOP1 is activated on this network interface and the G826 statistics displays errors, a conclusion can be made that the E1 network interface of the BlackBox Etherlink IV system is configured improperly or there is a malfunction.

7 APPENDICES

7.1 Quick Installation Guide for Etherlink IV LTU Devices

7.1.1 Enter an Etherlink IV Device

To enter in a subrack unit, use the Monitor (LCT, RS-232) interface with Hyper Terminal (or any equal program) or go with Telnet through the Ethernet interface.

Monitor (LCT, RS-232) Interface:

- Configure the COM port: Bits per second:9600, Data bits: 8, Parity: None, Stop bits: 1, Flow control: None
- Type <%SN> and press <ENTER>, where SN is the slot number in the Subrack. For SA-DESK-TOP-1 and Minirack type <%01> and press <ENTER>.

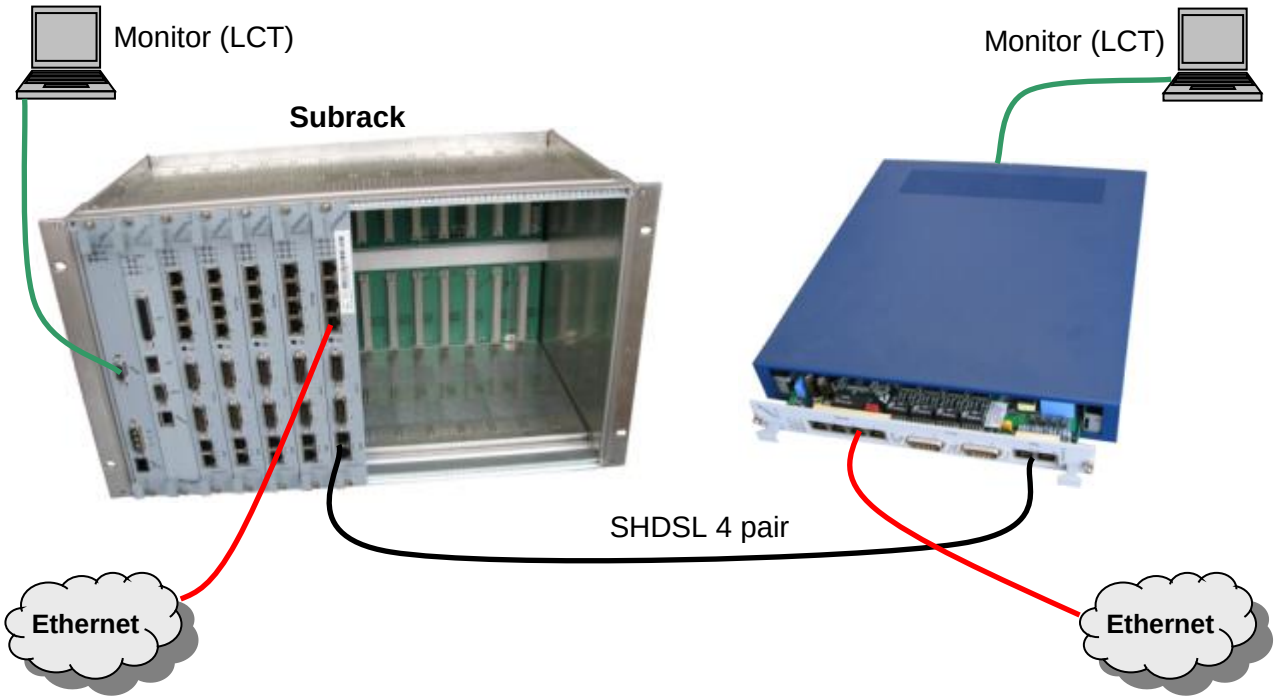
Telnet through Ethernet Interface:

- Type in command line <Telnet 192.168.0.235> and press <ENTER>. This is the default Ethernet Address for Etherlink IV devices.

After a successful entering the main menu of the device will be displayed.

7.1.2 Configure an Etherlink IV Device

A first installation example with the most important commands and points to care about is shown below. We just like to have an Ethernet transmission between the subrack and SA-DESK-TOP-1 equipment over 4 SHDSL copper pairs with a speed of 22.8Mbit/s. The pairs should aggregate (bundle) the data traffic and in case of any SHDSL pair failure, the remaining pairs should continue to work.



Subrack Unit: Enter in a subrack unit with the Monitor (LCT, RS-232) or Telnet interface.

Type following commands	Description
3 <↵>	Go to Configuration Management (CM)
<DEFAULT EVERYTHING> <↵>	Set everything to default configuration
<MASTER ON 1> <↵>	Configure SHDSL 1 as MASTER
<MASTER ON 2> <↵>	Configure SHDSL 2 as MASTER
<MASTER ON 3> <↵>	Configure SHDSL 3 as MASTER
<MASTER ON 4> <↵>	Configure SHDSL 4 as MASTER
<PAYLOAD WAN 1> <↵>	Configure Ethernet over SHDSL 1
<PAYLOAD WAN 2> <↵>	Configure Ethernet over SHDSL 2
<PAYLOAD WAN 3> <↵>	Configure Ethernet over SHDSL 3
<PAYLOAD WAN 4> <↵>	Configure Ethernet over SHDSL 4
<NET> <↵>	Go to NET menu
<SETIP 10.0.2.200> <↵>	Set the IP-address of the device
<NETMASK 255.0.0.0> <↵>	Set the subnet mask
<GATEWAY 10.0.0.101> <↵>	Set the default gateway
<M> <↵>	Go to Configuration Management (CM)
<M> <↵>	Go to Main Menu
2 <↵>	Go to Fault and maintenance management (FMM)
<APPLY ALL> <↵>	Apply all configurations (written in the running config.)
<CONFIRM> <↵>	Confirm all configurations (written in the startup config.)

