

FlexDSL MiniFlex

MINIFLEX DEVICES

TECHNICAL DESCRIPTION AND OPERATIONS MANUAL

Version 1.26
Document name UM_Flexdsl-Miniflex_V1-26.Docx
Revision 15 October 2018

© Copyright 2018 by FlexDSL Telecommunications AG. 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 FlexDSL Telecommunications AG. Published by FlexDSL Telecommunications AG. All rights reserved.

VERSION CONTROL.....	10
SAFETY REGULATIONS	12
EU DIRECTIVE 2002/96/EC AND EN50419	12
1 SELECTION GUIDE	13
2 PRECAUTION	15
3 TECHNICAL DESCRIPTION	16
3.1 General Information about FlexDSL MiniFlex	16
3.2 Description of MiniFlex Devices.....	18
3.2.1 SubRacks with Integrated Switch.....	19
3.2.1.1 SubRack with Integrated Gigabit Ethernet Switch (1000/2500Base-X uplinks)	19
3.2.1.2 SubRack with Integrated Fast Ethernet Switch (Gigabit Ethernet uplinks)	20
3.2.2 Power Supplies for the Subrack.....	22
3.2.3 FlatRack with Integrated Gigabit Ethernet Switch.....	22
3.2.4 Power Supply for the FlatRack.....	23
3.2.5 MiniRack.....	24
3.2.6 Dual Unit.....	26
3.2.7 SHDSL Line Card	27
3.2.7.1 Line Card SHDSL Interface	28
3.2.7.1.1 Master/Slave.....	28
3.2.7.1.2 Multipair Mode	28
3.2.7.1.3 Automatic Link Configuration	29
3.2.7.1.4 SHDSL Test Loop, Analogue Loop Back	29
3.2.7.1.5 SHDSL Performance Monitoring (Noise Margin, G.826)	30
3.2.7.2 Line Card Ethernet Interface.....	31
3.2.7.3 Line Card MAC Filter	33
3.2.7.3.1 Line Card MAC Filter Rules	34
3.2.7.4 Line Cards IEEE 802.1x Access Control.....	34
3.2.7.4.1 IEEE 802.1x Line Cards Settings.....	35
3.2.7.5 Line Card Rapid Spanning Tree Protocol	35
3.2.7.6 RADIUS.....	37
3.2.7.6.1 RADIUS Server Setup with Defined Vendor Specific Attributes	37
3.2.7.6.2 Simplified RADIUS Server Setup	39
3.2.7.6.3 RADIUS Server setup with defined Service-Type Attribute	40
3.2.7.6.4 Configuring User Access Rights	41
3.2.7.7 LLDP	42
3.2.7.8 Line Card Alarm and LED Description	43
3.2.7.9 Line Card Management with Local Craft Terminal and Ethernet.....	44
3.2.7.9.1 Telnet (Ethernet Interface).....	44
3.2.7.9.2 WEB (Ethernet Interface).....	44
3.2.7.9.3 SNMP (Ethernet Interface).....	46
3.2.7.9.4 SSH.....	48
3.2.8 SHDSL DINrail Modem	49
3.2.9 Single or Dual FOM & GFOM Line Card	49
3.2.9.1 Line Card SFP and Ethernet Interface	50
3.2.9.2 Line Card Alarm and LED Description	50
3.2.10 Single or Dual FOM & GFOM DINrail Modem	50
3.2.11 POE Line Card.....	51
3.2.11.1 Line Card LED Description	53
3.2.12 POE DINrail Unit.....	54
3.2.13 Managed Switch Line Card	54
3.2.13.1 Line Card LED Description	55
3.2.14 Managed Switch DINrail Unit	55
3.2.15 Serial RS-232/422/485 Interface Line Card.....	56
3.2.15.1 Line Card SFP and Ethernet Interface	56
3.2.15.2 Line Card Serial RS-232/422/485 Interface	56
3.2.15.3 Line Card Alarm and LED Description	57
3.2.16 Serial RS-232/422/485 Interface DINrail Modem.....	57
3.2.17 Serial RS-232 Line Card	58

3.2.17.1	Line Card Serial Interface	58
3.2.17.2	Line Card LED Description	58
3.2.18	Serial RS-232 DINrail Unit	59
3.2.19	E1 Interface Line Card	59
3.2.19.1	Line Card E1 Interface (G.703/704)	60
3.2.19.1.1	Framed and Unframed E1	60
3.2.19.1.2	CRC4 (Cyclic Redundancy Check)	60
3.2.19.1.3	AIS Detection (Alarm Indication Signal)	60
3.2.19.1.4	E1 Clock Modes	60
3.2.19.2	Line Card LED Description	61
3.2.20	E1 DINrail Unit	61
3.2.20.1	DINrail Ethernet Interface	62
3.2.20.2	DINrail LED Description	62
3.2.21	FXS/FXO/VF Interface VoIP Line Cards	62
3.2.21.1	VoIP Line Card LED Description	63
3.2.22	FXS/FXO/VF VoIP DINrail Unit	64
3.2.22.1	FXS/FXO/VF VoIP DINrail Unit LED Description	65
3.2.23	Input / Output Line Card	66
3.2.23.1	Input / Output Line Card LED Description	67
3.2.24	Input / Output DINrail Unit	67
3.2.24.1	Input / Output DINrail Unit LED Description	67
3.2.25	Default IP Address	68
3.2.25.1	DINrail Unit	68
3.2.25.2	MiniRack	68
3.2.25.3	Subrack with Integrated Switch	68
3.2.25.4	FlatRack with Integrated Switch	69
3.2.25.5	Line Card	69
4	PROGRAMMING GUIDE MINIFLEX SWITCH (MF-MR2N-SW-12ETH,V2 ONLY)	70
4.1	MiniFlex Command Line Interface	70
4.2	Getting Help	72
4.3	Read-Only and Privileged modes of operation	72
4.3.1	Entering to and exiting from privileged mode	73
4.4	User Management	73
4.4.1	Creating a user	73
4.4.2	Configuring user rights	73
4.4.3	Changing a password for privileged mode	73
4.4.4	Changing a login password for a user	73
4.4.5	Getting a list of users	73
4.4.6	Deleting a user	73
4.5	Setting up a System Date and Time	73
4.5.1	An automatic System Date and Time Settings	73
4.5.2	Manual System Date and Time Settings	74
4.5.3	System Date and Time Displaying	74
4.6	Understanding your environment	74
4.6.1	Checking your access rights	75
4.6.2	Checking who else is connected to a system	75
4.6.3	Dropping a session of another user	75
4.6.4	Checking a node, you connected to	75
4.6.5	Checking a contact person	75
4.6.6	Check software version	75
4.6.7	Setting an IP address of a switch	75
4.6.8	Deleting a IP address of a switch	76
4.6.9	Check an IP address and switching configuration of a node	76
4.6.10	List interface status	76
4.6.11	Display a forwarding database (FDB)	77
4.6.12	Get a technical support	77
4.7	Saving and restoring a system configuration	77
4.7.1	Saving a current configuration as a startup configuration	77
4.7.2	Saving current configuration as a backup configuration	78
4.7.3	Restoring a backup configuration	78
4.7.4	Restoring a factory defaults	78
4.7.5	Rebooting a switch	79

4.7.6	Viewing a configuration and storing it on a PC	79
4.7.6.1	Viewing a running configuration.....	79
4.7.6.2	Viewing a startup configuration.....	79
4.7.6.3	Viewing a backup configuration	79
4.7.6.4	Storing a configuration with Hyper Terminal	79
4.7.6.5	Storing a configuration with PuTTY	81
4.7.7	Download a configuration to a switch	82
4.8	Working with ports.....	82
4.9	Working with VLAN	85
4.9.1	Creating a Port-Based VLAN	86
4.9.2	Deleting a VLAN	87
4.9.3	Creating a TAG-based VLAN.....	88
4.9.4	Creating a Port and TAG-based VLAN.....	89
4.9.5	Creating an IP Subnet-based VLAN.....	90
4.9.6	Creating a MAC-Based VLAN.....	91
4.9.7	A list of commands related with plain VLAN	92
4.10	Forwarding Database	93
4.11	Rapid Spanning Tree	94
4.12	Link Aggregation Control Protocol	97
4.13	Trunks.....	98
4.14	Switch Ethernet Ring Protection.....	99
4.15	IGMP Snooping.....	101
4.16	Multicast VLAN registration	102
4.17	Multiple Spanning Tree Protocol.....	104
4.18	Q-in-Q and VLAN Translation.....	105
4.19	Jumbo Frames Support	106
4.20	Radius.....	106
4.20.1	Configuring Radius Attributes.....	106
4.20.2	Configuring Radius Authentication Service	107
4.20.3	Configure Radius Accounting Service	108
4.20.4	Configuring ISP-Domain	108
4.21	SNMP.....	109
4.22	Access control.....	109
4.23	802.1x Access control	111
4.23.1	Configuring Protocol parameters.....	113
4.23.2	Configuring 802.1x Control for the port	113
4.23.3	Setting the Re-authentication Mechanism.....	114
4.23.4	Configuring Keep-alive Mechanism.....	114
4.23.5	Forcing users to Log out from the Authentication Status	114
4.23.6	Configuring Session Timeout Mechanism	115
4.24	Configuring DHCP Relay, DHCP Option 82 and DHCP Snooping	115
4.24.1	DHCP Relay related commands	116
4.24.2	DHCP Snooping related commands.....	117
4.24.3	Secure Forwarding related commands.....	117
4.25	Quality of Service (QoS).....	118
4.25.1	Queues	118
4.25.2	Traffic to queues allocation mechanism	119
4.25.3	Configuring QoS	119
4.26	Configuring GVRP.....	120
4.27	Anti DoS protection	121
4.28	Static Routing.....	121
4.29	NAT/NPT feature.....	122
4.30	SNMP Message Forwarding.....	123
4.31	Enabling and disabling CLI access over Telnet, SSH and SNMP	123
5	PROGRAMMING GUIDE LINE CARDS, DINRAIL, MF-MR2N-SW-8ETH,V2 AND FLATRACK SWITCHES	124
5.1	Command Structure SHDSL, Serial and E1	124
5.2	Command Structure FOM, GFOM, IO, Switch, FlatRack / MF-MR2N-SW-8Eth,V2 ..	126
5.3	Line Cards, DIN-rail, FlatRack and MF-MR2N-SW-8Eth,V2 Switch Software	127
5.4	Configuration and Application Storage	127
5.5	Groups of Commands Requiring Confirmation	129

5.6	Command Syntax.....	129
5.7	Commands.....	130
5.7.1	Main Menu	130
5.7.1.1	System Invitation	130
5.7.2	General Commands.....	131
5.7.2.1	<H> Command.....	131
5.7.2.2	<APPLY [ALL/GROUP]> Command	131
5.7.2.3	<CONNECT N:1..13/R> Command	131
5.7.3	Performance Management Menu	131
5.7.3.1	<H> Command	131
5.7.3.2	<G826> Command	132
5.7.3.3	<G826 E1> Command.....	132
5.7.3.4	<ALLG826 N> Command	133
5.7.3.5	<RESETG826> Command	133
5.7.3.6	<RESETALLG826 N> Command	133
5.7.3.7	<NETSTAT [LAN/WAN]> Command	134
5.7.3.8	<NETERR [LAN/WAN]> Command	135
5.7.3.9	<RESETNETSTAT> Command.....	135
5.7.3.10	<LINKSTAT> Command.....	136
5.7.3.11	<LINKALARM> Command.....	136
5.7.3.12	<ALARMLOG [N]> Command	136
5.7.3.13	<LINKDIAG> Command	137
5.7.3.14	<M> Command.....	137
5.7.4	Fault and Maintenance Management Menu	138
5.7.4.1	<H> Command	138
5.7.4.2	<NM> & <LINKNM> Commands	139
5.7.4.3	<STATUS> Command.....	139
5.7.4.4	<STATUS ETH> Command.....	140
5.7.4.5	<STATUS L> Command.....	140
5.7.4.6	<STATUS SFP> Command.....	142
5.7.4.7	<STATUS IO> Command.....	143
5.7.4.8	<STATUS LLDP> Command.....	143
5.7.4.9	<STATUS DOT1X> Command.....	143
5.7.4.10	<STATUS RADIUS> Command	144
5.7.4.11	<STATUS ENCODE> Command.....	144
5.7.4.12	<STATUSPOE> Command	144
5.7.4.13	<LOOP1 [ON/OFF] [N=1..4]> Command	145
5.7.4.14	<LOOP2 [N:A/R] [ON/OFF]> Command	145
5.7.4.15	<ALARM> Command	146
5.7.4.16	<ACO [GROUP ON/OFF]> Command.....	147
5.7.4.17	<MACTABLE> Command	147
5.7.4.18	<LLDP STAT [IF/ALL]>.....	148
5.7.4.19	<STARTAL [N]> Command	148
5.7.4.20	<RESTART [N=1..2]> Command.....	148
5.7.4.21	<RESET> Command.....	148
5.7.4.22	<CONFIRM> Command	148
5.7.4.23	<BACKUP> Command	149
5.7.4.24	<RESTORE> Command	149
5.7.4.25	<DIFF N/R/S/B N/R/S/B> Command	149
5.7.4.26	<DUMP N/R/S/B> Command	149
5.7.4.27	<LOAD> Command.....	150
5.7.4.28	<TLM> Command	150
5.7.4.29	<TLM S [N:[Rnn-Rkk]] [ABC]> Command.....	151
5.7.4.30	<LOG> and <LOG C> Command	151
5.7.4.31	<SOFTUPDATE> Command.....	151
5.7.4.32	<TFTP [CMD] [ARG1] [ARG2]> Command.....	152
5.7.4.33	<SOFTCONFIRM> Command.....	152
5.7.4.34	<SOFTINFO> Command.....	152
5.7.4.35	<PING x.x.x.x> Command.....	153
5.7.4.36	<MODEMVIEW> Command	153
5.7.4.37	<SD SNAPSHOT> Command	153
5.7.4.38	<SD DIR> Command.....	153
5.7.4.39	<SD DEL [NAME]> Command.....	153

5.7.4.40	<SD SAVE [N=0..9]> Command.....	153
5.7.4.41	<SD LOAD [N=0..9]> Command.....	153
5.7.4.42	<SD BOOT [ON/OFF]> Command	153
5.7.4.43	<SD STATUS> Command.....	153
5.7.4.44	<RESETPOE> Command	154
5.7.4.45	<M> Command.....	154
5.7.4.46	<BERT> Command	154
5.7.4.47	<H> Command	154
5.7.4.48	<START> Command.....	154
5.7.4.49	<STOP> Command.....	155
5.7.4.50	<RES> Command	155
5.7.4.51	<SHOW> Command.....	155
5.7.4.52	<TRACE> Command.....	155
5.7.4.53	<SET [E11-E14] [INT/EXT]> Command.....	156
5.7.4.54	<TS [TX/RX] [list/NONE]> Command	156
5.7.4.55	<PATD [2En/bitstring]> Command.....	156
5.7.4.56	<CONF> Command.....	156
5.7.5	Configuration Management Menu	157
5.7.5.1	<H> Command	157
5.7.5.2	<ENCODE [NRSB]> Command.....	158
5.7.5.3	<ENCODE KEY [N]> Command.....	158
5.7.5.4	<ENCODE [ON/OFF] [N]> Command.....	158
5.7.5.5	<SECURE ON/OFF> Command.....	159
5.7.5.6	<USERS> Command	159
5.7.5.7	<USER> Command.....	159
5.7.5.8	<PASSWORD {users}> Command	161
5.7.5.9	<CONFIG [N/R/S/B] > Command	161
5.7.5.10	<MASTER ON/OFF [N = 1..2]> Command	163
5.7.5.11	<AUTO ON/OFF> Command	163
5.7.5.12	<EXT ON/OFF [N = 1..2]> Command.....	163
5.7.5.13	<BASERATE [M/AUTO] [N]> Command.....	164
5.7.5.14	<PAM [16/32] [N]> or <PAM [4-128] [N]> Command	164
5.7.5.15	<PAYLOAD list/NONE [N=1..2]> Command	164
5.7.5.16	<ANNEX A/B/AB [N=1..2]> Command.....	164
5.7.5.17	<SETCLOCK list [N=1..2]> Command.....	164
5.7.5.18	<MULTIPAIR [2/OFF]> Command.....	164
5.7.5.19	<RESERVE [list]> Command	164
5.7.5.20	<G704 ON/OFF [N]> Command	165
5.7.5.21	<CRC4 ON/OFF [N]> Command	165
5.7.5.22	<AISGEN ON/OFF [N]>, <AISDET ON/OFF [N]> Commands	165
5.7.5.23	<WANTS [list] [N=1..4]> Command (Ethernet over E1)	165
5.7.5.24	<E1CLOCK {source} [N/{list}]> Command	165
5.7.5.25	<E1MODE [HDB3/AMI] [SHORT/LONG] [N]> Command	165
5.7.5.26	<ID string> Command	165
5.7.5.27	<DEFAULT [0-4]> Command	166
5.7.5.28	<DEFAULT EVERYTHING> Command.....	166
5.7.5.29	<DEFAULT DESC> Command.....	166
5.7.5.30	<SERNUM> Command	166
5.7.5.31	<GSCOMPAT ON/OFF> Command	166
5.7.5.32	<NMTHR> Command.....	166
5.7.5.33	<LATHR> Command.....	167
5.7.5.34	<PTMP [ADD/DEL] [IF]> Command	167
5.7.5.35	<PTMP SHOW> Command.....	167
5.7.5.36	<MODE N> Command	167
5.7.5.37	<LICENSE> Command	167
5.7.5.38	<LICENSE ADD [key]> Command.....	167
5.7.5.39	<RSIP> Command	167
5.7.5.40	<RSRATE [N]> Command.....	169
5.7.5.41	<RSFORMAT [Format]> Command.....	170
5.7.5.42	<RSDUPLEX [F/H] Command	170
5.7.5.43	<RS [232/485] Command	170
5.7.5.44	<RS TERM [ON/OFF] Command	170
5.7.5.45	<4RS {option} {value} [N]> Command	170

5.7.5.46	<IOIP {OPTION} [IF]> Command	170
5.7.5.47	<IOCONFIG> Command	173
5.7.5.48	<NET> Command	173
5.7.5.49	<H> Command	173
5.7.5.50	<NETCONFIG [N/R/S/B]> Command	174
5.7.5.51	<COSCONFIG [N/R/S/B]> Command	176
5.7.5.52	<RSTP DEFAULT> Command	177
5.7.5.53	<RSTP CONF> Command	177
5.7.5.54	<RSTP STATE> Command	178
5.7.5.55	<RSTP DIAG> Command	179
5.7.5.56	<RSTP [A..E] [ON/OFF]> Command	179
5.7.5.57	<RSTP [A..E] PRIO [value]> Command	179
5.7.5.58	<RSTP [A..E] VLAN [1..8]> Command	179
5.7.5.59	<RSTP [A..E] HELLO [2..10]> Command	179
5.7.5.60	<RSTP [A..E] FWD [4..30]> Command	179
5.7.5.61	<RSTP [A..E] MA [6..40]> Command	180
5.7.5.62	<RSTP [IFACE] PRIO [0..240]> Command	181
5.7.5.63	<RSTP [IFACE] PCOST [AUTO/1..200000000]> Command	181
5.7.5.64	<RSTP [IFACE] EDGE [ON/OFF]> Command	181
5.7.5.65	<PBVLAN [IF] [A..E]> Command	181
5.7.5.66	<MODE [IF] [ACC/TRUNK/MIX]> Command	182
5.7.5.67	<VLAN [IF] [1..8]> Command	182
5.7.5.68	<QOS [IF] [0..7]> Command	182
5.7.5.69	<ALLOW [IF] [VLAN list]> Command	183
5.7.5.70	<VID [1-8] ID> Command	183
5.7.5.71	<VLANNAME> Command	183
5.7.5.72	<MACLIST SHOW> Command	183
5.7.5.73	<MACLIST [IF] ADD [MAC]> Command	184
5.7.5.74	<MACLIST [IF] DEL [MAC/N]> Command	184
5.7.5.75	<MACFILTER [IF] [ON/OFF]> Command	184
5.7.5.76	<MACRULE [IF] [RULE]> Command	184
5.7.5.77	<DOT1X [IF] {OPTION}> Command	185
5.7.5.78	<JUMBO SIZE [OFF,1,2] [N]> Command	185
5.7.5.79	<SETIP X.X.X.X> Command	185
5.7.5.80	<NETMASK X.X.X.X> Command	185
5.7.5.81	<GATEWAY X.X.X.X> Command	185
5.7.5.82	<MTU> Command	185
5.7.5.83	<WANIDLE [1/7E]> Command	185
5.7.5.84	<ETHSD [10H/10F/100H/100F/AUTO/OFF] [N]> Command	186
5.7.5.85	<FC [ON/OFF] [N]> Command	186
5.7.5.86	<IRATE [speed/OFF] [N]> Command	186
5.7.5.87	<ERATE [speed/OFF]> Command	187
5.7.5.88	<CRATE [speed] [CoS] [WAN]> Command	187
5.7.5.89	<COS [QOS/VLAN] [x] [0..3/OFF]> Command	187
5.7.5.90	<SNMP [V1/V2C/V3] [ON/OFF]> Command	188
5.7.5.91	<SNMPACL> Command	188
5.7.5.92	<TRAP [1/2] [IP/OFF]> Command	188
5.7.5.93	<TRAP [1/2] [V1/V2C]> Command	188
5.7.5.94	<TRAP [1/2] V3 [RO/RW]> Command	188
5.7.5.95	<COMMUNITY> Command	188
5.7.5.96	<SNMPSET [ON/OFF]> Command	188
5.7.5.97	<SNMP [RO/RW] NAME> Command	188
5.7.5.98	<SNMP [RO/RW] AUTH [MODE]> Command	189
5.7.5.99	<SNMP [RO/RW] PRIV [MODE]> Command	189
5.7.5.100	<SYSNAME [SET]> Command	189
5.7.5.101	<SYSLOCATION [SET]> Command	189
5.7.5.102	<SYSCONTACT [SET]> Command	189
5.7.5.103	<RMONALARM [N] [ON/OFF]> Command	189
5.7.5.104	<RMONEVENT [N] [ON/OFF]> Command	190
5.7.5.105	<LLDP [ON/OFF]> Command	190
5.7.5.106	<LLDP DEFAULT> Command	190
5.7.5.107	<LLDP [PARAM] [VALUE]> Command	191
5.7.5.108	<LLDP [RX/TX] [ON/OFF]> Command	191

5.7.5.109	<LLDP INT VLAN [ON/OFF]> Command	191
5.7.5.110	<LLDP CONFIG> Command	192
5.7.5.111	<SNTP [1/2] [IP/OFF]> Command	192
5.7.5.112	<SNTP TZ [+/-]HH:MM> Command	192
5.7.5.113	<DST [WINTER/SUMMER]> Command	192
5.7.5.114	<DST [OFF/INFO/NAME]> Command	193
5.7.5.115	<SYSLOG [1/2] [IP/OFF]> Command	194
5.7.5.116	<[SSH TELNET HTTP] [ON/OFF]>	194
5.7.5.117	<SSH PORT [N]>	194
5.7.5.118	<SSL [SHOW/DEL] [options]>	194
5.7.5.119	<RADIUS [1/2] SECRET>	195
5.7.5.120	<RADIUS [1/2] TEST>	195
5.7.5.121	<RADIUS [1/2] [IP:P/OFF]>	195
5.7.5.122	<RADIUS RETRIES [0..10]>	196
5.7.5.123	<RADIUS TIMEOUT [1..5]>	196
5.7.5.124	<POECONFIG> Command	196
5.7.5.125	<POEPORT [ON/OFF] [N]> Command	196
5.7.5.126	<NETDEFAULT> Command	196
5.7.5.127	<FACTORY DEFAULT> Command	197
6	SOFTWARE DOWNLOAD MINIFLEX SWITCH (MF-MR2N-SW-12ETH,V2 ONLY)	198
6.1	Using FTP / SFTP servers	198
6.1.1	Command line interface	198
6.1.2	SNMP	198
7	SOFTWARE DOWNLOAD LINE CARDS, DINRAIL, MF-MR2N-SW-8ETH,V2 AND FLATRACK SWITCHES	200
7.1	Software Download via USB Port (LCT) Using Xmodem Protocol	200
7.2	Software Download via Ethernet (1K-Xmodem and Telnet)	203
8	SERVICE INSTRUCTIONS	204
8.1	General Requirements	204
8.2	Evaluation of the SHDSL Channel Quality and Operation Parameters	204
9	APPENDICES	205
9.1	Quick Installation Guide for FlexDSL MiniFlex	205
9.1.1	Enter a FlexDSL MiniFlex	205
9.1.2	Configure a FlexDSL MiniFlex	205
9.1.3	Checking of Correct Working	208
9.1.4	Problem with FlexDSL MiniFlex	208
9.2	Connector Description	209
9.2.1	Alarm Connector (ALARM)	209
9.2.2	DC Power Connector (DC1, DC2)	209
9.2.3	Ethernet SFP Connector	209
9.2.4	Gigabit Ethernet Connector	210
9.2.5	10/100Mbps Ethernet Connector	210
9.2.6	POE Line Card Ethernet Connector	210
9.2.7	Serial Line Card & DINrail RS-232 & RS-232/422/485 Connector	210
9.2.8	E1 Line Card & DINrail E1 120 Ohm Connector	211
9.2.9	E1 75 Ohm Connector	211
9.2.10	VoIP Line Card & DINrail FXO/FXS/VF Connector	211
9.2.11	SHDSL Line Card & DINrail xDSL Connector	212
9.2.12	Input / Output Line Card & DINrail Connector	212
9.2.13	DINrail Power Connector	213
9.2.14	Local Craft Terminal (USB) Connector (LCT)	213
9.2.15	FlatRack Power Connector (Power Supply Module)	213
9.2.16	Connector Hoods and Cord Retaining	214
10	TECHNICAL SPECIFICATION	215
10.1	Interfaces	215
10.1.1	1000Base-X Gigabit Ethernet (P1, P2)	215

10.1.2	1000Base-T, Gigabit Ethernet (P3, P4).....	215
10.1.3	10/100Base-T Ethernet (P5-P12, SHDSL, FOM, POE, Serial and Switch).....	215
10.1.4	10/100/1000Base-T Ethernet (GFOM, FlatRack, MF-MR2N-SW-8Eth,V2).....	215
10.1.5	SHDSL Line Interface	215
10.1.6	100Base-FX Ethernet (FOM, Serial RS-232 Interface).....	216
10.1.7	100Base-FX / 1000Base-X Ethernet (GFOM)	216
10.1.8	1000Base-X / 2500Base-X Ethernet (FlatRack, MF-MR2N-SW-8Eth,V2)	216
10.1.9	E1 Line Interface.....	216
10.1.10	Serial RS-232 / RS-232/422/485 Interface	216
10.1.11	FXO Interface	217
10.1.12	FXS Interface	217
10.1.13	Voice Frequency (Analog) Interface	217
10.1.14	E&M Interface	218
10.1.15	Digital Input / Output Interface.....	218
10.1.16	Local Craft Terminal (USB) Interface	218
10.1.17	Alarm Interface	218
10.2	Power Supply	219
10.2.1	MiniFlex Mini DSLAM (Subrack)	219
10.2.2	MiniFlex FlatRack	219
10.2.3	MiniFlex MiniRack.....	220
10.2.4	MiniFlex Dual Unit.....	220
10.2.5	MiniFlex DINrail.....	220
10.3	Environment	221
10.3.1	Climatic Conditions	221
10.3.2	EMC and Safety Standards.....	221
10.4	Physical Dimensions and Weight	222
10.4.1	MiniFlex Mini DSLAM (Subrack)	222
10.4.2	MiniFlex MiniRack.....	222
10.4.3	MiniFlex Dual Unit.....	222
10.4.4	MiniFlex SHDSL, Single FOM, POE DINrail	223
10.4.5	MiniFlex Dual FOM, GFOM, Switch, Serial, E1, VoIP, IO DINrail	223
10.4.6	FlatRack	223

VERSION CONTROL

Manual Version	Date	Software Version	Major changes to previous version
1.0	16.03.2010	1.0.0	Initial Version
1.1	28.04.2010	1.0.0	DC-Power pinning changed
1.2	24.08.2010	1.1.5	Small change in Safety regulations
1.3	6.09.2010	1.1.5	Switch functions fully described
1.4	30.11.2010	1.1.5	DSL DINrail included
1.5	03.01.2011	1.3.4	RSTP in DSL Line card and DINRail added
1.6	29.08.2011	1.4.8	FOM Card integrated
1.7	21.10.2011	1.4.8	Software download corrected
1.8	30.12.2011	1.4.8	MiniRack added
1.9	03.12.2012	1.4.37	Alarm Command updated, LINKNM added, Commands adapted, MAC Filtering
1.10	26.03.2013	1.4.38	FOM2, PoE and Switch added
1.11	02.05.2013	1.4.38	Jumper Settings PoE changed
1.12	25.06.2013	1.4.38	Default IP address added, Port numbering, PoE Attention
1.13	22.10.2013	1.5.4	SSH & RADIUS added
1.14	05.05.2014	1.6.6	Table 3.15 corrected, Serial Interface Units added, SNMP& RADIUS updated, Commands updated incl. SD-Card

Manual Version	Date	Software Version	Major changes to previous version
1.15	03.03.2015	2.5 (Main Switch)	New command to generate key length for SSH VLAN support for LACP Software Download MiniFlex Switch chapter rewritten
1.16	09.07.2015	1.6.19	LLDP chapter included
1.17	29.10.2015	1.6.19	MiniFlex Dual Unit included (mini-rack)
1.18	12.02.2016	1.7.2	E1 cards included (Line Cards & Standalone) 802.1x included
1.19	06.10.2016	1.7.2	Input voltage for 230VAC models corrected to 100-370VDC
1.20	24.10.2016	1.7.2 (MiniFlex) 1.8.0 (VoIP units)	MiniFlex VoIP Line Cards and DINrail units included RSTP DEFAULT and RSTP CONF commands updated RSTP FWD and RSTP MA commands added.
1.21	10.02.2017	1.7.5 (MiniFlex) 1.8.3 (VoIP units)	RADIUS Server setup with defined Service-Type Attribute RFC-4133 Entity-MIB partially supported Rate example improved for IRATE, CRATE, ERATE commands RSTP commands improved
1.22	23.02.2017	1.7.5 (DSL & E1) 1.8.3 (VoIP units) 1.0.16 (Switch, FOM, IO, PoE)	New VLANNAME command Input Output Card and DINrail support
1.23	26.06.2017	1.0.17 (GFOM)	GigaFOM included
1.24	06.03.2018	1.7.7 (DSL & E1) 1.0.18 (Switch, FOM, GFOM, IO, PoE, FlatRack)	FlatRack included WEB and CLI screenshots updated Command structures and many command descriptions updated STATUS L, STATUS IO, STATUSPOE, RESETPOE, 4RS, IOCONFIG, JUMBO SIZE, FACTORY DEFAULT commands added BERT Menu commands for E1 cards added Privileges table updated SW Download Linecards or DINrail Chapter corrected Quick Installation Guide for FlexDSL MiniFlex Chapter corrected Environment Chapter updated Formatting/Corrections
1.25	04.09.2018	2.0.6 (DSL & E1) 1.0.18 (Switch, FOM, GFOM, IO, PoE, FlatRack)	Traffic Encryption support, commands ENCODE and STATUS ENCODE. HTTPs support, commands SSL, TFTP CA CERT KEY, HTTPS [ON OFF]
1.26	15.10.2018	2.0.0 (MF-MR2N-SW-8Eth,V2)	New sub-rack versions with Gigabit Ethernet Backplane included: MF-MR2N-SW-12Eth,V2 MF-MR2N-SW-8Eth,V2 MF-MR2N,V2 AC/DC Power Supplies for FlatRack included: MF-PS230-FR05N,V1 MF-PS120-FR05N,V1 Selection Guide and General Information updated.

SAFETY REGULATIONS

IF THE UNIT IS NOT USED IN ACCORDANCE TO REGULATIONS DESCRIBED AND DEFINED IN THE CHAPTERS "TECHNICAL DESCRIPTION" AND "TECHNICAL SPECIFICATIONS", FLEXDSL TELECOMMUNICATIONS AG 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 ACCORDING TO THE SAFETY STANDARD IEC/EN 60950-1.

THE DISCONNECTING DEVICE FOR THE RACK IS THE MAINS PLUG AND/OR THE APPLIANCE COUPLER. THE MAINS PLUG AND/OR THE APPLIANCE COUPLER HAS/HAVE TO BE EASILY ACCESSIBLE AND THE MAINS PLUG HAS TO BE NEXT TO THE RACK IF THE MAINS PLUG SERVES AS THE DISCONNECTING DEVICE.

IT'S ONLY ALLOWED TO USE THE UNITS WITH HOUSINGS SUPPLIED FROM FLEXDSL TELECOMMUNICATIONS AG (SUBRACKS, MINIRACK, UTTX). THE RACK HAS TO BE CONNECTED PERMANENTLY TO A RELIABLE PROTECTIVE EARTH CONDUCTOR. THE LTU UNIT AND LINECARDS HAVE TO 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 FLEXDSL 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

FlexDSL MiniFlex Models	Functionality	19", 2U Subrack/Minirack	19", 1/2 U Subrack/Minirack	Backside Mountable	18-72 VDC	90-264 VAC, 47-63 Hz	Redundancy Possibility	Front Panel		*BP	Point-to-Point	Point-to-Multipoint	Ring Applications	Spanning Tree	Link Aggregation	VLAN, QoS	Port Security	Multicast	Remote Power Receiver	Remote Power Source	Console Port Management	Telnet Management	Web Management	SNMP Management
								Ethernet 10/100Base-T	Ethernet 10/100Base-T															
MF-MR2N-SW-8Eth,V2		✓					✓				✓	✓	✓	✓	✓	✓	✓				✓	✓	✓	✓
MF-MR2N-SW-12Eth,V2		✓					✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓			✓	✓	✓	✓
MF-MR2N,V2		✓					✓																	
Power Supplies:																								
MF-PS48, V1				✓	✓		✓																	
MF-PS110/230, V1				✓		✓	✓																	

***BP:** back plane connection to Line Cards

FlexDSL MiniFlex Models	Functionality	19", 2U Subrack/Minirack	19", 1/2 U Subrack/Minirack	Backside Mountable	18-72 VDC	85-132 VAC, 47-63 Hz	170-264 VAC, 47-63 Hz	Redundancy Possibility	FP*		BP** Ethernet 10/100/1000Base-T	Point-to-Point	Point-to-Multipoint	Ring Applications	Spanning Tree	Link Aggregation	VLAN, QoS	Port Security	Multicast	Remote Power Receiver	Remote Power Source	Console Port Management	Telnet Management	Web Management	SNMP Management
									Ethernet 10/100/1000Base-T	Ethernet 1000/2500Base-X															
MF-FR05N-SW-2Eth,V1			✓					✓	✓	✓	✓	✓	✓	✓		✓	✓					✓	✓	✓	✓
MF-FR05N,V1			✓					✓																	
Power Supplies:																									
MF-PS48-FR05N,V1				✓	✓			✓																	
MF-PS230-FR05N,V1				✓			✓	✓																	
MF-PS120-FR05N,V1				✓		✓		✓																	

***FP:** front panel

****BP:** back plane connection to Line Cards

FlexDSL MiniFlex Models	Functionality	19", 2U Subrack/Minirack	19", 1/2 U Subrack/Minirack	2U Minirack, Rail or Wall	9-36 VDC	18-72 VDC	90-264 VAC, 47-63 Hz	Redundancy Possibility	Ethernet 10/100Base-T	Gigabit Ethernet 1000Base-T	Gigabit Ethernet SFP	Point-to-Point	Point-to-Multipoint	Ring Applications	Spanning Tree	Link Aggregation	VLAN, QoS	Port Security	Remote Power Receiver	Remote Power Source	Console Port Management	Telnet Management	Web Management	SNMP Management
MF-MR-RAIL-2U4S,V1				✓		✓		✓																
MF-DU-RAIL-2U2S-12V,V1				✓	✓																			
MF-DU-RAIL-2U2S-24V,V1				✓		✓																		
MF-DU-RAIL-2U2S-230V,V1				✓		✓	✓																	

FlexDSL MiniFlex Line Cards	Standalone	Rail Mounting	MiniFlex Subrack Module	Protected Housing	Single Pair	Dual Pair Bonding	Dual Pair Standby	Point-to-Point	Point-to-Multipoint	E1 (1200hm)	E1 (750hm) optional	TDM over IP	Ethernet Bridge	Ethernet Add/Drop	RS-232/422/485 Interface	RS-232 Interface	FXS Interface	FXO Interface	VF (Analog) Interface	E&M Type V support	Remote Power Receiver	Input / Output	Remote Power Source	Console Port Management	Telnet Management	Web Management	SNMP Management
MF-PAM-SR2L-2Eth,V1	✓		✓		✓	✓	✓	✓	✓				✓	✓										✓	✓	✓	✓
MF-FOM-SRL,V1	✓		✓		✓			✓	✓				✓	✓										✓	✓	✓	✓
MF-FOM-SR2L-2Eth,V1	✓		✓		✓		✓	✓	✓				✓	✓										✓	✓	✓	✓
MF-FOM-SR2L-SER/Eth,V1	✓		✓		✓		✓	✓	✓				✓	✓	✓	✓								✓	✓	✓	✓
MF-POE-SRL-2Eth,V1	✓		✓					✓	✓				✓	✓										✓	✓	✓	✓
MF-SW-SRL-8Eth,V1	✓		✓					✓	✓				✓	✓										✓	✓	✓	✓
MF-SER-SRL-4V24,V1	✓		✓					✓	✓							✓								✓	✓	✓	✓
MF-TDM-SRL-4E1B,V1	✓		✓					✓	✓	✓		✓												✓	✓	✓	✓
MF-VOIP-SRL-2Eth/2FXS,V1	✓		✓					✓	✓				✓				✓							✓	✓	✓	✓
MF-VOIP-SRL-2Eth/2FXO,V1	✓		✓					✓	✓				✓					✓						✓	✓	✓	✓
MF-VOIP-SRL-2Eth/2VF,V1	✓		✓					✓	✓				✓						✓	✓				✓	✓	✓	✓
MF-IO-SRL-4I4O/Eth,V1	✓		✓					✓	✓				✓									✓		✓	✓	✓	✓
MF-GFOM-SR2L-2Eth,V1	✓		✓		✓		✓	✓	✓				✓	✓										✓	✓	✓	✓

FlexDSL MiniFlex DINrail	Functionality																												
	Standalone	Rail Mounting	Protected Housing	Single Pair	Dual Pair Bonding	Dual Pair Standby	Point-to-Point	Point-to-Multipoint	E1 (1200hm)	TDM over IP	RS-232/422/485 Interface	RS-232 Interface	Ethernet Bridge	Ethernet Add/Drop	FXS Interface	FXO Interface	VF (Analog) Interface	E&M Type V support	Input / Output	9-18 VDC	18-72 VDC	90-264 VAC, 47-63 Hz	Remote Power Receiver	Remote Power Source	Console Port Management	Telnet Management	Web Management	SNMP Management	
MF-PAM-RAIL2N-2Eth-12V,V1	✓	✓		✓	✓	✓	✓	✓					✓	✓						✓					✓	✓	✓	✓	
MF-PAM-RAIL2N-2Eth-24V,V1	✓	✓		✓	✓	✓	✓	✓					✓	✓							✓					✓	✓	✓	✓
MF-PAM-RAIL2N-2Eth-230V,V1	✓	✓		✓	✓	✓	✓	✓					✓	✓								✓				✓	✓	✓	✓
MF-FOM-RAILN-Eth-24V,V1	✓	✓		✓			✓						✓								✓					✓	✓	✓	✓
MF-FOM-RAILN-Eth-230V,V1	✓	✓		✓			✓						✓									✓				✓	✓	✓	✓
MF-FOM-RAIL2N-2Eth-24V,V1	✓	✓		✓		✓	✓	✓					✓	✓							✓					✓	✓	✓	✓
MF-FOM-RAIL2N-2Eth-230V,V1	✓	✓		✓		✓	✓	✓					✓	✓								✓				✓	✓	✓	✓
MF-POE-RAILN-Eth-24V,V1	✓	✓					✓						✓																
MF-SW-RAIL-4Eth-24V,V1	✓	✓					✓	✓					✓	✓							✓				✓	✓	✓	✓	
MF-SW-RAIL-4Eth-230V,V1	✓	✓					✓	✓					✓	✓								✓				✓	✓	✓	✓
MF-FOM-RAIL2N-2V24-24V,V1	✓	✓		✓		✓	✓	✓				✓	✓	✓							✓				✓	✓	✓	✓	✓
MF-FOM-RAIL2N-2V24-230V,V1	✓	✓		✓		✓	✓	✓				✓	✓	✓								✓				✓	✓	✓	✓
MF-FOM-RAIL2N-SER/Eth-24V,V1	✓	✓		✓		✓	✓	✓			✓	✓	✓	✓							✓				✓	✓	✓	✓	✓
MF-FOM-RAIL2N-SER/Eth-230V,V1	✓	✓		✓		✓	✓	✓			✓	✓	✓	✓								✓				✓	✓	✓	✓
MF-TDM-RAILN-4E1B/2Eth-24V,V1	✓	✓					✓	✓	✓	✓			✓	✓							✓					✓	✓	✓	✓
MF-TDM-RAILN-4E1B/2Eth-230V,V1	✓	✓					✓	✓	✓	✓			✓	✓								✓				✓	✓	✓	✓
MF-VOIP-RAILN-2Eth/2FXS-24V,V1	✓	✓					✓	✓					✓		✓						✓					✓	✓	✓	✓
MF-VOIP-RAILN-2Eth/2FXS-230V,V1	✓	✓					✓	✓					✓		✓							✓				✓	✓	✓	✓
MF-VOIP-RAILN-2Eth/2FXO-24V,V1	✓	✓					✓	✓					✓			✓					✓					✓	✓	✓	✓
MF-VOIP-RAILN-2Eth/2FXO-230V,V1	✓	✓					✓	✓					✓			✓					✓					✓	✓	✓	✓
MF-VOIP-RAILN-2Eth/2VF-24V,V1	✓	✓					✓	✓					✓				✓	✓			✓					✓	✓	✓	✓
MF-VOIP-RAILN-2Eth/2VF-230V,V1	✓	✓					✓	✓					✓				✓	✓				✓				✓	✓	✓	✓
MF-IO-RAILN-4I4O/Eth-24V,V1	✓	✓					✓	✓					✓						✓		✓					✓	✓	✓	✓
MF-IO-RAILN-4I4O/Eth-230V,V1	✓	✓					✓	✓					✓						✓			✓				✓	✓	✓	✓
MF-GFOM-RAIL2N-2Eth-24V,V1	✓	✓		✓		✓	✓	✓					✓	✓							✓					✓	✓	✓	✓
MF-GFOM-RAIL2N-2Eth-230V,V1	✓	✓		✓		✓	✓	✓					✓	✓								✓				✓	✓	✓	✓

*Note: TDM over IP is available by using a special SW.

2 PRECAUTION

The present document describes devices of the MiniFlex 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. FLEXDSL TELECOMMUNICATIONS AG 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. FLEXDSL TELECOMMUNICATIONS AG 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.

**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 FOR THE PURPOSE OF REDUCING NOISE INTERFERENCE AND SAFETY HAZARDS.

3 TECHNICAL DESCRIPTION

3.1 General Information about FlexDSL MiniFlex

The FlexDSL MiniFlex platform is a special part of the Orion3 product family. Beside of having up to 10 dual Orion3 SHDSL.bis Extended line cards there is a managed layer 2 Ethernet switch included. This switch has 6 auto-sensing front accessible 10/100/1000Base-T ports as well as 2 Ethernet 1000/2500Base-X SFP ports that can be used for fiber or copper connectivity. The inside backplane connects this switch to all MiniFlex line cards through additional 10 Ethernet 10/100/1000Base-T ports.

The FlexDSL Orion3 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 (Orion1 & Orion2). The FlexDSL Orion3 supports TC-PAM8/16/32 and the new TC-PAM64/128 line-coding. The support of these line codes ensures compatibility with existing SHDSL equipment that is already installed, in order to protect customer investments, while at the same time providing an upgrade path to the newest DSL technologies.

SHDSL.bis Extended allows symmetrical data transmission at speeds up to 15.2Mbps over a single pair of copper. In addition, the dual Orion3 line card also supports DSL channel bonding for 2 copper pairs in order to achieve speeds to 30.4Mbps! Using the link aggregation feature of the additional integrated switch, the FlexDSL MiniFlex can transmit up to 300Mbps over 20 copper pairs. This incredible speed makes Fiber installations in a lot of places needless.

Like all FlexDSL Orion products, the MiniFlex and his Orion3 SHDSL.bis Extended line cards are based on industrial components and are manufactured according to highest quality standards providing additional value due to the extended temperature range and higher reliability. The combination of comprehensive functions providing maximum flexibility together with the higher quality of the FlexDSL MiniFlex makes it the perfect choice for your DSL needs.

The FlexDSL **MiniFlex** product family consists of:



MiniFlex Subrack (Line Termination Units)

Usually Central Office Equipment.

Can be locally powered with DC and AC



MiniFlex FlatRack (Line Termination Units)

Usually Central Office Equipment.

Can be locally powered with DC and AC



MiniFlex MiniRack (Network Termination Units)

Both, Central Office and Customer Premise Equipment.

Can be locally powered with DC



MiniFlex Dual Unit (Network Termination Units)

Both, Central Office and Customer Premise Equipment.
Can be locally powered with DC or AC



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.



RR devices (Repeater, Regenerator)

Increase (double) the distance.

RR's can be powered:

- locally with DC voltage.
- remotely.

Supported management features:

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

Supported operating modes:

- Point-to-Point, Point-to-Multipoint and Ring Applications

3.2.1 SubRacks with Integrated Switch

3.2.1.1 SubRack with Integrated Gigabit Ethernet Switch (1000/2500Base-X uplinks)

The SubRack is designed for a 19" rack and has a height of 2U (89mm). The depth is 180mm without any power supply and 248mm with the power supply equipped. All connections (except AC power!) are accessible from the front.

Beside the connection to two DC power supplies and the alarm relay outputs, there is an integrated layer 2 managed Gigabit Ethernet switch with the following main functionalities:

- RSTP IEEE 801.1d-2004
- Jumbo Frames support (up to 10240 bytes)
- IEEE 802.1q VLANs, Port-based VLAN
- 4 Priority Queues/port, Bandwidth Control per Port
- MAC-filtering
- IEEE 802.1p
- IEEE 802.1x Access Control and RADIUS support
- LLDP IEEE 802.1AB
- Management: Local Console Port (USB), Telnet/SSH, Web, SNMP v1, v2c, v3

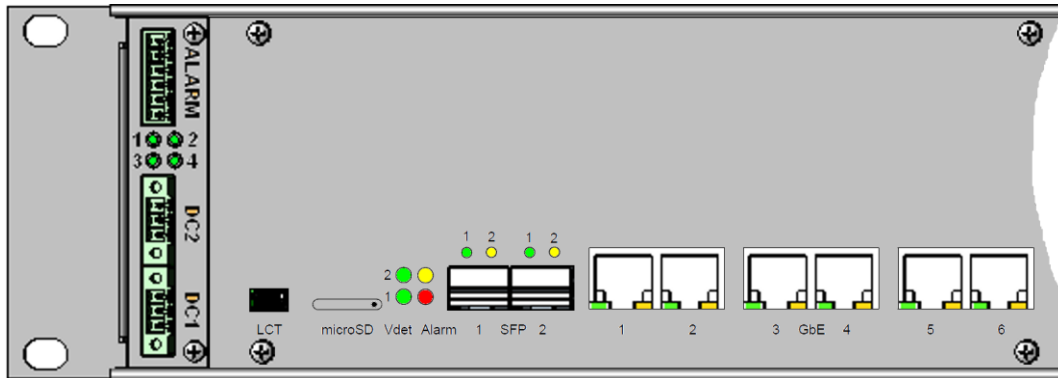


Figure 3.2 SubRack Frontplate

Element		Description
ALARM		ALARM Connector with Urgent/NonUrgent Alarm (6-Pin Phoenix Mini Combicom MC 1,5/6-G-3,5)
LED-1	LED-2	LED Red Urgent ALARM
LED-3	LED-4	LED Green DC1 ok
DC2		Power Supply Connector DC2 (3-Pin Phoenix Mini Combicom MC 1,5/3-GF-3,5)
DC1		Power Supply Connector DC1 (3-Pin Phoenix Mini Combicom MC 1,5/3-GF-3,5)
LCT		USB Connector Local Craft Terminal
microSD		Tray for microSD card
Vdet	2	LED Status DC2 (Green – DC2 is active / Off – DC2 is inactive)
	1	LED Status DC1 (Green – DC1 is active / Off – DC1 is inactive)
Alarm	Minor	Minor Alarm LED (Amber – non-urgent alarm is present / Green – no non-urgent alarm is detected)
	Major	Major Alarm LED (Red – urgent alarm is present / Green – no urgent alarm is detected)
SFP-1	SFP-2	SFP 1000/2500Base-X Ethernet Uplink Port 1
LED-1		LED1 Green Status SFP Interface
LED-2		LED2 Amber Status SFP Interface
GbE-1	GbE-2	RJ-45 10/100Mbps Ethernet Port 1 + two LED
GbE-3	GbE-4	RJ-45 10/100Mbps Ethernet Port 3 + two LED
GbE-5	GbE-6	RJ-45 10/100Mbps Ethernet Port 5 + two LED
Ethernet and SFP LED behavior:		
Eth Mode:		green LED
10H/10F		Act Blinking (340ms)
100H/100F		Act Blinking (170ms)
1000H/1000F		Act Blinking (84ms)
2500F		Act Blinking (84ms)
		Link ON

Table 3.1 Connectors and LEDs on the front panel of SubRack MiniFlex and LED behavior.