In Menu Configuration Management (CM) you can type <CONFIG> to see the following picture:

```
CO_01_CM>CONFIG
--------------------------------------------------------------------------------
Running Line Configuration
--------------------------------------------------------------------------------
xDSL                DSL1           DSL2           DSL3           DSL4
  Mode           :  Master(HTU-C)  Master(HTU-C)  Master(HTU-C)  Master(HTU-C)
  Extended rates:  OFF            OFF            OFF            OFF
  Line coding    :  PAM32          PAM32          PAM32          PAM32
  Baserate       :  89             89             89             89
  Annex          :  B              B              B              B
  Payload        :  WAN            WAN            WAN            WAN
  Clock source   :  E1-1,Int       E1-2,Int       E1-3,Int       E1-4,Int
  Reserve        :  ---            ---            ---            ---
  Power          :  OFF            OFF            OFF            OFF
  GS compatible  :  OFF

E1                  E1-1           E1-2           E1-3           E1-4
  G.704 framing  :  ON             ON             ON             ON
  CRC4           :  ON             ON             ON             ON
  AIS Detection  :  ON             ON             ON             ON
  AIS Generation:  ON             ON             ON             ON
  E1 clock       :  DSL            DSL            DSL            DSL
  TS into DSL    :  0-31           0-31           0-31           0-31
  TS into WAN    :  NONE           NONE           NONE           NONE
--------------------------------------------------------------------------------
CO_01_CM>
```

SA-DESK-TOP-1 Unit: Enter in a SA-DESK-TOP-1 unit with the Monitor (LCT, RS-232) or Telnet interface.

Type following commands	Description
3 <↵>	Go to Configuration Management (CM)
<DEFAULT EVERYTHING> <↵>	Set everything to default configuration
<MASTER OFF 1> <↵>	Configure SHDSL 1 as SLAVE
<MASTER OFF 2> <↵>	Configure SHDSL 2 as SLAVE
<MASTER OFF 3> <↵>	Configure SHDSL 3 as SLAVE
<MASTER OFF 4> <↵>	Configure SHDSL 4 as SLAVE
<PAYLOAD WAN 1> <↵>	Configure Ethernet over SHDSL 1
<PAYLOAD WAN 2> <↵>	Configure Ethernet over SHDSL 2
<PAYLOAD WAN 3> <↵>	Configure Ethernet over SHDSL 3
<PAYLOAD WAN 4> <↵>	Configure Ethernet over SHDSL 4
<NET> <↵>	Go to NET menu
<SETIP 10.0.2.201> <↵>	Set the IP-address of the device
<NETMASK 255.0.0.0> <↵>	Set the subnet mask
<GATEWAY 10.0.0.101> <↵>	Set the default gateway
<M> <↵>	Go to Configuration Management (CM)
<M> <↵>	Go to Main Menu
2 <↵>	Go to Fault and maintenance management (FMM)
<APPLY ALL> <↵>	Apply all configurations (written in the running config.)
<CONFIRM> <↵>	Confirm all configurations (written in the startup config.)

In Menu Configuration Management (CM) you can type <CONFIG> to see the following picture:

```
CP_01_CM>CONFIG
--------------------------------------------------------------------------------
Running Line Configuration
--------------------------------------------------------------------------------
xDSL                DSL1           DSL2           DSL3           DSL4
  Mode           :  Slave(HTU-R)   Slave(HTU-R)   Slave(HTU-R)   Slave(HTU-R)
  Extended rates:  OFF            OFF            OFF            OFF
  Line coding    :  PAM32          PAM32          PAM32          PAM32
  Baserate       :  89             89             89             89
  Annex          :  B              B              B              B
  Payload        :  WAN            WAN            WAN            WAN
  Clock source   :  E1-1,Int       E1-2,Int       E1-3,Int       E1-4,Int
  Reserve        :  ---            ---            ---            ---
  Power          :  OFF            OFF            OFF            OFF
  GS compatible  :  OFF

E1                  E1-1           E1-2           E1-3           E1-4
  G.704 framing  :  ON             ON             ON             ON
  CRC4           :  ON             ON             ON             ON
  AIS Detection  :  ON             ON             ON             ON
  AIS Generation:  ON             ON             ON             ON
  E1 clock       :  DSL            DSL            DSL            DSL
  TS into DSL    :  0-31           0-31           0-31           0-31
  TS into WAN    :  NONE           NONE           NONE           NONE
--------------------------------------------------------------------------------
CP_01_CM>
```

The idea is the following: the default settings help any device to be in an initial state, then the MASTER/SLAVE mode is enabled on the modem, then the transmit data is configured, then the network settings are configured (IP address, default subnet mask and default gateway) and finally, these settings are applied and then are written in the EEPROM.

ATTENTION
DON'T FORGET TO WRITE THE CONFIGURATION IN THE STARTUP CONFIGURATION WITH THE FOLLOWING COMMANDS:

2 <↵>	Go to Fault and maintenance management (FMM)
<APPLY ALL> <↵>	Apply all configurations (written in the running config.)
<CONFIRM> <↵>	Confirm all configurations (written in the startup config.)

7.1.3 Checking of Correct Working

The Noise Margin (NM) provides qualitative performance information of a specific SHDSL link according the ITU-T Rec. G.991.2. Perform the next commands to check the status of the unit.

Type following commands	Description
2 <↵>	Go to Fault and maintenance management (FMM)
<STATUS> <↵>	Displays the actual system status

```
CP_01_FMM>STATUS
-------------------------------------------------------------------------
Status                 :       DSL1       DSL2       DSL3       DSL4
-------------------------------------------------------------------------
I/F mode               :         CO         CO         CO         CO
SYNC                   :          1          1          1          1
SEGD                   :          1          1          1          1
Power backoff          :        0.0        0.0        0.0        0.0 dB
Far end power backoff  :        0.0        0.0        0.0        0.0 dbm
Loop attenuation       :       14.0       14.0       14.0       14.0 dB
NMR                    :        7.0        7.0        8.0        7.0 dB
Bitrate                :       5704       5704       5704       5704 kbit/s
SRU #                  :          0          0          0          0
Active sync. source    :   Internal   Internal   Internal   Internal
Remote power state     :        OFF        OFF        OFF        OFF
-------------------------------------------------------------------------
Temperature            :      39.750 C
-------------------------------------------------------------------------

CP_01_FMM>
```

ATTENTION
THE RECOMMENDED NM VALUE FOR A STABLE SHDSL CONNECTION IS > 6DB. AFTER INSTALLATION AND ANY CHANGE OF THE CONFIGURATION THIS VALUE SHOULD BE CHECKED.