Subrack LAN port numbering:

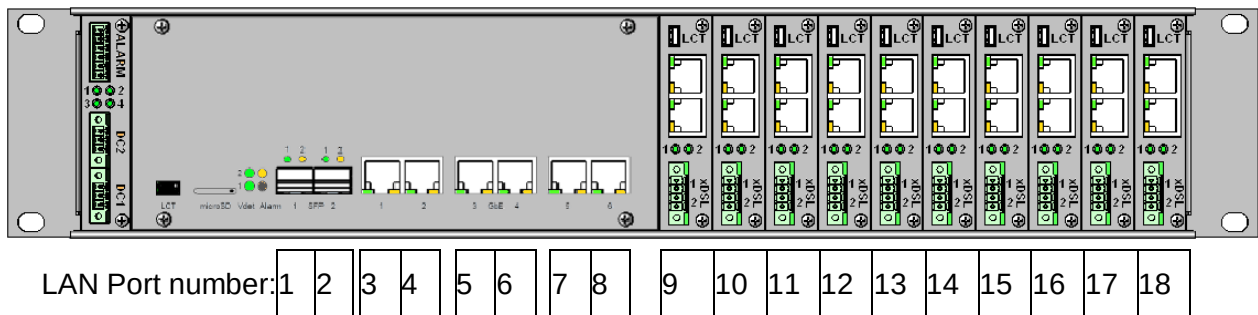


Figure 3.3 MiniFlex SubRack LAN Port numbering

LAN Port	Description
LAN1	LAN2
LAN3	LAN4
LAN5	LAN6
LAN7	LAN8
LAN9	LAN10
LAN11	LAN12
LAN13	LAN14
LAN15	LAN16
LAN17	LAN18

*BP: back plane connection to Line Card

Table 3.2 SubRack MiniFlex Ethernet Port Numbering.

3.2.1.2 SubRack with Integrated Fast Ethernet Switch (Gigabit Ethernet uplinks)

The SubRack is designed for a 19" rack and has a height of 2U (89mm). The depth is 180mm without any power supply and 248mm with the power supply equipped. All connections (except AC power!) are accessible from the front.

Beside the connection to two DC power supplies and the alarm relay outputs, there is an integrated layer 2 managed Ethernet switch with the following main functionalities:

Spanning Tree and Ethernet Ring

- IEEE 802.1D Spanning Tree Protocol (STP)
- IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)
- IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)
- Ethernet Ring Protection Mechanism, 50ms rapid In switching and protection
- Port Mirroring, Jumbo Frames support (up to 9216 bytes)

VLAN

- 4K IEEE 802.1q VLANs, Port-based VLAN, MAC-Based VLAN, Private VLAN
- GVRP, Q-in-Q, VLAN Translation

Link Aggregation

- Static Trunk, Dynamic Trunk, IEEE 802.3ad LACP, Load Balancing

Multicast Features

- IGMP v1. v2, v3, IGMP Snooping, IGMP Groups, Multicast VLAN

Quality of Service (QoS)

- 8 Priority Queues/port, Bandwidth Control per Port
- WRR, Strict Priority, WDRR, WRR+Strict Priority
- 802.1p, Port-Based CoS, CoS based on MAC DA/SA

Access Control List

- MAC+Port Binding, VLAN+Port Binding

Port Security

- Trust Port, Port Blocking, Private VLAN, Port Powering Off
- MAC address learning limit per port, DoS check, Management IP list

Management

- Local Console Port (USB), Telnet/SSH, Web, SNMP v1 and V2c

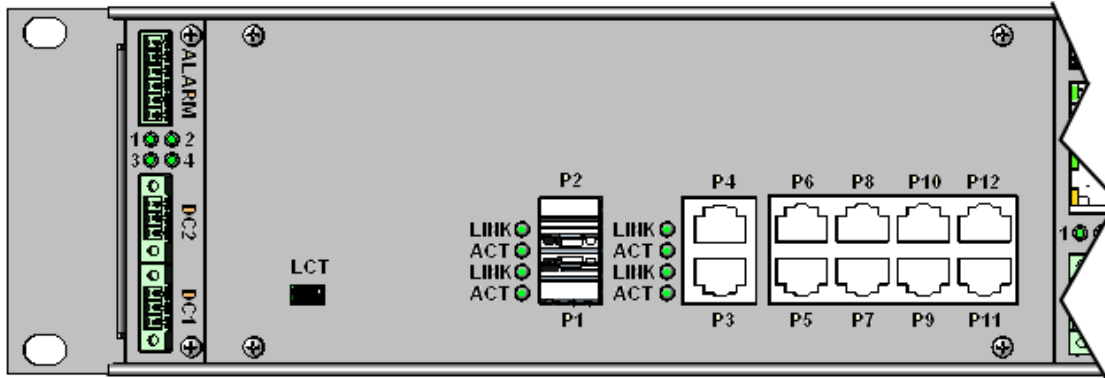


Figure 3.4 SubRack Frontplate

Element	Description
ALARM	ALARM Connector with Urgent/NonUrgent Alarm (6-Pin Phoenix Mini Combicom MC 1,5/6-G-3,5)
LED-1	LED Red Urgent ALARM
LED-2	LED Red NonUrgent ALARM
LED-3	LED Green DC1 ok
LED-4	LED Green DC2 ok
DC2	Power Supply Connector DC2 (3-Pin Phoenix Mini Combicom MC 1,5/3-GF-3,5)
DC1	Power Supply Connector DC1 (3-Pin Phoenix Mini Combicom MC 1,5/3-GF-3,5)
LCT	USB Connector Local Craft Terminal
P1	SFP Gigabit Ethernet Uplink Port 1
P2	SFP Gigabit Ethernet Uplink Port 2
LINK	LED Green Link corresponding Port 1-4
ACT	LED Green Activity corresponding Port 1-4
P3	RJ-45 Gigabit Ethernet Uplink Port 3
P4	RJ-45 Gigabit Ethernet Uplink Port 4
P5	RJ-45 10/100Mbps Ethernet Port 5 + two LED
P6	RJ-45 10/100Mbps Ethernet Port 6 + two LED
P7	RJ-45 10/100Mbps Ethernet Port 7 + two LED
P8	RJ-45 10/100Mbps Ethernet Port 8 + two LED
P9	RJ-45 10/100Mbps Ethernet Port 9 + two LED
P10	RJ-45 10/100Mbps Ethernet Port 10 + two LED
P11	RJ-45 10/100Mbps Ethernet Port 11 + two LED
P12	RJ-45 10/100Mbps Ethernet Port 12 + two LED

Table 3.3 Connectors and LEDs on the front panel of SubRack MiniFlex.

Subrack Ethernet port numbering:

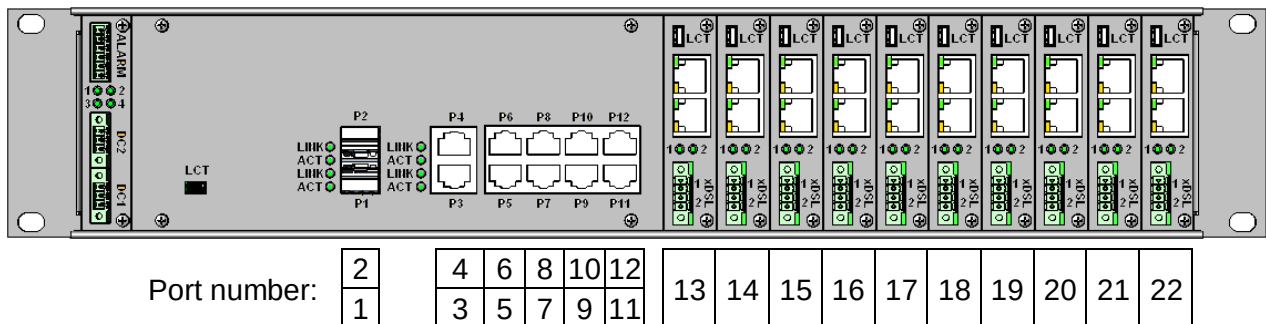


Figure 3.5 MiniFlex SubRack Ethernet Port numbering

Ethernet Port	Description
P1	Front: SFP Gigabit Ethernet Uplink
P2	Front: SFP Gigabit Ethernet Uplink
P3	Front: RJ-45 Gigabit Ethernet Uplink
P4	Front: RJ-45 Gigabit Ethernet Uplink
P5	Front: RJ-45 10/100Mbps Ethernet
P6	Front: RJ-45 10/100Mbps Ethernet
P7	Front: RJ-45 10/100Mbps Ethernet
P8	Front: RJ-45 10/100Mbps Ethernet
P9	Front: RJ-45 10/100Mbps Ethernet
P10	Front: RJ-45 10/100Mbps Ethernet
P11	Front: RJ-45 10/100Mbps Ethernet
P12	Front: RJ-45 10/100Mbps Ethernet
P13	Line Card 1: BP* 10/100Mbps Ethernet
P14	Line Card 2: BP* 10/100 Mbps Ethernet
P15	Line Card 3: BP* 10/100 Mbps Ethernet
P16	Line Card 4: BP* 10/100 Mbps Ethernet
P17	Line Card 5: BP* 10/100 Mbps Ethernet
P18	Line Card 6: BP* 10/100 Mbps Ethernet
P19	Line Card 7: BP* 10/100 Mbps Ethernet
P20	Line Card 8: BP* 10/100 Mbps Ethernet
P21	Line Card 9: BP* 10/100 Mbps Ethernet
P22	Line Card 10: BP* 10/100 Mbps Ethernet

*BP: back plane connection to Line Card

Table 3.4 SubRack MiniFlex Ethernet Port Numbering.

3.2.2 Power Supplies for the Subrack

There are two different power supplies available. One is for DC input power and the other one is for AC input power. Each MiniFlex can use one or two power supplies depending on the need of redundancy.

The power connector for the DC power is on the front of the subrack and the connector for the AC power is on the back directly at the power supply.

3.2.3 FlatRack with Integrated Gigabit Ethernet Switch

The 5 slot FlatRack is designed for a 19" rack and has a height close to 1/2U (24mm). Device occupies only 1U (43.6mm) in the rack together with cooling space. The depth is 293mm. All Line Card connections are accessible from the front:



Figure 3.6 FlexDSL MiniFlex FlatRack (front view with five MiniFlex Line Cards installed)

Besides five card-slots in front, there are two slots in the back for Power Supplies. Power Connectors and LEDs are in the back.

Device has Gigabit Ethernet backplane. The central slot in the back is for Integrated Gigabit Ethernet Switch. All Switch connections are in the back.

The Integrated Gigabit Ethernet Switch has the following main functionalities:

- RSTP IEEE 801.1d-2004
- Jumbo Frames support (up to 10240 bytes)
- IEEE 802.1q VLANs, Port-based VLAN
- 4 Priority Queues/port, Bandwidth Control per Port
- MAC-filtering
- IEEE 802.1p
- IEEE 802.1x Access Control and RADIUS support
- LLDP IEEE 802.1AB
- Management: Local Console Port (USB), Telnet/SSH, Web, SNMP v1, v2c, v3

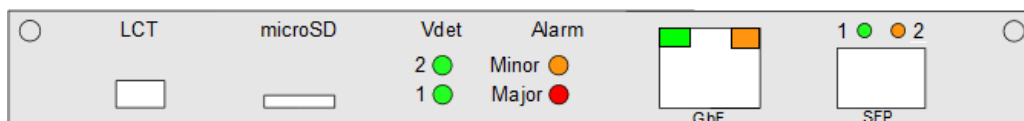


Figure 3.7 Integrated FlatRack Gigabit Ethernet Switch (back view)

Element	Description
LCT	USB Connector Local Craft Terminal
microSD	Tray for microSD card
Vdet	2 LED Status DC2 (Green – DC2 is active / Off – DC2 is inactive)
	1 LED Status DC1 (Green – DC1 is active / Off – DC1 is inactive)
Alarm	Minor Minor Alarm LED (Amber – non-urgent alarm is present / Green – no non-urgent alarm is detected)
	Major Major Alarm LED (Red – urgent alarm is present / Green – no urgent alarm is detected)
GbE	RJ-45 Gigabit Ethernet Uplink + two LED
LED-1	LED1 Green Status SFP Interface
LED-2	LED2 Amber Status SFP Interface
SFP	SFP 1000Base-X or 2500Base-X Ethernet Uplink

Table 3.5 Connectors and LEDs on the FlatRack Switch panel with behavior

Besides connectors and LEDs on the back panel, the Integrated Switch has seven Ethernet 10/100/1000BaseT ports to the backplane (see Figure below for LAN ports numbering):

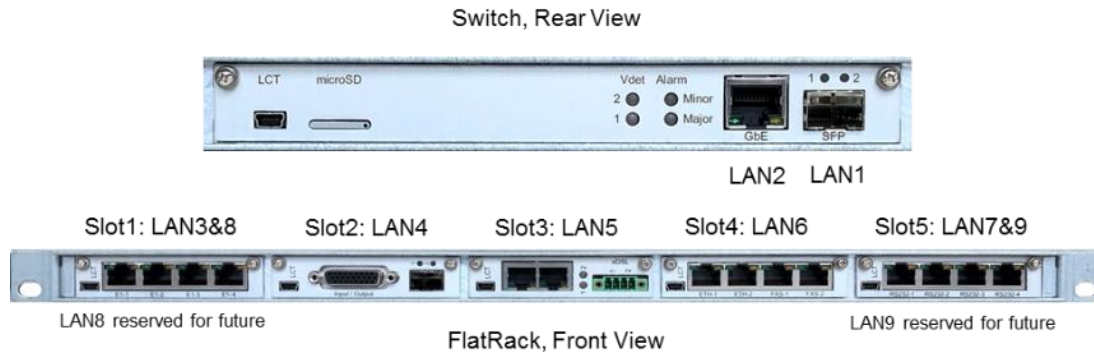


Figure 3.8 MiniFlex FlatRack LAN Port numbering

ATTENTION

The PoE and Managed Switch line cards cannot be used with the FlatRack. The next HW releases of the cards will be supported in the future

Please refer to “UM_FlexDSL_MiniFlex_FlatRack_v1-x” User Manual for more details.

3.2.4 Power Supply for the FlatRack

There are 3 different power supplies available. One is for 18-72VDC input power, the second is for 170-264VAC input power and the third is for 85-132VAC input power. The power connector(s) is on the back of the FlatRack.

Please use always the original Phoenix Combicon Connector that is included into delivery. Note, that the connectors supplied with MiniFlex DINrail units are not suitable for MiniFlex FlatRack:



Figure 3.9 FlatRack Power Supply

Power LED behavior:		
FlatRack without Switch (MF-FR05N,V1)	Green	Power Supply Module is active
	OFF	Power Supply Module is inactive
FlatRack with Switch (MF-FR05N-SW-2Eth,V1)	Green	Input Voltage is present
	OFF	No Input Voltage

Table 3.6 Power LED behavior

Please refer to “UM_FlexDSL_MiniFlex_FlatRack_v1-x” User Manual for more details.

3.2.5 MiniRack

The 5 slot MiniRack has a height of 2U (88mm) and a width of only 110mm. The depth is 181mm with power supply equipped. All connections are accessible in the front. There are connectors available for to two DC power inputs and the alarm relay outputs (Power supply is in slot 1).

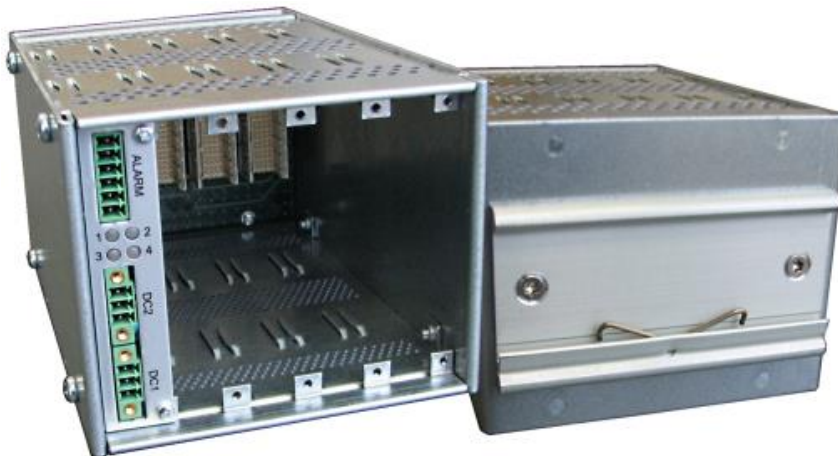


Figure 3.10 MiniRack Front- and Backside

Element		Description	
ALARM		ALARM Connector with Urgent/NonUrgent Alarm (6-Pin Phoenix Mini Combicom MC 1,5/6-G-3,5)	
LED-1	LED-2	LED Red Urgent ALARM	LED Red NonUrgent ALARM
LED-3	LED-4	LED Green DC1 ok	LED Green DC2 ok
DC2		Power Supply Connector DC2 (3-Pin Phoenix Mini Combicom MC 1,5/3-GF-3,5)	
DC1		Power Supply Connector DC1 (3-Pin Phoenix Mini Combicom MC 1,5/3-GF-3,5)	

Table 3.7 Connectors and LEDs on the front panel of MiniRack MiniFlex.

MiniRack Ethernet port numbering (when Switch is in slot 2, Line Cards in slot 3-5):



Port number:

1	5	6	7
2	8		
3			
4			

Figure 3.11 MiniFlex MiniRack Ethernet Port numbering

Ethernet Port		Description	
P1	P2	Switch Front: RJ-45 10/100Mbps Ethernet	Switch Front: RJ-45 10/100Mbps Ethernet
P3	P4	Switch Front: RJ-45 10/100Mbps Ethernet	Switch Front: RJ-45 10/100Mbps Ethernet
P5	P8	Line Card 1: RJ-45 10/100Mbps Ethernet	Line Card 1: POE-2, if PoE Line Card used
P6		Line Card 2: RJ-45 10/100Mbps Ethernet	
P7		Line Card 3: RJ-45 10/100Mbps Ethernet	

Table 3.8 SubRack MiniFlex Ethernet Port Numbering.

The backplane connections can be switched with a hidden Dip-Switch behind the DIN-rail clip. Please see in the following figure the standard backplane connections.

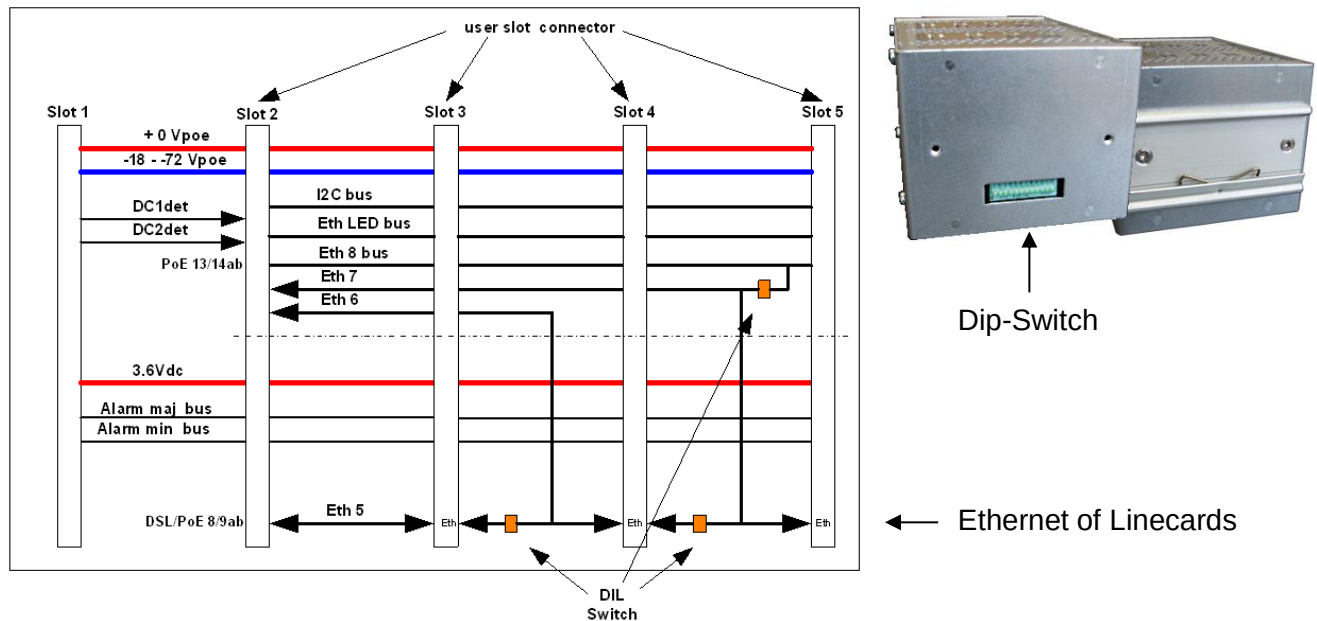


Figure 3.12 MiniRack backplane schematics

All backplane Ethernet interfaces of the available Line Cards (please see Eth5, Eth6, Eth7 on the schematics) are connected to slot 2. There is an Ethernet Switch Line Card available for slot 2. But the MiniRack can be used without the Ethernet Switch Line Card and the Ethernet interfaces can be connected as follows by the Dip-Switch:

Switch	Description
S1-S4 ON	Ethernet Slot5 (Eth7, P7) is connected to Ethernet Bus (Eth8 Bus, P8)
S5-S8 ON	Ethernet Slot4 (Eth6, P6) is connected to Ethernet Slot5 (Eth7, P7)
S9-S12 ON	Ethernet Slot3 (Eth5, P5) is connected to Ethernet Slot4 (Eth6, P6)

Table 3.9 Switch positions of MiniRack MiniFlex.

For the MiniFlex MiniRack unit there is a Wallmount Kit (MF-MR-RAIL-WALLMOUNT,V1) available.

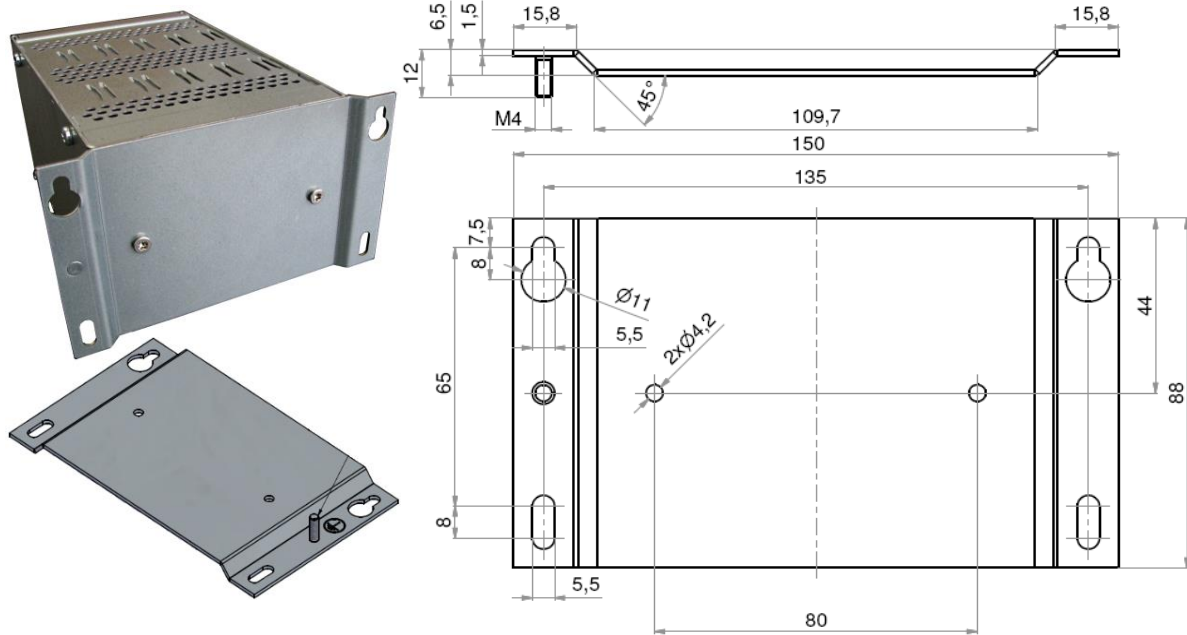


Figure 3.13 MiniRack Wallmount Kit

3.2.6 Dual Unit

The 2 slot Dual Unit has a height of 2U (87mm) and a width of only 50mm. The depth is 190mm with an included power supply. With the Dual Unit DIN-rail mini-rack you can combine different line cards for a high integrated solution according your needs. The Dual Unit has already integrated a DC or AC power supply as well as an alarm interface (urgent and not urgent). Both line cards are connected through the backplane by an Ethernet interface.



Figure 3.14 Dual Unit Front- and Backside



ATTENTION

The POE (power over Ethernet) line card cannot be used with the Dual Unit models MF-DU-RAIL-2U2S-230V, V1 and MF-DU-RAIL-2U2S-12V, V1. Please use only MF-DU-RAIL-2U2S-24V, V1 when POE is required.

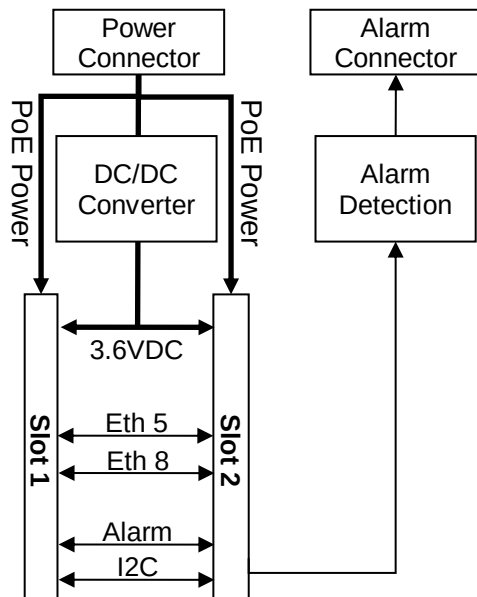


Figure 3.15 Dual Unit backplane schematics

3.2.7 SHDSL Line Card

The SHDSL Line Card has two DSL lines with the possibility for transmission speed up to 15.2Mbit/s per line. It means that one Line Card can transmit up to 30.4Mbit/s with the pair bonding. There is also a local craft terminal on every line card to manage and configure if there is any Ethernet failure of the main switch in the MiniFlex.

The two additional Ethernet interfaces on the front of the SHDSL line card can be used to manage the line card or to have an additional Ethernet interface to transmit data in every configured direction of the MiniFlex.



Figure 3.16 SHDSL Line Card

Element		Description
LCT		USB Connector Local Craft Terminal
		RJ-45 10/100Mbps Ethernet Port 1 + two LED
		RJ-45 10/100Mbps Ethernet Port 2 + two LED
LED-1	LED-2	LED Red/Green/Amber xDSL 1 LED Red/Green/Amber xDSL 2
xDSL 1/2		xDSL Connector 1/2 (4-Pin Phoenix Mini Combicom MC 1,5/4-GF-3,5)

Table 3.10 Connectors and LEDs on the front panel of SHDSL Line Card.

3.2.7.1 Line Card SHDSL Interface

The SHDSL 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.

Mode	Coding Type	Baserate	Standard	Transmission Data Rate
Master/Slave Fix Configuration	PAM16	3..60	Annex A, Annex B, Annex AB (autodetection)	Baserate* 64 kbit/s
	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 3.11 Line settings per SHDSL interface, single pair, normal mode.

Mode	Coding Type	Baserate	Standard	Transmission Data Rate
Master/Slave Fix Configuration	PAM4	2..39	Annex A, Annex B, Annex AB (autodetection)	Baserate* 64 kbit/s
	PAM8	3..79		
	PAM16	1..119		
	PAM32	1..159		
	PAM64	2..199		
	PAM128	4..238		
Master Autodetection	PAM16	Auto (1..119)	Annex AB (autodetection)	
	PAM32	Auto (1..159)		
	PAM4/8/64/128	Not possible		
Slave Autodetection	Auto (PAM4/8/16/32/64/128)	Auto (1..238)	Annex AB (autodetection)	

Table 3.12 Line settings per SHDSL interface, single pair, extended mode.

3.2.7.1.1 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.

3.2.7.1.2 Multipair Mode

If 2 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 transmission capacity. This transmission is also plesiochronous. In multipair mode, one SHDSL channel serves as a “master” channel, while the other SHDSL channel serves as “slave” channel. If the link in one channel fails, the links in the other channel break too and the procedure of connection/activation restarts. 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 extended mode, multipair operation is not possible!

3.2.7.1.3 Automatic Link Configuration

The SHDSL line card supports 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
- Links with regenerators

When the automatic configuration is used, the Slave-Modems and Regenerators receive nearly all configuration parameters for DSL through the link from the Master-Modem.

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.
- the 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, the Slave-Modem also 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).

3.2.7.1.4 SHDSL Test Loop, Analogue Loop Back

The possibility to activate a test loop on SHDSL line interface simplifies the device start-and-adjustment.

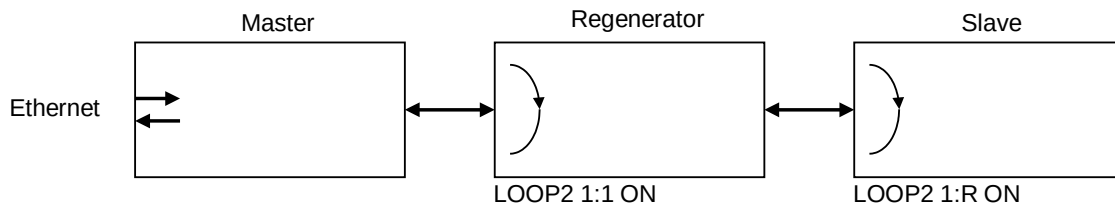


Figure 3.17. Test loops

Test loops can be activated for the Master and Slave devices as well as for the Regenerator.

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!

An analogue loop back is also possible. 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!

3.2.7.1.5 SHDSL Performance Monitoring (Noise Margin, G.826)

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} .

The error performance monitoring of a SHDSL link is also 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 SHDSL interfaces.

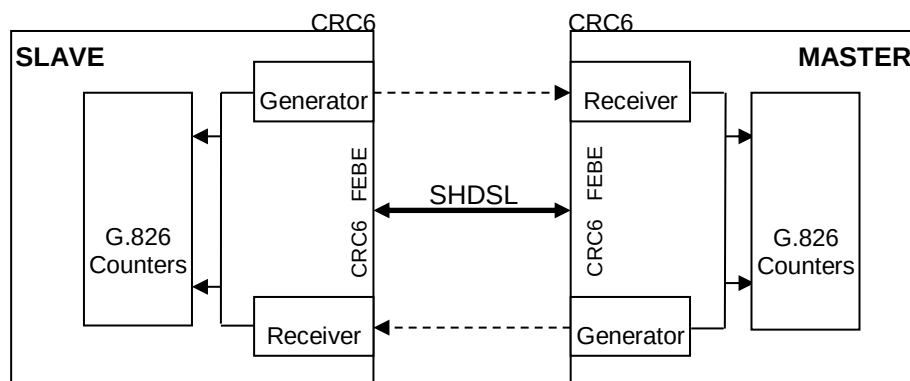


Figure 3.18 G.826 SHDSL performance evaluation

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.

The estimation of a bit error rate is not within the scope of G.826 calculations.

3.2.7.2 Line Card Ethernet Interface

The Ethernet interfaces of the SHDSL line card 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 SHDSL line card devices support Ethernet traffic priority according to the standard protocol IEEE 802.1P (so-called QoS, Quality of Service). It means to analyze the header content of each Ethernet frame to get information about the necessary priority of this application. The internal switch of the SHDSL line card places this data to the corresponding queue of the output port. The SHDSL line card 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. In the SHDSL line card devices three types of network interfaces exist:

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

The choice of the interface (DSL), which will be mapped to the corresponding WAN interface is performed by the <PAYLOAD> command.

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 3.13 Access, Trunk and Mixed Mode

SHDSL line card 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 SHDSL line cards, 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 3.14 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–WAN2) (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 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).

3.2.7.3 Line Card 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.

3.2.7.3.1 Line Card 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.

3.2.7.4 Line Cards 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. Orion3/MiniFlex 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 Orion3/MiniFlex 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.

3.2.7.4.1 IEEE 802.1x Line Cards Settings

The following IEEE 802.1x parameters can be changed on Orion3/MiniFlex 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, other 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.

3.2.7.5 Line Card Rapid Spanning Tree Protocol

The line card 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. If several DSL links 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:

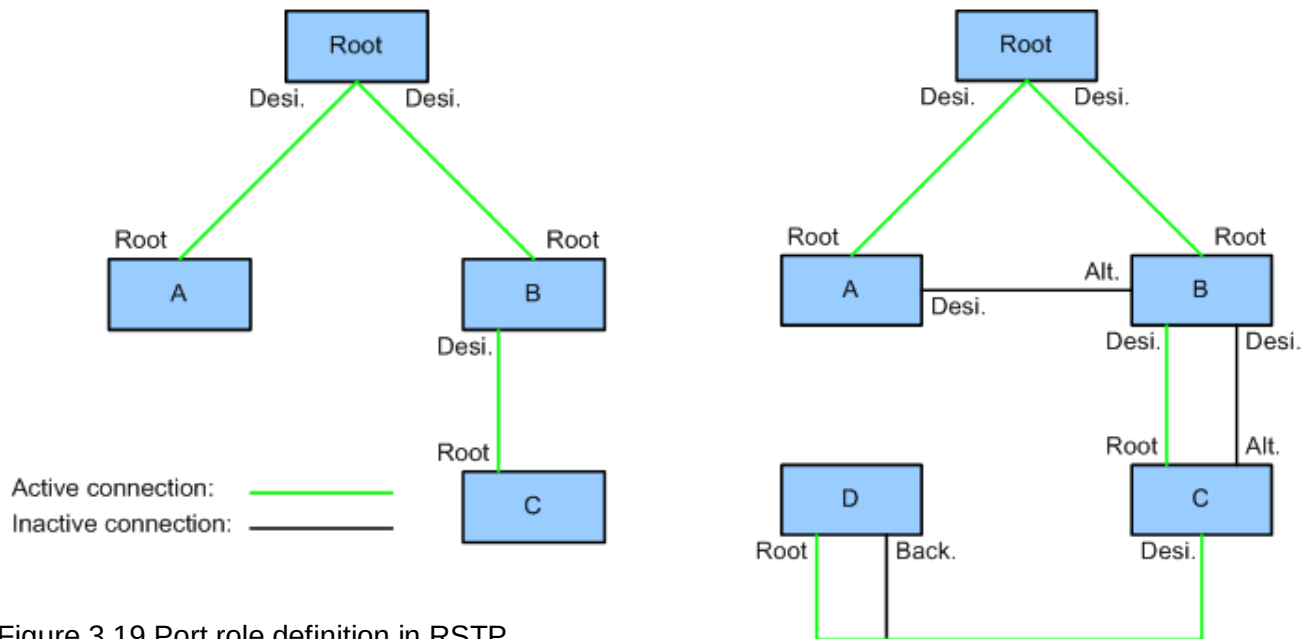


Figure 3.19 Port role definition in RSTP.

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

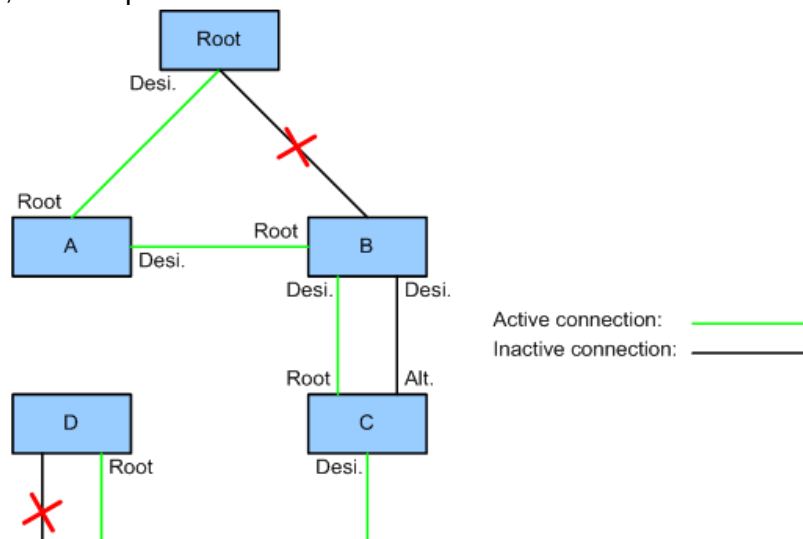


Figure 3.20 Change of Port role upon network failure.



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

3.2.7.6 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 must 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 MiniFlex 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.

MiniFlex 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.

3.2.7.6.1 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.flexdsl

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

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

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

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

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.flexdsl
```

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 FlexDSL Telecommunications AG. 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

```
# FlexDSL MiniFlex Clients
# Modems from network 192.168.1.0/24 will be authenticated using secret
# phrase. Don't forget to add "sharing secret" to Orion3 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

```
# MiniFlex User with Administration rights
MINIFLEXADMIN Cleartext-Password := "AdminPass"
    FlexDSL-Rights = ALL,
    Framed-IP-Address = 192.168.169.0,
    Framed-IP-Netmask = 255.255.255.0

# MiniFlex User with User rights. Basic change of configuration
MINIFLEXUSER Cleartext-Password := "UserPass"
    FlexDSL-Rights = CONTROL,
    FlexDSL-Rights += TEST,
    FlexDSL-Rights += STATUS,
    FlexDSL-Rights += CONFIG,
    Framed-IP-Address = 192.168.169.0,
    Framed-IP-Netmask = 255.255.255.0
```

```
# MiniFlex User with Read-only rights
MINIFLEXOPERATOR Cleartext-Password := "OperatorPass"
FlexDSL-Rights = TEST,
FlexDSL-Rights += STATUS,
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.

3.2.7.6.2 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`

```
# MiniFlex User with Administration rights
MINIFLEXADMIN Cleartext-Password := "AdminPass"
Vendor-Specific = ALL,
Framed-IP-Address = 192.168.1.0,
Framed-IP-Netmask = 255.255.255.0

# MiniFlex User with User rights. Basic change of configuration
MINIFLEXUSER 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

# MiniFlex User with Read-only rights
MINIFLEXOPERATOR Cleartext-Password := "OperatorPass"
Vendor-Specific = TEST,
Vendor-Specific += STATUS,
Framed-IP-Address = 192.168.1.0,
Framed-IP-Netmask = 255.255.255.0
```

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`

```
# FlexDSL MiniFlex Clients
# Modems from network 192.168.1.0/24 will be authenticated using secret
# phrase. Don't forget to add "sharing secret" to MiniFlex 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.

3.2.7.6.3 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 FlexDSL-Rights = ALL
- Type 7: NAS Prompt; modem grants access equal to FlexDSL-Rights += TEST, += STATUS

User configuration. File users

User records are in `/etc/freeradius/users`

```
# Orion3 User with Administration rights
ORION3ADMIN Cleartext-Password := "AdminPass"
  Framed-IP-Address = 192.168.169.0,
  Framed-IP-Netmask = 255.255.255.0,
  Service-Type = Administrative-user

# Orion3 User with Read-only rights
ORION3OPERATOR Cleartext-Password := "OperatorPass"
  Framed-IP-Address = 192.168.169.0,
  Framed-IP-Netmask = 255.255.255.0,
  Service-Type = NAS-Prompt-user
```

NOTE: Don't forget to restart freeradius server after changing configuration using `sudo service freeradius restart` command.

3.2.7.6.4 Configuring User Access Rights

The <Vendor-Specific> or <FlexDSL-Rights> 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	Group	Subgroup				
ALL	Commands of this level are available for everyone. No additional authorization is required			ACO	ALARM T	TLM
				ALARM	SOFTINFO	
	CONTROL [CTRL]		Operation of remote devices	CONNECT		
	TEST [T]		Test of the device	BERT Submenu	MACTABLE	RESTART
				LOOP1	MACTABLE C	STARTAL
				LOOP2	PING	
	ADMIN [A]		Administration of the device	ACO change	DUMP	SD
				APPLY	ID	SECURE
				BACKUP	LATHR	SERNUM
				CONFIRM	LICENSE	SOFTCONFIRM
				DEFAULT	LICENSE ADD	SOFTUPDATE
				DEFAULT DESC	LOAD	TFTP
				DEFAULT	LOG	TLM C
				EVERYTHING	NMTHR	TLM D
				FACTORY	PASSWORD	TLM S
				DEFAULT	RESET	USER
				DIFF	RESTORE	USERS
	STATUS [S]	:LINK	Link status	ALARMLOG	LINKALARM	STATUS
				ALLG826	LINKNM	STATUS EXT
				G826 [C]	LINKSTAT	STATUS L
				G826 E1 [C]	NM	STATUS T
		:LINKC	All commands from LINK + reset of the counters	ALARMLOG C	RESETALLG826	RESETG826
		:LAN	Ethernet status	ALARMLOG	NETSTAT	STATUS
				LLDP STAT	STATUS DOT1X	RADIUS
				MACTABLE	STATUS ETH	STATUS SFP
				NETERR	STATUS LLDP	
:LANC		All commands from LAN + reset of Ethernet counters and MAC table	ALARMLOG C	MACTABLE C	RESETNETSTAT	
CONFIG [C]	:VIEW	Displaying of device configuration	CONFIG	LLDP CONFIG	RSTP CONF	
			COSCONFIG	MACLIST SHOW	STATUS IO	
			IOCONFIG	NETCONFIG		
	:LINK	All commands from VIEW +line, E1 and Nx64 interface configuration	4RS	E1CLOCK	POWER	
			AISDET	E1MODE	PTMP	
			AISGEN	EXT	RESERVE	
			ANNEX	G704	RSDUPLEX	
			APPLY	GSCOMPAT	RSFORMAT	
			AUTO	IOIP	RSIP	
			AUTOLOOP	MASTER	RSRATE	
			BASERATE	MODE N	SETCLOCK	
			CONFIRM	MULTIPAIR	WANIDLE	
CRC4			PAM	WANTS		
DEFAULT	PAYLOAD					
:LAN	All commands from VIEW + LAN configuration	ALLOW	JUMBO SIZE	PING		
		APPLY	LLDP change	QOS		
		CONFIRM	LLDP DEFAULT	RSTP [CONF]		
		COS	MACFILTER	RSTP change		
		CRATE	MACLIST [IF]	RSTP DEFAULT		
		DOT1X	MACRULE	SETIP		
		ERATE	MODE [IF]	VID		
		ETHSD	MTU	VLAN		
		FC	NETDEFAULT	VLANNAME		
		GATEWAY	NETMASK			
		IRATE	PBVLAN			

ALL	CONFIG [C]	:SNMP	All commands from VIEW + SNMP configuration	APPLY COMMUNITY CONFIRM	RMONALARM RMONEVENT SNMP	SNMPACL SNMPSET TRAP
		:NET	All commands from VIEW + IP configuration	APPLY CONFIRM DST GATEWAY HTTP MTU NETMASK	PING RADIUS SETIP SNTP SSH PORT SSH SYSCONTACT	SYSLOCATION SYSLOG SYSLOG SYSNAME TELNET

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 MINIFLEXADMIN has full access to the device, because <Vendor-Specific> or <FlexDSL-Rights> field is set to ALL.

MINIFLEXUSER has partial access, because <Vendor-Specific> or <FlexDSL-Rights> field is set to CONTROL + TEST + STATUS + CONFIG.

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

3.2.7.7 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 FlexDSL Orion3 / MiniFlex devices can read and display the following parameters received from remote peer:

Parameter	Value	Description
Chassis ID	String	Manually assigned chassis ID or a 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 neighbors.

3.2.7.8 Line Card Alarm and LED Description

When managing the SHDSL line card via the local craft terminal (USB) or via Telnet, all LEDs, except the Ethernet LEDs will blink with a frequency of 1 Hz.

The LEDs display the normal operation conditions and the alarm conditions of each line card and of each interface according to the following tables. To display an urgent alarm has always the highest priority and will overwrite a non-urgent alarm.



Element	Description	Led Color		
Two LED on RJ-45	Status 1st Ethernet Interface Led1=Green, Led2=Amber	Status Ethernet Interface		
	Status 2nd Ethernet Interface Led1=Green, Led2=Amber	Connection is active	Led1	Green
				Off
		Data receive and/or transmit	Led2	Green Blinking
		100 Mbit/s receive/transmit rate		Amber
LED 1	Status 1st SHDSL Interface	10 Mbit/s receive/transmit rate		Off
	Status 2nd SHDSL Interface	Status SHDSL Interface		
LED 2		Power failure or power is off		Off
		Hardware or software failure		Red Blinking
		Normal operation		Green
		Non-urgent alarm		Amber
		Urgent alarm		Red

Table 3.15 SHDSL line card LED behavior according to the interface status.

Name	Group	Alarm status	LED 1/2 Status SHDSL	Description
LOS	DSL	Urgent	Red	Loss of signal in an SHDSL link
LOSW			Red	Loss of frame alignment in an SHDSL link
LOSD			Red	Loss of signal at the remote SHDSL side
BER-H			Red	Block-error-rate in an SHDSL line according to G.826 $\geq 30\%$
SEGD			Red	Loss of signal or an alarm on a regeneration segment (segment degradation)
ALB		Urgent & Non-urgent	Amber	SHDSL analogue loop back is activated
SEGA		Non-urgent	Amber	Data errors or loss of frame alignment on a regeneration segment (segment alarm)
NM			Amber	Noise Margin < setup NMTHR value
LA			Amber	Line Attenuation > setup LATHR value
LOOP2			Amber	Loop is activated from the remote device to the local device
RCONF			Red	Configuration of the remote device is not compatible with the configuration of the local device
HW-F	Maintenance		Red Blinking	Hardware failure
DSL-F			Red Blinking	DSL signal processor initialization failure

Table 3.16 Alarm correspondence to LED behavior

3.2.7.9 Line Card Management with Local Craft Terminal and Ethernet

Every SHDSL line card has some integrated management and diagnostic functionality, which can be used to configure the devices and to receive additional information like G.826 parameters or any G.SHDSL link quality. The access to this functionality is done by:

- Connecting the local craft terminal (LCT, USB 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. SNMP (Simple Network Management Protocol) is also integrated.
- Connecting the backplane Ethernet interface to access the unit through the integrated Switch.