7.1.4 Problem with Etherlink IV Device

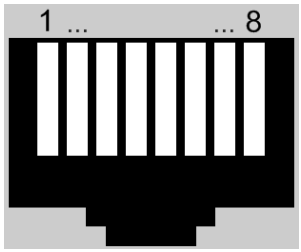
In case you have any trouble with the Etherlink IV device, please send following details to your BlackBox contact:

- Application Description
- Main Menu Picture of every device
- Configuration of every device (Please perform with the <DUMP> command

7.2 Connector Description

7.2.1 Ethernet Connector

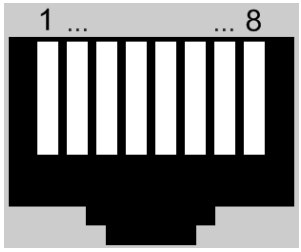
Type – RJ-45 (female), 8 pins.



Pin No.	Description
1	Tx+ (transmit data)
2	Tx- (transmit data)
3	Rx+ (receive data)
4	NC (not used)
5	NC (not used)
6	Rx- (receive data)
7	NC (not used)
8	NC (not used)

7.2.2 SHDSL Connector

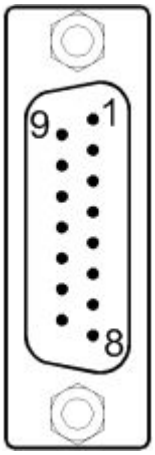
Type – RJ-45 (female), 8 pins.



Pin No.	Description
1	NC (not used)
2	NC (not used)
3	SHDSL interface B
4	SHDSL interface A
5	SHDSL interface A
6	SHDSL interface B
7	NC (not used)
8	NC (not used)

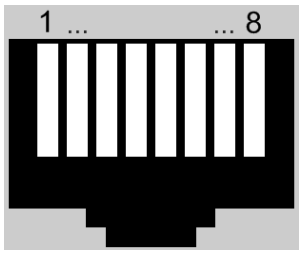
7.2.3 E1 120 Ohm Connector

Type – DB-15 (D-Sub, male), 15 pins.

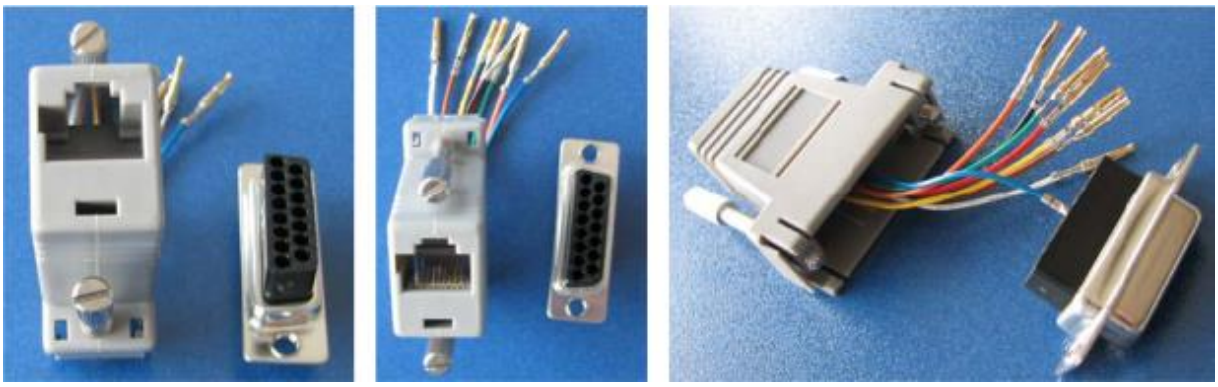


Pin No.	Signal	Description
1	TX_1/2A	E1 Output → CH1/2 Wire A
9	TX_1/2B	E1 Output → CH1/2 Wire B
2	FPE	Functional Protective Earth (cable shield Out CH1/2)
3	RX_1/2A	E1 Input → CH1/2 Wire A
11	RX_1/2B	E1 Input → CH1/2 Wire B
4	FPE	Functional Protective Earth (cable shield Inp CH1/2)
Only for V93 &V96 units		
6	TX_3/4A	E1 Output → CH3/4 Wire A
13	TX_3/4B	E1 Output → CH3/4 Wire B
7	FPE	Functional Protective Earth (cable shield Out_CH3/4)
8	RX_3/4A	E1Input → CH3/4 Wire A
15	RX_3/4B	E1Input → CH3/4 Wire B
5	FPE	Functional Protective Earth (cable shield Inp CH3/4)
10	NC	-
12	NC	-
14	NC	-

Type – RJ-45 (female), 8 pins.

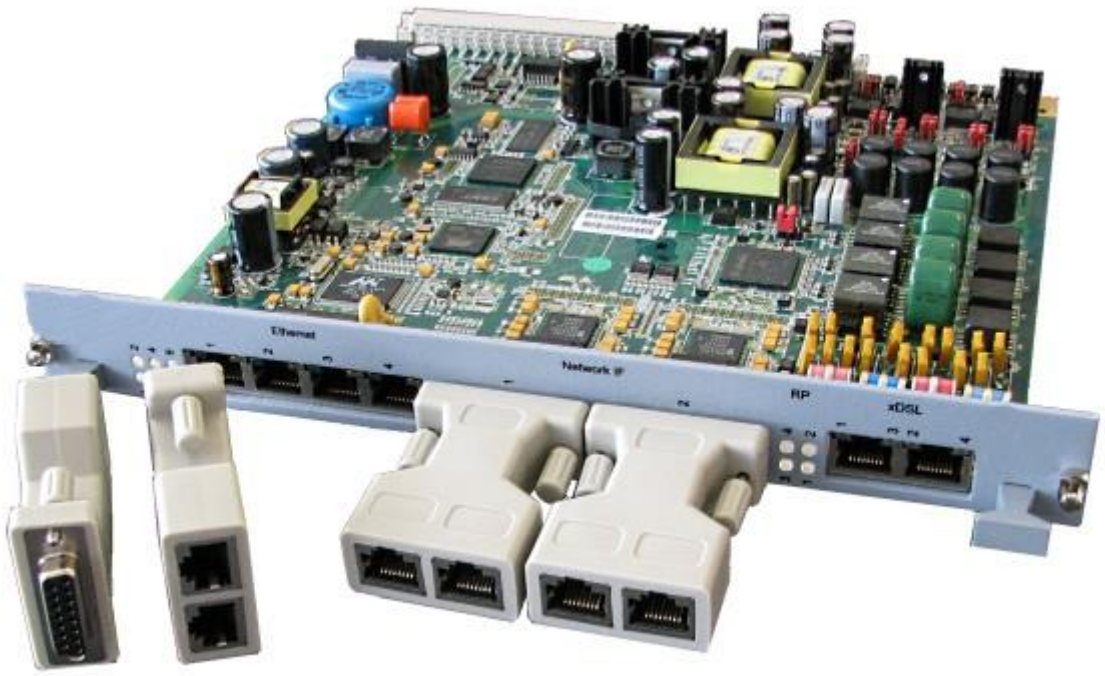


Pin No.	Description
1	E1 Input → CH1/2 Wire A
2	E1 Input → CH1/2 Wire B
3	NC (not used)
4	E1 Output → CH1/2 Wire A
5	E1 Output → CH1/2 Wire B
6	NC (not used)
7	NC (not used)
8	NC (not used)



Please order SA-ADAPT-E1B/RJ45 to convert DB-15 connector to RJ-45 (female) connector. Attention, per DB-15 only one RJ-45 is possible.

Modem		**RJ-45**	cable	**D-Sub-15**
RXA (input)		Pin1	blue	Pin3
RXB (input)		Pin2	orange	Pin11
TXA (output)		Pin4	red	Pin1
TXB (output)		Pin5	green	Pin9

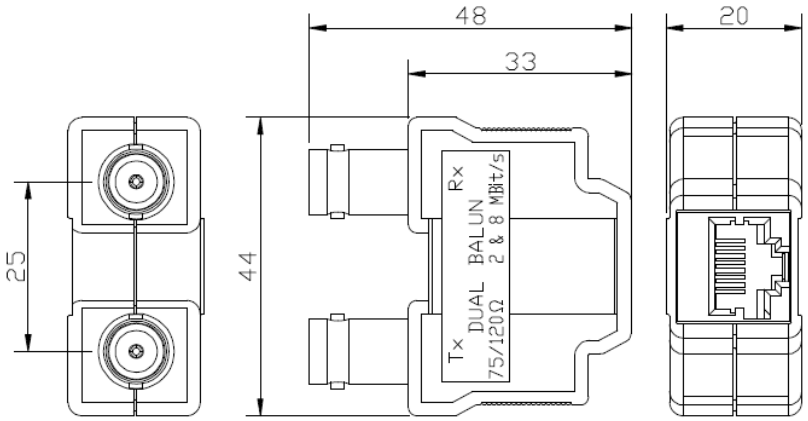


Please order SA-ADAPT-E1B/2xRJ45 to convert DB-15 connector to 2x RJ-45 (female) connector.

7.2.4 E1 75 Ohm Connector

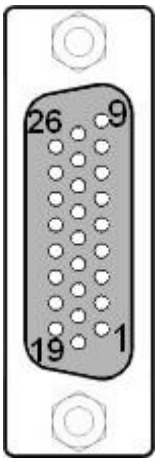
Type - BNC 75 Ω

Please order SA-ADAPT-E1B/E1U to convert RJ-45 connector to BNC.



7.2.5 Nx64, RS-232 and G.703/E0 Connector

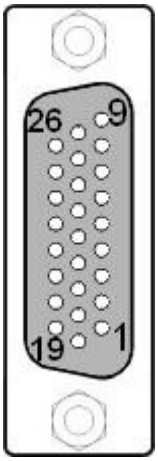
Type – DB-26H (D-Sub High Density, female), 26 pins.



Pin No.	Signal		Description	Direct.
	V.35/36/28	X.21		
1	M2		Mode Select Pin 2	DCE
2	M1		Mode Select Pin 1	DCE
3	M0		Mode Select Pin 0	DCE
4	DTE/DCE		Mode Select Pin DTE/DCE	DCE
5	LL		Local Loopback (141)	DCE
6	TXD(A)	Ta	Transmit Data (A,103a)	DCE
14	TXD(B)	Tb	Transmit Data (B,103b)	DCE
19	RXD(A)	Ra	Receive Data (A,104a)	DTE
10	RXD(B)	Rb	Receive Data (B,104b)	DTE
24	RTS(A)	Ca	Request to Send (A,105a), Control (A)	DCE
15	RTS(B)	Cb	Request to Send (B,105b), Control (B)	DCE
26	CTS(A)	Ia	Clear to Send (A,106a), Indication (A)	DTE
17	CTS(B)	Ib	Clear to Send (B,106b), Indication (B)	DTE
18	DSR(A)		Data Set Ready (A,107a)	DTE
9	DSR(B)		Data Set Ready (B,107b)	DTE
16	DTR(A)		Data Terminal Ready (A,108a)	DCE
25	DTR(B)		Data Terminal Ready (B,108b)	DCE
8	DCD(A)		Data Carrier Detect (A,109a)	DTE
7	DCD(B)		Data Carrier Detect (B,109b)	DTE
22	TTC(A)	Xa	Terminal Transmit Clock (A,113a), DTE Signal Element Timing (A)	DCE
13	TTC(B)	Xb	Terminal Transmit Clock (B,113b), DTE Signal Element Timing (B)	DCE
21	TXC(A)		Transmit Clock (A,114a)	DTE
12	TXC(B)		Transmit Clock (B,114b)	DTE

	20	RXC(A)	Sa	Receive Clock (A,115a), Signal Element Timing (A)	DTE
	11	RXC(B)	Sb	Receive Clock (B,115b),	DTE
				Signal Element Timing (B)	
	23	SG	G	Signal Ground (102)	

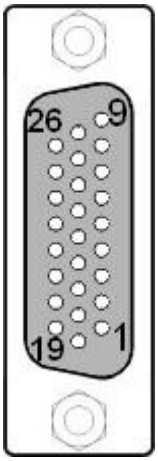
This connector description is only correct with the Nx64 daughter board. Type – DB-26H (D-Sub High Density, female), 26 pins.