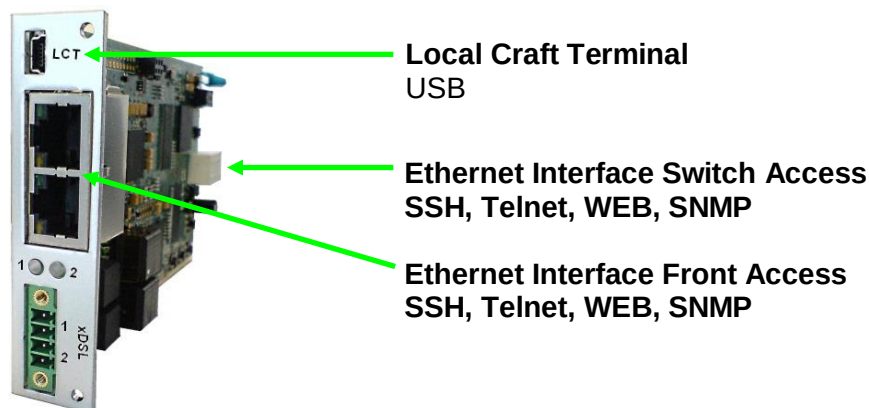


Figure 3.21 SHDSL Line Card showing Local Craft Terminal and Ethernet Interface

To use the USB interface as local craft terminal, you need to download and install the following driver http://www.flexdsl.ch/extranetfiles/Software/Orion3_USB_Driver.zip. This is an USB to serial driver and allow to have a COM port over USB.

3.2.7.9.1 Telnet (Ethernet Interface)

The **TELNET** (TELEcommunication NETwork) access is made through the Ethernet network. With any computer and a program with the Telnet protocol SHDSL line cards 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 SHDSL line card with an IP address can be reached; it does not matter if near end, far end or repeater.

3.2.7.9.2 WEB (Ethernet Interface)

The WEB interface is used to display statistics and do configuration when the SHDSL line cards are connected to the management computer via any 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** or **https://X.X.X.X** in 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):

Alarm Status xDSL	DSL1	DSL2
LOS	on	on
LOSW	on	on
SEGD	off	off
BER-H	off	off
SEGA	off	off
ALB	off	off
LOOP2	off	off
RCONF	off	off
NM	off	off
LA	off	off
TLM	off	off
Remote	off	off

Ethernet	Port 1	Port 2	Port 3
LOS-E	on	on	off

Maintenance	
HW-F	off
DSL-F	off
SW-MNT	off

Figure 3.22 WEB interface – “SHDSL Line Card 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 is then active and if you like to have the configuration stored you must change to the tab “Device Management” and press the “Confirm” button.

DSL settings

DSL mode

Active channels: 2 Multipair mode: OFF AUTO Slave mode: ☐

DSL

	DSL1	DSL2
Description:	DSL1	DSL2
Master/Slave:	Master	Master
Extended:	OFF	OFF
Baserate:	89 5.696 Mbit	32 2.048 Mbit
PAM:	PAM32	PAM32
ANNEX:	B	B
DSL sync:	Int	Int
Noise Margin:	OFF	dB (OFF/0..25)
Line Attenuation: thresholds	OFF	dB (OFF/0..25)

Save Apply All

MODEM CONFIGURATION WAS UPDATED BUT NOT ACTIVATED YET. PRESS "APPLY" BUTTON TO ACTIVATE IT NOW. AFTER ACTIVATION IT SHOULD BE CONFIRMED IF IT'S RIGHT.

Figure 3.23 WEB interface – “SHDSL Line Card Configuration”

Figure 3.24 WEB interface – “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.

3.2.7.9.3 SNMP (Ethernet Interface)

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 FlexView Network Management System (NMS) from FlexDSL Telecommunications AG is available too.

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 must 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.

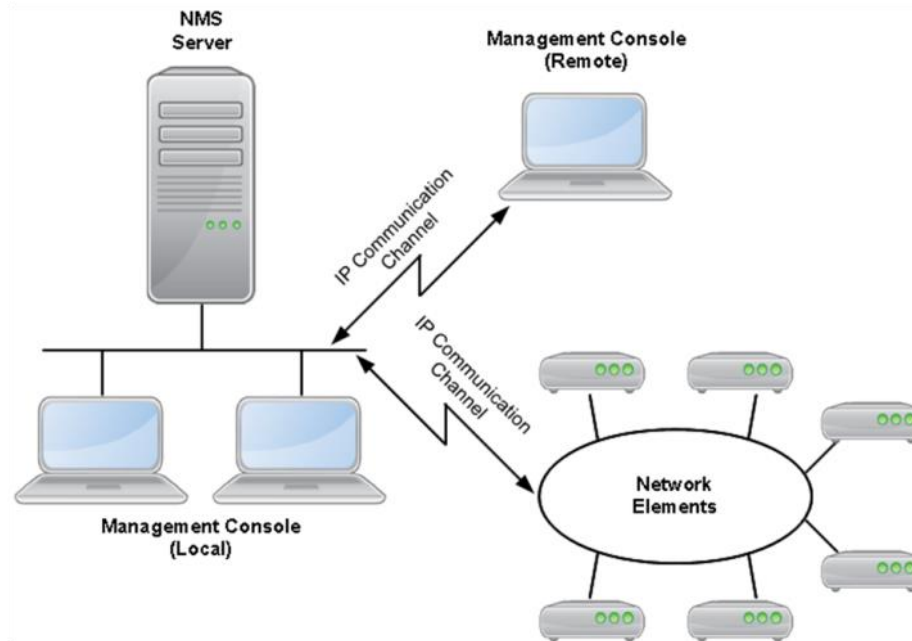


Figure 3.25 The structure of SNMP-based NMS.

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/FlexDSL 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 has 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)

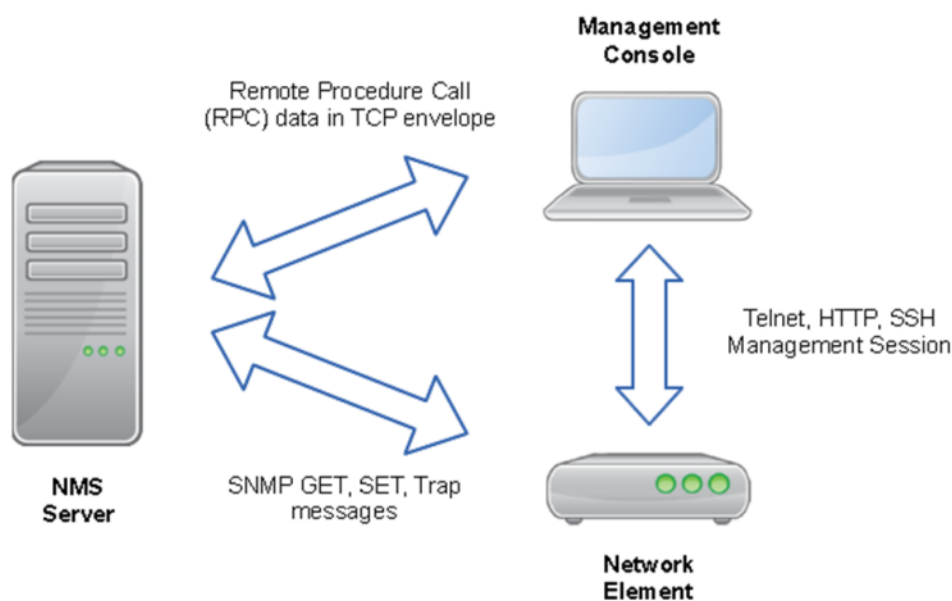


Figure 3.26 Message exchange in SNMP-based networks.

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.

3.2.7.9.4 SSH

The SSH (Secure SHell) protocol is used to access MiniFlex 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 MiniFlex 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 access to the CLI after successful login.

The SSH client is a software for PC. We suggest using 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 differs from the name of a user who initialises the SSH session.

3.2.8 SHDSL DINrail Modem

The SHDSL Line Card is available in a DINrail housing too. All the interfaces and the software functionality are exactly the same. The local power supply can be DC or AC Voltage:

- -24V models have 18-72VDC local power supply
- -230V models have 85-264VAC and 100-370VDC local power supply

The dimension is 143(W)x87(D)x37(H) mm or 153(W)x87(D)x37(H) mm with the clip.

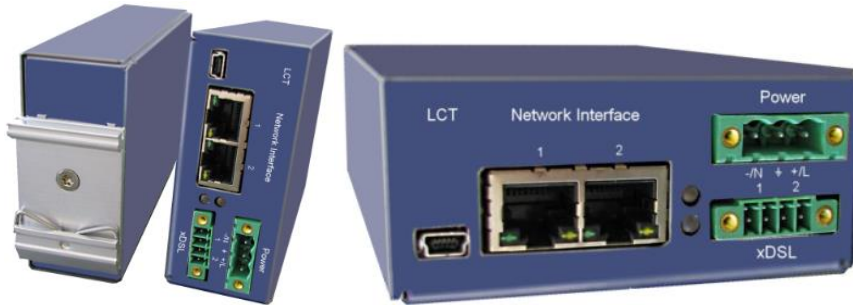


Figure 3.27 SHDSL DINrail Modem

3.2.9 Single or Dual FOM & GFOM Line Card

The FOM & GFOM Line Card has one or two SFP slot interface for any SFP module (FOM has 100Base-FX, GFOM has 100Base-FX/1000Base-X). There is also a local craft terminal on every line card to manage and configure if there is any Ethernet failure of the main switch in the MiniFlex.



Figure 3.28 Single and Dual FOM or GFOM Line Cards

Element	Description
LCT	USB Connector Local Craft Terminal
LED-1 LED-2	LED Red/Green/Amber Ethernet Backside LED Red/Green/Amber SFP slot Frontside
SFP	SFP slot for any module with speed up to 155Mbps.

Table 3.17 Connectors and LEDs on the front panel of the single FOM Line Card.

Element	Description
LCT	USB Connector Local Craft Terminal
	RJ-45 FOM 10/100Mbps / GFOM 10/100/1000Mbps Ethernet Port 1 + two LED
	RJ-45 FOM 10/100Mbps / GFOM 10/100/1000Mbps Ethernet Port 2 + two LED
LED-1-1 LED-1-2	LED Red/Green/Amber SFP slot Frontside
SFP	SFP slot for any module with speed up to 155Mbps or 1.25Gbps.
LED-1-1 LED-1-2	LED Red/Green/Amber SFP slot Frontside
SFP	SFP slot for any module with speed up to 155Mbps or 1.25Gbps.

Table 3.18 Connectors and LEDs on the front panel of the dual FOM and GFOM Line Card.

3.2.9.1 Line Card SFP and Ethernet Interface

Please see the interface description of the SHDSL line card.

3.2.9.2 Line Card Alarm and LED Description

The LEDs display the normal operation conditions and the alarm conditions of each line card and of each interface according to the following tables. To display an urgent alarm has always the highest priority and will overwrite a non-urgent alarm.

	Element	Description
	LED 1	Status Ethernet Interface Backplane
	LED 2	Status SFP Module

Led Color	
Status Ethernet Backplane Interface	
Connection is active	Green
Connection is not active	Off
Data receive and/or transmit	Amber Blinking
System Error	Red
Power fail	Off
Status SFP Interface	
Connection is active	Green
Data receive and/or transmit	Amber Blinking
No SFP module inserted	Off
Power fail	Off

Table 3.19 Single FOM Line Card LED behavior according to the interface status.

	Element	Description
	Two LED on RJ-45	Status 1st Ethernet Led1=Green, Led2=Amber
	Two LED on RJ-45	Status 2nd Ethernet Interface Led1=Green, Led2=Amber
	Two LED SFP	Status 1st SFP Ethernet Interface Led1=Green, Led2=Amber
	Two LED SFP	Status 2nd SFP Ethernet Interface Led1=Green, Led2=Amber

Led Color		
Status Ethernet and SFP Interface		
Connection is active	Led1	Green
Connection is not active		Off
Data receive and/or transmit	Led2	Green Blinking
100(0) Mbit/s receive/transmit rate		Amber
10 Mbit/s receive/transmit rate		Off

Table 3.20 Dual FOM or GFOM Line Card LED behavior according to the interface status.

3.2.10 Single or Dual FOM & GFOM DINrail Modem

The single and dual FOM & GFOM Line Card is available in a DINrail housing too. All the interfaces and the software functionality are exactly the same. The local power supply can be DC or AC Voltage:

- -24V models have 18-72VDC local power supply
- -230V models have 85-264VAC and 100-370VDC local power supply

The dimension for the single one is 143(W)x87(D)x37(H) mm or 153(W)x87(D)x37(H) mm with the clip. The dimension for the dual one is 143(W)x87(D)x43(H) mm or 153(W)x87(D)x43(H) mm with the clip.



Figure 3.29 Single and Dual FOM & GFOM DINrail Modem

3.2.11 POE Line Card

The POE (Power over Ethernet) line card has two Ethernet ports supporting the IEEE 802.3af standard with 15.4 Watts.

ATTENTION

This line card can only be used with the Minirack (MF-MR-RAIL-2U4S,V1) or with 24VDC version of Dual Unit (MF-DU-RAIL-2U2S-24V, V1) and not with the normal subrack (MF-MR2N-SW-12Eth,V1) or FlatRack (MF-FR05N-SW-2Eth,V1).

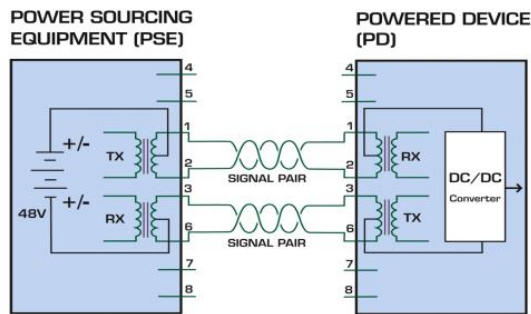


Figure 3.30 PoE Line Card

Element		Description	
		RJ-45 10/100Mbps Ethernet Port 1 + two LED	
		RJ-45 10/100Mbps Ethernet Port 2 + two LED	
LED-1	LED-2	LED Green POE status 1	LED Green POE status 2

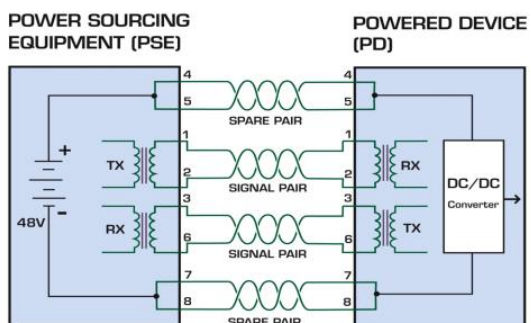
Table 3.21 Connectors and LEDs on the front panel of POE Line Card

The POE Line Card can be configured by jumpers for the wished powering scheme.



Mode A

802.3af POE Mode A combine's power onto the same wires as the data signal using a technique called Phantom Powering



Mode B

802.3af POE Mode B uses the Ethernet spare pairs 4/5 and 7/8 to carry power. Pairs 1/2 and 3/6 are left untouched and carry data for 10/100BaseT.



Figure 3.31 Jumpers on POE Line Card

Internal/External Power			
X301 & X302	Mode	Condition	Power at PD
Pin1-3 Pin2-4	Default Mode 15.4 Watts per Interface. IEEE802.3af	External Power must be 18-72VDC. PoE uses on board DC/DC converter.	12.95Watts
Pin3-5 Pin4-6	External Power Mode. 40.0 Watts per Interface IEEE802.3at	External Power must be 44-54VDC. PoE uses external power.	34.20Watts

Mode A and Mode B Configuration			
X404 & X405	Mode	Condition	Power at PD
Pin1-2 Pin5-6	Mode A	X404 for PoE-2 X405 for PoE-1	Depending X301 & X302 & X406
Pin3-4 Pin7-8	Mode B	X404 for PoE-2 X405 for PoE-1	Depending X301 & X302 & X406
Pin1-2 Pin3-4 Pin5-6 Pin7-8	Mode A & Mode B	X404 for PoE-2 X405 for PoE-1	Depending X301 & X302 & X406

Power Polarity MDI or MDI-X			
X402 & X403	Polarity	Mode A	Mode B
Pin1-3 Pin2-4	MDI-X	Pin1/2 -48VDC Pin3/6 0VDC	Pin4/5 -48VDC Pin7/8 0VDC
Pin3-5 Pin4-6	MDI	Pin1/2 0VDC Pin3/6 -48VDC	Pin4/5 0VDC Pin7/8 -48VDC

Special Combined Mode A and Mode B			
X406		Condition	Power at PD
Pin1-3 Pin2-4	PoE-1 Mode A PoE-1 Mode B PoE-2 not used	PoE-1 uses two on board DC/DC converter. One for Mode A other for Mode B.	2x 12.95Watts
Pin3-5 Pin4-6	PoE-1 normal use PoE-2 normal use	Default	Depending X301 & X302

3.2.11.1 Line Card LED Description

The LEDs display the normal operation conditions of each line card and of each interface according to the following table.

	Element	Description
	Two LED on RJ-45	Status 1st Ethernet Interface Led1=Green, Led2=Amber
	Two LED on RJ-45	Status 2nd Ethernet Interface Led1=Green, Led2=Amber
	LED 1	Status 1st Power over Ethernet
	LED 2	Status 2nd Power over Ethernet
	Led Color	
	Status Ethernet Interface	
	Connection is active	Green
	Connection is not active	Off
	Data receive and/or transmit	Green Blinking
	100 Mbit/s receive/transmit rate	Amber
	10 Mbit/s receive/transmit rate	Off
	Status POE on Ethernet Interface	
	Power is off	Off
	Normal operation, Power is on	Green

Table 3.22 POE Line Card LED behavior according to the interface status.

3.2.12 POE DINrail Unit

The PoE Line Card is available in a DINrail housing too. It has one Ethernet input (LAN) and one Ethernet with Power output (PoE). All interfaces functionality is exactly the same as for the line card. The local power supply is DC Voltage:

- -24V model has 18-72VDC local power supply

The dimension is 143(W)x87(D)x37(H) mm or 153(W)x87(D)x37(H) mm with the clip.



Figure 3.32 POE DINrail Unit

3.2.13 Managed Switch Line Card

The managed Switch Line Card has four 10/100Base-T Ethernet ports as front access and up to four additional 10/100Base-T Ethernet ports as back access (backplane).



ATTENTION

The four ports at the backplane can only be used with the Minirack (MF-MR-RAIL-2U4S,V1). When using with a normal Subrack or Dual Unit, there is only one Ethernet port available at the backplane.

This card cannot be used with the FlatRack (MF-FR05N-SW-2Eth,V1).



Figure 3.33 Managed Switch Line Card

Element	Description
LCT	USB Connector Local Craft Terminal
	RJ-45 10/100Mbps Ethernet Port 1 + two LED
	RJ-45 10/100Mbps Ethernet Port 2 + two LED
	RJ-45 10/100Mbps Ethernet Port 3 + two LED
	RJ-45 10/100Mbps Ethernet Port 4 + two LED

Table 3.23 Connectors and LEDs on the front panel of the managed Switch Line Card.

3.2.13.1 Line Card LED Description

The LEDs display the normal operation conditions of each line card and of each interface according to the following table.

	Element	Description	Led Color		
	Two LED on RJ-45	Status 1st Ethernet Interface Led1=Green, Led2=Amber	Status Ethernet Interface		
	Two LED on RJ-45	Status 2nd Ethernet Interface Led1=Green, Led2=Amber	Connection is active	Led1	Green
			Connection is not active		Off
			Data receive and/or transmit		Green Blinking
	Two LED on RJ-45	Status 3rd Ethernet Interface Led1=Green, Led2=Amber	100 Mbit/s receive/transmit rate	Led2	Amber
			10 Mbit/s receive/transmit rate		Off

Table 3.24 Managed Switch Line Card LED behavior according to the interface status.

3.2.14 Managed Switch DINrail Unit

The Managed Switch Line Card is available in a DINrail housing too. All the interfaces and the software functionality are exactly the same. The local power supply can be DC or AC Voltage:

- -24V models have 18-72VDC local power supply
- -230V models have 85-264VAC and 100-370VDC local power supply

The dimension is 143(W)x87(D)x43(H) mm or 153(W)x87(D)x43(H) mm with the clip.



Figure 3.34 Managed Switch DINrail Unit

3.2.15 Serial RS-232/422/485 Interface Line Card

The Serial RS-232/422/485 Line Card has one serial interface, two SFP slot interface for any SFP module (100Base-FX, OC-3/STM-1) and an additional 10/100Base-T Ethernet port as front access and one Ethernet ports as back access (backplane). There is also a local craft terminal on every line card to manage and configure if there is any Ethernet failure of the main switch in the MiniFlex.



Figure 3.35 Serial RS-232/422/485 Interface Line Card

Element	Description	
LCT	USB Connector Local Craft Terminal	
Serial	RJ-45 Serial Port + two LED	
Ethernet	RJ-45 10/100Mbps Ethernet Port + two LED	
LED-1-1	LED-1-2	LED Red/Green/Amber SFP slot Frontside
SFP	SFP slot for any module with speed up to 155Mbps.	
LED-1-1	LED-1-2	LED Red/Green/Amber SFP slot Frontside
SFP	SFP slot for any module with speed up to 155Mbps.	

Table 3.25 Connectors and LEDs on the front panel of the Serial RS-232/422/485 Interface Line Card.

3.2.15.1 Line Card SFP and Ethernet Interface

Please see the interface description of the SHDSL line card.

3.2.15.2 Line Card Serial RS-232/422/485 Interface

The serial interface can be configured to be RS-232 or RS-422/485 with following features:

- Speed 75, 150, 300, 600, 1200, 2400, 4800, 9600, 14400, 19200, 28800, 38400, 56000, 57600, 115200, 230400 bps
- number of data bits: 5...8
- number of stop bits: 1, 1.5 or 2
- parity: odd/even/mark/space

You can use the command `RSRATE [N]` to set the baud rate (N is baudrate, for instance 9600). The command `RSFORMAT [format]` is used to set the data format (example of format: 8N1).

3.2.15.3 Line Card Alarm and LED Description

The LEDs display the normal operation conditions and the alarm conditions of each line card and of each interface according to the following tables. To display an urgent alarm has always the highest priority and will overwrite a non-urgent alarm.

	Element	Description	Led Color		
			Status Ethernet and SFP Interface		
	Two LED on RJ-45	Status Serial Interface Led1=Green, Led2=Amber			
	Two LED on RJ-45	Status Ethernet Interface Led1=Green, Led2=Amber			
	Two LED SFP	Status 1st SFP Ethernet Interface Led1=Green, Led2=Amber			
	Two LED SFP	Status 2nd SFP Ethernet Interface Led1=Green, Led2=Amber			

Status Ethernet and SFP Interface		
Connection is active	Led1	Green
Connection is not active		Off
Data receive and/or transmit	Led2	Green Blinking
100 Mbit/s receive/transmit rate		Amber
10 Mbit/s receive/transmit rate		Off

Status RS-232/422/485 Interface		
RS-232 data receive/transmit	Led1	Green RX/TX
RS-422/485 data receive/transmit		Green RX/TX
RS-232 control RTS/CTS	Led2	Amber R/CTS
RS-422/485		Off

Table 3.26 Serial RS-232/422/485 Interface Line Card LED behavior according to the interface status.

3.2.16 Serial RS-232/422/485 Interface DINrail Modem

The Serial RS-232/422/485 Interface Line Card is available in a DINrail housing too. All the interfaces and the software functionality are exactly the same. The local power supply can be DC or AC Voltage:

- -24V models have 18-72VDC local power supply
- -230V models have 85-264VAC and 100-370VDC local power supply

The dimension is 143(W)x87(D)x43(H) mm or 153(W)x87(D)x43(H) mm with the clip.



Figure 3.36 Serial RS-232/422/485 Interface DINrail Modem

3.2.17 Serial RS-232 Line Card

The Serial RS-232 Line Card has four RS-232 (V.24/28) ports as front access and one 10/100Base-T Ethernet ports as back access (backplane).

	Element	Description
	LCT	USB Connector Local Craft Terminal
	RS232-1	RJ-45 RS-232 Port 1 + two LED
	RS232-2	RJ-45 RS-232 Port 2 + two LED
	RS232-3	RJ-45 RS-232 Port 3 + two LED
	RS232-4	RJ-45 RS-232 Port 4 + two LED

Table 3.27 Connectors and LEDs on the front panel of the Serial RS-232 Line Card.

3.2.17.1 Line Card Serial Interface

The serial RS-232 interfaces have following features:

- Speed 75, 1200, 2400, 9600, 19200, 38400, 57600, 115200, 230400 bps
- number of data bits: 5...8
- number of stop bits: 1, 1.5 or 2
- parity: odd/even/mark/space

You can use the command 4RS RATE [N] to set the baud rate (N is baudrate, for instance 9600). The command 4RS MODE [format] is used to set the data format (example of format: 8N1).

3.2.17.2 Line Card LED Description

The LEDs display the normal operation conditions of each line card and of each interface according to the following table.

	Element	Description
	Two LED on RJ-45	Status 1st RS-232 Interface Led1=Green, Led2=Amber
	Two LED on RJ-45	Status 2nd RS-232 Interface Led1=Green, Led2=Amber
	Two LED on RJ-45	Status 3rd RS-232 Interface Led1=Green, Led2=Amber
	Two LED on RJ-45	Status 4th RS-232 Interface Led1=Green, Led2=Amber

Led Color		
Status RS-232/422/485 Interface		
RS-232 data receive/transmit	Led1	Green RX/TX
RS-232 control RTS/CTS	Led2	Amber RTS/CTS

Table 3.28 Serial RS-232 Interface Line Card LED behavior according to the interface status.

3.2.18 Serial RS-232 DINrail Unit

The managed serial RS-232 Line Card is available in a DINrail housing too. But it has only two RS-232 interfaces and additionally it has two SFP slot interfaces for any SFP module (100Base-FX, OC-3/STM-1). The local power supply can be DC or AC Voltage:

- -24V models have 18-72VDC local power supply
- -230V models have 85-264VAC and 100-370VDC local power supply

The dimension is 143(W)x87(D)x43(H) mm or 153(W)x87(D)x43(H) mm with the clip.



Figure 3.37 Serial RS-232 DINrail Unit

3.2.19 E1 Interface Line Card

The E1 line card has four E1 ports as front access and one 10/100Base-T Ethernet port as back access (backplane). The Card operates in the so-called Converter Mode, when Ethernet data coming through backplane 10/100Base-T Ethernet port is switched between and transmitted over E1 interfaces (s.c. WAN interfaces) according to the device settings.

By the using special SW this device may also operate in the TDMoIP mode, i.e. when E1 data is transmitted over Ethernet/IP network. This TDMoIP mode is not under the scope of this User Manual. Please refer to “**UM_FlexDSL-TDMoE_SW_V2-x**” User Manual for details.

	Element	Description
	LCT	USB Connector Local Craft Terminal
	E1-1	E1 Port 1 + two LED
	E1-2	E1 Port 2 + two LED
	E1-3	E1 Port 3 + two LED
	E1-4	E1 Port 4 + two LED

Table 3.29 Connectors and LEDs on the front panel of the E1 Line Card.

3.2.19.1 Line Card E1 Interface (G.703/704)

3.2.19.1.1 Framed and Unframed E1

The E1 Line Card supports transmission of framed and unframed E1 interfaces.

In unframed (transparent) mode, the encapsulated Ethernet data is transmitted over E1 interface utilizing full E1 bandwidth (2048 kbps).

In framed mode (framing according to ITU-T G.704), the E1 data is processed by the on-board E1 framer. In this case it is possible to assign 1-31 timeslots of E1 stream to be a WAN interface. Device supported up to 4 WAN interfaces (by the number of E1 ports).

3.2.19.1.2 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 time slot 0 is not activated. If the TS0GEN mode is activated, the time slot 0 is generated without CRC4 sub-multiframes and checksum words.

3.2.19.1.3 AIS Detection (Alarm Indication Signal)

If this mode is enabled, the reception of an AIS through the E1 interface will cause a non-urgent alarm.



WARNING

IT IS RECOMMENDED TO ENABLE THE AIS DETECTION FOR ALL E1 NETWORK INTERFACES.

3.2.19.1.4 E1 Clock Modes

Line card has different possibilities to synchronize E1 interfaces. Usually the E1 interface takes the E1-clock from the E1-input and transmits it back to the E1-output. But we also support an internal clocking and clocking priorities.

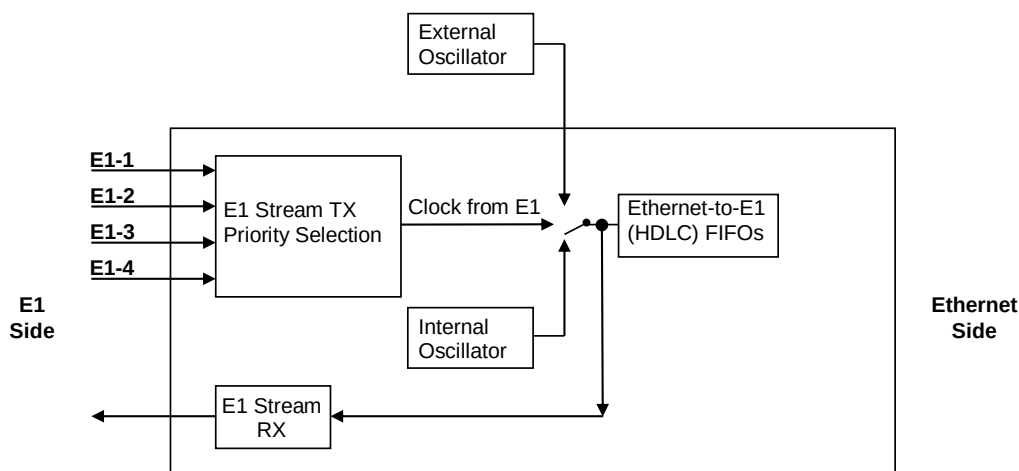


Figure 3.38. E1 clock modes

The following clock sources can serve as reference timing signals:

1. Clocking from external source
2. Clocking from E1 input stream (if available).
3. Clocking from the internal generator (**INTERNAL**).

Use **SETCLOCK** and **E1CLOCK** commands to configure the priority levels for the clock sources. The device automatically switches to the highest priority clock the when possible.

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.

Switching between clock sources occurs within 100 ms, after losing synchronization.

3.2.19.2 Line Card LED Description

The LEDs display the normal operation conditions of each line card and of each interface according to the following table.



Element	Description
Two LED on RJ-45	Status 1st E1 Interface Led1=Green, Led2=Amber
Two LED on RJ-45	Status 2nd E1 Interface Led1=Green, Led2=Amber
Two LED on RJ-45	Status 3rd E1 Interface Led1=Green, Led2=Amber
Two LED on RJ-45	Status 4th E1 Interface Led1=Green, Led2=Amber

LED Color		
Status of E1 Interface		
Normal operation	Led1	Green
Alarm at E1 interface		Off
E1 interface is not used for transmission		Off
Normal operation	Led2	Off
Alarm at E1 interface		Amber
E1 interface is not used for transmission		Off

Table 3.30 E1 line card LED behavior according to the interface status.

3.2.20 E1 DINrail Unit

The E1 line card is available in a DINrail housing too. But it has additionally two Ethernet interfaces on the front. The local power supply can be DC or AC Voltage:

- -24V models have 18-72VDC local power supply
- -230V models have 85-264VAC and 100-370VDC local power supply

The dimension is 143(W)x87(D)x43(H) mm or 153(W)x87(D)x43(H) mm with the clip.

	Element	Description
	Power	Power connector
	E1 2/4	E1 Ports 2 and 4 + two LED
	E1 1/3	E1 Ports 1 and 3 + two LED
	Eth 2	Eth Port 2 + two LED
	Eth 1	Eth Port 1 + two LED
	LCT	USB Connector Local Craft Terminal

Table 3.31 Connectors and LEDs on the front panel of the E1 DINrail Unit.

3.2.20.1 DINrail Ethernet Interface

Please see the interface description of the SHDSL line card.

3.2.20.2 DINrail LED Description

The LEDs display the normal operation conditions of each unit and of each interface according to the following table.

 1 Eth 2 1/3 E1 2/4	Element	Description	LED Color		
	Two LED on RJ-45	Status 2nd and 4th E1 Interfaces Led1=Green, Led2=Amber	Status of E1 Interface		
			Normal operation of both interfaces	Led1	Green
			Alarm at one or both E1 interfaces		Off
	Two LED on RJ-45	Status 1st and 3rd E1 Interfaces Led1=Green, Led2=Amber	E1 interfaces are not used for transmission	Led2	Off
			Normal operation of both interfaces		Off
			Alarm at one or both E1 interfaces		Amber
	Two LED on RJ-45	Status 2nd Ethernet Interface Led1=Green, Led2=Amber	E1 interfaces are not used for transmission	Led2	Off
			Normal operation of both interfaces		Off
			Alarm at one or both E1 interfaces		Amber
	Two LED on RJ-45	Status 1st Ethernet Interface Led1=Green, Led2=Amber	Status Ethernet Interface		
			Connection is active	Led1	Green
			Connection is not active		Off
			Data receive and/or transmit		Green Blinking
100 Mbit/s receive/transmit rate			Led2	Amber	
10 Mbit/s receive/transmit rate				Off	

Table 3.32 E1 DINrail unit LED behavior according to the interface status.

3.2.21 FXS/FXO/VF Interface VoIP Line Cards

The VoIP line card has two 10/100Base-T Ethernet ports and two voice (FXS, FXO or Voice Frequency, depending on the model) interfaces on the front and one 10/100Base-T Ethernet port as back access (backplane). The device works with a standard SIP-protocol and acts as a standard SIP User Agent (UA).

Please refer to “UM_FlexDSL_MiniFlex_VoIP_v1-x” User Manual for more details and programming.



Figure 3.39 MiniFlex VoIP Line Cards

Element	Description
LCT	USB Connector Local Craft Terminal
Eth-1	Eth Port 1 + two LED
Eth-2	Eth Port 2 + two LED
FXS-1	FXS Port 1 + two LED
FXS-2	FXS Port 2 + two LED
FXO-1	FXO Port 1 + two LED
FXO-2	FXO Port 2 + two LED
VF-1	VF Port 1 + two LED
VF-2	VF Port 2 + two LED

Table 3.33 Connectors and LEDs on the front panel of the VoIP Line Card.

3.2.21.1 VoIP Line Card LED Description

The LEDs display the normal operation conditions of each line card and of each interface according to the following table.

	Element	Description	LED Color		
	Status Ethernet Interface				
	Two LED on RJ-45	Status 1st Ethernet Interface Led1=Green, Led2=Amber	Connection is active	Led1	Green
			Connection is not active		Off
	Two LED on RJ-45	Status 2nd Ethernet Interface Led1=Green, Led2=Amber	Data receive and/or transmit	Led2	Green Blinking
			100 Mbit/s receive/transmit rate		Amber
	Two LED on RJ-45	Status 1st FXS Interface Led1=Green, Led2=Amber	10 Mbit/s receive/transmit rate	Led2	Off
			Status FXS interface		
	Two LED on RJ-45	Status 2nd FXS Interface Led1=Green, Led2=Amber	ON-HOOK state or FXS interface is not used	Led1	Off
			Ringing		Green Blinking
Two LED on RJ-45		OFF-HOOK state	Led2	Green	
		SIP registration alarm (REG) or HW-F alarm is ON		Amber	
Two LED on RJ-45		Both, SIP registration alarm (REG) and HW-F alarm, are OFF	Led2	Off	

Table 3.34 FXS interface VoIP line card LED behavior according to the interface status.



Element	Description
Two LED on RJ-45	Status 1st Ethernet Interface Led1=Green, Led2=Amber
Two LED on RJ-45	Status 2nd Ethernet Interface Led1=Green, Led2=Amber
Two LED on RJ-45	Status 1st FXO Interface Led1=Green, Led2=Amber
Two LED on RJ-45	Status 2nd FXO Interface Led1=Green, Led2=Amber

LED Color		
Status Ethernet Interface		
Connection is active	Led1	Green
Connection is not active		Off
Data receive and/or transmit		Green Blinking
100 Mbit/s receive/transmit rate	Led2	Amber
10 Mbit/s receive/transmit rate		Off
Status FXO interface		
ON-HOOK state or FXO interface is not used	Led1	Off
Ring detected		Green Blinking
OFF-HOOK state		Green
SIP registration alarm (REG) or HW-F alarm is ON	Led2	Amber
Both, SIP registration alarm (REG) and HW-F alarm, are OFF		Off

Table 3.35 FXO interface VoIP line card LED behavior according to the interface status.



Element	Description
Two LED on RJ-45	Status 1st Ethernet Interface Led1=Green, Led2=Amber
Two LED on RJ-45	Status 2nd Ethernet Interface Led1=Green, Led2=Amber
Two LED on RJ-45	Status 1st VF Interface Led1=Green, Led2=Amber
Two LED on RJ-45	Status 2nd VF Interface Led1=Green, Led2=Amber

LED Color		
Status Ethernet Interface		
Connection is active	Led1	Green
Connection is not active		Off
Data receive and/or transmit		Green Blinking
100 Mbit/s receive/transmit rate	Led2	Amber
10 Mbit/s receive/transmit rate		Off
Status VF interface		
Idle state (no connection to remote peer) or VF interface is not used	Led1	Off
Establishing connection to remote peer		Green Blinking
Remote peer connected (signal transmitted)		Green
SIP registration alarm (REG) or HW-F alarm is ON	Led2	Amber
Both, SIP registration alarm (REG) and HW-F alarm, are OFF		Off

Table 3.36 VF interface VoIP line card LED behavior according to the interface status.

3.2.22 FXS/FXO/VF VoIP DINrail Unit

The FXS/FXO/VF Interface VoIP line cards are also available in a DINrail housing. The DINrail unit has two 10/100Base-T Ethernet ports and two voice (FXS, FXO or Voice Frequency, depending on the model) interfaces on the front. The device works with a standard SIP-protocol and acts as a standard SIP User Agent (UA).

The local power supply can be DC or AC Voltage:

- -24V models have 18-72VDC local power supply
- -230V models have 85-264VAC and 100-370VDC local power supply

The dimension is 143(W)x87(D)x43(H) mm or 153(W)x87(D)x43(H) mm with the clip.

Please refer to “UM_FlexDSL_MiniFlex_VoIP_v1-x” User Manual for more details and programming.



Model	Element	Description
All	Power	Power connector
	LCT	USB Connector Local Craft Terminal
	Eth 1	Eth Port 1 + two LED
	Eth 2	Eth Port 2 + two LED
FXS	Voice 1	FXS Port 1 + two LED
	Voice 2	FXS Port 2 + two LED
FXO	Voice 1	FXO Port 1 + two LED
	Voice 2	FXO Port 2 + two LED
VF	Voice 1	VF Port 1 + two LED
	Voice 2	VF Port 2 + two LED

Figure 3.40 VoIP DINrail Unit

Table 3.37 Connectors and LEDs on the front panel of the VoIP DINrail Unit.

3.2.22.1 FXS/FXO/VF VoIP DINrail Unit LED Description

The LEDs display the normal operation conditions of each line card and of each interface according to the following table.



Element	Description	LED Color		
Two LED on RJ-45	Status 1st FXS Interface Led1=Green Led2=Amber	Status FXS interface		
		ON-HOOK state or FXS interface is not used	Led1	Off
		Ringing		Green Blinking
Two LED on RJ-45	Status 2nd FXS Interface Led1=Green Led2=Amber	OFF-HOOK state	Led2	Green
		SIP registration alarm (REG) or HW-F alarm is ON		Amber
		Both, SIP registration alarm (REG) and HW-F alarm, are OFF		Off
Two LED on RJ-45	Status 1st Ethernet Interface Led1=Green Led2=Amber	Status Ethernet Interface		
		Connection is active	Led1	Green
		Connection is not active		Off
Two LED on RJ-45	Status 2nd Ethernet Interface Led1=Green Led2=Amber	Data receive and/or transmit		Led2
		100 Mbit/s receive/transmit rate	Amber	
		10 Mbit/s receive/transmit rate	Off	

Table 3.38 FXS VoIP DINrail Unit LED behavior according to the interface status.

	Element	Description	LED Color		
	Two LED on RJ-45	Status 1st FXO Interface Led1=Green Led2=Amber	Status FXO interface		
			ON-HOOK state or FXO interface is not used	Led1	Off
			Ring detected		Green Blinking
	Two LED on RJ-45	Status 2nd FXO Interface Led1=Green Led2=Amber	OFF-HOOK state	Led2	Green
			SIP registration alarm (REG) or HW-F alarm is ON		Amber
			Both, SIP registration alarm (REG) and HW-F alarm, are OFF		Off
	Two LED on RJ-45	Status 1st Ethernet Interface Led1=Green Led2=Amber	Status Ethernet Interface		
			Connection is active	Led1	Green
			Connection is not active		Off
	Two LED on RJ-45	Status 2nd Ethernet Interface Led1=Green Led2=Amber	Data receive and/or transmit	Led2	Green Blinking
			100 Mbit/s receive/transmit rate		Amber
			10 Mbit/s receive/transmit rate		Off

Table 3.39 FXO VoIP DINrail Unit LED behavior according to the interface status.

	Element	Description	LED Color		
			Status VF interface		
	Two LED on RJ-45	Status 1st VF Interface Led1=Green Led2=Amber	Led1	Idle state (no connection to remote peer) or interface is off	Off
				Establishing SIP-connection	Green Blinking
				Remote peer connected (signal transmitted)	Green
	Two LED on RJ-45	Status 2nd VF Interface Led1=Green Led2=Amber	Led2	SIP registration alarm (REG) or HW-F alarm is ON	Amber
				Both, SIP registration (REG) and HW-F alarms, are OFF	Off
	Two LED on RJ-45	Status 1st Ethernet Interface Led1=Green Led2=Amber	Led1	Status Ethernet Interface	
				Connection is active	Green
				Connection is not active	Off
	Two LED on RJ-45	Status 2nd Ethernet Interface Led1=Green Led2=Amber	Led2	Data receive and/or transmit	Green Blinking
				100 Mbit/s receive/transmit rate	Amber
				10 Mbit/s receive/transmit rate	Off

Table 3.40 VF VoIP DINrail Unit LED behavior according to the interface status.

3.2.23 Input / Output Line Card

The Input / Output (IO) line card contains 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 MiniFlex or Orion3 units equipped with IO cards create IP-based channel. IO statuses being transmitted over it either with UDP or with TCP messages.



Figure 3.41 MiniFlex IO Line Card

Element	Description
LCT	USB Connector Local Craft Terminal
Input / Output	Input / Output connector
SFP	SFP Slot for any module with speed up to 155Mbps
1	Ethernet status LED
2	Ethernet speed LED

Table 3.41 Connectors and LEDs on the front panel of the IO Line Card.

3.2.23.1 Input / Output Line Card LED Description

	Element	Description	Led Color	
			Status Ethernet and SFP Interface	
			Led1	Connection is active
				Connection is not active
				Data receive and/or transmit
			Led2	100 Mbit/s receive/transmit rate
				10 Mbit/s receive/transmit rate
	1	Ethernet Status LED		
	2	Ethernet Speed LED		

Table 3.42 IO Line Card LED behavior according to the interface status.

3.2.24 Input / Output DINrail Unit

The Input / Output (IO) line cards are also available in DINrail unit housing.

The local power supply can be DC or AC Voltage:

- -24V models have 18-72VDC local power supply
- -230V models have 85-264VAC and 100-370VDC local power supply

The dimension is 143(W)x87(D)x43(H) mm or 153(W)x87(D)x43(H) mm with the clip.



Figure 3.42 MiniFlex IO DINrail Unit.

Element	Description
Power	Power connector
LCT	USB Connector Local Craft Terminal
Input / Output	Input / Output connector
Eth	Ethernet port + two LED
1	Ethernet status LED
2	Ethernet speed LED

Table 3.43 Connectors and LEDs on the front panel of the IO DINrail Unit.

3.2.24.1 Input / Output DINrail Unit LED Description



Led Color		
Status Ethernet and SFP Interface		
Led1	Connection is active	Green
	Connection is not active	Off
	Data receive and/or transmit	Green Blinking
Led2	100 Mbit/s receive/transmit rate	Amber
	10 Mbit/s receive/transmit rate	Off

Table 3.44 IO DINrail Unit LED behavior according to the interface status.

3.2.25 Default IP Address

3.2.25.1 DINrail Unit



Figure 3.43: The default IP address for a DINrail unit is 192.168.0.235.

3.2.25.2 MiniRack

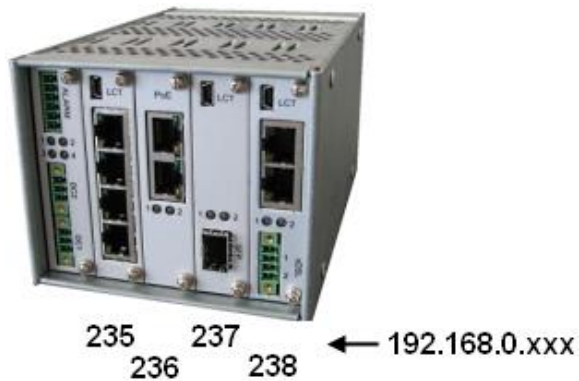


Figure 3.44: The default IP address for a MiniRack unit starts from left with 192.168.0.235 and ends on the right side with 192.168.0.238.

3.2.25.3 Subrack with Integrated Switch

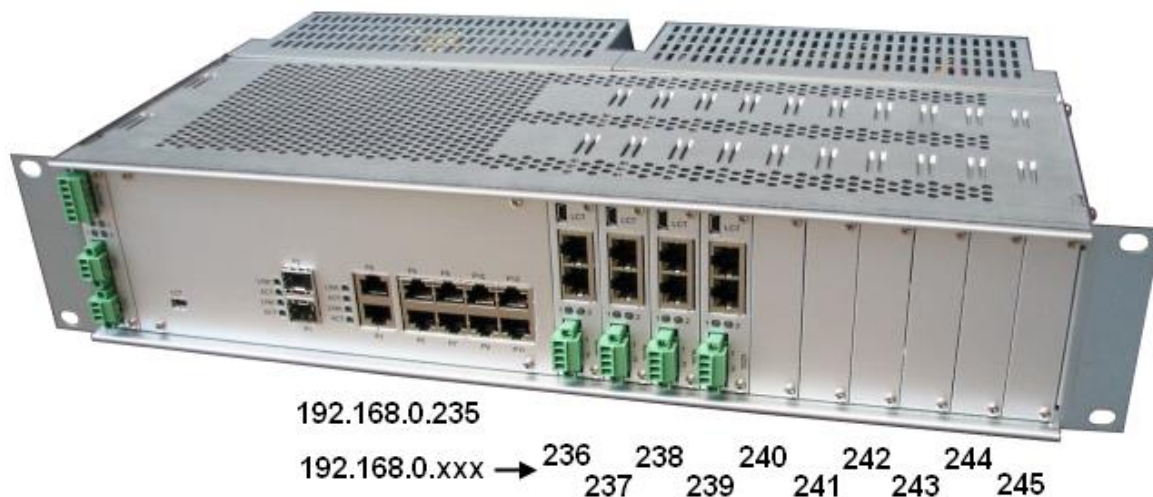


Figure 3.45: The default IP address for a subrack unit starts from left side with 192.168.0.235 for the included Switch. The line cards start from left side with 192.168.0.236 and end on the right side with 192.168.0.245.

3.2.25.4 FlatRack with Integrated Switch

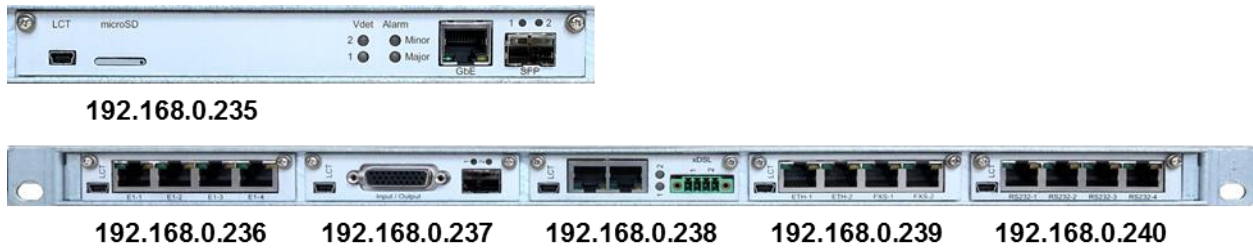


Figure 3.46: The IP address for a FlatRack is 192.168.0.235 (if the Switch included). The Line Cards start from left side with 192.168.0.236 and end on the right side with 192.168.0.240

3.2.25.5 Line Card



Figure 3.47: The default IP address for a single delivered line card is 192.168.0.236.