Pin No.	Signal RS-232		Description	Direct.
1	DTR		Data Terminal Ready	In
2	DSR		Data Set Ready	Out
3	CTS		Clear to Send	Out
6	DCD		Data Carrier Detect	Out
7	RXD		Receive Data	Out
8	RTS		Request to Send	In
9	TXD		Transmit Data	In
11	SG		Signal Ground	
12	SG		Signal Ground	
13	SG		Signal Ground	
14	SG		Signal Ground	
15	CC		Cable is Connected	In

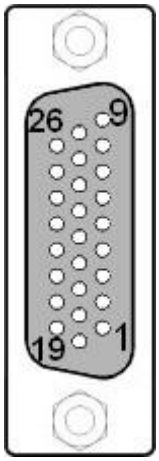
This connector description is only correct with the RS-232 daughter board (attention, the RS-232 daughter board is different than the Nx64 daughter board!).

Type – DB-26H (D-Sub High Density, female), 26 pins.



Pin No.	Signal RS-232		Description	Direct.
1	TXD-1		Transmit Data 1	In
2	RTS-1		Request to Send 1	In
3	TXD-2		Transmit Data 2	In
4	RTS-2		Request to Send 2	In
6	RXD-1		Receive Data 1	Out
7	CTS-1		Clear to Send 1	Out
8	RXD-2		Receive Data 2	Out
9	CTS-2		Clear to Send 2	Out
11	SG		Signal Ground	
12	SG		Signal Ground	
13	SG		Signal Ground	
14	SG		Signal Ground	In
15	CC		Cable is Connected	In
19	TXD-3		Transmit Data 3	In
20	RTS-3		Request to Send 3	In
21	TXD-4		Transmit Data 4	In
22	RTS-4		Request to Send 4	In
23	RXD-3		Receive Data 3	Out
24	CTS-3		Clear to Send 3	Out
25	RXD-4		Receive Data 4	Out
26	CTS-4		Clear to Send 4	Out

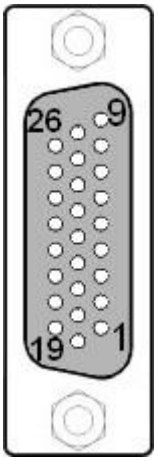
This connector description is only correct with the 4xRS-232 daughter board.



Pin No.	Signal RS-485/422		Description	Direct.
	FD	HD		
7	TXD+	TXD/RXD+	Transmit Data +	Out
9	RXD+		Receive Data +	In
16	TXD-	TXD/RXD-	Transmit Data -	Out
18	RXD-		Receive Data -	In
11			Signal Ground	
12			Signal Ground	
13			Signal Ground	
14			Signal Ground	
15			Cable is Connected	In

This connector description is only correct with the RS-485 daughter board (attention, the RS-485 daughter board is different than the Nx64 daughter board!).

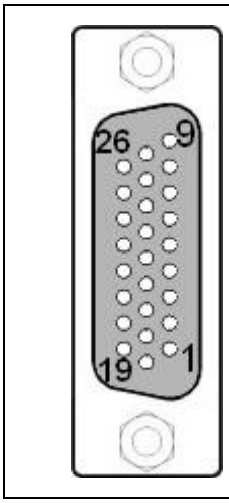
Type – DB-26H (D-Sub High Density, female), 26 pins.



Pin No.	Signal RS-485/422		RS-232	Description	Direct.
	FD	HD			
7	TXD1+	TXD/RXD1+	RXD1	Transmit Data +	Out
9	RXD1+		TXD1	Receive Data +	In
3	TXD1-	TXD/RXD1-	CTS1	Transmit Data -	Out
16	TXD1-	TXD/RXD1-	CTS1	Transmit Data -	Out
8	RXD1-		RTS1	Receive Data -	In
18	RXD1-		RTS1	Receive Data -	In
11			GND	Signal Ground	In
12			GND	Signal Ground	
13			GND	Signal Ground	
14			GND	Signal Ground	
15			CC	Cable is Connected	In
24	TXD2+	TXD/RXD2+	RXD2	Transmit Data +	Out
26	RXD2+		TXD2	Receive Data +	In
20	TXD2-	TXD/RXD2-	CTS2	Transmit Data -	Out
25	RXD2-		RTS2	Receive Data -	In

This connector description is only correct with the 2xRS-232/422/485 daughter board

Type – DB-26H (D-Sub High Density, female), 26 pins.



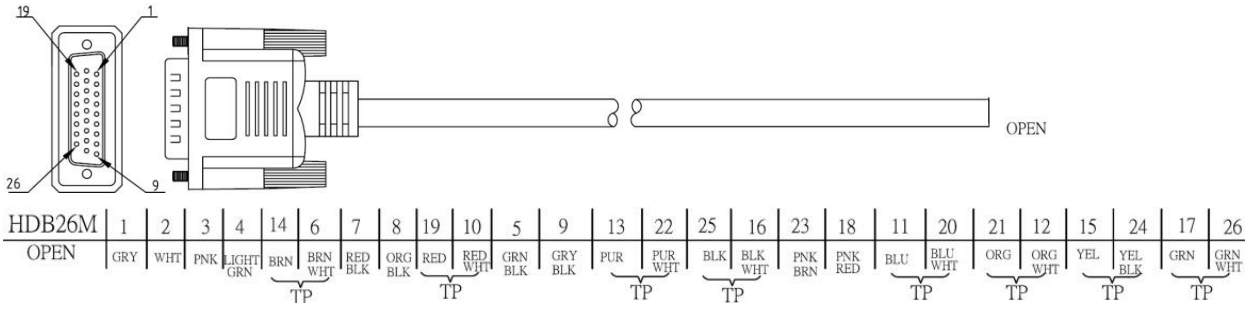
Pin No.	Signal G.703/E0		Description	Direct.
11	RXD+		Receive Data +	In
20	RXD-		Receive Data -	In
17	TXD+		Transmit Data +	Out
26	TXD-		Transmit Data -	Out
5			Signal Ground	
14			Signal Ground	
22			Signal Ground	
23			Signal Ground	
15			Cable is Connected	In

This connector description is only correct with the codirectional G.703/E0 64 kbps daughter board.