4 PROGRAMMING GUIDE MINIFLEX SWITCH (MF-MR2N-SW-12ETH,V2 ONLY)

4.1 MiniFlex Command Line Interface

MiniFlex command line interface (CLI) has a clear syntax and could be accessed from: Local Craft Terminal connected to USB interface; from Remote Host connected to MiniFlex over Telnet or SSH session. To configure all system parameters, user has to type command in a terminal window. Each **command** must be confirmed with **Enter** key. List of other useful key combinations represented in Table 4-1.

Key sequence	Description
BackSpace or Ctrl+h	Erase the character to the left of the cursor
The up arrow key or Ctrl+P	Recall the commands in the history buffer, beginning with the most recent command.
The left arrow key or Ctrl+B	Move the cursor back one character
The right arrow key or Ctrl+F	Move the cursor forward one character
The down arrow key or Ctrl+N	Selection of recent commands in the history buffer. Selection is valid after recalling the resent command by up arrow key or Ctrl+P
Ctrl+A	Move the cursor to the beginning of the command line
Ctrl+E	Move the cursor to the end of the command line
Ctrl+D	Delete the character at the cursor
Ctrl+K	Delete all characters from the cursor to the end of the command line
Ctrl+T	Transpose the current character and character located left from the cursor
Ctrl+U	Delete all characters from the cursor to the beginning of the command line
Ctrl+W	Delete the word to the left of the cursor

Table 4-1. MiniFlex CLI key combinations.

Any command could have several parameters. Parameters could be obligatory and optionally. Please refer to Table 4-2 for explanation of meanings of different fonts and symbols inside the user manual.

String	Description
command	A word with <i>Courier Italic</i> font is a command that user has to type. It must be confirmed with Enter key.
<parameter>	A word inside “ less than ” and “ greater then ” signs is an obligatory parameter that must be entered. It could be a string or a digital array
[parameter]	A word inside square braces is an obligatory parameter that must be chosen.
param1 param2	Parameter 1 or Parameter 2 should be used
{Parameter}*1	A parameter in Braces is optional. The command behind asterisk indicates the number of the commands in command line.
Text output	A text with <i>courier</i> font is a live screen capture of MiniFlex CLI

Table 4-2. Various fonts and symbols in the user manual.

Any command of CLI could be completed with **TAB** key. For example, a user type **sh** and press **TAB** key; CLI will complete a command and **show** will be displayed. If a user press **TAB** after completing a command, a list of all possible variants or a message that command is complete, will be shown:

```
FXOS> show
dhcp          dhcpr          dot1x          fdb
gvrp          history        idle-timeout   interface
port          radius         services       startup-config
syscontact    syslocation    terminal        version
FXOS> show
```

If a user types a question mark **?** symbol while typing a command, a list of available commands with their short meanings will be displayed:

```
FXOS>
clear          Clear screen
enable         Turn on privileged mode command
exit           Exit current mode and back to previous mode
help           Description of the interactive help system
list           Print command list
logout         Disconnect from switch and quit
no             Negate a command or set its defaults
ping           Ping command to test if the net is correct
quit           Disconnect from switch and quit
show           Show running system information
terminal       Set terminal line parameters
who            Display who is connected to the switch
FXOS>
```

If a user type **?** after typing a command or after typing a part of a command, for example **sh?**, a help for a command will be displayed:

```
FXOS> sh
show Show running system information
FXOS> show
dhcp          Show dhcp information
dhcpr         Show information of dhcp relay
dot1x         Show dot1x information
fdb           Config FDB entries information
gvrp          Show GARP Vlan Registration Protocol information
history       Display the session command history
idle-timeout  Idle timeout value in minutes and seconds
interface     Show interfaces in the system
port          Show port information
radius        Show RADIUS client information
services      Show information of system services status
startup-config Show contents of startup configuration
syscontact    Show the person who manage this host and how to contact this
              person
syslocation   Show the physical location of this host
terminal      Show terminal line parameters
version       Show version information
FXOS> show
```

It is possible to type only a part of a command, for example **sh ve** is equal to **show version** command.

A MiniFlex CLI will be accessible after successful boot of a device. A normal booting sequence is represented below:

```

Bootloader version 1.1
Check the system memory...OK

Checking the system flash file system...OK

OS is starting ...

Initializing Network Service .....

Initializing Management Service .....

Boot with empty configuration ...

#####
#                                     #
#                               Welcome to FXOS                               #
#                                     #
#       Press Return to connect and config this system.                     #
#                                     #
#####

```

Press Enter key to login into a system.



Default user name and password are admin

After successful login, system information will be displayed:

```

MODEL FG-MINIFLEX-SW18/4,V1
HWRV 00AA
SW Version 1.3(Build 0002 on 10:07:47 Jan 27 2010)
DATE 27-1-2010
HOSTNAME FlexDSL
SYSTEM_DATE_AND_TIME 1970/1/1 00:04:00
RUNS 0d 0:4:50
MODEL_DESC Minirack L2 18FE/4GE Ethernet Managed Switch
IP 192.168.0.254
MGMT_VLAN default
(c) FlexDSL Telecommunications AG
FXOS>

```

User could clear screen with **clear** command.

4.2 Getting Help

An easiest way to get help from command line is to type **help**

```
FXOS(config-vlan-research)#help
```

FXOS provides help feature as described below.

1. Anytime you need help, just press "?" and don't press Enter, you can see each possible command argument and its description.
2. You can also input "list" and then press Enter to execute this helpful command to view the list of commands you can use.

```
FXOS(config-vlan-research)#
```

To get a list of available commands type **list {command name}**. Command name could be not completed.

4.3 Read-Only and Privileged modes of operation

A MiniFlex CLI could work in read-only and in privileged modes. A command line prompt for read-only mode is **>**. In privileged mode, a command line prompt is **#**.

4.3.1 Entering to and exiting from privileged mode

enable to enter in privileged mode

exit to exit to read-only mode



Default password for privileged mode is admin

Commands that could affect a system operation are accessible in privileged mode only. They will not be displayed under ***help*** or ***list*** commands if executed from read-only mode.

4.4 User Management

There is only one user presents in a system by default. It has administrator rights and could access to privileged mode. Default user name is **admin**.

User could create other users and grant them rights of a normal user or of an administrator.

4.4.1 Creating a user

```
user add <username> login-password <login-password>
```

4.4.2 Configuring user rights

```
user role <username> [admin | normal]
```

4.4.3 Changing a password for privileged mode

```
user enable-password <enable-password> <username>
```

4.4.4 Changing a login password for a user

```
user login-password <username>
```

4.4.5 Getting a list of users

```
user list
```

4.4.6 Deleting a user

```
user delete <username>
```

4.5 Setting up a System Date and Time

A MiniFlex switch could synchronize its internal clock with a real-time clock server located in the Internet using Simple Network Time Protocol (SNTP), or a user could configure a system clock and date manually.

4.5.1 An automatic System Date and Time Settings

This case could be used if MiniFlex switch is connected to the Internet or to Intranet Network Time Protocol (NTP) server. An internal SNTP Client (SNTPC) should be configured according to the steps from Table 4-3.

#	Command	Description
1	<code>config sntpc serverip <A.B.C.D></code>	Setup an IP address of Network Time Protocol Server. 204.152.184.72 could be used as an example.
2	<code>config sntpc timezone <west east> <0 -12></code>	Configure a node time zone. East or West means where node is located from Greenwich meridian. 0 - 12 are time zone number, counted from it.
3	<code>config sntpc interval hours <0 - 1000> minutes <0 - 59></code>	Select a time update interval in hours and minutes
4	<code>config sntpc enable</code>	Type this command to enable a SNTP client.

Table 4-3. Setting up a SNTP Client

To check the status of the SNTP Client type:

show sntpc status

A following output will be shown:

```
FXOS(config)# show sntpc status
SNTP client status      : enable
SNTP client clock status : synchronized
SNTP reference server ip : 204.152.184.72
SNTP client poll interval : 0 hour(s) 1 minute(s)
SNTP client timezone    : east 1
FXOS(config)#
```



Please make sure that your node has access to Internet or Intranet NTP server.

4.5.2 Manual System Date and Time Settings

This case could be used if MiniFlex switch has no access to Internet and corporate network has no NTP server. User has to configure system date and time manually according to steps from Table 4-4.

#	Command	Description
1	<code>config sntpc disable</code>	Make sure that SNTP Client is disabled.
2	<code>config system date year <1970 - 2036> month <1 - 12> day <1 - 31></code>	Configure a node date
3	<code>config system hour <0 - 23> minute <0 - 59></code>	Configure a node time

Table 4-4. Manual Date and Time configuration.

4.5.3 System Date and Time Displaying

show system time

```
FXOS(config)# show system time
Year:2010 Month:2 Day:1
Hour:13 Minute:51 Second:8
FXOS(config)#
```

4.6 Understanding your environment

Before going deep, it is important to understand an existing configuration of your node. This chapter describes how to check it.

4.6.1 Checking your access rights

who am i

```
FXOS(config)# who am i
I am *Session [11] : user admin connected from console.
FXOS(config)#
```

4.6.2 Checking who else is connected to a system

who

```
FXOS(config)# who
SessionID. - UserName ----- LOCATION ----- MODE ----
11          admin              console              CONFIG    (That's me.)
13          testuser           192.168.169.12      VIEW
Total 2 sessions in current system.
FXOS(config)#
```

4.6.3 Dropping a session of another user

Check a session you want to drop with **who** command and then:

kill session <1 - 19999>

4.6.4 Checking a node, you connected to

show syslocation



User could configure system location with **config syslocation <.location (100 Char)>** command

4.6.5 Checking a contact person

show syscontact



User could add a contact person name and a phone with **config syscontact <.contact (100 Char)>** command

4.6.6 Check software version

show version

```
FXOS(config)# show version

MODEL FG-SW8/4-RAIL,V1
HWRV 00AA
SW Version 1.3(Build 0002 on 10:07:47 Jan 27 2010)
DATE 27-1-2010
MODEL_DESC DIN-Rail L2 8FE/4GE Ethernet Managed Switch
OS FXOS
SN HEM100300001 1001
MAC 00:0f:d9:da:c1:25

FXOS(config)#
```

4.6.7 Setting an IP address of a switch

To set up an IP address for a switch **ip <A.B.C.D/M> gateway <A.B.C.D>** command is used.

```
FXOS(config)# ip 192.168.100.137/24 gateway 192.168.100.254
```

4.6.8 Deleting a IP address of a switch

To delete an IP address a **no ip** command is used.

```
FXOS(config)# no ip
```

4.6.9 Check an IP address and switching configuration of a node

A node IP address is displayed after successful login:

```
Login: admin
Password:

MODEL FG-MINIFLEX-SW18/4,V1
HWRV 00AA
SW Version 1.3(Build 0002 on 10:07:47 Jan 27 2010)
DATE 27-1-2010
HOSTNAME FlexDSL
SYSTEM_DATE_AND_TIME 2010/2/1 17:04:00
RUNS 2d 23:35:17
MODEL_DESC DIN-Rail L2 8FE/4GE Ethernet Managed Switch
IP 192.168.169.239
MGMT_VLAN default
(c) FlexDSL Telecommunications AG

FXOS>
```

It is also possible to find an IP address and switching configuration with a command:

show interface vlan

```
FXOS> show interface vlan
Interface VLAN default:

Link status                :Up
Administrative status      :Up
Vlan ID                    :1
Vlan Type                  :Port-based
IP Address                 :192.168.169.239/24
Gateway                   :192.168.169.254
Learn status               :enable

Port member list:
  eth1/1(u)    eth1/2(u)    eth1/3(u)    eth1/4(u)
< -----Skipped----->

FXOS>
```

4.6.10 List interface status

show interface ethernet

```
FXOS(config)# show interface ethernet
Interface Ethernet eth1/1:

Link status                :Down
Administrative status      :Up
Port type                  :1000Base-TX
AutoNegotiation            :disabled
AutoNegotiation capability :1000M
Current speed              :1000M
Duplex                     :full
FlowControl                :disabled
Learning                   :enabled
MAC limit                  :0
Port-bridge                :disabled
Trust                      :enabled
Ip-vlan                    :disabled
Mac-vlan                   :disabled

Be added into vlan(s):
  Vlan name:default, vlan ID:1 , untagged

Interface Ethernet eth1/2:
< -----Skipped----->
```

4.6.11 Display a forwarding database (FDB)

show fdb

```
FXOS(config)# show fdb
----- Begin of FDB Table Information -----
```

VLAN name	Mac address	Type	Interface	Queue
default	000f.d9da.c125	permanent	CPU	3
default	0100.5e00.0001	mcast	CPU	0
default	001c.c423.5dcc	dynamic	1/4	0
default	0030.4f4d.c3bb	dynamic	1/4	0

```
-----
Total 4 MAC address filter entry showed.

----- End of FDB Table Information -----
FXOS(config)#
```

4.6.12 Get a technical support.

A User may be asked to provide full technical setup for possible debugging and solution reproducing at manufacturer's laboratory. It could happen if a user asks for a technical support. Please provide a live capture of a following command and send it to your support engineer:

show tech-support

4.7 Saving and restoring a system configuration

A MiniFlex switch has four different configurations:

- Startup configuration – a configuration that will be loaded during system startup
- Running configuration – a current configuration
- Backup configuration – a reserve copy of some configuration
- Factory default – an original configuration with default parameters.

Upon first system start a factory default configuration is loaded to MiniFlex Switch. Startup configuration has left unchanged until a User makes changes and saves a new configuration. A new configuration will be loaded during next system boot.

A User could save a second copy of current configuration as a backup configuration and restore it later as a startup configuration.

4.7.1 Saving a current configuration as a startup configuration

It is important to know that any command User types and confirms with **Enter** key become valid immediately. A User creates desired configuration command by command, and, if created configuration complies to his needs he can store it in system EEPROM. A User could also reboot a switch without saving a configuration. A previously made startup configuration will be loaded after system boot. If no startup configuration was created, a factory default configuration will be loaded during next system boot.

To save current configuration into startup configuration type:

save configuration

```
FXOS(config)# save configuration
Trying to save configuration to flash, please wait...
Preparing data for saving configuration...Done.

Starting writing configuration data to flash...Done.

Configuration saved to flash successfully.

FXOS(config)#
```

4.7.2 Saving current configuration as a backup configuration

Backup configuration gave an additional flexibility to a User. He could store a second working configuration as a backup and quick use it if new configuration was wrong. To save current configuration as a backup configuration type:

save backup-config

```
FXOS(config)# save backup-config
Trying to save configuration to flash, please wait...
Preparing data for saving configuration...Done.
```

```
Starting writing configuration data to flash...
Done.
```

```
Configuration saved to flash successfully.
```

```
FXOS(config)#
```

4.7.3 Restoring a backup configuration

To restore backup configuration type:

restore backup-config

```
FXOS(config)# restore backup-config
Trying to save backup configuration as startup configuration, please wait...
Preparing data for saving configuration...Done.
```

```
Starting writing configuration data to flash...Done.
```

```
Configuration saved to flash successfully.
```

```
FXOS(config)#
```

A backup-configuration will not be destroyed after restoring.



Please note that restored configuration will be effective only after system reboot

4.7.4 Restoring a factory defaults

To restore factory defaults a User needs to erase a startup configuration with a command:

erase startup-config

```
FXOS(config)# erase startup-config
Are you sure to erase startup-config? [Y/N]Y
```

```
Trying to erase all configuration from flash, please wait .....
Finished.
Successfully erase all config information from flash.
```

```
FXOS(config)#
```

A backup-configuration will not be destroyed after restoring.



Please note to reboot a switch to activate factory default configuration.

4.7.5 Rebooting a switch

During system reboot a switch rereads a startup configuration, if startup configuration exists. To reboot a switch please type a command:

```
reboot
FXOS(config)# reboot
Are you sure to reboot switch system? [Y/N]Y

System is going to reboot.....

Disconnected.
```

4.7.6 Viewing a configuration and storing it on a PC

It is possible to view startup, running and backup configuration and store it on a PC for future download or for archiving purposes. A method how to store a configuration depends on terminal software used for accessing to CLI.

4.7.6.1 Viewing a running configuration

```
show running-config
FXOS(config)# show running-config
!FXOS system config file
!Version 1.3(1.2.0)
!Basic information config
config sysname test123test
< -----Skipped----->
```

4.7.6.2 Viewing a startup configuration

```
show startup-config
FXOS(config)# show startup-config
!FXOS system config file
!Version 1.3(1.2.0)
!Basic information config
config sysname test123test
< -----Skipped----->
```

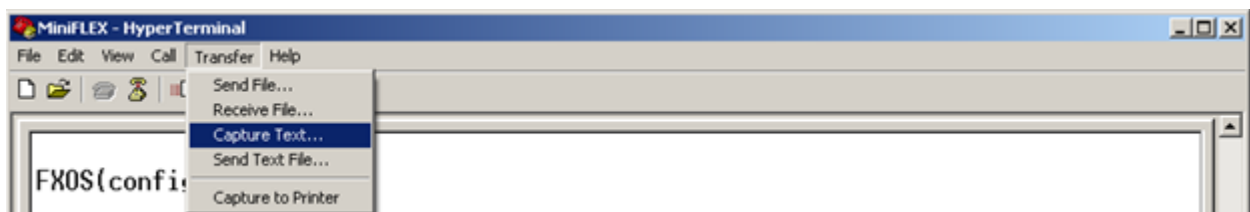
4.7.6.3 Viewing a backup configuration

```
show backup-config
FXOS(config)# show backup-config
!FXOS system config file
!Version 1.3(1.2.0)
!Basic information config
config sysname test123test
< -----Skipped----->
```

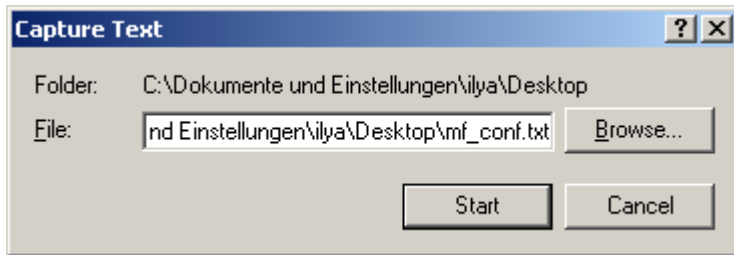
4.7.6.4 Storing a configuration with Hyper Terminal

A Hyper Terminal software is a popular terminal client that supports connection through serial interface or through Telnet protocol. It was included to Microsoft Windows 95, 98, ME, 2000 and XP, but it was discontinued in Windows Vista. If you have Hyper Terminal software you could store a MiniFlex configuration according to a step-by-step guide from this chapter.

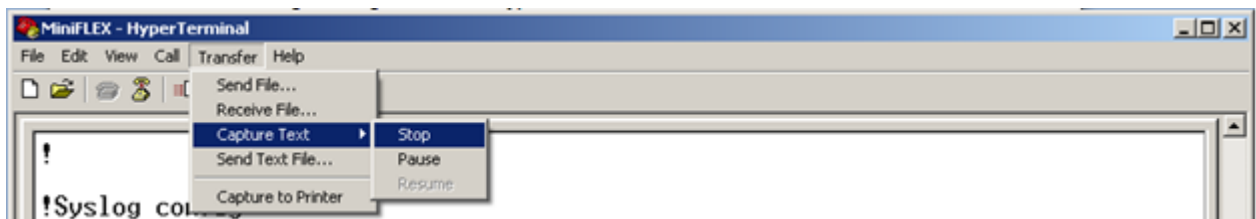
- Go to Transfer ---> Capture Text



- Select a file to save configuration, use txt extension for a file



- Click on Start to capture a screen output of a MiniFlex CLI
- Type a command from 4.7.6.1 - 4.7.6.3 to show desired configuration. Press any key so many times as needed until command prompt appears again.
- Go to Transfer ---> Capture Text ---> Stop and stop screen capturing



- Open a file you just saved and remove all unnecessary characters:
 - First line of a file should be:
!FXOS system config file
 - Last line of a file should be:
!End of config
 - Please remove **all** "--Press any key to continue Ctrl+c to stop--" messages from a file. Please keep a "!Parameter" string in the end of a line with "Press any key ..." message. For example:

String before modification:

```
!Dot1x config
!
--Press any key to continue Ctrl+c to stop--
!
```

!Serp config

String after modification:

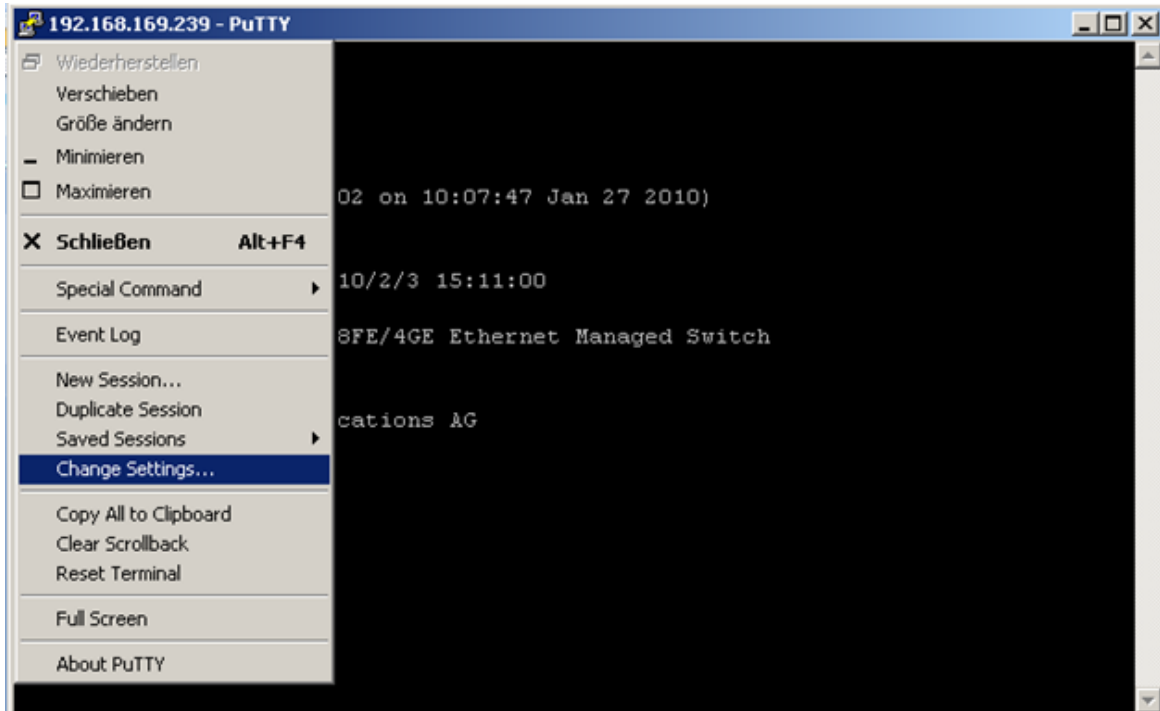
```
!Dot1x config
!
!Serp config
!
```

- Save file

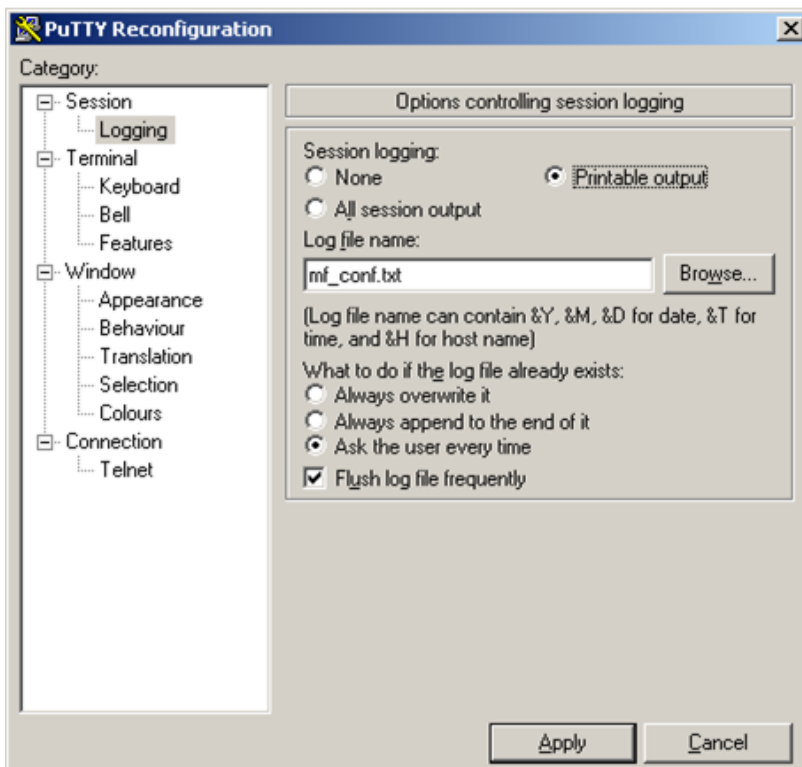
4.7.6.5 Storing a configuration with PuTTY

PuTTY is a freeware that supports serial connection as well as Telnet and SSH protocols. If you use PuTTY software, you could store a MiniFlex configuration according to a step-by-step guide from this chapter.

- Click on PuTTY icon on the left top side of a window, click on change settings



- Click on Session ---> Logging and select log file name. Use txt extension for a file. Click on Printable Output and on Apply button.



- Type a command from 4.7.6.1 - 4.7.6.3 to show desired configuration. Press any key so many times as needed until command prompt appears again.
- Click on PuTTY icon again and select Change settings. Stop logging by selecting "None" under Session ---> Logging dialog.
- Open a file you just saved and remove all unnecessary characters:
 - First line of a file should be:
!FXOS system config file
 - Last line of a file should be:
!End of config
 - Please remove **all** "--Press any key to continue Ctrl+c to stop--" messages from a file. Please keep a "!Parameter" string in the end of a line with "Press any key ..." message. For example:

String before modification:

```
!Dot1x config
!
--Press any key to continue Ctrl+c to stop--
!Serp config
```

String after modification:

```
!Dot1x config
!
!Serp config
!
```

- Save file

4.7.7 Download a configuration to a switch

It is possible to download a previously saved configuration file from a PC to a switch with FTP protocol. To download please make sure that FTP server is running and accessible from a MiniFlex switch and run a command:

```
download ftp config <A.B.C.D> <user> <pass> <filename>
```



Please restart a switch for applying a downloaded configuration

4.8 Working with ports

Any Port of MiniFlex switch acts as Ethernet Port. It could be located on a front panel or directed to backplane. Please refer to a picture below.

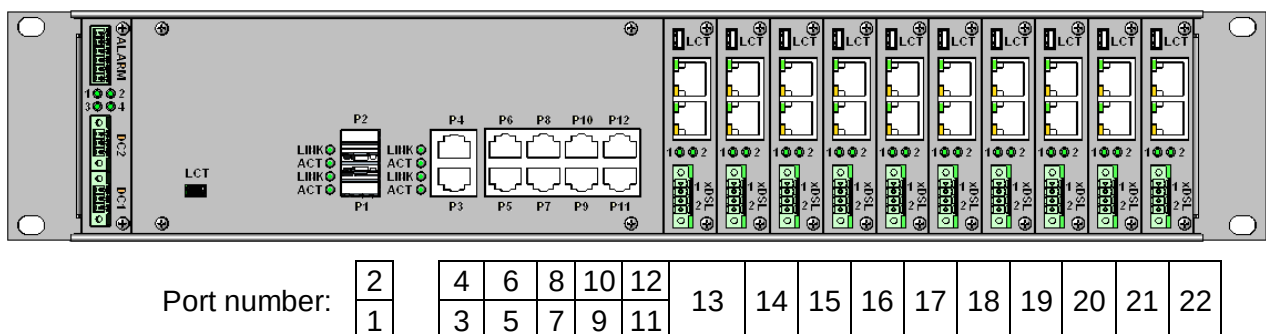


Figure 4.1 MiniFlex Port numbering

To configure any port a command **interface ethernet 1/<port>** is used. For example, to configure port number 12 type:

```
interface ethernet 1/12  
FXOS (config-if-eth1/12) #
```

A command prompt shows that user enable a configuration mode of port 1/12.

To exit from port configuration mode type:

```
exit  
FXOS (config) #
```

A full list of commands available in Port configuration mode is shown in Table 4-5.

#	Command	Description
1.	<code>access-list [enable disable] <lists></code>	Enables or disables an Access List on Ethernet interface. It is possible to add up to 63 lists with Access Control Rules to a port.
2.	<code>access-list [enable disable] default</code>	Enables or disables a Default Access List on a port. Default Access list has only one rule: "Deny Everything" and it will be enabled automatically if any of Access Lists would be enabled. The meaning of "Default" Access List is to deny everything, and then to open some rules defined in other Access Lists.
3.	<code>access-list {[<1-63> all]}*1</code>	Shows an information about defined Access List
4.	<code>auto [enable disable]</code>	Enables or disables an Auto Negotiation of a port. Default state: Enabled
5.	<code>broadcast-rate [dlf mcast bcast all] <0-1000000></code>	Sets a broadcast limit for different types of broadcast packets in kbps. Broadcast packets are: DLF: Destination Lookup Fail MCAST: Multicast BCAST: Broadcast All: All of mentioned above
6.	<code>capable [10 100 1000]</code>	Configures a capability of Ethernet interface in Mbps
7.	<code>clear</code>	Clears screen
8.	<code>clear statistics</code>	Clears port statistics
9.	<code>description <string> {<string>}*29</code>	Creates a string (strings) with port description. You could use it, for example; to identify a connected user.
10.	<code>discard [untag tag all none]</code>	This command tells which packets will be discarded upon receiving to a port: packets without VLAN tag, with tag, all or none
11.	<code>duplex [full half]</code>	Configures duplex settings of a port. Please make sure that Auto negotiation is disabled before applying.
12.	<code>egress-rate <0-1000000></code>	Configures an outgoing packets rate in kbps. Zero value disables rate limit.
13.	<code>exit</code>	Exits from port configuration mode
14.	<code>flowcontrol [enable disable]</code>	Configures flow control settings of a port
15.	<code>help</code>	Shows help

16.	<code>ingress-rate <0-1000000></code>	Configures an incoming packets rate in kbps. Zero value disables rate limit.
17.	<code>ip-vlan [enable disable]</code>	Enables or disables an IP VLAN on a port. IP VLAN means that packets from defined subnet will be mapped to dedicate VLAN.
18.	<code>isolate from <portlist></code>	Isolates current port from others. If port isolation function enabled, no traffic exchange is possible between isolated ports.
19.	<code>learning [enable disable]</code>	This command enables or disables MAC address learning for a port. It is enabled by default
20.	<code>list</code>	List of available commands
21.	<code>list <string></code>	List command that match a string
22.	<code>Logout</code>	Closes current session
23.	<code>mac-limit <0-16384></code>	Sets a limit of MAC address to a port
24.	<code>mirror [ingress egress] <portlist></code>	Enables or disables incoming or outgoing mirror for selected ports
25.	<code>mirror ingress <portlist> egress <portlist></code>	Enables or disables incoming or outgoing mirror for selected ports
26.	<code>no description</code>	Deletes a description of a port
27.	<code>no isolate</code>	Cancels port isolation function
28.	<code>no mirror</code>	Cancels port mirroring
29.	<code>no qos map [priority dscp]</code>	Cancels QoS settings of a port
30.	<code>no shutdown</code>	Cancels port shutdown
31.	<code>ping {[-t]}*1 {[-count] <1-65535>}*1 <A.B.C.D></code>	Performs ICMP requests with unlimited or limited (1 – 65535) attempts to defined IP address
32.	<code>port-bridge [enable disable]</code>	Enables or disables a port bridge function. If enabled, packets will be returned back to the direction they were received from. This feature could be used for connecting of wireless base stations.
33.	<code>qos bandwidth <0-7> [<64-1024000> 0]</code>	Defines a bandwidth in kbps for a queue number 0 – 7. If 0 is selected, bandwidth control is disabled.
34.	<code>qos default-priority <0-7></code>	Configures default QoS priority for a port
35.	<code>qos map dscp [enable disable]</code>	Enables or disables a DSCP mapping to a queue
36.	<code>qos map dscp-priority <0-63> to <0-7></code>	Map a DSCP enabled packet with specified marker to a queue number 0 – 7
37.	<code>qos map priority-queue <0-7> to <0-7></code>	Map an 802.1p TOS priority to QoS priority queue
38.	<code>qos queue-weight <0-15> <0-15> <0-15> <0-15> <0-15> <0-15> <0-15> <0-15></code>	Defines a WRR weight value for queues 0 to 7
39.	<code>qos sched-mode [pg wrr]</code>	Selects a QoS method: Strict Priority or Wight Round Robin
40.	<code>quit</code>	Exits from port configuration mode
41.	<code>rspan tpid <0-65535> vlan-id <0-4095></code>	Enables a remote mirror for TPID and VID. Default TPID for VLAN is HEX8100, DEC33024
42.	<code>show broadcast-rate {[dlf mcast bcst]}*1</code>	Shows a broadcast rate for dedicated group of packets
43.	<code>show default-priority</code>	Displays a default priority of a port
44.	<code>show discard</code>	Displays what packets are discarded on a port

45.	<code>show history</code>	Shows a history of commands
46.	<code>show interface ethernet {<portlist>}*1 {[statistics]}*1</code>	Displays an information about defined Ethernet interface and its statistics
47.	<code>show isolate</code>	Shows port isolation
48.	<code>show qos bandwidth {<0-7>}*1</code>	Displays a QoS bandwidth settings
49.	<code>show qos map [priority dscp]</code>	Shows QoS mapping for TOS or DSCP markers
50.	<code>show queue-configurations</code>	Displays a queues scheduling mode
51.	<code>show rate-limit {[ingress egress]}*1</code>	Shows a rate limit for incoming and outgoing packets in kbps
52.	<code>show running-config {[dhcp dot1x fdb gvrp interface login-auth nas nms radius-client snmp stp syslog usermanage]}*1</code>	Displays a running configuration of a whole system, or of defined part
53.	<code>show vlan-filter {[ingress egress]}*1</code>	Displays a status of VLAN filter function of a port
54.	<code>show {[configuration statistics]}*1</code>	Displays a configuration or statistics of a port
55.	<code>shutdown</code>	Shut down a port
56.	<code>speed [10 100 1000]</code>	Manually selects a speed of a port. Please make sure that Auto negotiation is disabled before applying.
57.	<code>trust [enable disable]</code>	Enables or disables a trust function of a port. Trust function means that if it is enabled, all packets will be forwarded to respective VLAN in tagged or in untagged mode. If Trust function is disabled, all packets will be forwarded to Default VLAN. It is enabled by default
58.	<code>vlan-filter [ingress egress] [enable disable]</code>	Enables or disables VLAN filtering function for incoming and outgoing traffic. VLAN filter function means, that, if enabled, packet will be forwarded to VLAN a port belongs to. If unknown packet arrives, it will be blocked. On another hand, if VLAN filter is disabled a packet with undefined VID arrived, it will be forwarded according to a rule of VLAN with VID even if a port is not a member of this VLAN.
59.	<code>vlan-prefer[ip mac]</code>	Sets which type of VLAN will be activated on a port: IP-subnet based, or source MAC based.

Table 4-5. Commands to configure Ethernet interface

4.9 Working with VLAN

MiniFlex switch supports several types of VLANs. A user could create a VLAN based on criteria listed below:

- Physical port
- IEEE 802.1q tag
- IP Subnet
- Source MAC address

It is also possible to mix some of criteria, for example to create VLAN based on a port and tag.

Port-Based VLAN usually used to separate one group of ports from another group of ports. Each port works in **untagged** mode what means that normal PC or another Ethernet device could be connected to it. It is important to know that one port could belong to one VLAN only in Port-Based mode. A Port-Based VLAN terminated in single switch, i.e. two or more switches could not share same Port-Based VLAN.

VLAN Based on TAG has been defined in IEEE 802.1q standard and usually used to carry separate data over common media, e.g. over single Ethernet electrical, fiber or xDSL link. Because of a VLAN tag, a port could share several VLAN. Port works in **tagged** mode what means that only equipment with 802.1q support, i.e. another Switch or Server with tag-enabled network card must be connected to it. A TAG Based VLAN is not limited by single Switch; it could pass through full network.

A combination of Port-Based and TAG-Based VLAN is the mostly used method to connect two or more remote locations over single media. This method combines Ethernet ports worked in **untagged** and **tagged** mode. Untagged ports are used for subscriber's connection while tagged ports are used as common transmission media.

IP subnet-based VLAN is used to create VLAN only for devices which belong to defined IP subnet. It could be used, for example, to separate traffic from VoIP devices in common network and to give them better QoS and priority.

MAC-based VLAN is used to create VLAN for defined device (devices). It could be used to separate them from others or to give them special QoS.

4.9.1 Creating a Port-Based VLAN

In a default configuration of a MiniFlex Switch all it ports are combined into single Port Based VLAN with name **default**. This means that all ports can exchange information between each other.



Example: To create two port-based VLAN with names "research" and "operation" and add four ports into each. Ports 1/5-1/8 will be added into VLAN "research"; ports 1/9 – 1/12 will be added into VLAN "operation". VLAN "operation" will be used for switch management. It will have IP address 192.168.100.137.

#	Command	Description
1.	FXOS(config)# interface vlan research	Create VLAN "research"
2.	FXOS(config-vlan-research)#add port 1/5-8 untagged	Add ports 1/5 – 1/8 in untagged mode to a VLAN research
3.	FXOS(config-vlan-research)#exit	Exit from VLAN configuration
4.	FXOS(config)# interface vlan operation	Create VLAN "operation"
5.	FXOS(config-vlan-operation)#add port 1/9-12 untagged	Add ports 1/9 – 1/12 in untagged mode to a VLAN research
6.	FXOS(config-vlan-operation)#exit	Exit from VLAN configuration
7.	FXOS(config)# management vlan operation	Set VLAN "operation" as management VLAN
8.	FXOS(config)# ip 192.168.100.137/24 gateway 192.168.100.254	Set an IP address for a switch

Check a new configuration:

show interface vlan

```
FXOS(config)# show interface vlan
Interface VLAN default:
```

```
Link status           :Down
Administrative status :Up
Vlan ID               :1
Vlan Type             :Port-based
Learn status          :enable

Port member list:
  eth1/1(u)  eth1/2(u)  eth1/3(u)  eth1/4(u)
  eth1/13(u) eth1/14(u)  eth1/15(u) eth1/16(u)
  eth1/17(u) eth1/18(u)  eth1/19(u) eth1/20(u)
  eth1/21(u) eth1/22(u)
```

```
Trunk member list:
```

```
Interface VLAN research:
```

```
Link status           :Up
Administrative status :Up
Vlan ID               :2
Vlan Type             :Port-based
Learn status          :enable

Port member list:
  eth1/5(u)  eth1/6(u)  eth1/7(u)  eth1/8(u)
```

```
Trunk member list:
```

```
Interface VLAN operation:
```

```
Link status           :Down
Administrative status :Up
Vlan ID               :3
Vlan Type             :Port-based
IP Address            :192.168.100.137/24
Gateway               :192.168.100.254
Learn status          :enable

Port member list:
  eth1/9(u)  eth1/10(u)  eth1/11(u)  eth1/12(u)
```

```
Trunk member list:
```

```
FXOS(config)#
```

4.9.2 Deleting a VLAN

To delete a VLAN a **no interface vlan <vlan name>** command is used

no interface vlan research

```
FXOS(config)# show interface vlan
Interface VLAN default:
```

```
Link status           :Up
Administrative status :Up
Vlan ID               :1
Vlan Type             :Port-based
Learn status          :enable

Port member list:
  eth1/1(u)  eth1/2(u)  eth1/3(u)  eth1/4(u)
  eth1/5(u)  eth1/6(u)  eth1/7(u)  eth1/8(u)
  eth1/13(u) eth1/14(u)  eth1/15(u) eth1/16(u)
  eth1/17(u) eth1/18(u)  eth1/19(u) eth1/20(u)
  eth1/21(u) eth1/22(u)
```

```
Trunk member list:
```

Interface VLAN operation:

```

Link status           :Up
Administrative status :Up
Vlan ID               :3
Vlan Type             :Port-based
IP Address            :192.168.100.137/24
Gateway               :192.168.100.254
Learn status          :enable

Port member list:
  eth1/9(u)    eth1/10(u)    eth1/11(u)    eth1/12(u)

Trunk member list:

```

FXOS(config)#

4.9.3 Creating a TAG-based VLAN

To create a TAG-based VLAN and add ports into it a few commands should be executed in configuration mode.



Example: To create a TAG-based VLAN with name “research” and VID 100 and add four ports: 1/5 – 1/8 into it.

#	Command	Description
1.	FXOS(config)# interface vlan research 100	Create VLAN “research” with VID = 100
2.	FXOS(config-vlan-research)#add port 1/5-8 tagged	Add ports 1/5 – 1/8 in tagged mode to a VLAN research
3.	FXOS(config-vlan-research)#exit	Exit from VLAN configuration

Check a new configuration:

show interface vlan

```

FXOS(config)# show interface vlan
Interface VLAN default:

```

```

Link status           :Up
Administrative status :Up
Vlan ID               :1
Vlan Type             :Port-based
IP Address            :192.168.169.137/24
Gateway               :192.168.169.254
Learn status          :enable

Port member list:
  eth1/1(u)    eth1/2(u)    eth1/3(u)    eth1/4(u)
  eth1/5(u)    eth1/6(u)    eth1/7(u)    eth1/8(u)
  eth1/9(u)    eth1/10(u)   eth1/11(u)   eth1/12(u)
  eth1/13(u)   eth1/14(u)   eth1/15(u)   eth1/16(u)
  eth1/17(u)   eth1/18(u)   eth1/19(u)   eth1/20(u)
  eth1/21(u)   eth1/22(u)

Trunk member list:

```

Interface VLAN research:

```

Link status           :Down
Administrative status :Up
Vlan ID               :100
Vlan Type             :Port-based
Learn status          :enable

Port member list:
  eth1/5(t)    eth1/6(t)    eth1/7(t)    eth1/8(t)

Trunk member list:

```

FXOS(config)#

As you see, ports 1/5-8 belong to two VLAN: “default” and “research”. This means that, if untagged packet will arrive to a port, it will be forwarded to “default” VLAN. If tagged packet with VID=100 will arrive to a port, it will be forwarder to “research” VLAN.

4.9.4 Creating a Port and TAG-based VLAN

Please execute a command sequence in configuration mode to create VLAN consisted of tagged and untagged ports



Example: to create two VLAN: “research” (ports 1/5-8, untagged), “operation” (ports 1/9-12). VLAN “research” should have VID=100, VLAN “operation” should have VID=101. Ports 1/1-4 must be added to both VLAN in tagged mode. VLAN operation will be used as managed VLAN

#	Command	Description
1.	FXOS(config)# interface vlan research 100	Create VLAN “research” with VID = 100
2.	FXOS(config-vlan-research)#add port 1/1-4 tagged	Add ports 1/1 – 1/4 in tagged mode to a VLAN “research”
3.	FXOS(config-vlan-research)#add port 1/5-8 untagged	Add ports 1/5 – 1/8 in untagged mode to a VLAN research
4.	FXOS(config-vlan-research)#exit	Exit from VLAN configuration mode
5.	FXOS(config)# int vlan operation 101	Create VLAN “operation” with VID = 101
6.	FXOS(config-vlan-operation)#add port 1/1-4 tagged	Add ports 1/1 – 1/4 in tagged mode to a VLAN “operation”
7.	FXOS(config-vlan-operation)#add port 1/9-12 untagged	Add ports 1/9 – 1/12 in untagged mode to a VLAN “operation”
8.	FXOS(config-vlan-operation)#exit	Exit from VLAN configuration mode
9.	FXOS(config)# management vlan operation	Set VLAN “operation” as Management VLAN
10.	FXOS(config)# ip 192.168.100.137/24 gateway 192.168.100.254	Set an IP address and gateway for a switch

Check a new configuration:

show interface vlan

```
FXOS(config)# show interface vlan
Interface VLAN default:
```

```
Link status           :Down
Administrative status :Up
Vlan ID               :1
Vlan Type             :Port-based
Learn status          :enable

Port member list:
  eth1/1(u)   eth1/2(u)   eth1/3(u)   eth1/4(u)
  eth1/13(u)  eth1/14(u)  eth1/15(u)  eth1/16(u)
  eth1/17(u)  eth1/18(u)  eth1/19(u)  eth1/20(u)
  eth1/21(u)  eth1/22(u)
```

```
Trunk member list:
```

```
Interface VLAN research:
```

```
Link status           :Up
Administrative status :Up
Vlan ID               :100
Vlan Type             :Port-based
Learn status          :enable

Port member list:
  eth1/1(t)   eth1/2(t)   eth1/3(t)   eth1/4(t)
  eth1/5(u)   eth1/6(u)   eth1/7(u)   eth1/8(u)
```

Trunk member list:

Interface VLAN operation:

```
Link status           :Up
Administrative status :Up
Vlan ID               :101
Vlan Type             :Port-based
IP Address            :192.168.100.137/24
Gateway              :192.168.100.254
Learn status         :enable
```

Port member list:

```
eth1/1(t)  eth1/2(t)  eth1/3(t)  eth1/4(t)
eth1/9(u)  eth1/10(u)  eth1/11(u)  eth1/12(u)
```

Trunk member list:

FXOS(config)#

4.9.5 Creating an IP Subnet-based VLAN

It is possible to create a VLAN based on IP subnet. Please execute a list of commands for that purpose.



Example: to create IP Subnet-Based VLAN: “research” with Network 192.168.100.0/24 and VID=100 and add port 1/6 to it.

#	Command	Description
1.	FXOS(config)# interface vlan research ip-subnet 192.168.100.0/24 100	Create VLAN “research” with VID = 100 for a subnet
2.	FXOS(config-vlan-research)#add port 1/6 untagged	Add port 1/6 – 1/4 in untagged mode to a VLAN “research”
3.	FXOS(config-vlan-research)#exit	Exit from VLAN configuration mode
4.	FXOS(config)# interface ethernet 1/6	Enter to Port 1/6 configuration mode
5.	FXOS(config-if-eth1/6)#ip-vlan enable	Enable an IP Subnet Based VLAN on a port
6.	FXOS(config-if-eth1/6)#exit	Exit from port configuration

Check a new configuration:

show interface vlan

FXOS(config)# show interface vlan
Interface VLAN default:

```
Link status           :Up
Administrative status :Up
Vlan ID               :1
Vlan Type             :Port-based
IP Address            :192.168.0.254/24
Gateway              :192.168.0.253
Learn status         :enable
```

Port member list:

```
eth1/1(u)  eth1/2(u)  eth1/3(u)  eth1/4(u)
eth1/5(u)  eth1/6(u)  eth1/7(u)  eth1/8(u)
eth1/9(u)  eth1/10(u)  eth1/11(u)  eth1/12(u)
eth1/13(u)  eth1/14(u)  eth1/15(u)  eth1/16(u)
eth1/17(u)  eth1/18(u)  eth1/19(u)  eth1/20(u)
eth1/21(u)  eth1/22(u)
```

Trunk member list:

Interface VLAN research:

```
Link status           :Up
Administrative status :Up
Vlan ID               :100
Vlan Type             :IP-based
Learn status         :enable
```

```
IP Subnet          :192.168.100.0
Network Mask      :255.255.255.0
```

```
Port member list:
  eth1/6(u)
```

```
Trunk member list:
```

```
FXOS(config)#
```

Please note that Port 1/6 becomes a member of two VLAN: “default” and “research”. A PC connected to a port 1/6 has two IP addresses: 192.168.100.24/24 and 192.168.169.24/24. Packets that belongs to IP Subnet 192.168.100.0/24 will be forwarded according to the rules of VLAN “research” while packets from IP subnet 192.168.196.0/24 will be forwarded according to rules of VLAN “default”.

Check a Forwarding Database:

```
FXOS(config)# show fdb
```

```
FXOS(config)# sh fdb
```

```
----- Begin of FDB Table Information -----
```

VLAN name	Mac address	Type	Interface	Queue
default	000f.d904.4700	permanent	CPU	3
default	0100.5e00.0001	mcast	CPU	0
default	0090.f53e.7a0b	dynamic	1/6	0
research	0090.f53e.7a0b	dynamic	1/6	0
default	001c.c460.fbb8	dynamic	1/12	0
<-----Skipped----->				
default	001c.c481.bfb8	dynamic	1/12	0
default	0016.3537.2c09	dynamic	1/12	0

```
Total 16 MAC address filter entry showed.
```

```
----- End of FDB Table Information -----
```

```
FXOS(config)#
```

Port 1/6 has two entries in Forwarding Database.

4.9.6 Creating a MAC-Based VLAN

It is possible to create a VLAN based on source MAC address. This could be used for additional security and flexibility. MiniFlex Switch will forward a packet with defined MAC into special VLAN. It is possible to add up to 128 MAC addresses into VLAN.



Example: to create MAC Based VLAN: “research” with source MAC 0090.f53e.7a0b connected to port 1/6 with VID=100.

#	Command	Description
1.	FXOS(config)# interface vlan research 100	Create a VLAN “research” with VID 100
2.	FXOS(config-vlan-research)#add port 1/6 untagged	Add port 1/6 in untagged mode
3.	FXOS(config-vlan-research)#exit	Exit from VLAN configuration mode
4.	FXOS(config)# mac-vlan add 0090.f53e.7a0b vlan research	Add a MAC address to VLAN “research”
5.	FXOS(config)# mac-vlan enable 1/6	Enable a MAC VLAN on port 1/6



To delete MAC based VLAN, a customer need to delete assigned MAC address first a command **mac-vlan delete [<H.H.H> | all]** used for this.

4.9.7 A list of commands related with plain VLAN

A full list of commands used for VLAN configuration is shown in Table 4-6.

#	Command	Description
1.	show interface vlan {vlan name}*1	Displays an information about all VLAN or about defined VLAN
2.	interface vlan <vlanname> {<1-4094>}*1	Creates a VLAN with “vlanname” and optionally defined VID. Command Line Goes to VLAN configuration mode.
3.	interface vlan <vlanname> ip-subnet <A.B.C.D/M> {<1-4094>}*1	Creates a IP-Subnet based VLAN with defined “vlanname”, IP subnet and optionally defined VID. Command Line Goes to VLAN configuration mode.
4.	mac-vlan [enable disable] [<portlist> all]	Enables MAC based VLAN for defined ports
5.	mac-vlan add <H.H.H> vlan <name> {priority <0-7>}*1	Adds a MAC entry to defined VLAN with defined priority.
6.	mac-vlan delete [<H.H.H> all]	Deletes a defined MAC entry or all entries from MAC based VLAN
7.	show mac-vlan	Displays an information about MAC-based VLAN
8.	management vlan <vlanname>	Sets a VLAN “vlanname” as management VLAN
9.	no interface vlan <vlanname>	Deletes a VLAN “vlanname”
10.	[add delete] port <portlist> [tagged untagged]	Adds or deletes a port (a list of ports) into VLAN in tagged or untagged mode
11.	[add delete] trunk <trunkname> [tagged untagged]	Adds or deletes a Trunk with “trunkname” into VLAN with tagged or untagged mode
12.	clear	Clears screen
13.	description <string> {<string>}*29	Adds a description to VLAN
14.	exit	Exits from VLAN configuration mode
15.	help	Shows Help
16.	learn [enable disable]	Enables or disables MAC address learning for a VLAN. It is enabled by default.
17.	list {<string>}*1	Shows a list of all commands or only commands that contains defined string.
18.	no description	Deletes a VLAN description
19.	pfm [drop flood all]	Configures a VLAN multicast filtering function. All: all Multicast packets will be forwarded into this VLAN Drop: Unknown Multicast packets will be dropped Flood: Unknown Multicast packets will be forwarded into this VLAN
20.	logout	Closes a session
21.	quit	Closes a session
22.	show interface vlan {vlan name}*1	Displays an information about all VLAN or about defined VLAN

Table 4-6. Commands to configure VLAN interface

4.10 Forwarding Database

All network devices have MAC address to uniquely identify themselves. These addresses are used for data transmission; each Ethernet packet has MAC address of source and destination. A plain Layer 2 Ethernet switch creates a forwarding database (FDB) and stores this information in it:

- Port number
- Egress MAC address

Upon receiving a packet, a switch looks into FDB and checks if destination MAC address exists. If FDB has a record with destination MAC address, a packet will be forwarded to an egress port.

MiniFlex is not a plain Layer 2 Ethernet switch, it has VLAN functionality. It means that same port could carry several VLAN. A FDB entry could be dynamical, permanent or used by System, so a MiniFlex FDB has following entries:

- Egress interface (Port or Trunk)
- Egress MAC address
- VLAN name a MAC address belongs to
- Type of entry (static, dynamic or system)

A FDB table can store up to 16384 records with default aging time equal to 300 seconds. Default system settings allow storing of every new entry in FDB. A list of commands related with FDB is shown in Table 4-7.

#	Command	Description
1.	<code>fdb agingtime [0 <1-3600>]</code>	Selects an FDB aging time in seconds. If 0 is selected, then an entry will not be aged. Default value is 300 seconds
2.	<code>fdbentry mac <H.H.H> vlan <name> <slot/port> {queue <0-7>}*1</code>	Manually adds a MAC address and binds it to VLAN, port with selected priority queue.
3.	<code>fdbentry mac <H.H.H> vlan <name> <trunkname> {queue <0-7>}*1</code>	Manually adds a MAC entry to Trunk interface with selected queue
4.	<code>fdbentry mac <H.H.H> vlan <name> drop</code>	Writes an entry into black list. All packets will be dropped from this address
5.	<code>no fdb agingtime</code>	Deletes aging time settings and restores default settings
6.	<code>no fdbentry drop mac <H.H.H> vlan <name></code>	Removes an entry from black list
7.	<code>no fdbentry mac <H.H.H> vlan <name></code>	Removes a permanent entry from FDB
8.	<code>show fdb agingtime</code>	Shows a FDB aging time settings
9.	<code>show fdb drop</code>	Shows a list of entries to drop packets from (a black list)
10.	<code>show fdb {[count]}*1 {[dynamic permanent mcast]}*1 {[port trunk] <name>}*1 {[mac] <H.H.H>}*1 {[vlan] <name>}*1</code>	Shows FDB entries: dynamic, permanent, multicast, by MAC, VLAN

Table 4-7. Commands to configure FDB

4.11 Rapid Spanning Tree

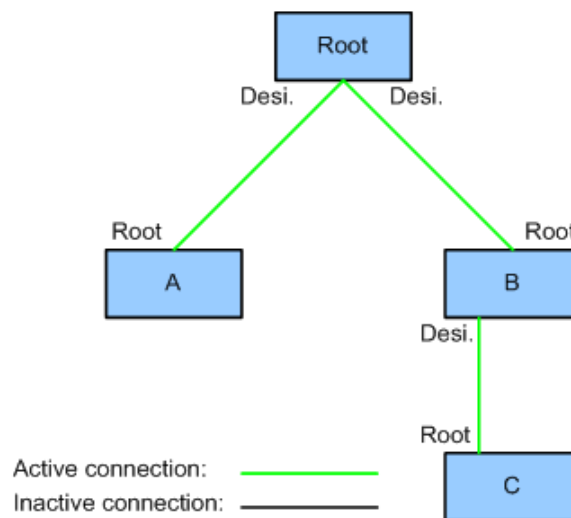
Rapid Spanning Tree Protocol (RSTP) is based on IEEE 802.1w standard. It used for dynamic link switching in networks with ring topology. The ring topology improves reliability of data networks; nevertheless, Ethernet networks must have only one active path between any of two nodes to prevent packet loop. 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

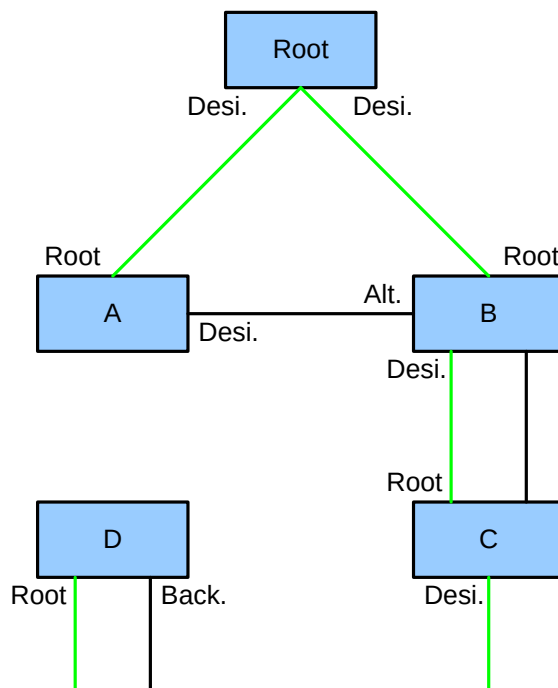
One switch in a RSTP-enabled network must acts as Root Bridge. Root Bridge selection will be done automatically according to Bridge ID – a unique ID that each member of RSTP network has. Bridge ID is a combination of Switch MAC address and Bridge Priority. Switch with smallest Bridge Priority will act 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 behavior. 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 like it is shown on picture below:

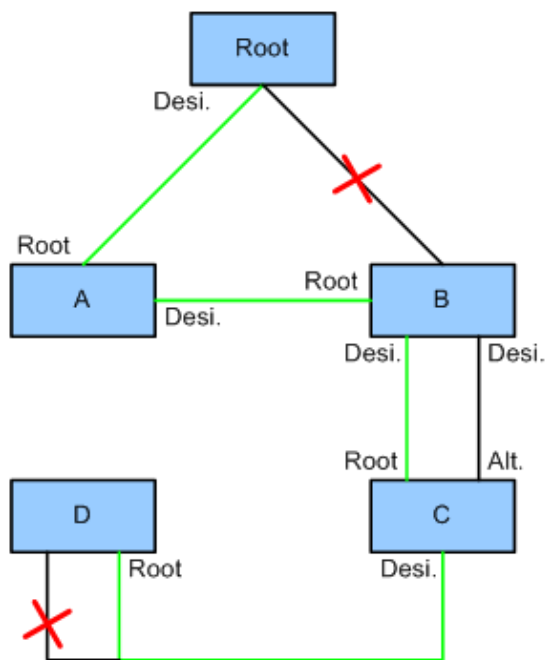


A Root and Designated ports are active, they learn and Forward packets. Other ports have blocking state. They could act as Alternate port or as Backup port. Please take a look on below picture for reference:



Active connection: —
Inactive connection: —

If active path will not be present any more, the second path will be automatically selected.



Active connection: —
Inactive connection: —

RSTP configuration must be done in accordance with a following schedule:

- Enabling or disabling a RSTP function for a switch
- Enabling or disabling a RSTP function for an interface (Trunk or Port)
- Configuring a RSTP parameters

A list of RSTP related commands is shown in Table 4-8.

#	Command	Description
1.	<code>spanning-tree mode [cst mst]</code>	Select a Spanning Tree Protocol operation mode: Common Spanning Tree or Multiple Spanning Tree
2.	<code>show running-config stp</code>	Shows current Spanning Tree Configuration
3.	<code>config spanning-tree</code>	Enters into Spanning Tree Configuration Mode
4.	<code>show spanning-tree</code> <code>show spanning-tree mst <0-30></code> <code>show spanning-tree mst port <sl/port></code> <code>show spanning-tree mst summary</code> <code>show spanning-tree mst trunk <trunkname></code> <code>show spanning-tree port <slot/port></code> <code>show spanning-tree trunk <trunkname></code>	Shows Spanning Tree configuration for port or trunk interface; for CST or for MST
#	Commands in Spanning Tree configuration mode	Description
5.	<code>debug spanning-tree</code>	Starts a debugging for some parameters: all, bridge, edge, info, migrate, p2p, pcost, rolesel, roletrans, sttrans, topoch, transmit Parameters
6.	<code>exit</code>	Exits from STP configuration mode
7.	<code>no debug spanning-tree</code>	Stops STP debugging
8.	<code>no spanning-tree [forward-delay hello-time maximum-age priority]</code>	Resets a STP parameters to default
9.	<code>no spanning-tree port <slot/port> [edge non-stp p2p path-cost priority]</code>	Resets a STP parameters of a port to default
10.	<code>no spanning-tree trunk <trunkname> [path-cost priority non-stp p2p edge]</code>	Resets a STP parameters of a trunk to default
11.	<code>show debug spanning-tree</code>	Shows a debug information
12.	<code>show spanning-tree port <slot/port></code>	Shows an STP information of a port
13.	<code>show spanning-tree trunk <trunkname></code>	Shows an STP information of a trunk
14.	<code>spanning-tree [enable disable]</code>	Enables or disables a STP for a switch
15.	<code>spanning-tree [forward-delay] <4-30></code>	Sets a forward-delay interval in seconds. This parameter indicates a time period while a port will be in listening and learning state, i.e. will build an FDB table. When a forward-delay period will be over, a port will turn into forwarding state. Default value is 15 seconds.
16.	<code>spanning-tree [hello-time] <1-10></code>	Sets a time period "hello-time". This period indicates that BPDU packet will be send every "hello-time". Default value is 2 seconds.
17.	<code>spanning-tree [maximum-age] <6-40></code>	Sets a maximum-age interval. This interval is used to detect that data path is defected.

		Data path could become defected if three consecutive BPDU packets were not reached, or if "maximum-age" time counter expires. Default maximum-age time is 20 seconds.
18.	<code>spanning-tree [priority] <0-61440></code>	Sets a priority for STP-enabled switch. Switch with lower STP priority value will become a root in RSTP enabled network. Default switch priority is 32768. If all switches in a network have same default priority settings, a switch with lower MAC address will be selected as a root. STP priority must be multiple of 4096
19.	<code>spanning-tree [port <slot/port> trunk <trunkname>] [edge] [yes no]</code>	Selects an Edge attribute for an interface. If selected, a port will not participate in RSTP tree construction. Upon receiving a BPDU packed to a port with Edge attribute it will become a normal port and will participate in RSTP tree construction. Edge ports must be connected to terminal stations.
20.	<code>spanning-tree [port <slot/port> trunk <trunkname>] [non-stp] [yes no]</code>	Selects if an interface will participate in RSTP network construction or not.
21.	<code>spanning-tree [port <slot/port> trunk <trunkname>] [p2p] [yes no auto]</code>	Selects a P2P attribute for an interface. A PTP attribute could be activated for an interface that is connected to another switch.
22.	<code>spanning-tree [port <slot/port> trunk <trunkname>] [path-cost] [auto <1-200000000>]</code>	Selects a path cost for an interface. A path with lower cost will be selected for data transmission.
23.	<code>spanning-tree [port <slot/port> trunk <trunkname>] [priority] <0-240></code>	Selects a priority for an interface. In interface with lower priority will be selected as root port. Default priority value is 128 and it must be multiple to 16.

Table 4-8. Commands to configure RSTP



The values for Hello-time, Max-Age and Forward-Delay must meet the following rule:
 $2 * (\text{Hello-time} + 1) \leq \text{Max-Age} \leq 2 * (\text{Forward-Delay} - 1)$

4.12 Link Aggregation Control Protocol

A Link Aggregation Control Protocol (LACP) is based on IEEE 802.3ad and used to activate dynamic link aggregation and de-aggregation between two peers by sending a LACPDU (link Aggregation Control Protocol Data Units).

LACP must be activated between two nodes. One node must be set to Active, while another node can be active or passive.

LACP can be used for load balancing or for redundant links creation.

A list of LACP related commands is shown in Table 4-9

#	Command	Description
1.	config lacp [enable disable]	Enables or disables a LACP for a node
2.	config lacp port <portlist> mode [active passive off]	Adds port (ports) into trunk with Active (will send LACPDU) or Passive mode. Deletes port (ports) from a trunk.
3.	config lacp system-priority <0-65535>	Configures a system priority. It is an optional value. Default is 32768. Higher values represent lower priority.
4.	config lacp port <portlist> priority <0-255>	Optionally sets a priority for a port (ports)
5.	config lacp port <portlist> key <0-1023>	Optionally sets a LACP administrative key.
6.	config lacp port <portlist> [add delete] vlan <vlanname>	This command allows VLAN assign or dissociate to a group of ports participating in the LACP construction. These VLANs will be transmitted even if only one port from LACP channel is present. This command must be executed before <code>config lacp port mode</code> command
7.	show interface trunk	Displays active trunk status.
8.	show running-config lacp	Displays active trunk configuration

Table 4-9. Commands to configure LACP

4.13 Trunks

Trunks are used to enhance a throughput between two Ethernet switches by combining of several Ethernet interfaces into single bundle. Both peers must have same group configuration to prevent Ethernet data loops. One port in a group acts as “Master” port. It must be in operational state while trunk group creation. A port with lower number will become a “Master” port.

A list of Trunk related commands is shown in Table 4-10

#	Command	Description
1.	interface trunk <trunkname>	Creates a Trunk interface with “Trunkname”
2.	no interface trunk <trunkname>	Deletes a Trunk Interface “Trunkname”
3.	show interface trunk {<trunkname>}*1 {[statistics]}*1	Shows information about a Trunk or its statistics
4.	show trunk-policy	Show Trunk Policy
5.	trunk-policy [dmac-based smac-based dmac-smac-based dip-based sip-based dip-sip-based]	Sets a Trunk policy: Destination MAC, Source MAC, Destination IP, Source IP
#	Commands in Trunk configuration mode	Description
6.	clear	Clears screen
7.	clear statistics	Clears interface statistics
8.	description <string> {<string>}*29	Adds a description to an interface
9.	exit	Exits from Trunk configuration mode
10.	grouping <portlist>	Adds ports to a Trunk group. It is possible to have 2 Trunk groups with up to 8 ports in each
11.	mac-limit <0-16384>	Sets a MAC limit for an interface
12.	no description	Deletes an Interface description
13.	no grouping	Deletes ports from Trunk group

Table 4-10. Commands to configure Trunk

4.14 Switch Ethernet Ring Protection

A Switch Ethernet Ring Protection (SERP) mechanism improves performance of Ethernet rings. Unlike STP/RSTP rings, a SERP enabled network allows rapid loop protection and path convergence with time period less than 1 sec. Most networks could have convergence time less than 50 msec. SERP protocol doesn't limit a number of nodes in a ring and doesn't increase a protection switching time with increasing of nodes in a ring.

Concept

All nodes working in a SERP enabled ring share same **Domain**. A node could act as **Master** node or as **Transit** node. One node in a ring becomes a Master node, other acts as Transit nodes. Every node is connected to a ring with two ports: **Primary Port** and **Secondary Port**. Primary Port of Master node used to forward traffic, while Secondary port of Master node works in blocking state. A Primary and Secondary ports of Transit nodes work in forwarding state. A secondary port of a node should be connected to a primary port of previous node. And so on and so forth in a ring.

A Master node checks a ring health with **Control VLAN**. Please add only primary and secondary ports of every node into it to achieve fastest switching time. An interval between Control VLAN data units is user selectable. On the other hand, a **Protected VLAN** is used to carry time sensitive data traffic. SERP examples are shown on Figure 4.2 and Figure 4.3

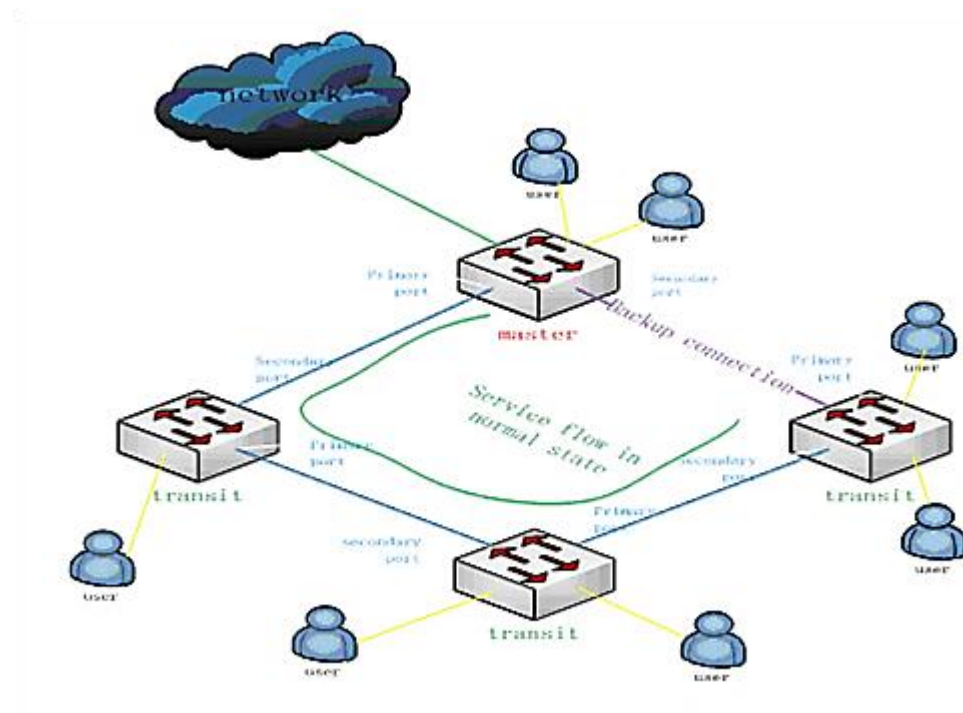


Figure 4.2. SERP concept: normal mode

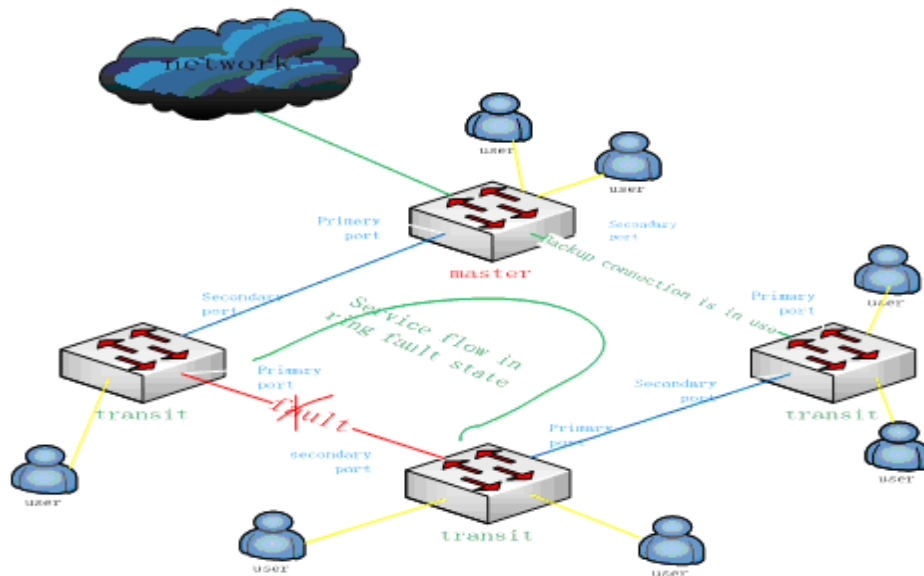


Figure 4.3. SERP concept: failure appears

A list of SERP related commands is shown in Table 4-11

#	Command	Description
1.	config serp	Opens a SERP configuration submenu
2.	show running-config serp	Shows SERP Running Configuration
3.	show serp domain {[<name>]}*1	Show SERP domain information
#	Commands in SERP configuration mode	Description
4.	serp [enable disable]	Enables or Disables SERP
5.	create serp domain <name> {<1-1>}*1	Create SERP domain "Name" with optional ID. It is only one domain supported with current firmware.
6.	config serp domain <name> [enable disable]	Enables or disables SERP domain.
7.	config serp domain <name> mode [master transit]	Sets a Role for a Node in SERP domain
8.	config serp domain <name> add control_vlan <name>	Adds a Control VLAN into SERP domain
9.	config serp domain <name> delete control_vlan	Deletes a control VLAN from SERP domain
10.	config serp domain <name> [add delete] protected_vlan <name>	Adds or deletes protected VLAN into or from SERP domain
11.	config serp domain <name> add [primary_port secondary_port] <slot/port>	Adds primary or secondary port into SERP domain
12.	config serp domain <name> delete [primary_port secondary_port]	Deletes a primary or secondary port from SERP domain
13.	config serp domain <name> [hello_time hello_fail_time] <time>	Sets a timing interval for keep alive messages inside Control VLAN. A <time> parameter must follow the rule: $1 \leq \text{hello time} * 3 \leq \text{hello fail time} \leq 500$ 1 represents 100ms
14.	config serp domain <name> upflush_fail_time <time>	Configures an SERP domain upflush fail time
15.	no config serp domain <name> [hello_time hello_fail_time]	Restores default timing settings for hello time and for hello fail time
16.	no config serp domain <name> upflush_fail_time	Restores default timing settings for upflush fail time
17.	no create serp domain <name>	Deletes a SERP domain

Table 4-11. Commands to configure SERP

4.15 IGMP Snooping

The IGMP Snooping feature helps to reduce unnecessary traffic in IP Multicast network scenarios. In general IP Multicast was designed to reduce network load due to the fact that several users could share same stream from multimedia server, for example IPTV stream. In that case only users that have correct subscription would receive data while other will be blocked. However, because IP Multicast runs on Layer 3 level and there are no Layer 2 multicast control protocols exist, a switch has to build own Layer 2 forwarding database from IP Multicast headers. This translation is called IGMP Snooping.

A list of IGMP Snooping related commands is shown in Table 4-12

#	Command	Description
1.	<code>igmp-snooping [enable disable]</code>	Enables or disables IGMP Snooping
2.	<code>igmp-snooping addmemberport <slot/port> vlan <vlanname></code>	In order to realize the IGMP protocol for a specified VLAN, it is possible to add a static multicast member port
3.	<code>igmp-snooping addmemberport trunk <trunkname> vlan <vlanname></code>	In order to realize the IGMP protocol for a specified TRUNK, it is possible to add a static multicast member port
4.	<code>igmp-snooping addqueryport <portlist></code>	IGMP Snooping query is used in networks where IGMP and PIM are not implemented because Multicast traffic has not to be routed. After the IGMP Snooping query will be enabled on a switch, it will send out IGMP queries that will trigger the ports on listening switch (with IGMP snooping enabled). The IGMP Snooping enabled switch will trigger ports depending on these queries. There must be only one switch in a VLAN that will send IGMP query. The command adds port or ports to query send list.
5.	<code>igmp-snooping addqueryport trunk <trunkname></code>	The command adds TRUNK to query send list.
6.	<code>igmp-snooping addrouter <slot/port> vlan <name></code>	Manually adds IGMP or PIM router to desired port and VLAN
7.	<code>igmp-snooping addrouter trunk <name> vlan <name></code>	Manually adds IGMP or PIM router to desired TRUNK
8.	<code>igmp-snooping delete all</code>	Deletes all IGMP Snooping configuration
9.	<code>igmp-snooping delete vlan <name> group [<A.B.C.D> all]</code>	Deletes Multicast group A.B.C.D or ALL groups from VLAN
10.	<code>igmp-snooping delmemberport <slot/port> vlan <name></code>	Manually deletes member port
11.	<code>igmp-snooping delmemberport trunk <trunkname> vlan <vlanname></code>	Manually deletes member TRUNK
12.	<code>igmp-snooping delqueryport trunk <trunk></code>	Deletes query TRUNK
13.	<code>igmp-snooping delqueryport <portlist></code>	Deletes query port
14.	<code>igmp-snooping delrouter <slot/port> vlan <name></code>	Deletes Multicast router from port and VLAN
15.	<code>igmp-snooping delrouter trunk <name> vlan <name></code>	Deletes Multicast router from a TRUNK
16.	<code>igmp-snooping grouplife [<10- 1000> default]</code>	Sets IGMP Snooping aging time. Default is 250 seconds

17.	<code>igmp-snooping queryinterval [<10-300> default]</code>	Sets IGMP common query interval. Default is 125 seconds
18.	<code>igmp-snooping responsetime [<10-25> default]</code>	Set IGMP Snooping response time. Default is 10 seconds
19.	<code>igmp-snooping robust [<1-100> default]</code>	Set IGMP Snooping specific query interval. Default is 2 seconds
20.	<code>igmp-snooping routerlife [<20-600> default]</code>	Set IGMP Snooping router aging time. Default is 250 seconds
21.	<code>show igmp-snooping</code>	Displays actual IGMP Snooping information
22.	<code>show igmp-snooping grouplife</code>	Shows IGMP Snooping group aging time
23.	<code>show igmp-snooping hosttimeout</code>	Shows IGMP host aging time
24.	<code>show igmp-snooping memberport</code>	Shows IGMP Snooping members
25.	<code>show igmp-snooping queryinterval</code>	Shows IGMP standard query interval
26.	<code>show igmp-snooping queryport</code>	Shows IGMP query port
27.	<code>show igmp-snooping responsetime</code>	Shows IGMP Snooping response time
28.	<code>show igmp-snooping robust</code>	Shows IGMP specific query interval
29.	<code>show igmp-snooping router</code>	Shows IGMP router
30.	<code>show igmp-snooping routerconfig</code>	Shows IGMP Snooping router configuration
31.	<code>show igmp-snooping routerlife</code>	Show IGMP Snooping router aging time

Table 4-12. Commands to configure IGMP Snooping

4.16 Multicast VLAN registration

Multicast VLAN Registration (MVR) is a technology that can be used as an alternative to Protocol Independent Multicast (PIM) to create large Multicast Networks for IPTV providers. In Ethernet networks sending multiple multicast streams to several receivers in separate VLANs will cause traffic multiplication because each VLAN will carry same traffic. The Multicast VLAN Registration allows sharing Multicast data between several subscribers VLAN without affecting their private data.

In general MVR technology is similar to IGMP Snooping. Both technologies listen to Multicast messages (Join and Leave) and build Layer 2 forwarding database respectively. The difference between IGMP Snooping and MVR is that IGMP Snooping can work over dedicated VLAN, while MVR can work with hosts over different VLANs over Layer 2 network.

Both MVR and IGMP Snooping technologies can coexist in one switch. In case if MVR and IGMP Snooping are enabled on a switch, a MVR will react on join and leave messages from Multicast groups configured under MVR.

The MiniFlex Switch supports MVR static and MVR dynamic operational modes.

In static mode, a multicast data received by MVR-enabled host, will be forwarded to all MVR-enabled user ports if these ports are configured as MVR receiver and are added into the multicast group with defined VLAN. The multicast data will be forwarded only to MVR-enabled ports that were statically configured. IGMP messages received from MVR-enabled hosts will never be forwarded from MVR data ports that were statically configured.

In dynamic mode, the multicast data received by MVR-enabled hosts will be forwarded only to those MVR user ports that have been joined a group ether by IGMP messages or by MVR static configuration. IGMP messages received from MVR-enabled hosts will never be forwarded from MVR data ports that were statically configured.

You must configure a port with defined VLAN as MVR receiver. No MVR receiver ports exist in a switch by default. The MVR receiver must not belong to MVR VLAN.

Important knowledge about Multicast VLAN Registration

- Only one MVR VLAN is supported
- If VLAN is destined for MVR VLAN, all ports in this VLAN shouldn't belong to any other VLAN
- MVR receivers (user ports) could be in different VLAN but they shouldn't belong to MVR VLAN
- an MVR receiver can be neither IGMP Snooping router port nor IGMP Snooping member
- The maximum number of multicast entries (MVR group addresses) that can be configured on a switch is 256
- You should enable IGMP Snooping before setting MVR to dynamic mode. The warning message will be displayed otherwise.
- You can't delete a VLAN with **no interface vlan <vlanname>** command if it is a MVR VLAN. You have to cancel the MVR feature on it firstly with **delete mvrvlan <vlanname>** command.
- If VLAN has MVR receivers, you have to delete them before deleting a VLAN. Otherwise a warning message will be shown.

A list of Multicast VLAN Registration related commands is shown in Table 4-13.

#	Command	Description
1.	<code>show running-config mvr</code>	Shows active MVR running config
2.	<code>config mvr</code>	Enters to a MVR configuration mode
3.	<code>enabled</code>	Enables MVR feature
4.	<code>disabled</code>	Disables MVR feature
5.	<code>mvr mode [static dynamic]</code>	Configures MVR static or dynamic mode of operation
6.	<code>add receiver port <portlist> {vlan <vlanname>}*1</code>	Before using a MVR function, you must add ports as MVR receiver. You could add ports only once. Use <portlist> and VLAN name to specify the source. If VLAN parameter is missed, then MVR function will listen all VLAN a port belongs to.
7.	<code>mvr vlan <vlanname></code>	Configures VLAN with defined <vlanname> as MVR VLAN. After entering this command, a CLI will go to MVR VLAN configuration mode.
8.	<code>add group <A.B.C.D> sport <slot/port> sip <A.B.C.D> {count <1-256>}*1</code>	In MVR VLAN configuration mode you must configure one or more (up to 256) multicast groups. A.B.C.D is a multicast group IP; sport is source port; sip is source IP
9.	<code>add user port <portlist> vlan <vlanname> group <A.B.C.D> {sip <A.B.C.D>}*1</code>	In MVR VLAN configuration mode you must add user ports <portlist> and connect them to multicast group with A.B.C.D IP address. Optionally it is possible to set source IP <sip>
10.	<code>delete group <A.B.C.D> sport <slot/port> sip <A.B.C.D> {count <1-256>}*1</code>	In MVR VLAN configuration mode this command deletes multicast group
11.	<code>delete user port <portlist> vlan <vlanname> group <A.B.C.D> {sip <A.B.C.D>}*1</code>	In MVR VLAN configuration mode this command deletes user ports
12.	<code>exit</code>	Exits MVR VLAN configuration mode back to MVR configuration mode
13.	<code>no mvr vlan <vlanname></code>	Cancels MVR VLAN. The VLAN <vlanname> will not be deleted.
14.	<code>show mvr {vlan <vlanname>}*1</code>	Shows information about MVR VLAN <vlanname>
15.	<code>show receiver {port <slot/port>}*1</code>	Shows receiver information
16.	<code>exit</code>	Exist from a MVR configuration mode

Table 4-13. Commands to configure Multicast VLAN Registration

4.17 Multiple Spanning Tree Protocol

The Multiple Spanning Tree Protocol was defined in IEEE 802.1s standard and later was merged in IEEE 802.1Q – 2003. It has backward compatibility with IEEE 802.1d STP and IEEE 802.1w rapid Spanning Tree and allows construction of several spanning tree instances in several VLANs. Each of VLAN could have own spanning tree topology.

In general, MSTP could be used for load balancing and for construction of large networks with high reliability therefore the failure in single instance of STP will not affect other STP instances.

Important knowledge about MSTP

- MSTP allows usage of several legacy STP instances in IEEE 802.1q enabled network
- VLANs could belong to different STP instances
- Each STP instance inside MSTP uses RSTP protocol for best convergence
- MSTP Region
 - A group of interconnected switches with same MSTP configuration organize an MSTP region
 - MSTP advantages could be used inside of a same region. Two or more regions have same Spanning Tree instance for all VLANs
 - To create a region all switches must have same:
 - Configuration name
 - Configuration Revision Number
 - VLAN to STP instances (STPI) map
- It is important to set MSTP protocol manually because RSTP is used by default
- It is important to set root switch for MSTP tree

A list of MSTP related commands is shown in Table 4-14.

#	Command	Description
1.	spanning-tree mode [cst mst]	Set spanning tree working mode. Default is common spanning tree (RSTP). You need to set it mst (Multiple Spanning Tree) manually
2.	config spanning-tree	Enters to a STP configuration mode
3.	spanning [enable disable]	Enables or disables spanning tree protocol support for a switch
4.	spanning-tree mst name <name>	Set name for MSTP copy. Name could have up to 32 characters.
5.	spanning-tree mst revision <0-65535>	Set the MSTP revision number
6.	spanning-tree map vlan <vlanlist> mst <0-30>	Map VLAN <vlanlist> for an MSTP Instance (0 – 30). <vlanlist> is a simple list, for example: for example:"1","1,2","1-10,13". If MST Instance is set to 0 the standard RSTP protocol will be used. It is compatibility mode.
7.	spanning-tree priority <0-61440> mst <0-30>	Set spanning tree priority for an MST Instance. Priority should be a multiplication of 4096. The switch with lowest priority value will become a root for defined MST Instance. It is important to set different switches as roots for different MST Instances. Please refer to chapter 4.11 «Rapid Spanning Tree» for Root Bridge definition.
8.	show spanning-tree mst <0-30>	Shows MST Instance information
9.	show spanning-tree mst summary	Shows MST summary
10.	show spanning-tree mst port <slot/port>	Shows an MST information of a port
11.	show spanning-tree mst trunk <trunkname>	Shows an MST information of a trunk
12.	exit	Exits from MST configuration mode

Other commands are equal to RSTP configuration. Please refer to Table 4-8 for details.

Table 4-14. Commands to configure Multiple Spanning Tree

4.18 Q-in-Q and VLAN Translation

The IEEE 802.1ad specification, commonly named as Q-in-Q or provider bridging, extends the IEEE 802.1Q standard by providing of a second tier of VLANs in a bridged network. It is mainly used in Metro Ethernet networks to create several independent paths between end customers. They can use same VLAN numbers for own purposes and, unlike pure IEEE802.1Q, their traffic will not be mixed up in backbone network.

Q-in-Q technology uses a second VLAN tag in Ethernet packet to separate and split user traffic. It increases a number of VLANs in L2 network. The total number could be $4096 \times 4096 = 116777216$.

Q-in-Q interface could work in UNI (User-to-Network Interface) or NNI (Network-to-Network Interface). NNI interface is connected to core network and always works in Tagged mode. UNI interface is connected to customer network and can work in tagged or in untagged mode.

FXOS allows TPID change. TPID means Tag Protocol Identifier and has 0x8100 value to identify that packet has IEEE 802.1Q format. It is default TPID value for MiniFlex Switch for Q-in-Q outer TAG, but it could be changed manually. Commonly used TPID values are: 0x9100, 0x9200 or 0x9300. IEEE 802.1ad specifies 0x88a8 value for service-provider outer tag.

Q-in-Q implementations

There are two types of Q-in-Q implementations: Basic Q-in-Q and Selective Q-in-Q

- Basic Q-in-Q

Basic Q-in-Q mode means that single defined TAG will be added when Ethernet packet will ingress to UNI port and egress from NNI port. The ingress packet could be tagged or untagged. If received packet has TAG already a second TAG will be added to it. If packet has no TAG, first of all it will be tagged with TAG of default VLAN and then second Q-in-Q TAG will be added.

- Selective Q-in-Q

Selective Q-in-Q gives more flexibility to Basic Q-in-Q. In this mode it is possible to tag frames with different outer VLAN tags depending on TAG of ingress packet (inner TAG). FXOS will work in selective Q-in-Q mode when user will configure UNI interface in tagged mode. VLAN translation table could be created in this mode.

A list of Q-in-Q related commands is shown in Table 4-15.

#	Command	Description
1.	<code>qinq [enable disable]</code>	Enables or disables a Q-in-Q feature for a switch
2.	<code>config qinq <portlist> [uni nni]</code>	Set interface role as NNI or UNI for <portlist>
3.	<code>config qinq <portlist> [add delete] <innervidrange> {<1-4094>}*1</code>	This command adds or deletes ports <portlist> with VLAN <innervidrange> to outer VLAN <1-4096>. The VLAN translation table has 1024 records. It means that maximum 1024 VLAN from <innervidrange> could be added
4.	<code>config qinq <portlist> tpid <hex_value></code>	Set TPID value for outer Q-in-Q packet for selected <portlist>. You could configure up to 3 different TPID
5.	<code>clear qinq tpid <hex_value></code>	You can clear the TPID through this command. If interface which has this TPID was added to a non-default VLAN, it will not clear the TPID.
6.	<code>show qinq vlan translation table</code>	Shows VLAN translation table
7.	<code>show qinq {<portlist>}*1</code>	Shows Q-in-Q information for <portlist>

Table 4-15. Commands to configure Q-in-Q

4.19 Jumbo Frames Support

MiniFlex Switch supports jumbo frames with up to 9216 bytes. A list of commands is shown in Table 4-16.

#	Command	Description
1.	<code>jumbo [enable disable]</code>	Enables or disables Jumbo Frame support
2.	<code>show jumbo</code>	Show Jumbo Frame support status

Table 4-16. Commands to configure Jumbo frames

4.20 Radius

RADIUS (Remote Authentication Dial In User Service) is a universal authentication and accounting protocol. It provides authentication and authorization of equipment or users connected to the LAN. Through such authentication, point-to-point user authentication mode can be provided in such a multi-point access environment as LAN. The port here refers to a single-point structure connected to the LAN. It can be the MAC address of the authenticated system, a physical interface of a server or network equipment that is connected to the LAN, or a workstation and access point defined in the IEEE 802.11 wireless LAN environment.

The RADIUS protocol has Client – Server structure. Its original client is the NAS (Net Access Server), and clients are running on PC or other network devices that shall be authenticated.

When a user accesses the NAS, the NAS submits the user information to the RADIUS server in the Access-Require data packet, including information of user name and password. Among them, the user password is encrypted with MD5. Both parties use the shared key that is not transmitted on the network.

The RADIUS server and the NAS server communicate with each other via the UDP protocol. The 1812 port of RADIUS server is responsible for authentication, while the 1813 port for accounting. The UDP is adopted since in most cases the NAS server and the RADIUS server are located in the same LAN and the UDP is quicker and more convenient.

4.20.1 Configuring Radius Attributes

The MiniFlex Switch used as the Network Access Switch (NAS). It communicates with Radius servers through Radius packets. Attributes in these packets are used to transmit the detailed information of authentication, authorization and accounting. The attributes in the current NAS version refer to the standard ones specified in RFC2865, RFC2866 and RFC2869. The system currently supports the following RADIUS standard attributes:

Serial #	Attribute name	Attribute Description
1	User-Name	Authenticated user name
2	User-Password	PAP authentication password
3	CHAP-Password	CHAP authentication password
4	NAS-IP-Address	IP address of the NAS equipment initiating the authentication request
5	NAS-Port	Physical port of the NAS equipment used for user access
6	Service-type	Service type requested by the user
7	Framed-Protocol	Link layer protocol of user access
8	Framed-IP-Address	IP address distributed to the user in the Radius mode
18	Relay-Message	Text information displayed for the user
24	State	Radius server state
25	Class	Class attribute send by Radius server
27	Session-Timeout	By-duration prepayment support

Serial #	Attribute name	Attribute Description
28	Idle-Timeout	Maximum timeout time of user idle
31	Calling-Station-ID	MAC address of the broadband access user
32	NAS-Identifier	NAS equipment ID
40	Acct-Status-Type	Accounting status (start or end)
44	Acct-Session-ID	User accounting ID
45	Acct-Authentic	User authentication mode
46	Acct-Session-Time	By-duration accounting
47	Acct-Input-Packets	Total input packets of the account
48	Acct-Output-Packets	Total output packets of the account
49	Acct-Terminate-Cause	Accounting termination cause
60	CHAP-Challenge	CHAP authentication support
61	NAS-Port-Type	Port type of the NAS equipment
79	EAP-Message	EAP-MD5 authentication support
80	Message-Authenticator	EAP-MD5 authentication support
85	Acct-Interim-Interval	Real-time accounting support

4.20.2 Configuring Radius Authentication Service

MiniFlex Switch supports Radius Authentication Service. A list of commands is shown in Table 4-17.

#	Command	Description
1.	<code>radius authentication [enable disable]</code>	Enables or disables Radius Authentication Service
2.	<code>radius authentication add-server id <0-4> server-ip <A.B.C.D> client-ip <A.B.C.D> {udp-port <1-6500>}*1</code>	Adds Radius authentication record. A Server ID is used for server selection. A Radius server with smallest ID will be selected firstly. It is possible to add up to 5 Radius servers. If server ID exists and you adding a new server with same ID, you must delete an old one firstly. Client IP is an IP address of a Radius Client. UDP port will be used for radius messages. It is 1812 by default
3.	<code>radius authentication delete-server id <0-4></code>	Deletes Radius authentication record for defined Radius server ID
4.	<code>radius authentication config-server id <0 - 4> shared-secret <secret></code>	Configures a "shared secret" for defined Radius server
5.	<code>radius authentication config-server id <0-4> retransmit-interval <5-300></code>	Sets retransmission interval for Radius server
6.	<code>radius authentication config-server id <0-4> max-retransmit-count <2-10></code>	Sets maximal retransmission count for radius server
7.	<code>show radius</code>	Shows Radius setup

Table 4-17. Commands to configure Radius Authentication

4.20.3 Configure Radius Accounting Service

MiniFlex Switch supports Radius Accounting Service. A list of commands is shown in Table 4-18.

#	Command	Description
1.	radius accounting [enable disable]	Enables or disables Radius Accounting Service
2.	radius accounting add-server id <0-4> server-ip <A.B.C.D> client-ip <A.B.C.D> {udp-port <1-6500>}*1	Adds Radius accounting record. A Server ID is used for server selection. A Radius server with smallest ID will be selected firstly. It is possible to add up to 5 Radius servers. If server ID exists and you adding a new server with same ID, you must delete an old one firstly. Client IP is an IP address of a Radius Client. UDP port will be used for radius messages. It is 1812 by default
3.	radius accounting delete-server id <0-4>	Deletes Radius accounting record for defined Radius server ID
4.	radius accounting config-server id <0 - 4> shared-secret <secret>	Configures a "shared secret" for defined Radius server
5.	radius accounting config-server id <0-4> retransmit-interval <5-300>	Sets retransmission interval for Radius server
6.	radius accounting config-server id <0-4> max-retransmit-count <2-10>	Sets maximal retransmission count for radius server
7.	show radius	Shows Radius setup

Table 4-18. Commands to configure Radius Accounting

4.20.4 Configuring ISP-Domain

The ISP-Domain concept becomes popular in access networks. The idea of ISP-Domain is that user send authentication message with username @ domainname. The Network Access Server send user authentication to particular server, a domainname belongs to. Therefore, users can choose several ISP to connect.

A list of ISP-Domain related commands is shown in Table 4-19.

#	Command	Description
1.	create isp-domain <domain>	Creates ISP-Domain <domain>
2.	config isp-domain <domain> authentication [enable disable]	Enables or Disables authentication for ISP-Domain <domain>
3.	config isp-domain <domain> authentication [add-server delete-server] id <0-4>	Add or delete Radius authentication server with ID <0-4> to ISP-Domain <domain>
4.	config isp-domain <domain> accounting [enable disable]	Enables or Disables accounting for ISP-Domain <domain>
5.	config isp-domain <domain> accounting [add-server delete-server] id <0-4>	Add or delete Radius accounting server with ID <0-4> to ISP-Domain <domain>
6.	config isp-domain <domain> accounting interim-update-accounting interval <10-65535>	Configures the interim update accounting interval in seconds
7.	config isp-domain <domain> accounting interim-update-accounting disable	Disable the interim update accounting interval
8.	show isp-domain <domain>	Shows information about ISP-Domain

Table 4-19. Commands to configure ISP-Domain

After the ISP-Domain is set up, and when a RADIUS server is added to the system, it can be used only after domain is allocated to it. By default, the system has a domain named “default”. If no domain is created, the system will send all user authentication requests to the RADIUS authentication server in this default domain. To delete a domain, RADIUS servers belonging to, you should delete Radius server from it firstly.

4.21 SNMP

The SNMP (Simple Network Management Protocol) is commonly used for configuration of network devices and for network status monitoring. FXOS currently supports SNMP V1 and V2c. A list of SNMP related commands is shown in Table 4-20.

#	Command	Description
1.	<code>service snmp [enable disable]</code>	Enables or disables the SNMP Service
2.	<code>config snmp community [readonly readwrite] <string></code>	Configures SNMP community string for read-only and for read and write access. Default community string for read-only access is “public”, for read and write access is “private”
3.	<code>service snmp trap [enable disable]</code>	Enables or disables SNMP trap service
4.	<code>config snmp trapreceiver add <A.B.C.D> version [v1 v2c] {community <string>}*</code>	Configures a SNMP trap receiver. It is a SNMP manager with A.B.C.D IP address. You could optionally define TRAP community. If not defined the read-only community will be used for TRAP messages.
5.	<code>config snmp trapreceiver delete <A.B.C.D></code>	Deletes SNMP trap receiver
6.	<code>config snmp trap type [all interface start] [on off]</code>	Set SNMP traps “on” or “off”. You can define SNMP Trap behavior for interface traps, for start up traps and for all traps
7.	<code>config snmpauthentrap [enable disable]</code>	Enables or disables authentication trap message
8.	<code>service snmp rmon [enable disable]</code>	Enables or disables the RMON service
9.	<code>show snmp community-string</code>	Shows SNMP current community strings
10.	<code>show snmp trap type</code>	Shows active SNMP traps that will be send by the system
11.	<code>show snmp trapreceiver</code>	Show SNMP Manager address
12.	<code>show debug snmp</code>	Show SNMP debug information

Table 4-20. Commands to configure SNMP

4.22 Access control

Access Control List (ACL) allows traffic filtering according to defined rules. It is possible to filter traffic in dependence of MAC address, IP address or TCP/UDP port numbers.