Available cables:

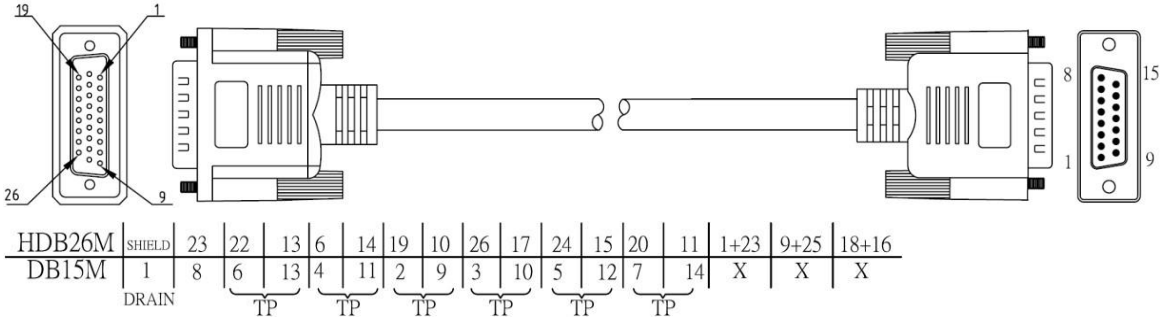
SA-CAB-DB26-ETH-IV-OPEN

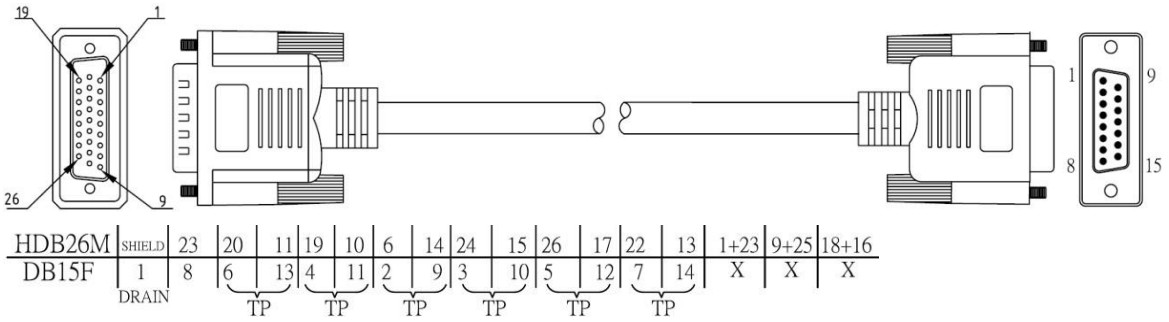
Cable Etherlink IV Universal, DB26MH to Open, 1.0m, UL2464, AWG-26, OD=8mm



SA-CAB-N21-ETH-IV-DCE

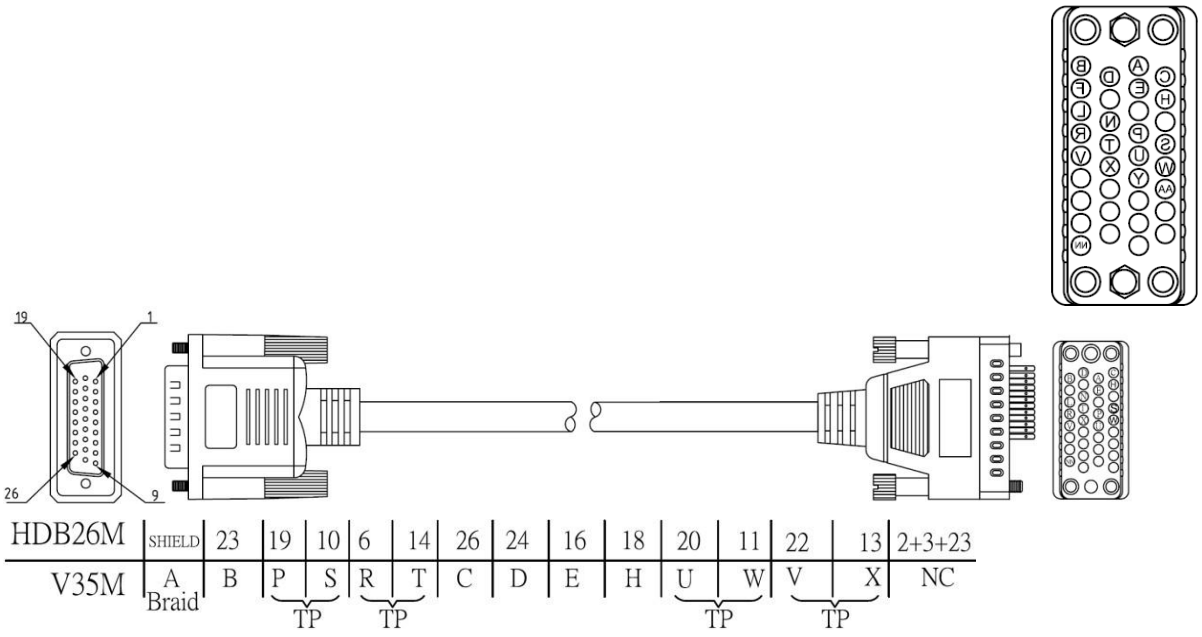
Cable Etherlink IV Nx64 to X.21, DB26MH to DB15M, DCE, 1.0m, UL2464, AWG-28, OD=5mm