Access Control List has more than one rule. It should be attached to a port, or to a group of ports or trunk. Each rule in an ACL has own priority. Please note following statements while configuring an ACL:

- Creating a rule
As an Access List consists of rules, a user need to create rule first
Each rule has own number in range of 1 – 1023 and could operate with source and destination MAC address, source and destination IP address, source and destination switch Port number, VLAN ID and TCP/UDP protocol number or protocol name.

- **Creating a List**
Access Control List could have up to 63 rules . They have numbers from 1 to 63 and they can coexist. Therefore, up to 63 rules could be added into access control list.
- **Rule priority in a list**
FXOS starts to execute rules according to their positions in a list. The rule that exists on the top of the list will be executed as the latest; or other say, rules will be executed in the **reverse order** as they were added to the list. For example: configuration order: rule1, rule2, rule3; execution order: rule3, rule2, rule1
- **Default role action**
Default role action is “deny”. It is possible to change it to “permit” state.
- **Assigning an ACL to a port**
After you create at least one role and add it to at least one access list, you need to attach access list to a port. It is possible to attach up 63 ACL to a port. Each ACL has its own number and priority. Therefore, several ACL could coexist on same port. They will be executed according to the sequence they were added and according to the priority.
- **Execution of ACL based on priority value**
Priority is a value in range from 1 to 255. An ACL with higher priority will be executed as the latest. For example: ACL1 has priority 10, while ACL2 has priority 30. Therefore, the execution section will be: ACL1, then ACL2.
- **Executing of ACL with same priority**
If you add several ACL with same priority they will be executed in the **direct order**: first added, first executed. For example: configuration order: acl1, acl2, acl3; execution order: acl1, acl2, acl3.
- **“Default” ACL**
As soon as you add one or more ACL to a port, a default ACL will be added to the same port too. It has “deny” rule to all packets. You could delete “default” ACL from a port if at least one user-defined ACL is assigned to it. You couldn't assign single “Default” ACL to a port.



You could display an ACL configuration in port configuration mode or in ACL configuration mode with `access-list`

A list of ACL related commands is shown in Table 4-21.

#	Command	Description
1.	<code>acl</code>	Enters to Access Control List configuration mode
2.	<code>access-list {<1-63>}*1</code>	Displays ACL information about all or defined ACL
3.	<code>exit</code>	Exits from ACL configuration mode
4.	<code>rule <1-1023> [create destroy]</code>	Creates or deletes access rule
5.	<code>rule {<1-1023>}*1</code>	Shows information about all access rules or about defined rule
6.	<code>rule <1-1023> add dip <A.B.C.D/M></code> <code>rule <1-1023> add sip <A.B.C.D/M></code>	Add Destination or Source IP to a rule with defined number. You could use /30 or /32 mask
7.	<code>rule <1-1023> add dmac <h.h.h></code> <code>rule <1-1023> add smac <h.h.h></code>	Add Destination or Source MAC address to a rule with defined number
8.	<code>rule <1-1023> add dport <portrange></code> <code>rule <1-1023> add sport <portrange></code>	Add Destination or Source Port to a rule with defined number

9.	rule <1-1023> add protocol [tcp udp icmp igmp <0-254>]	Add protocol based on its name or protocol number as defined in RFC1700
10.	rule <1-1023> add vlan <1-4094>	Add VLAN with defined VID number to a defined rule.
11.	rule <1-1023> remove [sport dport vlan smac dmac sip dip protocol]	Remove item from a defined rule
12.	access-list <1-63> [create destroy]	Creates or Deletes access list with given number
13.	access-list <1-63> [add remove] <rulelist>	Add or remove rule or list of rules to defined access list. "rulelist" can be "1-4,6,8" for example, at most 16 rules are supported for each list
14.	access-list <1-63> action <rulelist> [permit deny]	Defines an action "permit" or "deny" for defined access list. Default rule action is "deny"
15.	access-list <1-63> priority <1-255>	Set a priority for defined access list
16.	access-list [enable disable] <lists>	Enable or disable defined ACL on a port. Lists can be "1-8,9,16" for example. 63 lists can be added to each port at most. Note: you must enter port configuration mode to access this command. Please refer to Chapter 4.8 "Working with ports" for details.
17.	access-list [enable disable] default	Configures default access list on current port, whose action is deny. Note: you must enter port configuration mode to access this command. Please refer to Chapter 4.8 "Working with ports" for details.
18.	install	This command is available in ACL configuration mode and has the following meaning. As soon as you attach an ACL to a physical port it will keep its "disabled" state. ACL rules don't work. To enable all ACL lists on all ports, type <code>install</code> command.
19.	uninstall	This command is available in ACL configuration mode. It switches all ACL to "disabled" state but don't unbind them from physical ports.

Table 4-21. Commands to configure Access Control List

4.23 802.1x Access control

The IEEE 802.1x protocol nowadays commonly used in LAN environment that generally was developed as "multi-point to multi-point" 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. switch or wireless access point. The IEEE 802.1x protocol divides network elements into three parties.

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 an Authentication Server and acts as an intermediate agent between supplicants and network.

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 block a network access for **the Supplicant**. The Authentication server could additionally manage bandwidth and QoS settings for a user.

The Supplicant is connected to the Authenticator via so called PAE (Port Access Entry). Until the Authentication Server will grant network access to a Supplicant, the PAE can accept only EAPOL (Extensible Authentication Protocol Over LAN) frames. These frames carry authentication and authorization messages. The other traffic is blocked until Authentication Server will unlock it.

Default 802.x settings are shown in Table 4-22.

#	Parameter	Default Value
1.	802.1x authentication service (enable/disable) on the Ethernet interface	Disable Modifiable configuration
2.	Control mode of the port (MAC-based/port-based)	MAC-based Modifiable configuration
3.	The authentication status of the port (Auto/forceauth/forceunauth)	Auto Modifiable configuration
4.	Verification method(chap/eap-md5/eap-tls/pap)	eap-md5 Modifiable configuration
5.	Keepalive (enable/disable)	Disable Modifiable configuration
6.	Authentication system send authentication request to a client(polling)	Disable Modifiable configuration
7.	Maximum no response count (keepalive max-no-response-count)	5 times Modifiable configuration
8.	Interval of sending keepalive packet(period)	300 seconds Modifiable configuration
9.	Maximum count allowed for the switch to retransmit data frames to the client (reAuthMax)	2 times Unmodifiable configuration
10.	Maximum count allowed to retransmit data frames to the network access device (max-req)	2 times Modifiable configuration
11.	Quiet period during which the authentication system will not accept any authentication request from the client system (quiet-period)	60 seconds Modifiable configuration
12.	Re-authentication mechanism (enable/disable)	Disable Modifiable configuration
13.	Interval of re-authentication (re-authentication period)	3600 seconds Modifiable configuration
14.	Timeout for the authentication system to receive data packets from the authentication server (server-timeout)	30 seconds Modifiable configuration
15.	Timeout for the authentication system to receive data packets from the client system (supp-timeout)	30 seconds Modifiable configuration
16.	Interval for the authentication system to re-transmit EAP-Request/Identity data frames to the client system (tx-period)	30 seconds Modifiable configuration
17.	Configuring the Session Timeout handling mechanism(reauthentication/logoff)	Logoff Modifiable configuration

Table 4-22. Default IEEE 802.1x Settings

4.23.1 Configuring Protocol parameters

A step-by step list to configure 802.1x protocol related commands is shown in Table 4-23.

#	Command	Description
1.	config dot1x quiet-period <0-65535>	Set the quiet period within which the authentication system will not accept any authentication request from the client system
2.	config dot1x tx-period <1-65535>	Configure the interval for the authentication system to re-transmit EAP (Extensible Authentication Protocol) -Request/Identity data frames to the client system
3.	config dot1x max-req <1-10>	Configure the maximum count of the authentication system to re-transmit the data frame to the client
4.	config dot1x supp-timeout <1-65535>	Configure the timeout for the authentication system to receive data packets from the client system
5.	config dot1x server-timeout <1-65535>	Configure the timeout for the authentication system to receive data packets from the authentication server
6.	show dot1x	Show 802.1x protocol parameter

Table 4-23. Commands to configure IEEE 802.1x protocol parameters

4.23.2 Configuring 802.1x Control for the port

A port has three authentication states: auto, force-authorized and force-unauthorized. A port is controlled in two modes: port-based control and MAC-based control.

In the **port-based control mode**, once a legal user has passed the authentication on one port, all the other users connecting to the port can obtain the access authority without being authenticated.

However, in the **MAC-based control mode**, all users at a port will be separately authenticated and charged. Only those users passing the authentication can obtain the authority to access the network. At different ports of the same authentication system, two different control modes can be configured. In the MAC-based control mode, one port can support multiple authentication users. PAP, CHAP, EAP-MD5 and EAP-TLS identity verification methods are available.

A list of steps to configure 802.1x control for a port is shown in Table 4-24.

#	Command	Description
1.	config port [<portlist> all] dot1x [enable disable]	Enable/disable the 802.1x authentication service
2.	config port [<portlist> all] dot1x authcontrolledportcontrol [auto forceauth forceunauth]	Configure the authentication status of the port
3.	config port [<portlist> all] dot1x port-control-mode [mac-based port-based]	Configure the port control mode
4.	config port [<portlist> all] dot1x max-hosts <1-16>	Configure the maximum number of the clients allowed to access the specified port (this command is only valid for the port based on the MAC control mode)
5.	config dot1x authenticate-protocol [chap eap-md5 pap eap-tls peap]	Configure the authentication mode of the user
6.	show port [<portlist> all] dot1x	Show 802.1x Control of the port
7.	show dot1x authenticate-protocol	Show the authentication methods of different users

Table 4-24. Commands to configure IEEE 802.1x control for a port

4.23.3 Setting the Re-authentication Mechanism

To ensure that the link between users and the authentication system (MiniFlex switch) is in active status, and the accuracy of user accounting will not be affected due to the abnormal program suspension resulting from the equipment failure at the user side, the authentication system can periodically initiate the re-authentication process.

A list of steps to configure re-authentication mechanism is shown in Table 4-25.

#	Command	Description
1.	config port [<portlist> all] dot1x [enable disable]	Enable/disable the 802.1x authentication service
2.	config dot1x re-authentication [enable disable]	Enable/disable the re-authentication mechanism
3.	config dot1x re-authentication period <1-65535>	Configure the re-authentication interval
4.	show dot1x	Show 802.1x protocol parameter

Table 4-25. Commands to configure re-authentication mechanism

4.23.4 Configuring Keep-alive Mechanism

Besides the re-authentication mechanism, to check whether an access user is in the connected status, the access module provides another kind of detection mechanism, named the Keep-alive mechanism. For the re-authentication mechanism, it needs to initiate a complete authentication process for each online user. If the number of users is tremendous, authentication packets will be frequently generated as a result of enabling the re-authentication function, therefore increasing the load of the switch to a certain amount. However, for the Keep-alive mechanism, it only needs to exchange a few packets to identify whether a user is online. With the keep-alive method, the switch periodically sends detection request packets, which adopts the EAP (Extensible Authentication Protocol) Request/Identity packet defined in the 802.1x protocol, to the client. If the switch has received the EAP Request/Identity response from the client, it indicates that the user is online. Otherwise, the user has already gone offline.

A list of steps to configure Keep-alive mechanism is shown in Table 4-26.

#	Command	Description
1.	config port [<portlist> all] dot1x [enable disable]	Enable/disable the 802.1x authentication service
2.	config dot1x keepalive [enable disable]	Enable/disable the Keep-alive function
3.	config dot1x keepalive period <10-3600>	Set the interval to send a detection packet
4.	config dot1x keepalive max-no-response-count <2-30>	Set the Max No Keep-alive Response Count
5.	show dot1x	Show 802.1x protocol parameter

Table 4-26. Commands to configure keep-alive mechanism

4.23.5 Forcing users to Log out from the Authentication Status

For the providing of management and security, the MiniFlex switch allows the administrator to force one or more users to log out from the authentication status according to the following conditions:

- Force the user to log out from the authentication status based on user name
- Force the user to log out from the authentication status based on client MAC address
- Force all users to log out from the authentication status

A list of commands to configure user status is shown in Table 4-27.

#	Command	Description
1.	<code>config dot1x pae force-logoff username <username></code>	Force the user to log out from the authentication status based on username
2.	<code>show dot1x pae username <username></code>	Show the PAE (Port Access Entry) state machine based on username
3.	<code>config dot1x pae force-logoff port <port></code>	Force the user to log out from the authentication status based on the port number
4.	<code>show dot1x pae port <port></code>	Show the PAE state machine based on the port
5.	<code>config dot1x pae force-logoff all</code>	Force all users to log out from the authentication status
6.	<code>show dot1x pae all</code>	Show the PAE information

Table 4-27. Commands to configure user-status

4.23.6 Configuring Session Timeout Mechanism

Session Timeout is an attribute transmitted by the Radius Server through the Access Accept packet. In RFC2866, it means the duration of the access service used by an authorized user. If the time is out, the Radius Server will terminate the access service and force the user to get offline. This attribute has been extended by the access module used in the MiniFlex switch so that it can be used according to the standard specified in RFC2866, and also explained as that the server intends to re-authenticate a user. The value of Session Timeout is the re-authentication interval:

```
config dot1x session-timeout-type [reauthentication|logoff]
```

4.24 Configuring DHCP Relay, DHCP Option 82 and DHCP Snooping

The Dynamic Host Configuration Protocol (DHCP) provides a framework for passing configuration information to hosts on a TCP/IP network. The DHCP relay on the MiniFlex Switch transfers DHCP packets from other VLAN and allows DHCP clients, which belong not to the same VLAN with DHCP server, to use DHCP protocol to get IP address. The DHCP relay also supports Option 82

DHCP Option 82 that named the "Relay Agent Information" provides a mechanism for generating IP addresses based on location the client device is in the network. Information about its location can be sent along with the request to the server. The DHCP server makes a decision what IP should be assigned based on this information.

The DHCP Option 82 and DHCP relay agent are defined in RFC 3046.

The DHCP Snooping technique is used for ensuring the security of DHCP-enabled networks. It is based on Layer 2 and prevents DHCP clients to receive IP address from non-trusted DHCP servers, fake servers. It also prevents unauthorized IP change at user side.

4.24.1 DHCP Relay related commands

A list of commands to configure DHCP Relay is shown in Table 4-28.

#	Command	Description
1.	<code>config dhcpr [enable disable]</code>	Enables or disables the DHCP relay
2.	<code>config dhcp serverip add <A.B.C.D></code>	The MiniFlex switch should know an IP address of the DHCP server or servers it has to forward clients requests to. This command adds DHCP server with A.B.C.D IP address. It is possible to have up to 32 servers in a system, IP addresses shouldn't be duplicated. The server should be reachable from the MiniFlex Switch over IP protocol.
3.	<code>config dhcp serverip delete [<A.B.C.D> all]</code>	Deletes a DHCP Server by its IP address from the DHCP relay table. User can delete all DHCP servers from the relay table. If no DHCP server address exists in the table, the DHCP relay will send nothing. The DHCP relay table will be automatically cleared after disabling the dhcp service.
4.	<code>show dhcp serverip</code>	Shows DHCP relay Server table
5.	<code>show dhcpr statistic</code>	Shows DHCP Relay statistics
6.	<code>show dhcpr status</code>	Shows the DHCP Relay status
7.	<code>config dhcpr hoplimit <1-16></code>	Configures number of hops in packets have to be send to DHCP Server. Default hop limit is 4. When MiniFlex switch receives REQUEST DHCP packet it will add 1 to its "hop" value and sends it further to DHCP Server.
8.	<code>no dhcpr hoplimit</code>	Sets hop limit value to default: 4 hops.
9.	<code>config dhcpr option82 [enable disable]</code>	Enables or disables Option 82 for DHCP relay service. DHCP Relay Option 82 should be used when DHCP Server and Clients belongs to different VLANs and can't exchange information directly.
10.	<code>config dhcp l2 option82 [enable disable]</code>	Enables or disables Layer 2 Option 82 for DHCP. This mode is used when DHCP Server and Client share same VLAN. Note: L2 Option 82 and DHCP Relay couldn't be enabled simultaneously.
11.	<code>config dhcp l2 option82 type [circuit-id remote-id both]</code>	Configures Layer 2 DHCP option 82 for circuit-ID, remote-ID or circuit-ID & remote-ID. By default, it is circuit-ID& remote-ID.
12.	<code>config dhcp l2 option82 remote-id [mac ip hostname]</code>	Configures Layer 2 DHCP Option 82 remote-ID for switch MAC, switch IP or switch hostname. By default, it is switch MAC.
13.	<code>config dhcp l2 option82 [circuit-id remote-id] <string></code>	Gives you an option to freely specify Option 82 for circuit-id or remote-id with <text>
14.	<code>show dhcp l2 option82 statistic</code>	Shows Layer 2 DHCP Option 82 statistics
15.	<code>show dhcp l2 option82 status</code>	Displays Layer 2 DHCP Option 82 status

Table 4-28. Commands to configure DHCP Relay

4.24.2 DHCP Snooping related commands

When a user contacts a DHCP server and asks for an IP address a normal DHCP sequence has to be analyzed by IGMP Snooping function of MiniFlex Switch. The new record will be created, and traffic will pass from and to the User port. If user will change his IP address manually the traffic will be blocked by DHCP Snooping function. A Network Administrator has to create static entries in case if he allows User to create static IP address. He has to add it into DHCP Snooping binding table.

A list of commands to configure DHCP Snooping is shown in Table 4-29.

#	Command	Description
1.	<code>config dhcp-snooping [enable disable]</code>	Enables or disables the DHCP Snooping feature
2.	<code>config dhcp-snooping add-ip <A.B.C.D> port <slot/port> vlan <vlanname></code>	Adds the static record into DHCP Snooping table
3.	<code>config dhcp-snooping delete-ip <A.B.C.D> port <slot/port> vlan <vlanname></code>	Deletes the static record from DHCP Snooping table
4.	<code>show dhcp-snooping</code>	Shows DHCP Snooping table

Table 4-29. Commands to configure DHCP Snooping

4.24.3 Secure Forwarding related commands

In the Ethernet Network several users share common media and could affect the data transmission and create malfunctions for a whole network willfully or unintentionally. For example, user could create own DHCP server and break an originally designed IP plan. To protect a network from such malfunction a *config port <portlist> [customer | uplink]* command is used. A DHCP server connected to customer port will become not valid. All packets from it will be blocked by DHCP Snooping feature. Only the DHCP Server connected to the uplink port will become valid. Please note that you must enable DHCP Snooping to activate protection against fake DHCP server.

 Default port role is "Uplink" for GE ports and "Customer" for FE ports. To display port role type `show port type`

A Network Administrator could configure his network that way, so the customers could connect only with the gateway, but not between each other. This feature named Secure Forwarding.

A list of Secure Forwarding related commands is shown in Table 4-30.

#	Command	Description
1.	<code>secureforward [enable disable]</code>	Enables or disables the Secure Forwarding feature. When enabled, switch will look into DHCP packets and get information from them.
2.	<code>secureforward [manual dynamic]</code>	Configures the way how the Secure Forwarding function will learn information about gateway. In dynamic mode it will be learned from DHCP packet "Default Gateway" field. In Manual mode you have to configure it yourself.
3.	<code>secureforward add router vlan <1-4094> ip <A.B.C.D> mac <H.H.H></code>	Configures gateway in manual mode
4.	<code>secureforward customer port <portlist> [enable disable]</code>	Configures secure forwarding feature between ports their role is set to "customer". If disabled, the customers can exchange information. If enabled, the customers can exchange information with "uplink" ports only.
5.	<code>secureforward delete router vlan <1-4094></code>	Deletes gateway information

#	Command	Description
6.	show secureforward [<1-4094> all]	Shows secure forwarding information
7.	show secureforward customer port {<portlist>}*1	Shows secure forwarding status for customers ports
8.	show secureforward mode	Shows secure forwarding operational mode

Table 4-30. Commands related to Secure Forwarding

4.25 Quality of Service (QoS)

Quality of Service (QoS) technique has to be used in case if different types of traffic share the common transmission media. For example, over single Ethernet interface, user sends high priority traffic, i.e. VoIP and surfs WEB. System shall grant as less as possible delivery delay for VoIP packets, while HTTP traffic could be transmitted slowly. Another aim of correct QoS handling is to grant delivery and bandwidth to business-critical applications and left the best effort to bulk traffic.

4.25.1 Queues

The MiniFlex switch is able to prioritize user traffic and sort it into several queues. Each queue will belong to own Class of Service and will be treated according to its priority. 8 queues are supported for each Fast Ethernet and Gigabit Ethernet port in egress direction. Current FXOS version supports Strict Priority (SP), Weighted Round Robin (WRR) and SP + WRR queue scheduling management per port.

- Strict Priority

The Strict Priority scheduling mechanism means that each queue associated with the egress port is serviced according to the priority order from highest 7 to lowest 0. All traffic for a given queue is transmitted before the scheduler proceeds to the next highest priority queue. The purpose of strict priority scheduling is to ensure lower latency and priority transmission of critical traffic by always transmitting higher priority traffic before lower priority traffic. The Strict Priority scheduling mechanism in the MiniFlex switch is not preemptive. Once a packet from a given queue is selected for transmission, the scheduler completes the sending of that packet before determining the next queue to service.

- Weighted Round Robin

Weighted Round Robin (WRR) scheduling mechanism services each queue in round robin order from highest priority to lowest priority. WRR mechanism provides a weighted access to the egress port bandwidth at the packet level. A configurable weight from 1 to 15 could be assigned to each queue. This value represents the number of packets that will sent back to back from a given queue when the queue is serviced assuming there are sufficient packets in the queue. If there are less packets in the queue than the weight assigned to the queue, the scheduler sends all packets in the queue and then begins servicing the next queue.

The WRR mechanism provides sharing of the egress port bandwidth across multiple queues. However, the ability to share the bandwidth is limited because the packet length is not fixed, and it is not considered when scheduling mechanism sends packets from a queue. Therefore, assuming equal weights, a queue in which the average packet size is larger will get a larger share of the link bandwidth.

In case if we consider that all Ethernet packets have same size the bandwidth allocation for each queue could be calculated as:

$$\text{queue_bandwidth} = \text{given_queue_weight} / \text{sum_of_all_queues_weight} * \text{total_bandwidth}$$

- Strict Priority + Weighted Round Robin

The MiniFlex Switch supports a scheduling mechanism that mixes strict priority scheduling and weighted round robin scheduling. This allows some of the queues on an egress port to be scheduled according to a strict priority algorithm and other queues on the same egress port to be scheduled according to the WRR scheduling algorithm. This flexibility allows a network administrator to select some queues to be scheduled with Strict Priority, i.e. with smallest possible delay, and to share the rest of the bandwidth between other queues, that are not so critical to delays. To achieve such mechanism, the system administrator needs to select WRR mechanism for scheduling and assign “0” weight to queues he wants to have Strict Priority.

4.25.2 Traffic to queues allocation mechanism

The MiniFlex switch could map user traffic into internal CoS queues by IEEE 802.1p priority field or by DSCP field in IPv4 packet. The DSCP to CoS mapping is disabled by default. The 802.1p priority is mapped “one to one” to CoS queues of MiniFlex switch. The queue 7 and 802.1p priority “7” have the highest scheduling priority while queue 0 and 802.1p priority “0” have the lowest scheduling priority:

-----802.1p Priority-----	-----Queue -----
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7
-----	-----

When enabled, the default DSCP mapping will assign all 64 DSCP code pointers to CoS queue “0” of MiniFlex Switch.

4.25.3 Configuring QoS

The list of commands related to QoS configuration is represented in Table 4-31.

#	Command	Description
1.	<code>qos default-priority <0-7></code>	This command sets default CoS priority for a port. The ingress untagged packet without IEEE 802.1p tag will have defined QoS value in the header. When added to VLAN, the packet will be processed according to the TOS value in the VLAN header. The command is available under Ethernet port configuration mode. The packet has no QoS settings by default.
2.	<code>show default-priority</code>	Shows default CoS priority for a port. The command is available under Ethernet port configuration mode.
3.	<code>qos map priority-queue <0-7> to <0-7></code>	Sets the mapping between IEEE 802.1p value and CoS queue of the MiniFlex switch. The command is available under Ethernet port configuration mode.
4.	<code>no qos map priority</code>	Sets QoS mapping to default values “one to one”. The command is available under Ethernet port configuration mode.
5.	<code>qos map dscp [enable disable]</code>	Enables or disables DSCP to CoS mapping for a port. It is disabled by default.

		The command is available under Ethernet port configuration mode.
6.	<code>qos map dscp-priority <0-63> to <0-7></code>	Sets the mapping between IPv4 DSCP field and CoS queue of the MiniFlex Switch. The command is available under Ethernet port configuration mode.
7.	<code>no qos map dscp</code>	Sets DSCP to CoS mapping to default values. The command is available under Ethernet port configuration mode.
8.	<code>show qos map [priority dscp]</code>	Shows CoS mapping table for 802.1p or for DSCP. The command is available under Ethernet port configuration mode.
9.	<code>qos bandwidth <0-7> [<64-1024000> 0]</code>	Sets the bandwidth limitation for each queue <0 - 7> in kbps. The value must be a factor of 64 and must not be greater than the port capabilities. Value "0" means that bandwidth will not be limited. The command is available under Ethernet port configuration mode.
10.	<code>show qos bandwidth</code>	Shows bandwidth settings for each CoS queue. The command is available under Ethernet port configuration mode.
11.	<code>qos sched-mode [pq wrr]</code>	Sets the scheduling mechanism: Priority Queue (PQ) is the Strict Priority while WRR is Weighted Round Robin. Default scheduling mechanism is PQ. The command is available under Ethernet port configuration mode.
12.	<code>qos queue-weight <0-15> <0-15> <0-15> <0-15> <0-15> <0-15> <0-15></code>	Sets a weight for every queue. The command has a meaning only if QoS scheduling mechanism is set to WRR. If queue weight is set to "0", the Strict Priority scheduling mechanism will be used. The command is available under Ethernet port configuration mode.

Table 4-31. Commands related to QoS configuration

4.26 Configuring GVRP

The GVRP (GARP (Generic Attribute Registration Protocol) VLAN Registration Protocol) is useful for automatic VLAN configuration in Layer 2 network. To get the benefit of GVRP protocol it must be enabled on all switches in the network and NIC (Network Interface Cards) of terminal stations must support it as well.

The GVRP Protocol uses GVRP BPDU (GVRP Bridge Protocol Data Units) for sharing information about enabled VLANs in the network. If a GVRP-enabled switch will receive GVRP BPDU it will automatically build VLAN configuration. The switch will forward GVRP BPDU further through other GVRP-enabled ports except the one, which receives initial GVRP BPDU. Therefore, the whole network will be automatically configured from initial request of GVRP-enabled host.

A list of GVRP related commands is shown in Table 4-32.

#	Command	Description
1.	<code>config gvrp [enable disable]</code>	Enables or disables the GVRP function on the MiniFlex switch
2.	<code>show gvrp</code>	Shows the GVRP status
3.	<code>config gvrp port [<portlist> all] [enable disable]</code>	Enables or disables the GVRP function for a port or group of ports. If GVRP function is enabled on a port it will participate in GVRP BPDU exchange mechanism.
4.	<code>config gvrp port [<portlist> all] registration [normal forbidden]</code>	This command selects the port registration mode. GVRP have two port registration modes: Normal and Forbidden. In normal mode a port can dynamically register/deregister a VLAN and distribute the VLAN information. In forbidden mode a port can't register/deregister VLANs. It distributes only VLAN VID1 information
5.	<code>config gvrp timer [join leave leaveall] <1-100000></code>	This command configures the GVRP join and leave timers in milliseconds.

Table 4-32. Commands related to GVRP

4.27 Anti DoS protection

The MiniFlex switch supports several Deny of Service (DOS) prevention mechanisms. To enable Anti-DoS protection, type ***anti-dos-attack enable*** command. When enabled, the following cases will be blocked:

- Source IP and Destination IP are equal
In case if IP packet has same Source and Destination IP, it will be blocked by the switch. The rule is valid for UDP or TCP packets.
- ICMP packet oversize
If ICMP packet has greater size than defined (excluded Header), it will be blocked. You could define a ICMP packet maximum size in bytes with ***config icmppktoversize <0-16383>*** command.
- Equal port number
If packet has same source and destination port number, such packet will be blocked. The rule is valid for TCP and for UDP packets
- TCP flags conditions
In case if SYN and FIN flag is set to 1, or FIN, URG and PSH are set to 1 and packet sequence number is set to 0, or if Fragment offset is set to 1, or when all flags are set to 0 and sequence number is set to 0, the packet will be blocked.

The network administrator could limit the broadcast and multicast rate for defined port manually. Please refer to record 42 in Table 4-5 for details.

4.28 Static Routing

MiniFlex Switch has built-in static routing option.

The list of commands is shown in the table below:

#	Command	Description
1	<code>config routing</code>	Enters the Routing configuration mode
2	<code>routing [enable disable]</code>	Enables or disables the Routing mode
3	<code>Quit</code>	Quit the Routing configuration mode

4	<code>ip host [add delete] <A.B.C.D/Mask></code>	To add or to Delete the Host from routing table. The host here is a PC or LTU/NTU device with IP address with direct connection to SWU card
5	<code>ip route add <A.B.C.D/Mask> <a.b.c.d></code>	Adds a static route to A.B.C.D/Mask network via a.b.c.d next Hop.
6	<code>ip route delete <A.B.C.D/Mask></code>	Delete the static route to A.B.C.D/Mask network
7	<code>show ip host</code>	Show IP Host table
8	<code>show ip route</code>	Show IP Route table

To create a static route, the administrator needs to assign the IP address to interface such as VLAN or Trunk. Those commands should be used for that purpose:

#	Command	Description
1	<code>interface [vlan {vlan_name} trunk <trunk_name>]</code>	Enters to interface (VLAN or Trunk) configuration mode. Use main menu as a starting point
2	<code>ip <A.B.C.D/Mask> gateway <A.B.C.D></code>	Configures an IP address and default gateway for an interface
3	<code>no ip</code>	Deletes an IP address from interface
4	<code>Exit</code>	Exit from interface configuration mode

4.29 NAT/NPT feature

The Network Address Translation/Network Port Translation NAT/NPT feature can be used if it is required to access the whole node, including the remote modems through single IP address. The NAT/NPT feature arrange the path between two virtual interfaces WAN and LAN. The WAN interface is dedicated into the direction to the public network, while the LAN interface is dedicated to the direction of the private network.

The list of command is represented below:

#	Command	Description
1	<code>config nat</code>	Enters to NAT configuration mode. Use main menu as a starting point
2	<code>nat [enable disable]</code>	Enables or disables NAT for device
3	<code>forward add <A.B.C.D:xxx> <a.b.c.d:yyy></code>	Add a port forwarding rule for a source IP A.B.C.D. A packet with destination port xxx will be forwarder to IP address a.b.c.d to port yyy. The forwarding rule affects Ingres direction: from WAN to LAN
4	<code>forward delete <A.B.C.D:xxx></code>	Deletes a port forwarding rule for IP address A.B.C.D and port xxx
5	<code>forward show</code>	Shows port forwarding table
6	<code>exit</code>	Exit from NAT configuration mode

To create a NAT/NPT, the administrator needs to assign the IP address to interface such as VLAN or Trunk. Those commands should be used for that purpose:

#	Command	Description
1	<code>interface [vlan {vlan_name} trunk <trunk_name>]</code>	Enters to interface (VLAN or Trunk) configuration mode. Use main menu as a starting point
2	<code>nat [lan wan none]</code>	Configures an interface NAT role
3	<code>Exit</code>	Exit from interface configuration mode



NAT/PAT depends on routing feature. It must be enabled firstly.

4.30 SNMP Message Forwarding

SNMP Proxy of MiniFlex Switch analyses the SNMP packet and forward it according to the defined rules. SNMP Proxy analyses SNMP flow in egress and in ingress directions.

Ingress direction means that packet arrives from the core network and has to be forwarded to the devices inside the rack.

Egress direction means that packet is going from the device in the rack to the core network.

The SNMP message forwarding function analyses SIP (Source IP), DIP (Destination IP) and community of the packet.

SNMP Message forwarding function has following commands:

#	Command	Description
1	<code>config snmp-proxy</code>	Enters to SNMP proxy configuration mode
2	<code>proxy ingress <community_in> ip <A.B.C.D> {<community_out>}*1</code>	Set a path for inbound SNMP requests. They will be analyzed by community-in string and will be forwarded to IP A.B.C.D with optional community-out string
3	<code>no proxy ingress community-in <community></code>	Deletes a path for incoming SNMP messages
4	<code>proxy egress ip <A.B.C.D> to <a.b.c.d> {<community>}*1 {<e.f.g.h>}*1</code>	Set a path for outgoing connection. A SNMP packet from IP A.B.C.D will be forwarded to NMS server IP a.b.c.d and optionally to e.f.g.h. Community can be changed
5	<code>no proxy egress ip <A.B.C.D></code>	Delete a path for outgoing connection for a defined IP address.
6	<code>show snmp-proxy [ingress egress]</code>	Shows SNMP proxy forwarding table for ingress or for egress directions.
7	<code>snmp-proxy [enable disable]</code>	Enables or disables a SNMP proxy



SNMP Message Forwarding depends on routing feature. It must be enabled firstly.

4.31 Enabling and disabling CLI access over Telnet, SSH and SNMP

In some cases, it is required to disable unsecure protocols like Telnet for device access and enable secure connection over SSH. It can be done with the help of the following commands:

#	Command	Description
1	<code>service [telnet ssh snmp] [enable disable]</code>	By using service [service name] command User can enable or disable desired management service.
2	<code>create ssh rsa [512 1024 2048]</code>	This command allows RSA key generation with desired length for CLI access over SSH. Please note that RSA key must be generated before enabling SSH service. Once created RSA key will be stored into configuration.
3	<code>service snmp [rmon trap] [enable disable]</code>	This command allows user to enable or disable SNMP RMON or TRAP services.

5 PROGRAMMING GUIDE LINE CARDS, DINRAIL, MF-MR2N-SW-8ETH,V2 AND FLATRACK SWITCHES

- The Programming of **E1** line cards and DINrail units in **TDMoIP mode** is not under the scope of this User Manual. Please refer to “**UM_FlexDSL-TDMoE_SW_V2-x**” **User Manual**.
- The Programming of **FXS/FXO/VF** line cards and DINrail units is not under the scope of this User Manual. Please refer to “**UM_FlexDSL_MiniFlex_VoIP_v1-x**” **User Manual**.

5.1 Command Structure SHDSL, Serial and E1

Main Menu		
PM Performance management	FMM Fault and maintenance management	CM Configuration management
G826	NM	ENCODE
G826 C	LINKNM	ENCODE KEY [N]
G826 E1	LINKALARM	ENCODE [ON/OFF] [N]
G826 E1 C	ALARMLOG [N]	SECURE [ON/OFF]
ALLG826 N	ALARMLOG C	USERS
RESETG826	LINKDIAG	USER [name]
RESETALLG826 N	STATUS	USER [name] DEL
NETSTAT [LAN/WAN]	STATUS T	USER [name] [+/-] [PRIV]
NETERR [LAN/WAN]	STATUS SFP	USER [name] [IP] [subnet]
RESETNETSTAT	STATUS L	USER [name] [LOCAL/ALL]
LINKSTAT	STATUS ETH	PASSWORD {user}
LINKALARM	STATUS LLDP	AUTO [ON/OFF]
ALARMLOG [N]	STATUS DOT1X	CONFIG
ALARMLOG C	STATUS RADIUS	CONFIG [N/R/S/B]
LINKNM	STATUS ENCODE	MASTER [ON/OFF] [N]
LINKDIAG	LOOP1 [ON/OFF] [N]	EXT [ON/OFF] [N]
APPLY [ALL/GROUP]	LOOP2 [N:[A/R]] [ON/OFF]	BASERATE [M/AUTO] [N]
CONNECT [N:[1-13/R]]	ALARM	PAM [4/8/16/32/64/128] [N]
M(AIN)	ALARM T	PAYLOAD [list] [N]
H(ELP)	ACO	ANNEX [A,B,A/B] [N]
	ACO [GROUP] [ON/OFF]	SETCLOCK [list] [N]
	MACTABLE C	MULTIPAIR [2/OFF]
	MACTABLE [1-8/OTHER/Port]	RESERVE [list]
	MACTABLE	G704 [ON/OFF] [N]
	LLDP STAT [IF/ALL]	CRC4 [ON/OFF] [N]
	STARTAL [N]	AISDET [ON/OFF] [N]
	RESTART [N]	AISGEN [ON/OFF] [N]
	RESET	WANTS [list] [N]
	CONFIRM	E1CLOCK {source} [N/{list}]
	BACKUP	E1MODE {mode} [N]
	RESTORE	ID string
	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	MODE [N]
	TFTP [CMD] [ARG1][ARG2]	LICENSE
	SOFTCONFIRM	LICENSE ADD [key]
	SOFTINFO	APPLY [ALL/GROUP]
	PING x.x.x.x	CONNECT [N:[1-13/R]]
	LINKSTAT	RSIP [I/O] [addr] [IF]
	RSTP [CONF/STATE]	RSIP {option} [IF]
	MODEMVIEW	RSRATE [N]
	SD SNAPSHOT	RSFORMAT [Format]
	SD DIR	RSDUPLICATION [F/H]
	SD DEL [NAME]	RS TERM [ON/OFF]
	SD SAVE [N=0..9]	RS [232/485]
	SD SAVE [N=0..9]	4RS {option} {value} [N]
	SD BOOT [ON/OFF]	NET → NETCONFIG
	SD STATUS	M(AIN) → NETCONFIG [N/R/S/B]
	APPLY [ALL/GROUP]	H(ELP) → COSCONFIG

CONNECT [N:[1-13/R]]	COSCONFIG [N/R/S/B]
BERT →	RSTP DEFAULT
M(AIN)	RSTP [CONF/STATE/DIAG]
H(ELP)	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 [IF] [ON/OFF]
	MACRULE [IF] [rule]
	DOT1X [IF] {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]
	TRAP [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]
	[SSH TELNET HTTP] [ON/OFF]
	SSH PORT [N]
	SSL [SHOW/DEL] [options]
	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]
	SYSNAME [SET]
	SYSLOCATION [SET]
	SYSCONTACT [SET]
	NETDEFAULT
	APPLY [ALL/GROUP]
	CONNECT [N:[1-13/R]]
	M(AIN)
	H(ELP)

Table 5.1 Command structure according to ITU-T Rec. M.3400 (Telecommunication Management Networks)

5.2 Command Structure FOM, GFOM, IO, Switch, FlatRack / MF-MR2N-SW-8Eth,V2

Main Menu		
PM Performance management	FMM Fault and maintenance management	CM Configuration management
NETSTAT NETERR RESETNETSTAT ALARMLOG ALARMLOG C APPLY [ALL/GROUP] M(AIN) H(ELP)	STATUS STATUS IO STATUS SFP STATUS LLDP STATUS DOT1X STATUS RADIUS STATUSPOE ALARM ALARM T ACO ACO [GROUP] [ON/OFF] MACTABLE C MACTABLE [1-8/OTHER/Port] MACTABLE LLDP STAT [IF/ALL] RESET RESETPOE CONFIRM BACKUP RESTORE DIFF [N/R/S/B] [N/R/S/B] DUMP [N/R/S/B] LOAD LOG LOG C SOFTUPDATE TFTP [CMD] [ARG1][ARG2] SOFTCONFIRM SOFTINFO PING x.x.x.x RSTP [CONF/STATE] MODEMVIEW SD SNAPSHOT SD DIR SD DEL [NAME] SD SAVE [N=0..9] SD LOAD [N=0..9] SD BOOT [ON/OFF] SD STATUS APPLY [ALL/GROUP] M(AIN) H(ELP)	SECURE [ON/OFF] USERS USER [name] USER [name] DEL USER [name] [+/-] [PRIV] USER [name] [IP] [subnet] USER [name] [LOCAL/ALL] PASSWORD {user} ID string SERNUM NETCONFIG NETCONFIG [N/R/S/B] IOCONFIG 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/S] MODE [IF] [ACC/TRUNK/MIX] VLAN [IF] [1..8] VLANNNAME [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 [LAN1-9] [ON/OFF] MACRULE [IF] [rule] JUMBO SIZE [OFF,1,2] [N] DOT1X [IF] {OPTION} SETIP x.x.x.x GATEWAY x.x.x.x NETMASK x.x.x.x MTU [68..1500] ETHSD [MODE] [N=1-9] FC [ON/OFF] [N=1-9] IRATE [speed/OFF] [N=1-9] ERATE [speed/OFF] [N=1-9] COS [QOS/VLAN] [x] [0..3/OFF] SNMP [V1 V2C V3] [ON/OFF] SNMPACL [1/2] [IP/OFF] TRAP [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] SYSNAME [SET] SYSLOCATION [SET] SYSCONTACT [SET] 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 DST WINTER DST [OFF/INFO/NAME]

```
SYSLOG [1/2] [IP/OFF]
NETDEFAULT
SSH|TELNET|HTTP [ON/OFF]
SSH PORT [N]
RADIUS [1/2] SECRET
RADIUS [1/2] SECRET OFF
RADIUS [1/2] TEST
RADIUS [1/2] [IP:PORT/OFF]
RADIUS RETRIES [0..10]
RADIUS TIMEOUT [1..5]
DEFAULT 0
DEFAULT EVERYTHING
DEFAULT DESC
FACTORY DEFAULT
IOIP {option} [IF]
POECONFIG
POEPORT [ON/OFF] [N]
APPLY [ALL/GROUP]
M(AIN)
H(ELP)
```

Table 5.2 Command structure according to ITU-T Rec. M.3400 (Telecommunication Management Networks)

5.3 Line Cards, DIN-rail, FlatRack and MF-MR2N-SW-8Eth,V2 Switch Software

Every Line card & DINrail 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.

5.4 Configuration and Application Storage

The whole the system stores four configurations: running configuration, startup 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 etc.). During initialization the initial parameters of the running configuration are loaded from the startup configuration.

The **startup configuration** contains all configuration values which will be used to configure the device after its restart. The startup 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 startup 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 startup 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 startup configuration into the running one and thus become valid.

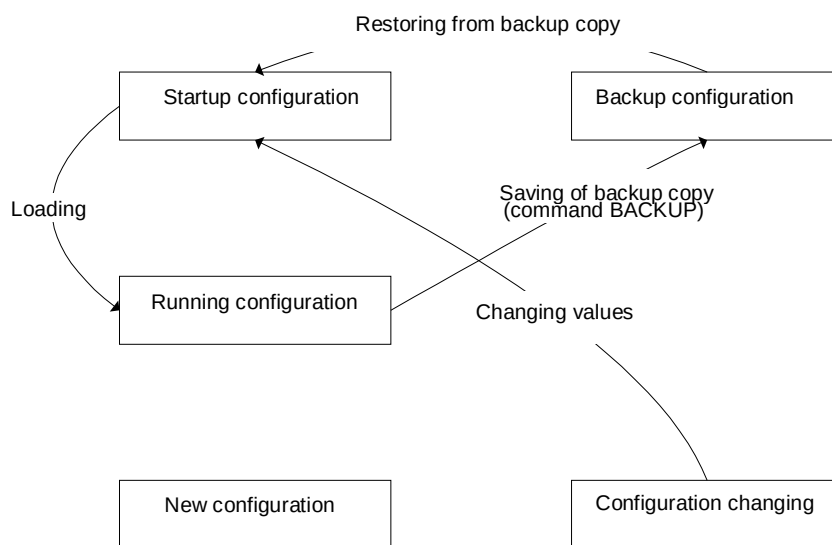


Figure 5.1 Operations of the configuration parameters after the restart

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

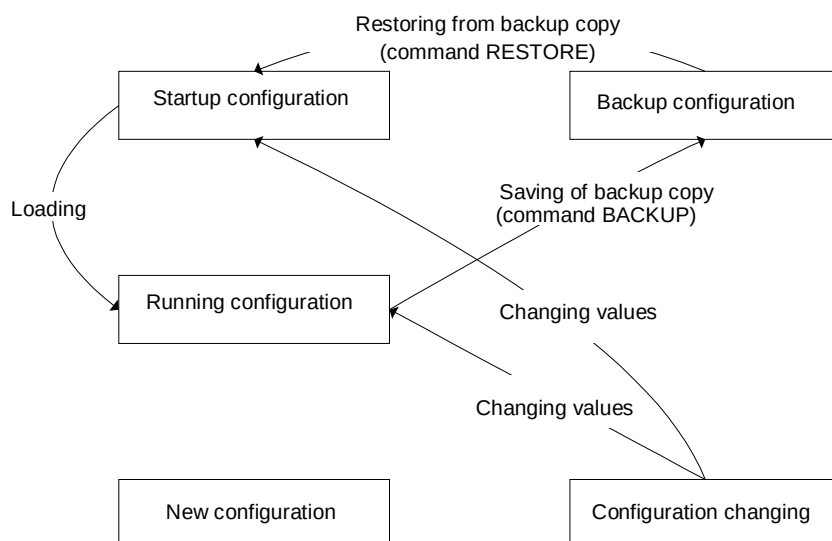


Figure 5.2 Operations of the configuration parameters with the instant application

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 startup configuration.

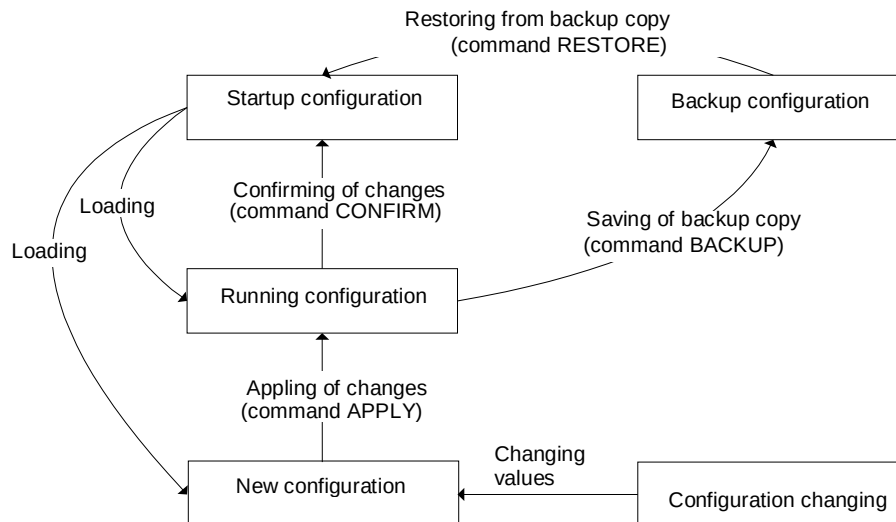


Figure 5.3 Operations of configuration parameters that should be confirmed

5.5 Groups of Commands Requiring Confirmation

In the SHDSL line card & DINrail 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 USB interface but via Telnet the management session breaks and the unit wait 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 startup configuration of the unit. Therefore, it is possible to restore the configurations of the unit. A “successful” configuration can become the startup configuration by using the CONFIRM command.

5.6 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>

5.7 Commands

5.7.1 Main Menu

The main menu is presented as shown below:

```
MODEL MF-PAM-SR2L-2Eth, V1
HW 5.1
SW 1.7.7 EXT rates,Security
DATE 30-11-2017
ID
RUNS 0d 08:02:09
ALARM URGENT
STATUS LINK DOWN
MODEL_DESC MiniFlex Dual xDSL/Dual Ethernet 120 Ohm
IP 192.168.1.236
```

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

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

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

5.7.1.1 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)

sf is the short form of the current menu:

- MM – Main Menu
- PM – Performance Management
- FMM – Fault and Maintenance Management
- CM – Configuration Management
- NET – Network Interfaces Management
- BERT – Bit-Error Tester Management.