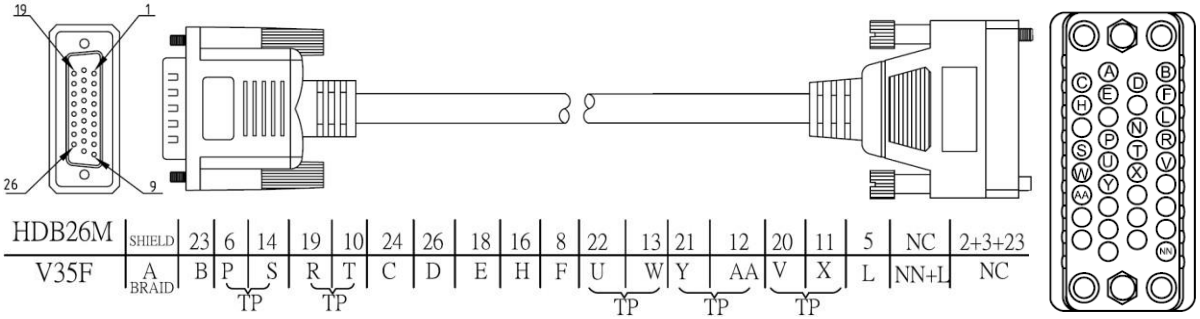
SA-CAB-N35-ETH-IV-DCE

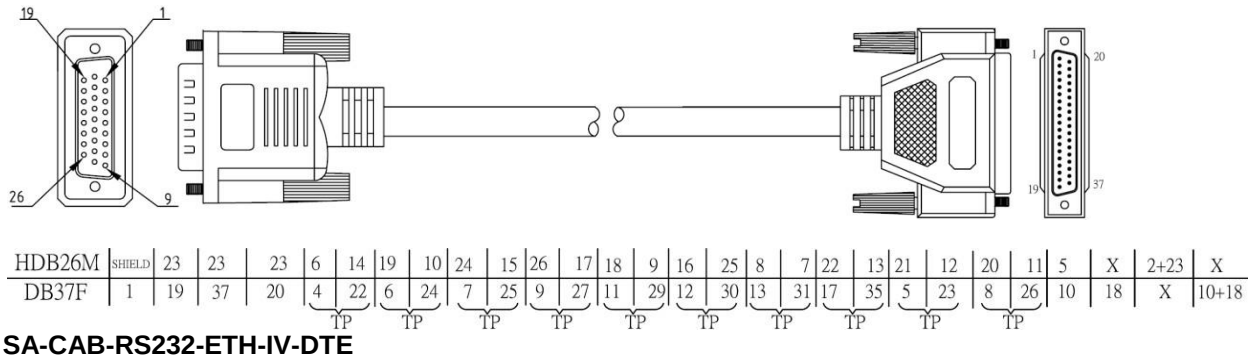
Cable Etherlink IV Nx64 to V.35, DB26MH to MRAC34M, DCE, 1.0m, UL2464, AWG-26, OD=8.5mm



SA-CAB-N35-ETH-IV-DTE

Cable Etherlink IV Nx64 to V.35, DB26MH to MRAC34F, DTE, 1.0m, UL2464, AWG-26, OD=8.5mm

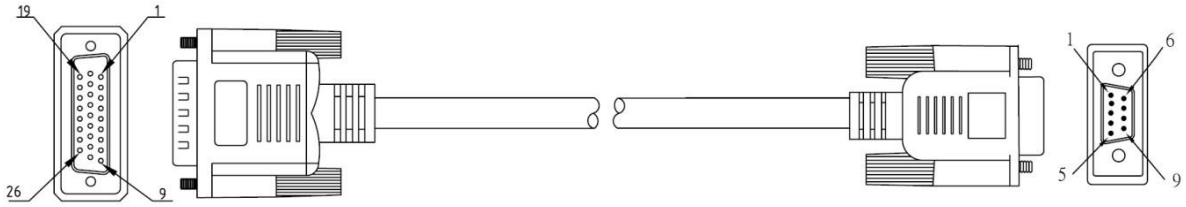




HDB26M	SHIELD	23	23	23	6	14	19	10	24	15	26	17	18	9	16	25	8	7	22	13	21	12	20	11	5	X	2+23	X
DB37F	1	19	37	20	4	22	6	24	7	25	9	27	11	29	12	30	13	31	17	35	5	23	8	26	10	18	X	10+18
					TP	TP	TP	TP	TP	TP	TP	TP	TP	TP	TP	TP	TP	TP	TP	TP	TP	TP	TP	TP				

SA-CAB-RS232-ETH-IV-DTE

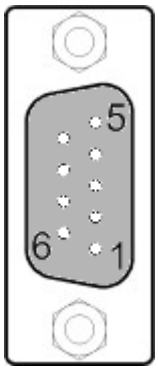
Cable Etherlink IV RS-232, DB26MH to DB9F, DTE, 1.0m, UL2464, AWG-28, OD=5mm



HDB26M	14	9	7	8	3	2	1	6	14+15
DB9F	5	3	2	7	8	6	4	1	X

7.2.6 Monitor (LCT, Local Craft Terminal) Connector (ACU, Minirack, SA-DESKTOP-x)

Type – DB-9 (D-Sub, female), 9 pins.

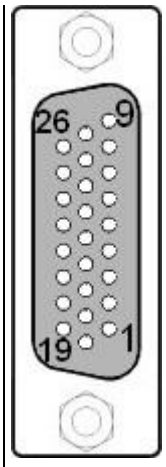


Pin No.	Signal	Description
1	DA_COM/SA	Urgent-alarm contact / protection ground
2	TXD	Transmit data (to the modem)
3	RXD	Receive data (from the modem)
4	ND_COM/COM	Non-urgent alarm contact / common contact
5	SGND	Signal ground
6	DA_NC	Urgent alarm contact, normally closed
7	DA_NO	Urgent alarm contact, normally open
8	ND_NC	Non-urgent alarm contact, normally closed
9	ND_NO	Non-urgent alarm contact, normally open

7.2.7 Digital Input / Output Interface (4I4O) connector

Type – DB-26H (D-Sub High Density, female), 26 pins.

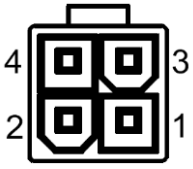
Pin No.	Signal		Description	Direct.
1	IN1a		Input 1 a	In
19	IN1b		Input 1 b	In
2	IN2a		Input 2 a	In
20	IN2b		Input 2 b	In
3	IN3a		Input 3 a	In
21	IN3b		Input 3 b	In
4	IN4a		Input 4 a	In
22	IN4b		Input 4 b	In
10	GND		Signal Ground	
11	GND		Signal Ground	
12	GND		Signal Ground	
13	GND		Signal Ground	



5	+3.3V		Power	Out
14	CC		Cable is Connected	In
9	OUT1nc		Output 1 normally closed	Out
18	OUT1com		Output 1 common	Out
26	OUT1no		Output 1 normally open	Out
8	OUT2nc		Output 2 normally closed	Out
17	OUT2com		Output 2 common	Out
25	OUT2no		Output 2 normally open	Out
7	OUT3nc		Output 3 normally closed	Out
16	OUT3com		Output 3 common	Out
24	OUT3no		Output 3 normally open	Out
6	OUT4nc		Output 4 normally closed	Out
15	OUT4com		Output 4 common	Out
23	OUT4no		Output 4 normally open	Out

7.2.8 -48VDC Connector (SA-DESKTOP-x)

Type – MiniFit, 4 pins.