For example: CO_PM>

means the device is in the Master mode and we are in the Performance Management menu.

5.7.2 General Commands

5.7.2.1 <H> Command

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

5.7.2.2 <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_PM>APPLY LINE
Applying configuration changes in group LINE to running configuration
```

5.7.2.3 <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.

5.7.3 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_PM>
```

5.7.3.1 <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_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
ALLG826 N           Display xDSL G.826 statistics for all link
RESETG826           Reset G.826 statistics
RESETALG826 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
M                  Return to Main Menu
H                  Show available commands
-----
```

5.7.3.2 <G826> Command

This command displays the ITU-T G.826 performance parameters of the two SHDSL lines.

```
CO_PM>G826
-----
G.826 Error Performance :   CRC6 1       CRC6 2
-----
Errored blocks          : 0000000000 0000000000
Errored seconds         : 0000000000 0000000000
Severely errored seconds : 0000000000 0000000000
Background block errors : 0000000000 0000000000
ESR [%]                 :          0.00      0.00
SESR [%]                :          0.00      0.00
BBER [%]                :          0.00      0.00
Available time          : 0000000000 0000000000
Unavailable time        : 0000023365 0000023365
-----
```

Option: C – update the table continuously.

Parameter	Description
CRC6	Cyclic redundancy check indicating errored blocks received on the SHDSL side
Errored blocks	Blocks (transmission duration 6ms) with one or more bit-errors
Errored seconds	Seconds with one or more Errored blocks or at least one defect
Severely errored seconds	Seconds with 30% or more Errored blocks . Severely errored seconds are a subset of Errored seconds
Background block errors	Errored blocks not occurring as a part of Severely errored seconds
ESR	The ratio of Errored seconds to total seconds in Available time
SESR	The ratio of Severely errored seconds to the total number of error-free seconds in Available time
BBER	The ratio of Background block errors to the total number of error-free seconds in Available time
Available time	The period when measurements of the parameters are possible
Unavailable time	The period when the measurements of the parameters are impossible

5.7.3.3 <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
-----
```

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
-----
```

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

```
CO_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
-----
```

Option: C – update the table continuously.

Parameter	Description
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 indicating errored submultiframe received on the E1 side
E-Bit	CRC4 indication bit denoting received errored submultiframe on the opposite E1 side
FAS	Errored frame alignment signal (FAS) received on the E1 side
EB (Errored Blocks)	Blocks with one or more bit-errors
ES (Errored seconds)	Seconds with one or more EB or at least one defect
SES (Severely errored seconds)	Seconds with more than 805 EB per second (if CRC4 options are enabled) or with more than 28 FAS per second. SES are a subset of ES
BBE (Background block errors)	EB not occurring as a part of SES
ESR	The ratio of ES to total seconds in Available time
SESR	The ratio of SES to the total number of error-free seconds in Available time
BBER	The ratio of BBE to the total number of error-free seconds in Available time
Available time	The period when measurements of the parameters are possible
Unavailable time	The period when the measurements of the parameters are impossible

5.7.3.4 <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
-----
```

Please see G826 command description for the explanation of the different parameters.

5.7.3.5 <RESETG826> Command

This command clears all ITU-T G.826 error performance counters of the local SHDSL interfaces or E1 interfaces.

5.7.3.6 <RESETALLG826 N> Command

This command clears all 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.

5.7.3.7 <NETSTAT [LAN/WAN]> Command

This command shows the main network (LAN or WAN & MWAN) interface counters. The parameter [LAN/WAN] must be entered only for SHDSL, Serial and E1 line cards.

SHDSL, Serial and E1 line cards					FOM, GFOM, IO, PoE & Switch, FlatRack Switch				
CO_PM>NETSTAT LAN					CO_PM>NETSTAT				
Interface		LAN1	LAN2	INT	Interface		LAN1	LAN2	INT
Description					Description		SFP1	ETH2	
Mode	:	DOWN	DOWN		Mode	:	DOWN	DOWN	
In					In				
Octets	:	0	0	0	Octets	:	0	0	0
Packets	:	0	0	0	Packets	:	0	0	0
B/mcast	:	0	0	0	B/mcast	:	0	0	0
Speed, kbit:		0	0	0	Speed, kbit:		0	0	0
Size					Size				
64	:	0	0	0	64	:	0	0	0
65-128	:	0	0	0	65-128	:	0	0	0
129-256	:	0	0	0	129-256	:	0	0	0
257-512	:	0	0	0	257-512	:	0	0	0
513-1024	:	0	0	0	513-1024	:	0	0	0
>1024	:	0	0	0	>1024	:	0	0	0
Out					Out				
Octets	:	0	0	0	Octets	:	0	0	0
Packets	:	0	0	0	Packets	:	0	0	0
B/mcast	:	0	0	0	B/mcast	:	0	0	0
Speed, kbit:		0	0	0	Speed, kbit:		0	0	0

Parameter	Value	Description
Interface	LANx WANx MWANx	Port identifier of the internal Ethernet Switch.
Description	String	Port Description (ifAlias).
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,kbit	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,kbit	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.

5.7.3.8 <NETERR [LAN/WAN]> Command

This command shows the main network (LAN or WAN & MWAN) interface error counters. This command shows the main network (LAN or WAN & MWAN) interface counters. The parameter [LAN/WAN] must be entered only for SHDSL, Serial and E1 line cards.

SHDSL, Serial and E1 line cards					FOM, GFOM, IO, PoE & Switch, FlatRack Switch				
CO_PM>NETERR LAN					CO_PM>NETERR				
Interface	LAN1	LAN2	LAN3	INT	Interface	LAN1	LAN2	INT	
In					In				
Bad octets:	0	0	0	0	Bad octets:	0	0	0	
Discards :	0	0	0	0	Discards :	0	0	0	
Undersize :	0	0	0	0	Undersize :	0	0	0	
Oversize :	0	0	0	0	Oversize :	0	0	0	
Fragments :	0	0	0	0	Fragments :	0	0	0	
Jabber :	0	0	0	0	Jabber :	0	0	0	
MAC error :	0	0	0	0	MAC error :	0	0	0	
Bad FCS :	0	0	0	0	Bad FCS :	0	0	0	
Out					Out				
FCS error :	0	0	0	0	FCS error :	0	0	0	
Deferred :	0	0	0	0	Deferred :	0	0	0	
Collisions:	0	0	0	0	Collisions:	0	0	0	
.Late :	0	0	0	0	.Late :	0	0	0	
.Excessive:	0	0	0	0	.Excessive:	0	0	0	
.Single :	0	0	0	0	.Single :	0	0	0	
.Multiple :	0	0	0	0	.Multiple :	0	0	0	
Pause					Pause				
In pause :	0	0	0	0	In pause :	0	0	0	
Out pause :	0	0	0	0	Out pause :	0	0	0	

Parameter	Value	Description
Interface	LANx WANx MWANx	Port identifier of the internal Ethernet Switch.
Description	String	Port Description (ifAlias).
IN	Bad octets Discards Undersize Oversize Fragments Jabber MAC error Bad FCS	Total number of octets (bytes) received with error. Total number of discarded packets even when no error. Total number of received packets with size <64 bytes (68 when tagged). Total number of received packets with size more than set by JUMBO SIZE cmd. Received packets that were undersized and had either FCS or alignment Error. Received packets that were oversized and had either FCS or alignment Error. Total number of packets that were dropped due to hardware errors in receiver Total number of received frames that had bad FCS (Frame Check Sequence).
OUT	FCS error Deferred Collisions .Late .Excessive .Single .Multiple	Total number of frames transmitted incorrectly due to internal transmitter error. LAN half-duplex: Number of successfully transmitted packets that were delayed because the medium was busy then were transmitted without collisions. Number of collisions not including those counted as Late or Excessive. Number of late collisions. LAN half-duplex, number of dropped frames due to excessive number of coll.. LAN half-duplex, number of successfully transmitted frames that experienced only single collision. LAN half-duplex, number of successfully transmitted frames that experienced multiple collisions.
Pause	In pause Out pause	Number of received MAC pause frames (Flow control). Number of sent MAC pause frames.

5.7.3.9 <RESETNETSTAT> Command

This command resets NETSTAT and NETERR statistics.

5.7.3.10 <LINKSTAT> Command

This command shows an actual quick status of the whole link for each DSL interface.

```
-----
DSL 1                DSL 2
-----
CO    up             CO    up
CP    up             CP    up
-----
CO_PM>
```

5.7.3.11 <LINKALARM> Command

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

```
-----
Local Alarm: Major
-----
DSL 1                DSL 2
-----
CP    None
-----
CO_PM>
```

5.7.3.12 <ALARMLOG [N]> Command

The <ALARMLOG [N]> command displays the alarm log (list of all alarms that were detected) for the specified SHDSL interface (SHDSL cards only).

```
CO_PM>ALARMLOG 1
-----
Time ago | Unit | Event | Description
-----
02:52s | CO | DSL | LOS ---- - - - - -
02:50s | CO | DSL | LOS LOSW - - - - -
02:03s | CO | DSL | --- LOSW - - - - -
02:02s | CO | DSL | --- - - - - -
-----
```

Option: C – clears the Alarm log

Parameter	Description
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.
Description	List of alarms, that were detected on interface.

The <ALARMLOG> command displays the alarm log (list of all alarms that were detected) for device interfaces (FOM, GFOM, IO, PoE & Switch, FlatRack Switch).

```
CO_PM>ALARMLOG
-----
Time ago | Interface | Alarm | Event
-----
06:50s | LAN3 | LOS-ETH | UP
06:50s | LAN4 | LOS-ETH | UP
06:50s | LAN5 | LOS-ETH | UP
06:50s | LAN6 | LOS-ETH | UP
06:50s | LAN7 | LOS-ETH | UP
06:50s | LAN8 | LOS-ETH | UP
-----
```

Option: C – clears the Alarm log

Parameter	Description
Time ago	Time since the alarm was detected.
Interface	The Interface that reported about alarm.
Alarm	The type of detected alarm.
Event	Information if the alarm arose (UP) or disappeared (DOWN).

5.7.3.13 <LINKDIAG> Command

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

```
CO_PM>LINKDIAG
```

```
Querying link data: DSL1(.)
```

DSL	Unit	NM	G.826(ES)	Status	Alarms	Description
1	local (CO)	20.0	000000000	up	None	DSL1
	remote (CP)	20.0	000000000	up	None	DSL1
2	local (CO)	---.-	000000000	pre act	LOSW	DSL2

Parameter	Value	Description
DSL	1 ... 2	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

5.7.3.14 <M> Command

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

5.7.4 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_FMM>
```

5.7.4.1 <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].

```
CO_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 DOT1X            Show IEEE 802.1x status
STATUS RADIUS [NRSB]    Show RADIUS server status and parameters
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 startup 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
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
APPLY [ALL/GROUP]       Apply changes to running configuration
CONNECT [N:[1-13/R]]    Establish connection to remote unit
M                        Return to Main Menu
H                        Show available commands
-----
```

5.7.4.2 <NM> & <LINKNM> Commands

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].

```
xDSL NM: 20.0 0.0 dB
xDSL NM: 20.0 0.0 dB
xDSL NM: 20.0 0.0 dB
xDSL NM: 20.0 0.0 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).

```
-----
DSL 1          DSL 2
-----
CO 20.0        CO ---.-
CP 20.0
-----
CO_FMM>
```

A normal quality of a SHDSL data transmission is possible for $NM \geq 6$ dB.

5.7.4.3 <STATUS> Command

This command displays the actual status of the device.

SHDSL card:

```
CO_FMM>STATUS
-----
Status          :      DSL1      DSL2
-----
I/F mode        :      CO      CO
SYNC            :      -      -
SEGD            :      -      -
Power backoff   :      0.0      0.0      dbm
Far end power backoff :      0.0      0.0      dbm
Loop attenuation :      0.0      0.0      dB
NMR             :      0.0      0.0      dB
Bitrate         :      0      0      kbit/s
SRU #           :      0      0
Active sync. source :      Internal Internal
-----
Temperature     :      39.750 C
-----
CO_FMM>
```

Option: T – update the table continuously.

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 Internal	External sync Internal sync source
Temperature	N	Unit temperature [C°]

FOM, GFOM, IO, PoE & Switch, FlatRack Switch:

```
CO_FMM>STATUS
```

```
-----
```

```
Status
```

```
SFP1-Module : present
SFP1-Link   : inactive
LAN2        : 1000 FULL
LAN3        : inactive
LAN4        : 100 FULL
LAN5        : inactive
LAN6        : inactive
LAN7        : inactive
LAN8        : inactive
LAN9        : inactive
```

```
DC1 Voltage : present
DC2 Voltage : present
```

```
PoE1 port   : switched off
PoE2 port   : switched on
PoE3 port   : absent
PoE4 port   : absent
```

```
SD Card     : present
```

```
USB         : present
Temperature : 29.250 C
```

```
-----
```

Parameter	Description
SFPx-Module	Indicates the SFP-Module presence: present or absent
SFPx-Link	Indicates the SFP-Link status: inactive/100H/1000F/2500F
LANx	Indicates the LANx status
DCx Voltage	Indicates the DCx Power Supply status: present (active) /absent (inactive) (Switches only)
PoEx port	Indicates the PoE port status: switched on/ switched off/absent (Switches only)
SD Card	Indicates the SD card status: present/absent
USB	Indicates the LCT (USB) status: present/absent
Temperature	Unit temperature [C°]

5.7.4.4 <STATUS ETH> Command

This command displays parameters of the Ethernet ports, the rate and the operation mode (SHDSL, Serial and E1 only).

```
CO_FMM>STATUS ETH
LAN1 speed/duplex: 100 FULL
LAN2 speed/duplex: ---
CO_FMM>CO_FMM>
```

5.7.4.5 <STATUS L> Command

This command displays current xDSL, E1 or Serial interface configuration and status.

SHDSL card:

```
CO_FMM>STATUS L
```

```
-----
```

```
Runtime modem status
```

```
-----
```

```
xDSL          DSL1          DSL2
Description   : DSL1          DSL2
Mode          : Master, down
Extended rates: OFF
PAM, Baserate : PAM32,89 (x2) Multipair
Annex         : B              with DSL1
Payload       : WAN
Clock source  : Int
Reserve       : ---          ---
GS compatible : OFF
NM/LA alarm   : OFF/OFF
```

```
-----
```

Parameter	Description
Description	Port Description (ifAlias)
Mode	Mode: Master/Slave, Status: up/down
Extended rates	Extended DSL feature ON/OFF
PAM, Baserate	Type of the line encoding (PAM128, PAM64, PAM32, PAM16, PAM8, PAM4), Data Transmission Rate on SHDSL line (BR*64kbit/s).
Annex	Transmission Mode (ANNEX A, ANNEX B, ANNEX AB)
Payload	Data Transmission interfaces: (always WAN)
Clock source	Priority list of clock sources
Reserve	Shows Reserve group, if configured
GS compatible	Enables the Globespan (Conexant) compatibility
NM/LA alarm	Shows NM or LA alarms, if set by NMTHR or LATHR commands

Quad RS232 card:

```
CO_FMM>STATUS L
```

```
-----  
Runtime modem status  
-----
```

```
4xRS 4RS  
1 8N1 600, LOCAL  
  Break : PASS  
  UDP(OFF), Listen 5000  
  Out 192.168.0.1:5000  
2 8N1 600, REMOTE  
  Break : Ignore  
  UDP(OFF), Listen 5001  
  Out 192.168.0.1:5001  
3 8N1 600, OFF  
  Break : Ignore  
  UDP(OFF), Listen 5002  
  Out 192.168.0.1:5002  
4 8N1 600, OFF  
  Break : Ignore  
  UDP(OFF), Listen 5003  
  Out 192.168.0.1:5003  
-----
```

Parameter	Description
(First string for interface)	Interface Mode: <format> <baudrate>, <Signaling: OFF/LOCAL/REMOTE >
Break	Break signal handling PASS/Ignore:
UDP/Server/Client	RSIP mode: UDP/Server/Client and Port to listen.
Out	Destination IP:Port

RS232/RS485 card:

```
CO_FMM>STATUS L
```

```
-----  
Runtime modem status  
-----
```

```
RS:RS-232 RS  
  Mode      : RS<->IP  
  Rate      : 9600  
  Format     : 8N1  
RS<->IP (Server, ON)  
  Out 192.168.0.1  
  Listen    : 5000  
  Break     : Ignore  
  Signaling : OFF  
-----
```

Parameter	Description
Mode	Interface Mode: RS<->IP/Unused
Rate	Interface Baudrate>, <Signaling: OFF/LOCAL/REMOTE >
Format	Data Format (for Example: 8N1, 7O1)
RS<->IP	RSIP mode: UDP/Server/Client, ON/OFF)
Out	Destination IP:Port
Listen	Port to listen
Break	Break signal handling PASS/Ignore
Signaling	RTS/CTS signaling mode: OFF/LOCAL/REMOTE RSIP

E1 card:

```
CO_FMM>STATUS L
```

```
-----  
Runtime modem status  
-----
```

```
E1          E1-1          E1-2          E1-3          E1-4
Description  : E1-1          E1-2          E1-3          E1-4
G.704 framing : ON           ON           ON           ON
CRC4         : ON           ON           ON           ON
TS into WAN  : 24-31        24-31        24-31        24-31
AIS Det/Gen  : ON/ON        ON/ON        ON/ON        ON/ON
E1 clock     : INT          INT          INT          INT
E1 mode      : HDB3/LONG    HDB3/LONG    HDB3/LONG    HDB3/LONG
```

```
-----  
Temperature  : 49.000 C  
-----
```

Parameter	Description
Description	Port Description (ifAlias)
G.704 framing	ON: ITU-T G.704 framed mode / OFF: unframed mode
CRC4	ON: CRC4 mode is active / OFF: CRC4 mode is inactive
TS into WAN	Timeslots of E1 channel for transmission of WAN Ethernet data.
AIS Det/Gen	AIS Detection/Generation mode ON/OFF
E1 clock	E1 clock source: RX/INT/XCON
E1 mode	E1 interface line code HDB3/AMI / short (SHORT)/long (LONG) haul mode
Temperature	Unit temperature [C°]

5.7.4.6 <STATUS SFP> Command

This command displays parameters of the SFP Transceiver.

```
CO_FMM>STATUS SFP
```

```
-----  
Interface      LAN1      LAN2  
Description     SFP1      SFP2  
Module Information  
Module Type    : ---      ---  
Module PN      : ---      ---  
Module REV     : ---      ---  
Vendor Name    : ---      ---  
Vendor ID      : ---      ---  
Calibration    : ---      ---  
Module Status  
Temperature    : ---      ---      C  
Voltage        : ---      ---      V  
Bias current   : ---      ---      mA  
RX Power       : ---      ---      mW / dBm  
TX Power       : ---      ---      mW / dBm  
-----
```

Parameter	Description
Interface	Port identifier of the internal Ethernet switch.
Description	Port Description (ifAlias)
Module Information:	
Module Type	Type of the module
Module PN	Part number of the module
Module REV	Revision number of the module
Vendor Name	Vendor name
Vendor ID	Vendor IEEE ID
Calibration	SFP calibration information
Module Status:	
Temperature	Internally measured SFP temperature
Voltage	Internally measured SFP supply voltage
Bias current	Internally measured SFP TX bias current
RX Power	Internally measured SFP RX input power
TX Power	Internally measured SFP TX output power

5.7.4.7 <STATUS IO> Command

This command shows the extended status information of inputs and outputs.

```
CO_FMM>STATUS IO
-----
Port  Status Desc. Normal Mode Remote
-----
IN-1  Open   IN1      NO, UDP:5000 <-> 192.168.0.234:6000 > discon
IN-2  Open   IN2      NO, UDP:5002 <-> 192.168.0.234:6002 > discon
IN-3  Open   IN3      NO, UDP:5004 <-> 192.168.0.234:6004 > discon
IN-4  Open   IN4      NO, UDP:5006 <-> 192.168.0.234:6006 > discon
OUT-1 Open   OUT1     NO, UDP:5001 <-> 192.168.0.234:6001 > discon
OUT-2 Open   OUT2     NO, UDP:5003 <-> 192.168.0.234:6003 > discon
OUT-3 Open   OUT3     NO, UDP:5005 <-> 192.168.0.234:6005 > discon
OUT-4 Open   OUT4     NO, UDP:5007 <-> 192.168.0.234:6007 > discon
-----
Input insensitivity: 4000 ms
-----
```

Parameter	Description
Port	Port function (IN/OUT) – Port number (1..4)
Status	Port status: Open/Closed.
Description	Port Description (ifAlias)
Normal	Normal state of the interface: NO (Normally Open)/NC (Normally Closed)
Mode	The interface mode: OFF/UDP/TCP Client/TCP Server/Urgent alarm/NonUrgent alarm
Input insensitivity	The input insensitivity in ms

5.7.4.8 <STATUS LLDP> Command

This command shows LLDP neighborhood.

```
CO_FMM>STATUS LLDP
LAN1 neighbour:
  Port description: LAN1
  System name: Wolken_4V24
  Management address: 192.168.1.238
  Chassis ID: 00:0f:d9:12:26:df
  Port ID: LAN1
  System description: MF-SER-SRL-4V24, V1 (SW: 1.7.7 HW: 9.0)
```

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

5.7.4.9 <STATUS DOT1X> Command

This 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
=====
```

Parameter	Description
Authorized (Port)	Displays if LAN port received permission from server to pass traffic
Authorized (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

5.7.4.10 <STATUS RADIUS> Command

This command displays the actual status of RADIUS servers

```
CO_FMM>STATUS RADIUS
```

```
-----
Status      :      Server 1      Server 2
-----
Status      :      Connected      Not connected
Server IP    :      192.168.100.155      255.255.255.255
Server port  :      1812      1812
Shared key   :      entered      empty
Retries      :      2
Timeout, seconds :      2
-----
```

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.

5.7.4.11 <STATUS ENCODE> Command

This command shows status of encoded WAN channel.

```
CO_01_FMM>STATUS ENCODE
```

```
-----
Destination :   WAN1           WAN2           WAN3           WAN4
-----
Status      :   DSL1           DSL2           DSL3           DSL4
Enabled     :   no            no            no            no
Remote      :
Key         :
-----
```

```
CO_01_FMM>
```

Parameter	Description
Destination	Name of WAN channel
Status	The physical channel where logical WAN channel operate. Can be either DSL or E1.
Enabled	Shows if encoding is enabled or disabled on this channel.
Remote	Status of remote unit: Waiting: waiting for peer Detected: peer detected
Key	Status of cipher exchange with remote unit: Initiated: cipher exchange initiated Confirmed: cipher exchange successful; keys match Not confirmed: cipher exchange failure; keys don't match

5.7.4.12 <STATUSPOE> Command

This command displays the actual PoE status.

```
CO_FMM>STATUSPOE
```

```
-----
Status PoE
-----
```

```
PoE Card    : absent
Port 1      : off
Current 1   : -    mA
Port 2      : off
Current 2   : -    mA
```

Parameter	Description
PoE card	Indicates the presence of at least one PoE card: present/absent
Portx	Indicates the PoE port status: on/off
Currentx	Indicates the actual measured current in mA

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

This command activates/deactivates the local loop back on the 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
```

5.7.4.14 <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). 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_FMM>LOOP2 1:R ON
Loop2 set is initiated.
Loop2 is successfully set.
CO_FMM>LOOP2 1:R OFF
Loop2 reset is initiated.
Loop2 is successfully cleared.
```

5.7.4.15 <ALARM> Command

This command displays the actual alarm status of the local device. For devices with different numbers and types of interfaces, the number of displayed columns and content are different too.

CP_FMM>ALARM

-----			-----		
	xDSL	:	DSL1		
-----			-----		
	LOS	:	off		
	LOSW	:	off		
	SEGD/SEGA	:	off/off		
	BER-H	:	off		
	ALB	:	off		
	LOOP2	:	off		
	RCONF	:	on		
	NM/LA	:	off/off		
	TLM	:	off		
	Remote	:	MAJ		
-----			-----		
Ethernet	:	1	2	Maintenance	
-----			-----		
LOS-E	:	on	on	HW-F	: off
				DSL-F	: off
				SW-MNT	: off
-----			-----		

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 (Serial interface)	
ECA	Cable is not connected
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/SEGA	A failure in the line (segment degradation) / Errored data or errored frame alignment (segment alarm)
BER-H	The block error rate in the line is according to G.826 $\geq 30\%$
ALB	Analogue loop back is active
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.
TLM	External alarms from the regenerators in the active line
Remote	Alarm of the remote device
Definitions (Backplane)	
MAJOR	ON – at least one Line Card in the Rack has Major alarm / OFF – no alarm detected
MINOR	ON – at least one Line Card in the Rack has Minor alarm / OFF – no alarm detected
Definitions (Maintenance)	
HW-F	Hardware failure
DSL-F	DSL failure
SW-MNT	OFF: No Software maintenance operation is in progress. UPD: Software update is active. ERR: Software update ended with error and software image is corrupted. NEW: Software download ended successfully, reboot is needed. NCONF: Software image needs to be confirmed with SOFTCONFIRM command. SNAPSHOT: Device SW or Configuration does not match SD-Card copy

Table 5.3 <ALARM> definitions

5.7.4.16 <ACO [GROUP ON/OFF]> Command

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

```
CO_FMM>ACO
E1-1, ETH1
```

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

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 Ethernet, enter the ACO command twice: first, with the parameter E1-1, and second, with the parameter ETH.

```
CO_FMM>ACO E11 ON
E1-1
CO_FMM>ACO ETH ON
E1-1, ETH1
```

Available alarm groups:

SHDSL, Serial and E1		FOM, GFOM, IO, PoE & Switch, FlatRack Switch	
GROUP	Description	GROUP	Description
E1-1 or E11	1 st E1 channel	LANx	x th Ethernet port
E1-2 or E12	2 nd E1 channel	LAN	All Ethernet ports
E1-3 or E13	3 rd E1 channel	BKPM AJ	Backplane MAJOR alarm
E1-4 or E14	4 th E1 channel	BKPM IN	Backplane MINOR alarm
E1	All E1 channels	BKP	All Backplane alarms
ETH1 or ETHERNET1	1 st Ethernet port	EC1	All IO's alarms
ETH2 or ETHERNET2	2 nd Ethernet port		
ETH3 or ETHERNET3	3 rd Ethernet port		
ETH or ETHERNET	All Ethernet ports		
DSL1 or SHDSL1	1 st DSL channel		
DSL2 or SHDSL2	2 nd DSL channel		
DSL or SHDSL	All DSL channels		
RCONF	RCONF alarm		
EC1	Serial cable connection		

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

Note: By default, the Ethernet or LAN alarms are blocked in all configurations.

5.7.4.17 <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.

```
CO_FMM>MACTABLE
d8:eb:97:bf:2b:38 LAN1 VLAN1
22:c9:d0:2b:6b:cc LAN1 VLAN1
00:0f:d9:12:36:0d WAN1 VLAN1
00:0f:d9:12:33:1a INT VLAN1
```

5.7.4.18 <LLDP STAT [IF/ALL]>

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

```
CO_FMM>LLDP STAT ALL
IfIndex 7 neighbors
00:0f:d9:12:36:0d age: 3 ttl: 121
    Chassis ID: MAC address 00:0f:d9:12:36:0d
    Port ID: Interface name WAN1
    TTL: 121
    Port description: WAN1
    System description: MF-PAM-RAIL2N-2Eth, V1 (SW: 1.7.7 HW: 5.2)
    System capabilities: system: 0x4 enabled: 0x4
    Management address: IPv4 192.168.1.235 ifIndex(2): 5
    Management VID: 1
    Maximum frame size: 2048
    MED capabilities: device type: 1, capabilities: 0x21
    Hardware Revision: 5.2
    Software Revision: 1.7.7
    Serial Number: CCS134703688
    Model Name: MF-PAM-RAIL2N-2Eth, V1
```

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
Management VID	Integer	Management VLAN ID
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

5.7.4.19 <STARTAL [N]> Command

This command starts/stops (toggles) the analogue loop back at the SHDSL line interface on the device with the number N.

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

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

5.7.4.20 <RESTART [N=1..2]> Command

This command restarts the corresponding SHDSL channel. First it causes the loss of sync between modems which later will be restored.

```
CO_FMM>RESTART 1
Restarting channel 1
```

5.7.4.21 <RESET> Command

This command restarts the device.

5.7.4.22 <CONFIRM> Command

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

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

5.7.4.23 <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
```

5.7.4.24 <RESTORE> Command

This command restores the startup 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
```

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

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

```
CO_FMM>DIFF R B
-----
Running configuration      Backup configuration
-----
VLAN.VLANMASK.3
00 01                    | 00 07
-----
```

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 ---
-----
```

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

This command displays the dump of the corresponding configuration: New, Running, Startup 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
NET.MAC_SPEED
5A
SNMP.TRAPIP.0
00 00 00 00
SNMP.TRAPIP.1
00 00 00 00
02 ...
-----
```

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.

5.7.4.27 <LOAD> Command

This command downloads the configuration file obtained with the help of the DUMP command into 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.
```

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.

5.7.4.28 <TLM> Command

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

```
CO_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 |
-----
```

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

```
CO_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 |
-----
```

Option C - Clears the status of the TLM table.

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

This command sets some device 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 - device will show this alarm by 'TLM' command.

2 - device will indicate minor remote alarm and show this alarm by 'TLM' command.

3 - device will indicate major remote alarm and show this alarm by 'TLM' command.

```
CO_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 |
-----
```

5.7.4.30 <LOG> and <LOG C> Command

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

5.7.4.31 <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.

5.7.4.32 <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.
- CERT: Download X.509 Certificate into the unit
- KEY: Loads Private Key into the unit
- CA: Download Certificate of Certification Authority (Intermediate Certificate)
- 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 FPGAUPDATE 172.16.53.1 FPGA_PROG.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
- TFTP CERT 172.16.53.1 CERT.PEM
- TFTP KEY 172.16.53.1 KEY.PEM
- TFTP CA 172.16.53.1 CA.PEM

5.7.4.33 <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
```

5.7.4.34 <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.

```
CO_FMM>SOFTINFO
Loader : 5.7
  fpga : universal 0.0.1, length: 133k, CRC OK
1: ver.: 1.7.7, date: 30.11.2017, length: 693k, CRC OK, fixed
  dsl : 1.7.5__001, length: 64k, CRC OK
  fpga : universal 0.0.1, length: 133k, CRC OK
2: * ver.: 1.7.7, date: 30.11.2017, length: 693k, CRC OK, confirmed
  * dsl : 1.7.5__001, length: 64k, CRC OK
  * fpga : universal 0.0.1, length: 133k, CRC OK
```

The asterisk shows the running downloaded version (starts after power on).

Item	Description
Loader	The number of the bootloader version.
fpga	The description and number of internal FPGA software version.
ver	The number of the main software version.

Item	Description
date	The date of the main software creation.
length	The size in bytes.
dsl	The number of the DSL software version.
CRC OK/FAIL	A label showing if the software is damaged or not.
The main software status 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.

5.7.4.35 <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.

```
CP_FMM>PING 192.168.1.11
```

5.7.4.36 <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.

5.7.4.37 <SD SNAPSHOT> Command

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

5.7.4.38 <SD DIR> Command

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

5.7.4.39 <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_FMM>SD DEL /O3MF/APP.BIN
```

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

This 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.

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

This 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.

5.7.4.42 <SD BOOT [ON/OFF]> Command

This 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_XXX.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.

5.7.4.43 <SD STATUS> Command

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

```
CO_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.

5.7.4.44 <RESETPOE> Command

This command forces a hardware reset on the PoE unit.

5.7.4.45 <M> Command

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

5.7.4.46 <BERT> Command

The <BERT> command allows entering the BERT submenu (E1 cards only):

```
BER tester menu activated
Enter 'M' to return to FMM, or 'H' for HELP information
```

```
CO_BERT>
```

5.7.4.47 <H> Command

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

```
CO_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-E14] [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
M              Return to Fault and Maintenance Menu
H              Show available commands
-----
```

5.7.4.48 <START> Command

This command starts internal BERT tester.

```
CO_BERT>START
BERT is started
```

5.7.4.49 <STOP> Command

This command stops internal BER tester.

5.7.4.50 <RES> Command

This command resets BERT statistics.

```
CO_BERT>RES
Restarting BERT ...
```

5.7.4.51 <SHOW> Command

This command shows BERT statistic.

```
CO_BERT>SHOW
Testing E1-1, External output
-----
BERT status          G.826
-----
Sync                : Sync loss          Errors                : 0
                    : Pattern loss detected Errored seconds     : 0
Bitrate TX           : 1984000            Severely errored seconds : 0
Bitrate RX           : 1984000            Background block errors  : 0
Bit errors           : 0                  ESR [%]                 : 0.00
Pattern time         : 0                  SESR[%]                  : 0.00
Error ratio          : 0                  BBER [%]                  : 0.00
No errors for        : 0                  Available time           : 0
Total test time      : 73                 Unavailable time         : 73
-----
```

Parameter	Description
<table header "Testing...">	E1-n – indicates E1 interface for which BERT is active (1 , 2 , 3 and 4 indicate the 1st, 2nd, 3rd and 4th E1 interface) External – means testing of E1 path, i.e. the test pattern is sent to E1 output, while bit error test is performed for the data coming to E1 input Internal – not valid option for E1 line card
BERT status	Description
Sync	Synchronization: OK or Sync loss
<BERT status>	Possible status: - No errors – no bit errors and pattern loss detected since BERT starting or resetting of the statistic - Errors detected – at least one bit error was detected - Pattern loss detected – at least one pattern loss was received - ALL 1s – receiving of all ones - ALL 0s- receiving of all zeros
Bitrate TX	Transmission bit-rate
Bitrate RX	Receiving bit-rate
Bit errors	Number of bit errors detected
Pattern time	Indicates the total time of test pattern receiving.
Error ratio	Indicates result bit error ratio in E-notation (for example: 3.16E-10)
No errors for	Indicates time since the last bit error or pattern synchronization loss
Total tests time	Indicates elapsed time since entering of START command
G.826 statistic	Description
Errors	A block in which one or more bits are in error.
Errored Second	A number of seconds with one or more errored blocks or at least one defect
Severely Errored Second	A number of seconds that contain ≥30% of errored blocks or at least one defect. Severely Errored Second (SES) is a subset of Errored Second (ES).
BBER (Background Block Error)	Errored blocks not occurring as a part of SES.
ESR (Errored Second Ratio)	The ratio of ES to total seconds in Available time.
SESR (Severely Errored Seconds Ratio)	The ratio of SES to the total number of error-free seconds in Available time.
BBER (Background Block Error Ratio)	The ratio of Background Block Errors (BBE) to total blocks in Available time. The count of total block excludes all blocks during SESSs.
Available time	The period when measurements of the parameters are possible.
UAT (Unavailable time)	The period when the measurements of the parameters are impossible.

5.7.4.52 <TRACE> Command

This command shows BERT statistic continuously.

5.7.4.53 <SET [E11-E14] [INT/EXT]> Command

This command selects E1 interface and the test path.

First parameter [E11-E14]: E1 interface which will be used for BER-testing (E11-E14)

Second parameter [INT/EXT]: Test path:

- EXT – means testing of E1 path, i.e. the test pattern is sent to E1 output, while bit error test is performed for the data coming to E1 input
- INT – not valid option for E1 line card

```
CO_BERT>SET E11 EXT
```

5.7.4.54 <TS [TX/RX] [list/NONE]> Command

This command selects timeslots to be used for generating/receiving a test pattern.

First parameter [TX/RX]:

- TX – sets a list of time slots to be used for generating of the test pattern
 - RX – sets a list of time slots to be used for receiving of the test pattern
- If parameter is omitted, timeslots are set both for generating and receiving.

Second parameter [list/NONE]:

- list – a comma-separated list of timeslots/intervals
- NONE – clear list of time-slots

```
CO_BERT>TS 1-23
```

5.7.4.55 <PATD [2En/bitstring]> Command

This command defines a test pattern for BERT.

Parameter:

- 2En – $2^N - 1$ pattern ($n=7,9,11,15$) to check BER-ratio
- DALY – 55*8-bit pattern with low correlated 8-bit blocks to check timing recovery
- QRSS – has period of 1048575-bit pattern for jitter measurements
- bitstring – a bit string like 0111010 (max. 32 digits)

```
CO_BERT>PATD 2E15
```

5.7.4.56 <CONF> Command

This command shows BERT configuration.

```
CO_BERT>CONF
```

```
-----
Current BERT configuration:
-----
Interface   : E1-1, External output
Pattern     : 2E15

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
-----
```

Parameter	Description
Interface	E1-n – indicates E1 interface for which BERT is active (1, 2, 3 and 4 indicate the 1st, 2nd, 3rd and 4th E1 interface) External – means testing of E1 path, i.e. the test pattern is sent to E1 output, while bit error test is performed for the data coming to E1 input Internal – not valid option for E1 line card
Pattern	Shows the test pattern: 2En, DALY, QRSS or bit string
TX Slots	A list of time slots to be used for the test pattern generation (PG)
RX Slots	A list of time slots to be used for BER testing (BT)

5.7.5 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_CM>
```

The content of the configuration management menu depends on the device model and the operation mode of the device (for SHDSL line cards). There are four possible modes of the SHDSL line card:

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 WAN streams is received from the SHDSL line, automatic config.

5.7.5.1 <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_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 [4/8/16/32/64/128] [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/OFF]         Select or turn off multipair mode
RESERVE [list]            Set the list of channels for the reserve group
ID [string]               Set/Clear device 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]                  Sets the 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
M                          Return to Main Menu
H                          Show available commands
-----
```

5.7.5.2 <ENCODE [NRSB]> Command

This command shows encoding configuration.

```
CO_01_CM>ENCODE
Running configuration
```

```
-----
Encoding      :  WAN1      WAN2      WAN3      WAN4
-----
Destination   :  DSL1      DSL2      DSL3      DSL4
Key           :   set      set       set       set
Enabled       :   no       no        no        no
-----
```

```
CO_01_CM>
```

Optional parameters describe what configuration must be shown: **N**ew, **R**unning, **S**tartup, **B**ackup.

Definitions	
Encoding	Name of WAN channel
Destination	The physical channel that carries logical WAN channel. It can be either DSL or E1.
Key	Tells if Key has been entered or not.
Enabled	Shows if encoding is enabled or disabled on this channel.

5.7.5.3 <ENCODE KEY [N]> Command

This command enters pre-shared secret Key for selected WAN channel [N]:

```
CP_CM>ENCODE KEY 1
Please enter encryption key [mykey1]:
Please repeat encryption key:
```

```
-----
Encoding      :  WAN1      WAN2      WAN3      WAN4
-----
Destination   :  DSL1      DSL2      DSL3      DSL4
Key           :   set      set       set       set
Enabled       :   yes      yes        yes        yes
-----
```

```
Warning: New Encoding configuration is shown, because it differs from running.
To view new encoding configuration, type 'ENCODE N'.
To view running encoding configuration, type 'ENCODE R'.
To apply changes in configuration, type 'APPLY'.
Do not forget to 'CONFIRM' a good working configuration.
```

```
CP_CM>
```

The pre-shared Key must contain only the following characters: ! " # \$ % & ' () * + , - . / 0 1 2 3 4 5 6 7 8 9 ; : < = > ? @ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [\] _ ` a b c d e f g h i j k l m n o p q r s t u v w x y z { | } ~. Spaces will be truncated.

NOTE: Pre-shared Key can be unique for every channel or common. For unique keys please be sure that keys on both sides of WAN channels match.

5.7.5.4 <ENCODE [ON/OFF] [N]> Command

This command activates or deactivates link-layer encryption on selected WAN channel [N]:

```
CO_01_CM>ENCODE ON 1
```

```
-----
Encoding      :  WAN1      WAN2      WAN3      WAN4
-----
Destination   :  DSL1      DSL2      DSL3      DSL4
Key           :   set      set       set       set
Enabled       :   yes      no        no        no
-----
```

```
Warning: New Encoding configuration is shown, because it differs from running.
To view new encoding configuration, type 'ENCODE N'.
To view running encoding configuration, type 'ENCODE R'.
To apply changes in configuration, type 'APPLY'.
Do not forget to 'CONFIRM' a good working configuration.
```

```
CO_01_CM>
```

5.7.5.5 <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.

5.7.5.6 <USERS> Command

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

```
CO_CM>USERS
-----
Security mode: Advanced
-----
Username      Controls                               IP ACL
-----
ADMIN         ALL                                     Any IP
USER          CTRL, S{LINKC, LAN}, C{VIEW}          Any IP
-----
```

5.7.5.7 <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	Group	Subgroup				
ALL	Commands of this level are available for everyone. No additional authorization is required			ACO ALARM	ALARM T SOFTINFO	TLM
	CONTROL [CTRL]		Operation of remote devices	CONNECT		
	TEST [T]		Test of the device	BERT Submenu LOOP1 LOOP2	MACTABLE MACTABLE C PING	RESTART STARTAL
	ADMIN [A]		Administration of the device	ACO change APPLY BACKUP CONFIRM DEFAULT DEFAULT DESC DEFAULT EVERYTHING DIFF FACTORY DEFAULT	DUMP ID LATHR LICENSE LICENSE ADD LOAD LOG NMTHR PASSWORD RESET RESTORE	SD SECURE SERNUM SOFTCONFIRM SOFTUPDATE TFTP TLM C TLM D TLM S USER USERS
	STATUS [S]	:LINK	Link status	ALARMLOG ALLG826 G826 [C] G826 E1 [C]	LINKALARM LINKNM LINKSTAT NM	STATUS STATUS EXT STATUS L STATUS T
		:LINKC	All commands from LINK + reset of the counters	ALARMLOG C	RESETALLG826	RESETG826
		:LAN	Ethernet status	ALARMLOG LLDP STAT MACTABLE NETERR	NETSTAT STATUS DOT1X STATUS ETH STATUS LLDP	STATUS RADIUS STATUS SFP
		:LANC	All commands from LAN + reset of Ethernet counters and MAC table	ALARMLOG C	MACTABLE C	RESETNETSTAT
	CONFIG [C]	:VIEW	Displaying of device configuration	CONFIG COSCONFIG IOCONFIG	LLDP CONFIG MACLIST SHOW NETCONFIG	RSTP CONF STATUS IO
		:LINK	All commands from VIEW +line, E1 and Nx64 interface configuration	4RS AISDET AISGEN ANNEX APPLY AUTO AUTOLOOP BASERATE CONFIRM CRC4 DEFAULT	E1CLOCK E1MODE EXT G704 GSCOMPAT IOIP MASTER MODE N MULTIPAIR PAM PAYLOAD	POWER PTMP RESERVE RSDUPLEX RSFORMAT RSIP RSRATE SETCLOCK WANIDLE WANTS
		:LAN	All commands from VIEW + LAN configuration	ALLOW APPLY CONFIRM COS CRATE DOT1X ERATE ETHSD FC GATEWAY IRATE	JUMBO SIZE LLDP change LLDP DEFAULT MACFILTER MACLIST [IF] MACRULE MODE [IF] MTU NETDEFAULT NETMASK PBVLAN	PING QOS RSTP [CONF] RSTP change RSTP DEFAULT SETIP VID VLAN VLANNAME
		:SNMP	All commands from VIEW + SNMP configuration	APPLY COMMUNITY CONFIRM	RMONALARM RMONEVENT SNMP	SNMPACL SNMPSET TRAP
		:NET	All commands from VIEW + IP configuration	APPLY CONFIRM DST GATEWAY HTTP MTU NETMASK	PING RADIUS SETIP SNTP SSH PORT SSH SYSCONTACT	SYSLOCATION SYSLOG SYSLOG SYSNAME TELNET

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 SSH, 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.

5.7.5.8 <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 USB interface, the password is not requested.

5.7.5.9 <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

The outlook of the CONFIG table depends of the model.

SHDSL Line Card:

```
CO_CM>CONFIG
```

```
-----
Running Line Configuration
-----
```

xDSL	DSL1	DSL2
Description :	DSL1	DSL2
Mode :	Master (HTU-C)	Master (HTU-C)
Extended rates:	OFF	OFF
PAM, Baserate :	PAM32,89	PAM32,89
Annex :	B	B
Payload :	WAN	NONE
Clock source :	Int	Int
Reserve :	{===== Reserve group A =====}	
GS compatible :	OFF	
NM/LA alarm :	OFF/OFF	

```
-----
```

Group of SHDSL parameters

Description	Interface Description (ifAlias)
Mode	Master, Slave, Multipair All slave, configured by master All slave, MULTIPAIR xx, configured by master
Extended rates	Extended DSL feature ON/OFF
PAM, Baserate	Type of the line encoding (PAM4-128), Transmission Rate (BR*64kbit/s). Auto – adaptation mode
Annex	Transmission Mode (ANNEX A, ANNEX B, ANNEX AB)
Payload	Data Transmission interfaces: WAN or NONE
Clock source	Priority list of clock sources. Always Int (internal clock)
Reserve	Reservation Group, if configured by RESERVE command
GS compatible	Globespan (Conexant) compatibility: ON or OFF
NM/LA alarm	Noise Margin / Loop Attenuation alarm settings

Serial RS-232/422/485 Interface Line Card:

CO_CM>CONFIG

Running Line Configuration

```
RS:RS-232
Mode      : RS<->IP
Rate      : 9600
Format    : 8N1
RS<->IP (Server, ON)
Out 192.168.0.1
Listen    : 5000
Break     : Ignore
Signaling : OFF
-----
```

Group of RS-232/422/485 parameters

RS	Interface HW mode: RS-232 or RS-485
Mode	RS<->IP or Unused
Rate	Serial baudrate in bps
Format	Serial data format, for example: 8N1
RS<->IP	RS<->IP Mode: (Server/Client/UDP, ON/OFF)
Out	IP address and port of remote system where serial data will be transferred to
Listen	Port for reception of serial data packets
Break	Break signal mode: Ignore/PASS
Signaling	RTS/CTS signaling mode: OFF/LOCAL/REMOTE

Serial RS-232 Interface Line Card:

CO_CM>CONFIG

New Line Configuration

```
4xRS 4RS
1 8N1 600, LOCAL
Break : PASS
Server(OFF), Listen 5000
Out 192.168.0.1
2 8N1 600, REMOTE
Break : Ignore
UDP(OFF), Listen 5001
Out 192.168.0.1:5001
3 8N1 600, OFF
Break : Ignore
UDP(OFF), Listen 5002
Out 192.168.0.1:5002
4 8N1 600, OFF
Break : Ignore
UDP(OFF), Listen 5003
Out 192.168.0.1:5003
-----
```

Group of RS-232 parameters of four RS-232 ports

(first string)	(serial data format) (serial baudrate in bps), (RTS/CTS signaling mode: OFF/LOCAL/REMOTE)
Break	Break signal mode: Ignore/PASS
(third string)	RS<->IP Mode: Server/Client/UDP (ON/OFF), Port for reception of serial data packets
Out	IP address and port of remote system where serial data will be transferred to

E1 Interface Line Card:

CO_CM>CONFIG

Running Line Configuration

```

E1              E1-1          E1-2          E1-3          E1-4
Description    : E1-1          E1-2          E1-3          E1-4
G.704 framing  : ON            ON            ON            ON
CRC4           : ON            ON            ON            ON
TS into WAN    : NONE         24-31         24-31         24-31
AIS Det/Gen    : OFF/OFF      ON/ON      ON/ON      ON/ON
E1 clock       : INT          INT          {=====XCON=====}
E1 mode        : HDB3/LONG    HDB3/LONG  HDB3/LONG  HDB3/LONG
-----
Temperature    : 49.750 C
-----

```

Group of E1 parameters	
Description	Interface Description (ifAlias)
G.704 framing	Framing mode
CRC4	CRC4 mode
AIS Det/Gen	AIS detection/generation modes
E1 clock	Clock source: RX, INT, XCON
E1 mode	Line code: HDB3/AMI/Receiver gain: SHORT or LONG haul mode

5.7.5.10 <MASTER ON/OFF [N = 1..2]> Command

This command activates/deactivates the «MASTER» mode on the interface with the number N.

CP_CM>MASTER ON 1

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

5.7.5.11 <AUTO ON/OFF> 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.

5.7.5.12 <EXT ON/OFF [N = 1..2]> Command

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

Note: The EXT ON feature needs a special LICENSE KEY that must 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

5.7.5.13 <BASERATE [M/AUTO] [N]> Command

This command sets the transmission rate M to the line SHDSL interface, where N is the number of the SHDSL interface. The data transmission is $\text{BASERATE} * 64\text{ kbit/s}$.



WARNING

FOR LOW BASERATES YOU SHOULD USE THE LOWEST POSSIBLE NUMBER OF CODE LEVELS. FOR A STANDARD 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.

5.7.5.14 <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.