Pin No.	Signal	Description
1	-PWR1	Negative power supply terminal
2	PGND	Protection ground
3	-PWR2	Negative power supply terminal
4	+PWR	Positive power supply terminal

8 TECHNICAL SPECIFICATION

8.1 Interfaces

8.1.1 SHDSL Line Interface

Specification	ITU-T G.991.2-G.shdsl, ITU-T G.991.2-G.shdsl.bis
Line Code	TC-PAM16/32, Extended: TC-PAM4/8/64/128
Impedance	135Ω
Transmit Power	13.5 (Annex A) or 14.5 (Annex B) dBm @ 135Ω
Number of Pairs	1,2 or 4
Bit Rate	192 to 5704kbit/s, Extended: 128 to 15232kbit/s
Connector Type	RJ-45, 8 pin
Overvoltage Protection	ITU-T Rec. K.20/K.21
Wetting Current	2-4mA @ 47VDC
Remote Power	60/90mA @ 120VDC
Remote Power	60/90/125mA @ 200VDC

8.1.2 E1 Line Interface

Specification	ETS 300 166, ITU-T Rec. G.703, G.704
Number of Interfaces	2 or 4
Line Code	HDB3
Impedance	either 120Ω or 75Ω
Jitter	ITU-T Rec. G.823, ETSI TS 101 135
Bit Rate	2048kbit/s ± 50 ppm
Connector Type	either DB15 male (120Ω) or two BNC 75Ω
ESD Protection	8kV (Air discharge)

8.1.3 Nx64 and RS-232/RS-485 Interface

Specification	ITU-T Rec V.35/V.36/X.21/V.28 or RS-232/485
Number of Interfaces	1
Bit Rate	1..128 x 64 kbps (synchronous) for V.35/V.36/X.21 1..3 x 64 kbps (synchronous) for V.28 75, 1200..230400 bps (asynchronous) for RS-232/485
Format RS-232/485	Bits: 5…8 Stop bits: 1/1.5/2 Parity: odd/even/odd/mark/space
Connector Type	DB26 high density female
Adapter Cable Connector Type	V.35 ISO2593 (34 Pin MRAC) V.36 ISO4902 (37 Pin Dsub) X.21 ISO4903 (15 Pin Dsub) X.28 ISO2110 (25 Pin Dsub) RS-232 EIA/TIA-574 or ISO2110 (9 Pin or 25 Pin Dsub)
ESD Protection	8kV (Air discharge)

8.1.4 G.703/E0 Interface

Specification	ITU-T Rec G.703 codirectional interface
Number of Interfaces	1
Impedance	120□
Jitter	ITU-T Rec. G.823
Bit Rate	64 kbit/s s ± 500 ppm
Range	500 m
Connector Type	DB26 high density female
ESD Protection	8kV (Air discharge)

Isolation	1500 Vrms

8.1.5 Monitor or Local Craft Terminal (RS-232) Interface

Specification	EIA-232 / V.28
Data Rate	9600 baud, asynchronous
Protocol	8 bit, no parity, 1 stop bit , flowcontrol none, no linefeed with carriage return
Signal Level	V.28
Connector Type	DB9 female connector

8.1.6 Ethernet

Standard:	IEEE-802.3, VLAN IEEE-802.1Q, QoS IEEE-802.1P
Data Rate	10/100BaseT, Full/Half Duplex
Protocols	Data, Telnet, SNMP, WEB
Signal Level	Ethernet
MDI / MDI-X auto crossover	Supported
Auto Negotiation	Supported
Connector Type	RJ45, 8 pin

8.1.7 Digital Input / Output Interface (4I4O)

Number of Inputs per card	4
Max Input Voltage	72VDC
Isolation	2000Vrms
Output Voltage	3.3V +/- 5%
Maximal Output Current:	20mA
Number of Outputs per card	4
Maximal switching Voltage	120VDC, <1A
Maximal switching Power	<30W
Isolation	1500Vrms
Connector Type	DB26 high density female

8.2 Power Supply

Specification	ETSI ETS 300 132-2
Voltage	38-72VDC
Power Consumption @ 48VDC	Typ. 5.0W, SA-RC-ETHERLINK_IVL-2E1B/4Eth-RP, V90
(All DSL links up, Ethernet on,	Typ. 5.0W, SA-RC-ETHERLINK_IVL-2E1B/N64/4Eth-RP, V91
Remote Power off)	Typ. 6.1W, SA-RC-ETHERLINK_IV2L-4E1B/4Eth-RP, V93
	Typ. 6.1W, SA-RC-ETHERLINK_IV2L-2E1B/N64/4Eth-RP,V94
	Typ. 8.1W, SA-RC-ETHERLINK_IV4L-4E1B/4Eth-RP, V96
	Typ. 7.1W, SA-RC-ETHERLINK_IV4L-4Eth, V98
Remote Power per DSL channel	< 10.0W @ 120VDC/60mA
	< 13.0W @ 120VDC/90mA
	< 15.0W @ 120VDC/125mA

8.3 Environment

8.3.1 Climatic Conditions

Storage:	ETS 300 019-1-1 Class 1.2	(-25°C … +55°C)

Transportation:	ETS 300 019-1-2 Class 2.3	(-40°C … +70°C)
Operation:	ETS 300 019-1-3 Class 3.2	(-5°C … +45°C)

Higher Operation Temperature range available on request (-20°C … +80°C)

8.3.2 EMC and Safety Standards

EN 300386 V1.4.1:2008
EN 50121-4:2006
EN 60950-1:2006
EN 55022:2006, Class B
EN 55024/A2:2003
EN 61000-4-2/A2:2001
EN 61000-4-3:2006
EN 61000-4-4:2004
EN 61000-4-5:2006
EN 61000-4-6:2007
EN 61000-4-6/A1:2001

8.4 Physical Dimensions and Weight

Dimension PCB:	233(W)x220(D)x1.6(H) mm
Dimension Unit	262(W)x247(D)x30(H) mm
Weight	< 0.6kg for LTU
	< 3.8kg in Minirack
	< 3.3kg in SA-DESK-TOP-1