```
CO_CM>PAM 16 1
```

5.7.5.15 <PAYLOAD list/NONE [N=1..2]> Command

This command sets the list of streams transmitted over the SHDSL channel. N is the number of the SHDSL channel. The parameter list must be WAN (Ethernet) or NONE. The parameter NONE deactivates transmission of WAN over this SHDSL interface.

```
CO_CM>PAYLOAD WAN
CO_CM>PAYLOAD NONE
```

5.7.5.16 <ANNEX A/B/AB [N=1..2]> 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.

5.7.5.17 <SETCLOCK list [N=1..2]> 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 must be INT, INTERNAL.

```
CO_CM>SETCLOCK INT
```

5.7.5.18 <MULTIPAIR [2/OFF]> Command

This command activates the multipair mode, which allows to merge DSL channels. Both channels will be merged.

```
CO_CM>MULTIPAIR 2
CO_CM>MULTIPAIR OFF
```

5.7.5.19 <RESERVE [list]> Command

This command allows combining both SHDSL channels into a group in order to reserve them. The only one group is possible. The parameter sets the list of channel numbers separated by a comma: 1,2. To configure the reserve group, type the following command:

```
CO_CM>RESERVE 1,2
```

The parameter NONE deactivates reservation.

```
CO_CM>RESERVE NONE
```

5.7.5.20 <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 device starts operating in the so-called transparent mode.

```
CO_CM>G704 ON 1
```

5.7.5.21 <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
```

5.7.5.22 <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
```

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

This command selects timeslots of E1 channel for transmission of WAN Ethernet data. 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
```

5.7.5.24 <E1CLOCK {source} [N/{list}]> Command

This command sets the E1 output clock source.

First parameter {source}:

- RX – E1 input clock is looped back to output
- INT – E1 output stream is clocked from internal clock source
- XWAN – E1 output stream is synchronized from another E1's input stream and all unused data slots are cross-connected with this E1 (corresponding timeslots should be unused in both E1s)

Second parameter [N/{list}]:

- N – number of the E1 interface (for INT or RX mode)
- {list} – defines which channels will be cross-connected (for XWAN mode). Available lists (pairs) of channels are: 1,2 and 3,4.

```
CO_CM>E1CLOCK RX 2
CO_CM>E1CLOCK XCON 1,2
```

5.7.5.25 <E1MODE [HDB3/AMI] | [SHORT/LONG] [N]> Command

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.

```
CO_CM>E1MODE HDB3 2
CO_CM>E1MODE SHORT 2
```

5.7.5.26 <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.

5.7.5.27 <DEFAULT [0-4]> Command

The <DEFAULT N> command sets the default operation mode, where N is the mode number.

SHDSL Line Card (five default operation modes):

- The DEFAULT 0 command sets the following mode: PAM 32, BASERATE 89, ANNEX B, transmission Ethernet over SHDSL. MASTER/SLAVE setting is not affected.
- The DEFAULT 1 command sets the following mode: MASTER, PAM 32, BASERATE 89, ANNEX B, transmission Ethernet over SHDSL.
- The DEFAULT 2 command sets the following mode: SLAVE, LINECODING AUTO, BASERATE AUTO, ANNEX A/B, transmission of Ethernet over SHDSL.
- The DEFAULT 3 command sets the following mode: MASTER, PAM 32, BASERATE 89, ANNEX B, transmission Ethernet over SHDSL.
- The DEFAULT 4 command sets the following mode: SLAVE, LINECODING AUTO, BASERATE AUTO, ANNEX A/B, transmission of Ethernet over SHDSL.

Serial RS-232/422/485 Interface Line Card:

- The DEFAULT 0..4 command sets the following mode: Mode: Unused, Rate 9600, Format 8N1, Duplex FULL, Termination ON, RSIP mode: UDP, Out: 192.168.0.1:5000, Listening port: 5000. RS 232/485, BREAK and SIGNALING settings are not affected.

Serial RS-232 Interface Line Card:

- The DEFAULT 0..4 command sets the following mode: Mode: Rate 600, Format 8N1, RSIP mode: UDP (OFF), Out: 192.168.0.1:5000-5003, Listening port: 5000-5003. BREAK and SIGNALING settings are not affected.

E1 Interface Line Card:

- The DEFAULT 0 command sets the following mode: G.704 ON, CRC4 ON, WANTS 24-31, AIS Det/Gen ON/ON, E1 clock: XCON, E1 mode: HDB3/LONG.

Note, that, default network configuration is not affected (use 'NETDEFAULT' from 'NET' menu for this).

For FOM, GFOM, IO, PoE & Switch and FlatRack Switch the DEFAULT 0 command is equal to NETDEFAULT command.

5.7.5.28 <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
```

5.7.5.29 <DEFAULT DESC> Command

This command writes default Port Description (ifAlias).

```
CO_CM>DEFAULT DESC
```

5.7.5.30 <SERNUM> Command

This command shows the production serial number of the unit.

5.7.5.31 <GSCOMPAT ON/OFF> Command

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

5.7.5.32 <NMTHR> Command

This 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

5.7.5.33 <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

5.7.5.34 <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:

- 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.

5.7.5.35 <PTMP SHOW> Command

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

5.7.5.36 <MODE N> Command

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

For example: The MODE 1 in a two-channel unit disables channel 2.

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

5.7.5.37 <LICENSE> Command

This command shows the active licenses.

```
CP_CM>LICENSE
=====
Option name                Status
=====
1) Extended DSL rates      Enabled
2) Advanced security       Enabled
4) eXtra WAN channel       Disabled
=====
```

Use hardware code below to request activation key for additional options.
When you get an activation code, type the LICENSE ADD [KEY] command.

BCBKC-NL4PR-M2FLZ-ZN2NZ

5.7.5.38 <LICENSE ADD [key]> Command

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

5.7.5.39 <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 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 other 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 omitted when only one RS232/422/485 interface is available.

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

Examples:

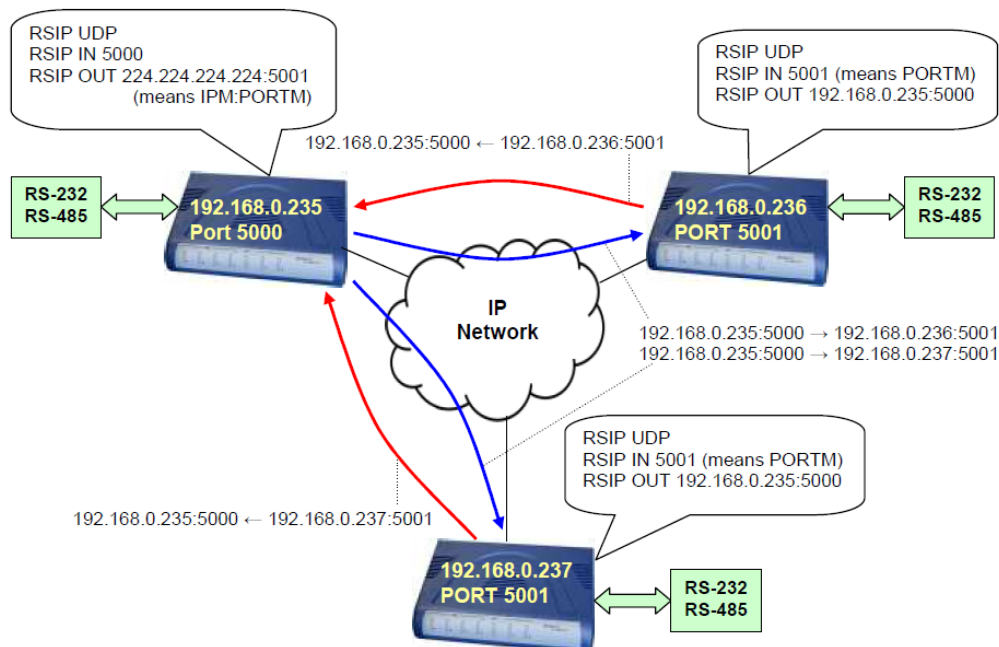
RSIP ON RS: Enable RS<->IP

RSIP UDP RS: Select UDP mode

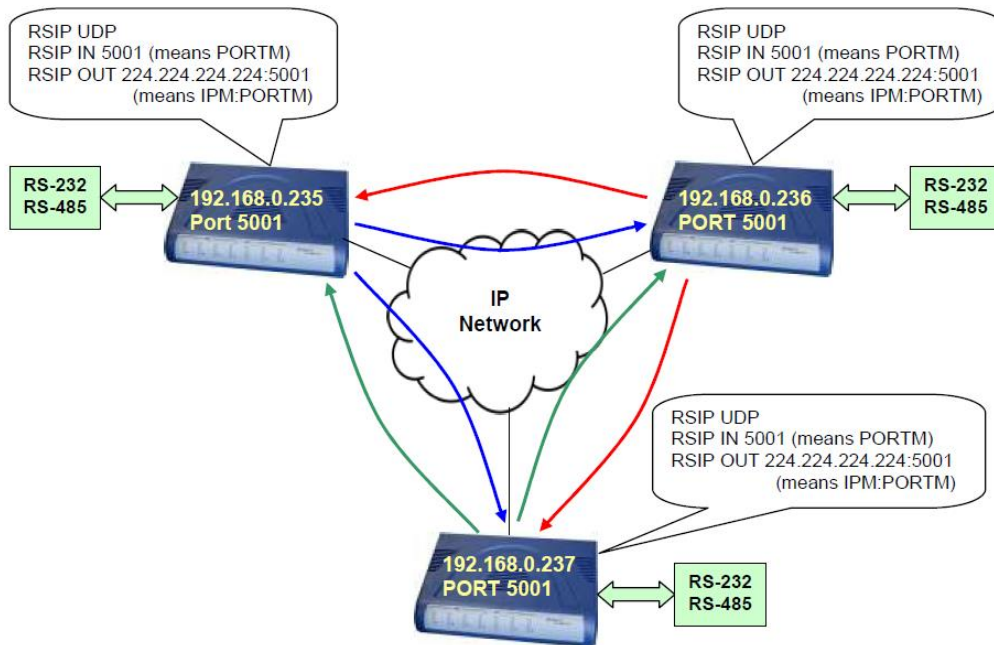
RSIP IN 5000 RS: Means to select port 5000 for the reception of serial data packets

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.

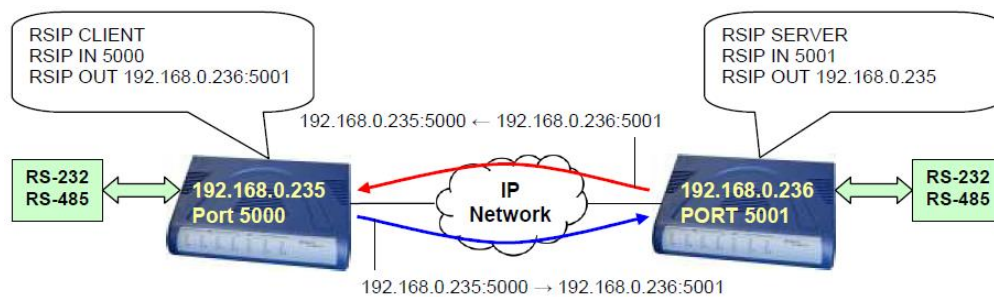
UDP Point to Multipoint (Multicast addresses are IP addresses in the range from 224.0.0.0 to 239.255.255.255):



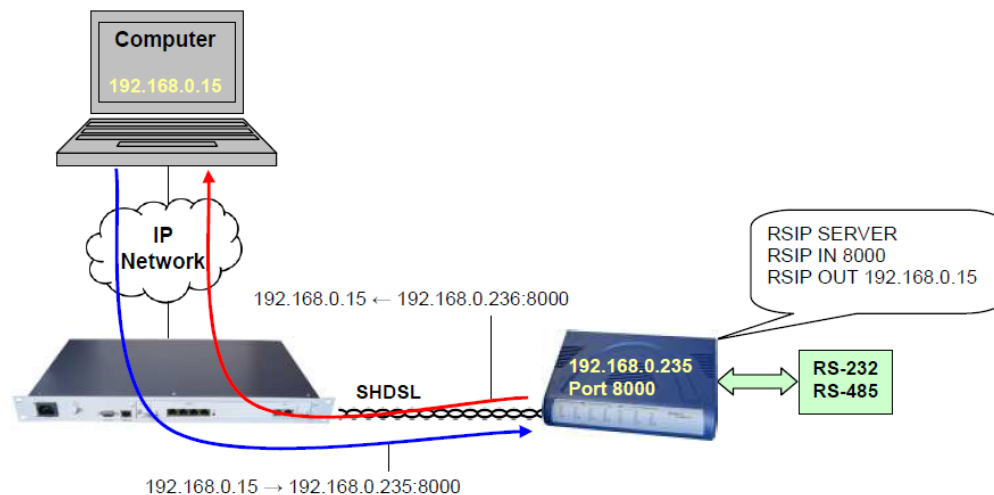
UDP Broadcast:



TCP Point to Point:



COM Server:



5.7.5.40 <RSRATE [N]> Command

This command sets the bitrate of the serial interface in bps (for Serial RS-232/422/485 Interface Line Card). The available rates are: 75, 150, 300, 600, 1200, 2400, 4800, 9600, 14400, 19200, 28800, 38400, 56000, 57600, 115200 and 230400.

```
CO_CM>RSRATE 115200
```

5.7.5.41 <RSFORMAT [Format]> Command

This command defines the RS-232/RS-485 data format (for Serial RS-232/422/485 Interface Line Card). [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

```
CO_CM>RSFORMAT 8N1
```

5.7.5.42 <RSDUPLEX [F/H] Command

This command sets the operating mode of the RS-422/485 interface:

- F means FULLDUPLEX
- H means HALFDUPLEX

5.7.5.43 <RS [232/485] Command

This command defines the physical interface for the serial interface: RS-232 or RS-422/485.

5.7.5.44 <RS TERM [ON/OFF] Command

This command sets the line termination (120 Ohm) of the RS-422/485 on or off.

5.7.5.45 <4RS {option} {value} [N]> Command

This command configures for Serial RS-232 Interface Line Card the bitrate of serial interface and symbol format options.

Syntax: 4RS RATE {rate} [N]
4RS MODE {mode} [N]

[N] is a channel of 4RS card

{rate} is a rate for selected channel. Supported rates are: 75, 150, 300, 600, 1200, 2400, 4800, 9600, 14400, 19200, 28800, 38400, 56000, 57600, 115200, 230400.

{mode} is a size and format of physical symbol. Supported formats are:

- 5x1, 5x1.5, [6,7,8]x[1,2], where x is parity:
 - N - None O - ODD
 - E - Even M - Mark
 - S - Space

5.7.5.46 <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.

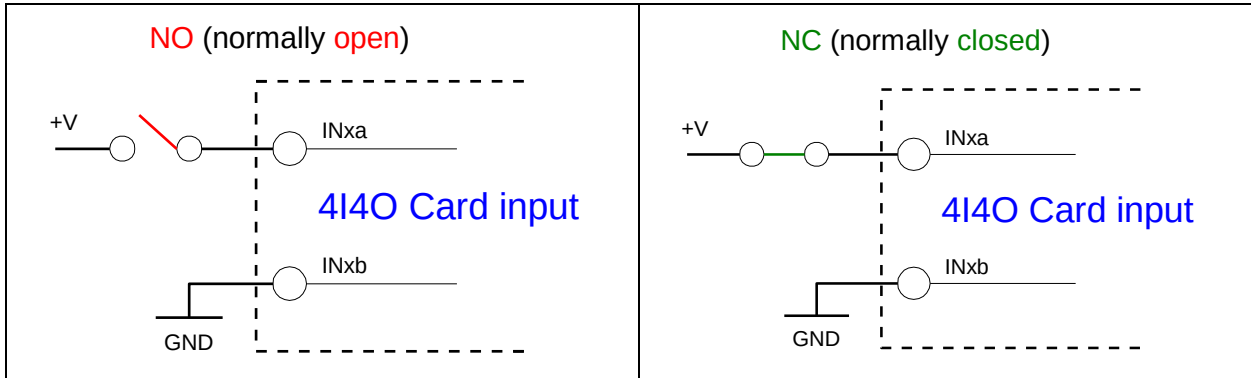
<IOIP [UA/NUA/OFF] [NO/NC] [IF]> Command

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-4 or OUT-1 ... OUT-4



<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-4 or OUT-1 ... OUT-4

<IOIP LOCAL [PORT] [IF]> Command

This command sets local IP port for an IF interface, an IF interface 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-4 or OUT-1 ... OUT-4

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

<IOIP REMOTE [IP:PORT] [IF]> Command

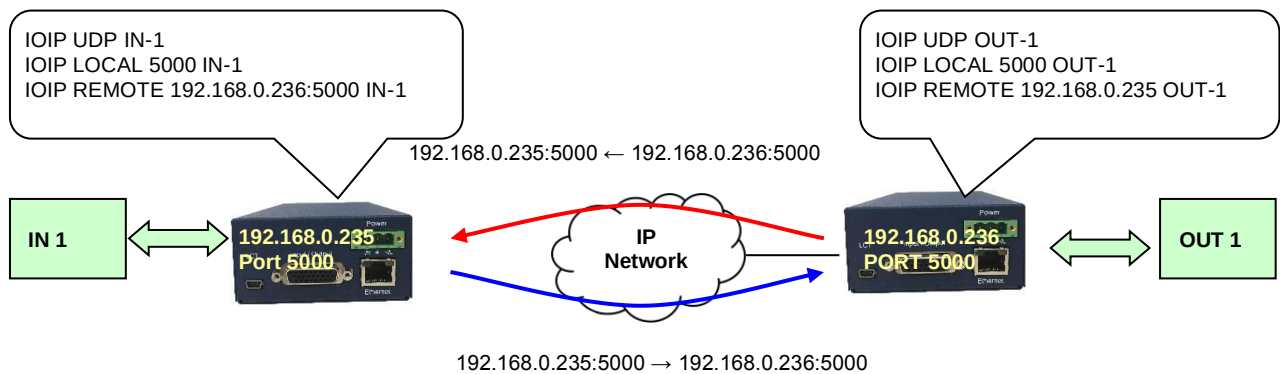
This command defines remote IP address and IP port number a local interface should be connected with.

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.

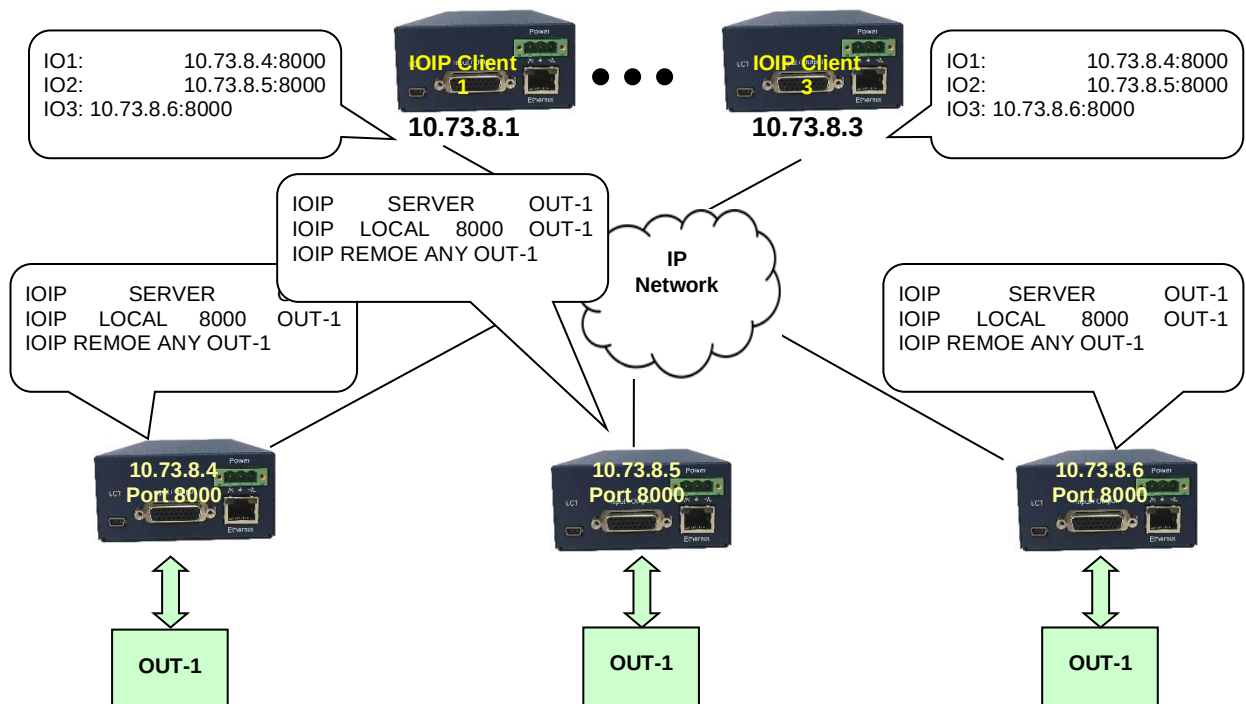
Examples:

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
IOIP LOCAL 6000 OUT-1	Set local port for interface OUT-1
IOP REMOTE ANY OUT-1	Set any remote connection for interface OUT-1

Example 1 Point-to-Point connection:



Example 2 Point-to-Multipoint connection:



5.7.5.47 <IOCONFIG> Command

This command displays configuration of Inputs and Outputs of the unit.

```
CO_CM>IOCONFIG
-----
Running IO Configuration
-----
IO : 4I4O-1
Input      : IN-1          IN-2          IN-3          IN-4
Description: IN1          IN2          IN3          IN4
Mode       : UDP          UDP          UDP          UDP
Local port : 5000         5002         5004         5006
Remote IP  : 192.168.0.234 192.168.0.234 192.168.0.234 192.168.0.234
Remote port: 6000         6002         6004         6006
NO alarm   : NO           NO           NO           NO

Output     : OUT-1          OUT-2          OUT-3          OUT-4
Description: OUT1          OUT2          OUT3          OUT4
Mode       : UDP          UDP          UDP          UDP
Local port : 5001         5003         5005         5007
Remote IP  : 192.168.0.234 192.168.0.234 192.168.0.234 192.168.0.234
Remote port: 6001         6003         6005         6007
NO alarm   : NO           NO           NO           NO

Insensitivity : 4000 ms
-----
```

Input/Output configurations	
Input	Input identifier
Output	Output identifier
Description	Port Description (ifAlias)
Mode	Interface mode: OFF/UDP/TCP Client/TCP Server/Urgent alarm/NonUrgent alarm
Local port	Local IP port for an interface, an interface listens on
Remote IP	Remote IP address a local interface is connected with
Remote port	Remote IP port number a local interface is connected with
NO alarm	Specifies that interface IN-x is normally opened (NO) or normally closed (NC)
Insensitivity	The sensitivity of an Input signal in millisecond

5.7.5.48 <NET> Command

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

5.7.5.49 <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].

```
CP_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
DOT1X [LAN1-5] [ON/OFF] Enable/disable 802.1X
DOT1X [LAN1-5] [SHOST/MHOST/MAUTH] Select 802.1X mode
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=1-2]     Set Nth Ethernet port speed
FC [ON/OFF] [N=1-2]      Set Ethernet port flow control
IRATE [speed/OFF] [N=1-2] 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
RMON EVENT 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 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 [1-13/R]         Establish connection to remote unit
M                         Return to Configuration Management Menu
H                         Show available commands
-----

```

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

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

```

CP_NET>NETCONFIG
-----
Running Network Configuration
-----
Ethernet settings : LAN1 LAN2 WAN1 WAN2 WAN3 WAN4 INT
Description       : LAN1 LAN2 WAN1 WAN2 WAN3 WAN4 INT
Destination      : DSL1
Access/Trunk      : ACC ACC Trunk Trunk Trunk Trunk ACC
Port-based VLAN   : [A] [A] [A] [A] [A] [A] [A]
VLAN              : 1 1 1 1 1 1 1
QoS               : 2 2 2 2 2 2 2
1: VLAN1 VID=1    : + + + +
2: VLAN2 VID=2    : + + + +
3: VLAN3 VID=3    : + + + +
4: VLAN4 VID=4    : + + + +
5: VLAN5 VID=5    : + + + +
6: VLAN6 VID=6    : + + + +
7: VLAN7 VID=7    : + + + +
8: VLAN8 VID=8    : + + + +
OTHER VLANS       : + + + +
Speed             : AUTO AUTO

```

```

Flow control      : OFF   OFF
System settings
IP address       : 192.168.0.235   MAC address      : 00:0f:d9:12:36:0d
Subnet mask      : 255.255.255.0   Management MTU : 1500
Default gateway  : 192.168.0.254   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
-----
CP_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 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.

5.7.5.51 <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
CoS 3 :   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 behavior!

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.

5.7.5.52 <RSTP DEFAULT> Command

This 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
-----
```

Warning: New configuration is shown! To apply changes use "APPLY" command.
Use APPLY/CONFIRM commands to make these setting permanent!
CO_NET>

5.7.5.53 <RSTP CONF> Command

This command shows running RSTP configuration for all instances.

```
CO_NET>RSTP CONF
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
-----
CO_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	Forward Delay time in seconds
MaxAge	Maximal Age
RSTP configuration for an interface	
IFACE	Interface name
DESCR	Interface description (ifAlias)
Prio	Interface priority
PathCost	Interface Path Cost
Edge	Port Edge behavior: Yes: means port can become "Edge" No: means port will never be "Edge"

5.7.5.54 <RSTP STATE> Command

This command shows actual RSTP status.

```
CP_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/---	---	

```
CP_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.

5.7.5.55 <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 neighbors.

```
P_NET>RSTP DIAG
RSTP A 32768:00-0F-D9-12-36-0D :
  1. LAN1    32768:00-0F-D9-12-36-0D
  2. LAN2    32768:00-0F-D9-12-36-0D
  3. INT     32768:00-0F-D9-12-36-0D
  4. WAN1    32768:00-0F-D9-12-36-0D
  5. WAN2    32768:00-0F-D9-12-36-0D
  6. WAN3    32768:00-0F-D9-12-36-0D
  7. WAN4    32768:00-0F-D9-12-36-0D
  8. MWAN1   32768:00-0F-D9-12-36-0D
  9. MWAN2   32768:00-0F-D9-12-36-0D
RSTP B 32768:00-0F-D9-12-36-0D :
  1. MWAN1   0:00-00-00-00-00-00
  2. MWAN2   0:00-00-00-00-00-00
RSTP C 32768:00-0F-D9-12-36-0D :
  1. MWAN1   0:00-00-00-00-00-00
  2. MWAN2   0:00-00-00-00-00-00
RSTP D 32768:00-0F-D9-12-36-0D :
  1. MWAN1   0:00-00-00-00-00-00
  2. MWAN2   0:00-00-00-00-00-00
RSTP E 32768:00-0F-D9-12-36-0D :
  1. MWAN1   0:00-00-00-00-00-00
  2. MWAN2   0:00-00-00-00-00-00
```

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

This command enables/disables RSTP for specific PBVLAN. 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.

5.7.5.57 <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 its 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.

5.7.5.58 <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 rely on network topology covered by selected VLAN, that's why a VLAN that covers all network should be selected. Default VLAN is 1.

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

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

5.7.5.60 <RSTP [A..E] 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:

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

- 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

5.7.5.61 <RSTP [A..E] MA [6..40]> Command

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								

5.7.5.62 <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

5.7.5.63 <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

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

This command sets EDGE attribute of a selected interface. If EDGE is ON, the port will not forward RSTP BPDU packets in egress direction and will work in Designated state. Other packets will be forwarded. But if it will receive BPDU in ingress direction, it will switch its role to EDGE OFF and will fall into Forwarding or Blocked state depends on network topology. If EDGE is manually set to OFF, it will never become EDGE port, i.e. if BPDU packet will not be received after 30 seconds the port will fall into Blocked state. Available interfaces are:

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

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

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

```
CO_NET>PBVLAN LAN1 B
CO_NET>PBVLAN INT B
```

```
-----
New Network Configuration
```

```
-----
Ethernet settings : LAN1  LAN2  LAN3  LAN4  WAN1  WAN2  WAN3  WAN4  INT
Description       : LAN1  LAN2  LAN3  LAN4  WAN1  WAN2  WAN3  WAN4  INT
Destination       :      DSL1  DSL2  DSL3  DSL4
Access/Trunk      :  ACC   ACC   ACC   ACC   Trunk Trunk Trunk Trunk
Port-based VLAN   :  [B]   [A]   [A]   [A]   [A]   [A]   [A]   [A]   [B]
```

```
...
```

```
...
```

PBVLANS are used 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, PBVLAN 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.

5.7.5.66 <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.

5.7.5.67 <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.

5.7.5.68 <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.

5.7.5.69 <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_NET>ALLOW LAN1 1,2,3
CP_NET>ALLOW WAN2 5,3,OTHER
CP_NET>ALLOW WAN4 ALL
```

5.7.5.70 <VID [1-8] ID> Command

This 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.

5.7.5.71 <VLANNNAME> Command

This command allows you specify VLAN name. After entering command, you will be prompted for VLAN name.

5.7.5.72 <MACLIST SHOW> Command

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

```
CO_CM>MACLIST SHOW
```

```
-----
Running MAC Filter Configuration
-----
```

Port	LAN1	LAN2	LAN3	LAN4
Desc	ETH1	ETH2	ETH3	ETH4
Mode	ON/FILTER	ON/INDICATE	ON/BLOCK	OFF/BLOCK
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
Desc	Port description (ifAlias)
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.

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

This command adds MAC address to the White List of the specified [IF] interface. It is allowed to use interface number or interface name, for example LAN1. System accepts ":" or "-" symbols as MAC address separator. It is possible to enter MAC address without separator at all:

```
CO_CM>MACLIST 1 ADD 00-90-F5-3E-7F-AC
```

```
-----  
Running MAC Filter Configuration  
-----
```

Port	LAN1	LAN2	LAN3	LAN4
Desc	ETH1	ETH2	ETH3	ETH4
Mode	ON/FILTER	ON/INDICATE	ON/BLOCK	ON/BLOCK
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	---	---	---	---

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

This command deletes [MAC] address or entry number [N] from the White List of [IF] interface:

```
CO_CM>MACLIST LAN1 DEL 5
```

5.7.5.75 <MACFILTER [IF] [ON/OFF]> Command

The <MACFILTER [IF] [ON/OFF]> command enables/disables MAC Filter option on selected interface.

```
CO_CM>MACFILTER 4 OFF
```

```
-----  
Running MAC Filter Configuration  
-----
```

Port	LAN1	LAN2	LAN3	LAN4
Desc	ETH1	ETH2	ETH3	ETH4
Mode	ON/FILTER	ON/INDICATE	ON/BLOCK	OFF/BLOCK
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	---	---	---	---

5.7.5.76 <MACRULE [IF] [RULE]> Command

This command changes MAC Filter [RULE] for selected interface:

```
CO_CM>MACRULE 4 INDICATE
```

```
-----  
Running MAC Filter Configuration  
-----
```

Port	LAN1	LAN2	LAN3	LAN4
Desc	ETH1	ETH2	ETH3	ETH4
Mode	ON/FILTER	ON/INDICATE	ON/BLOCK	OFF/INDICATE
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, but the SNMP trap will be generated. Extended Traps must be activated.
BLOCK	If unlisted MAC will arrive the Port will be blocked, and the SNMP trap will be generated. Type ETHSD 10H/10F/100H/100F/AUTO X to restore port back.

5.7.5.77 <DOT1X [IF] {OPTION}> Command

The <DOT1X> Command configures IEEE 802.1x access control option on selected LAN interface.

Syntax:

DOT1X [LAN1-9] [ON/OFF] Enables or disables 802.1x option

DOT1X [LAN1-9] [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.

5.7.5.78 <JUMBO SIZE [OFF,1,2] [N]> Command

This command sets the jumbo frame size on selected interface.

The first parameter selects the maximum frame size in bytes (depends on the model):

- OFF - jumbo frames OFF -> 1522 bytes
- 1 - jumbo frame size -> 2048 bytes
- 2 - jumbo frame size -> 10240 bytes

The second parameter [N] is the LAN port number.

Use the same jumbo frame size for all ports within the same PBVLAN.

5.7.5.79 <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).

5.7.5.80 <NETMASK X.X.X.X> Command

The <NETMASK A.B.C.D> command sets the subnet mask of the modem.

5.7.5.81 <GATEWAY X.X.X.X> Command

The <GATEWAY X.X.X.X> sets the default IP address of the router.

5.7.5.82 <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.

5.7.5.83 <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.

5.7.5.84 <ETHSD [10H/10F/100H/100F/AUTO/OFF] [N]> Command

The <ETHSD [10H/10F/100H/100F/1000H/1000F/2500F/AUTO/OFF] [N]> command sets the operating mode of the Ethernet port, where N is the number of the Ethernet port, 10/100/1000/2500 is the rate of 10, 100, 1000 or 2500Mbit/s, F is full duplex, and H is half duplex. The <ETHSD AUTO> command activates the rate and duplex auto detection.

```
CO_CM>ETHSD 10H 1
CO_CM>ETHSD AUTO 2
```

5.7.5.85 <FC [ON/OFF] [N]> Command

This command enables and disables IEEE 802.3x flow control on LAN ports.

5.7.5.86 <IRATE [speed/OFF] [N]> 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.

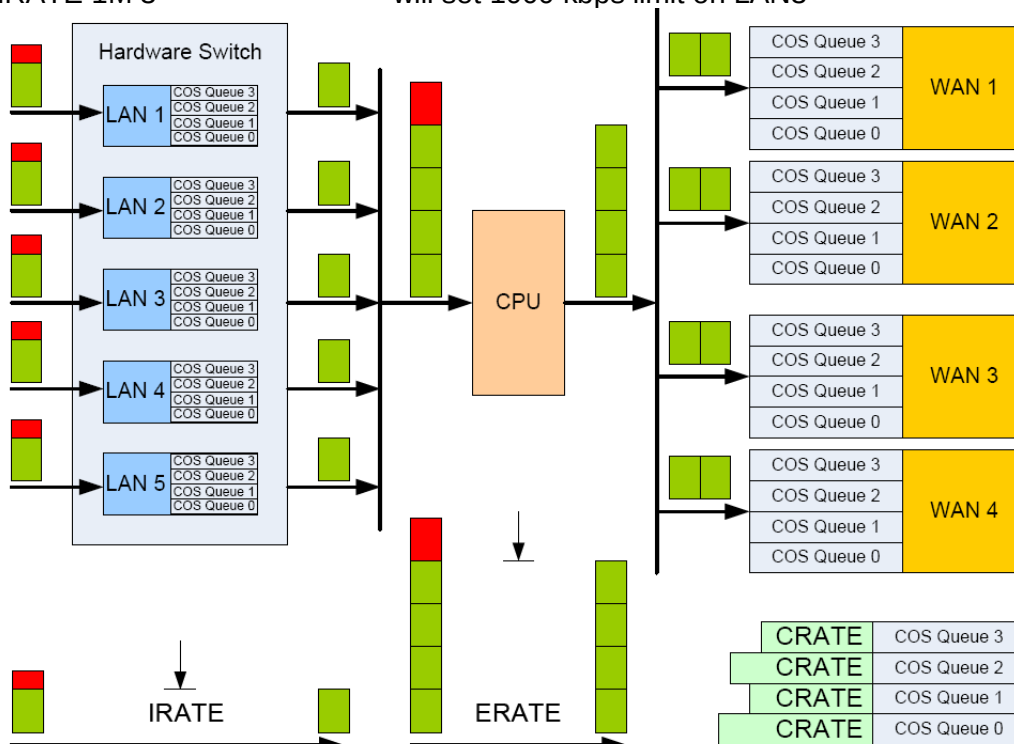
IRATE command counts all arriving traffic without discrimination between ingress VLAN numbers and QoS settings. It means that IRATE command should be used when the LAN port is set to ACCESS mode, so all traffic will be processed by the internal switch with selectable VLAN and QoS settings. If incoming 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



5.7.5.87 <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 must 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

5.7.5.88 <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 FlexDSL Orion3 and MiniFlex 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

5.7.5.89 <COS [QOS/VLAN] [x] [0..3/OFF]> Command

This command sets the VLAN to CoS and QoS to CoS mapping.

Syntax: COS [VLAN/QOS] [V=1..8/Q=0..7] [CoS=0..3/OFF]

- | | |
|-------------------|--|
| First parameter: | <ul style="list-style-type: none">• VLAN - change VLAN-to-CoS mapping• QOS - change QoS-to-CoS mapping |
| Second parameter: | <ul style="list-style-type: none">• V - VLAN number (1..8) according to NETCONFIG table• Q - IEEE 802.1p QoS (0..7) |
| Third parameter: | <ul style="list-style-type: none">• CoS- resulting CoS (0..3)• OFF- turns off VLAN-to-CoS mapping for selected VLAN |

CO_NET>COS VLAN 1 3- all frames in VLAN 1 will have CoS 3

5.7.5.90 <SNMP [V1|V2C|V3] [ON|OFF]> Command

This command activates or deactivates various SNMP versions.

- SNMP V3 ON - enable SNMP v3.
- SNMP V1 OFF - disable SNMP v1.

5.7.5.91 <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.

5.7.5.92 <TRAP [1/2] [IP/OFF]> Command

This command specifies one or two IP addresses to send SNMP traps to.

- TRAPIP 1 192.168.1.1 - set IP 192.168.1.1 as Trap Receiver 1
- TRAPIP 2 192.168.1.2 - set IP 192.168.1.2 as Trap Receiver 2
- TRAPIP 2 OFF - remove 2-nd IP from Trap receivers list

5.7.5.93 <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 - set SNMP version to v1 for 1-st Trap receiver.
- TRAP 2 V2C - set SNMP version to V2c for 2-nd Trap receiver.

5.7.5.94 <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 - assign RO SNMP user as "author" of Trap messages headed to 1-st Trap receiver.
- TRAP 2 V3 RW - assign RW SNMP user as "author" of Trap messages headed to 2-nd Trap receiver.

5.7.5.95 <COMMUNITY> Command

This command allows changing of SNMP community for SET/GET/TRAP messages.

- COMMUNITY [GET/SET/TRAP] - set GET, SET or TRAP community
- COMMUNITY - set all 3 community strings to the same value.

5.7.5.96 <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.

5.7.5.97 <SNMP [RO|RW] NAME> Command

This command set SNMPv3 user name with Read-Only (RO) or Read-Write (RW) access rights.

- SNMP RO NAME - set SNMP user with Read-Only access rights.
- SNMP RW NAME - set SNMP user with Read-Write access rights.

5.7.5.98 <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 RW AUTH MD5 - set MD5 authentication type for SNMP user with Read-Write access rights
- SNMP RO AUTH NONE - disable authentication for SNMP user with Read-Only access rights

5.7.5.99 <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 - set DES encryption type for SNMP user with Read-Only access rights
- SNMP RW PRIV AES - set AES encryption type for SNMP user with Read-Write access rights
- SNMP RO PRIV NONE - disable encryption for SNMP user with Read-Only access rights

5.7.5.100 <SYSNAME [SET]> Command

This command shows/sets sysName variable.

```
CO_CM>SYSNAME SET
Enter SYSNAME (ESC to cancel):
tdm_device_1
CO_CM>SYSNAME
tdm_device_1
```

5.7.5.101 <SYSLOCATION [SET]> Command

This command shows/sets sysLocation variable.

```
CO_CM>SYSLOCATION SET
Enter SYSLOCATION (ESC to cancel):
new_orlean_node_2
CO_CM>SYSLOCATION
new_orlean_node_2
```

5.7.5.102 <SYSCONTACT [SET]> Command

This command shows/sets sysContact variable.

```
CO_CM>SYSCONTACT SET
Enter SYSCONTACT (ESC to cancel):
Trap A. Larm 09645269799
CO_CM>SYSCONTACT
Trap A. Larm 09645269799
```

5.7.5.103 <RMONALARM [N] [ON/OFF]> Command

This command adds/removes RMON group 3 alarms. There may be up to 8 alarms, numbered 1-8. Command allows entering all alarm data interactively.

Command with ON parameter enables alarm and prompts for alarm parameters. Created RMON alarm immediately becomes visible in SNMP RMON alarm table.

Command with OFF parameter disables an alarm.

```
CO_CM>RMONALARM 1 ON
Setup RMON alarm 1
Variable OID [default ]: 1.3.6.1.2.1.2.2.1.14.1
Sample type (1 - Absolute, 2 - Delta) [1..2, default 2]: 1
Sample interval, sec [1..65535, default 65535]: 10
Rising threshold [-2147483648..2147483647, default -1]: 50
Falling threshold [-2147483648..49, default -1]: 10
Rising event(0 - No event) [0..8, default 15]: 1
Falling event(0 - No event) [0..8, default 15]: 1
Startup alarms (1 - Rising, 2 - Falling, 3 - Both) [1..3, default 3]: 1
RMON Alarm 1 is enabled
```

Refer to RMON specification for the meaning of all parameters.

When prompted for any parameter, press <Enter> to select default value indicated in square brackets. Most of the time, default values are those entered in previous uses of a command. OID should be entered in decimal form and should be full OID. Only OIDs of integer values, counters, gauges should be used according to the RMON specification. It is checked that OID really points to a variable in device's MIB database.

Any single SNMP variable should be ended with '.0'.

For example: OID of 'ifNumber' according to MIB is '1.3.6.1.2.1.2.1'.

Its real OID is 'ifNumber.0' - '1.3.6.1.2.1.2.1.0'.

OID pointing to the member of MIB variable array should end with an index.

For example: OID of 'ifInOctets' is '1.3.6.1.2.1.2.2.1.10'. LAN2 interface index is 2.

Then OID of ifInOctets for LAN2 would be 'ifInOctets.2' or '1.3.6.1.2.1.2.2.1.10.2'.

Event numbers refer to RMON group 9 events, which are created/disabled with 'RMONEVENT' command and visible in the SNMP RMON event table.

5.7.5.104 <RMONEVENT [N] [ON/OFF]> Command

This command adds/removes RMON group 9 events. There may be up to 8 events, numbered 1-8. Command allows entering all event parameters interactively.

Command with ON parameter enables event and prompts for its parameters. Created RMON event immediately becomes visible in SNMP RMON event table.

Command with OFF parameter disables an event.

```
CO_CM>RMONEVENT 1 ON
Setup RMON event 1
Action (1 - none, 2 - log, 3 - trap, 4 - log and trap) [1..4, default 4]: 3
RMON Event 1 is enabled
```

Refer to RMON specification to understand RMON alarms and events.

When prompted, press <Enter> to select default value indicated in square brackets. Most of the time, default values are those entered in previous uses of a command.

Currently, only trap action is supported. Logging is not supported.

5.7.5.105 <LLDP [ON/OFF]> Command

This command enables or disables LLDP messages exchange with all peers through all interfaces. It is global setting.

```
CO_CM>LLDP ON
-----
LLDP                                     : Enabled
-----
Retransmission Interval                 : 30
Transmission Multiplier                  : 4
Reinitialize Delay                       : 2
Transmission Delay                       : 2
Notification Interval                   : 5
MED Fast Start Counter                   : 3
LLDPDU Transmission                      : Enabled
LLDPDU Reception                        : Enabled
LLDP INT VLAN                           : Disabled
-----
CO_CM>
```

5.7.5.106 <LLDP DEFAULT> Command

This 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
LLDPDU Transmission	Enabled
LLDPDU Reception	Enabled
LLDP internal VLAN	Enabled

5.7.5.107 <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:

$$1 \leq Transmission_Delay \leq (0.25 * Retransmission_Interval)$$

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 Behavior used to advertise only few capabilities of the device designed for as fast as possible call processing after device start-up.

5.7.5.108 <LLDP [RX/TX] [ON/OFF]> Command

This command enables or disables LLDP messages transmission and reception.

5.7.5.109 <LLDP INT VLAN [ON/OFF]> Command

This 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 device and the device will "see" the service-provider switch. Despite the fact that such behavior 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 behavior. 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.

5.7.5.110 <LLDP CONFIG> Command

This command shows actual LLDP configuration.

```
CO_CM>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
-----
CO_CM>
```

5.7.5.111 <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 the 1st or the 2nd IP address in x.x.x.x format
- SNTP [1/2] OFF - remove the 1st or the 2nd IP address

5.7.5.112 <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 +1:00- set CET (Central European time)
- SNTP TZ -8:00 - set PST (Pacific Standard time)

5.7.5.113 <DST [WINTER/SUMMER]> Command

This 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 - a 3-letter 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:

```
FC_NET>DST SUMMER
Month [MAR] : MAY
Day [lastSUN] : FIRSTMON
Time to advance the clock [01:00] : 02:00
Offset (relative to Standard zone time) [60 min] : 1:00
```

5.7.5.114 <DST [OFF/INFO/NAME]> Command

This command configures Daylight Saving Time (DST) adjustable rules.

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 Zealand
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	
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 APR firstSUN (6) 02:00s +0min	State Victoria
EU	MAR lastSUN (30) 01:00u +60min OCT lastSUN (26) 01:00u +0min	European Union

Name	Rules	Description
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

5.7.5.115 <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.

It is possible to add up to 2 Syslog servers. The SYSLOG command is used for that purpose.

- SYSLOG [1/2] x.x.x.x - set the 1st or the 2nd address in x.x.x.x format
- SYSLOG [1/2] OFF - remove the 1st or the 2nd IP address

5.7.5.116 <[SSH|TELNET|HTTP] [ON/OFF]>

These commands allow enabling or disabling of defined service.

Note: Factory Default running management servers are TELNET and HTTP

5.7.5.117 <SSH PORT [N]>

This command changes port, the SSH server listens for incoming connections.

```
CO_CM>SSH PORT 2022
-----
New Network Configuration

<----- cut ----->

Services          : SSH(2022), HTTP
Syslog servers    : 192.168.0.121      192.168.0.122
SNTP servers      : 192.168.0.121      192.168.0.122      TZ: UTC+00:00
```

5.7.5.118 <SSL [SHOW/DEL] [options]>

Command displays or deletes certificate or private key from the memory.

```
CP_01_NET>SSL SHOW KEY
<-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEA20jIDlMugcsjFsduYdP6MvMisF+liukPsTPCDKy3W+k4DbEu
uYb539oNQIV9QYks4KDX1BKK5cW2rHSd0Vz2V0xuljHx7MLmjJdvCshxMKcVDIk8
JTKY37sAYtiz85JfA7Qew4nNuDabyAzDTLZYzwdBakRippudCxN7KtxxejgWgLFJ
mguzIk32XB5rsVJA3V0lBmlWJZr/dmJeRB+Hp0ovhsE2rZVXdwEQb6VqbKWVYPJK
tBj0DZdcPIintrattT3u9IhHbPvAo8Aru7unaOrNf65D1AKTsGWCad3g3vA17GY/u
Q47lZJRghbNUHcNvWwvKrkRCfNS5xZLZg4XXwIDAQABAoIBAQCpfIGUANrrWvTO
AGrilhLGG0JvTB4JVCxZMqYDYeN+2K2Id7AjmZ28VS709bgwVSAQGoF22solBjIA
7UmlrnKAWuW37PaObR5ooZPka7To49szC0c/gPIDyuerfs7nrfReSnOUswgcH6kc
YDD7M9lEduzzyvaR6HcCt9Oq34BadXRl79AbH+dAVHgVHjHoz252GhF8HqmnJEVYD
DK9sUOT+lsBmXdolTzZxOF6Jgfa4CH6xY63ZyRNAP3encxXbnw0WnVmfGpDvtEv+
M0eFf05s28mRCLTZ9sPORK21Z4HSAyQ4U9SDUGI9Sii0arIjWxzzjzYy7yTyw8bws
iomMVQcBAoGBAP2fiqScfmlnKiN7YNMdoPBRzfyyFMTIsZVw9RxjDTIBNjrFfqEu
n2qzzOmF06tl1QuIxKogBfJB6HuSI+TZHCB9H5tj2FAficanZFnULYax8vE9Anbur
G3oSFpraimXdB0YcOh15QpUC/8ihoGEjUHh15m23MYEUSLq8RV/af4EfAoGBAN1W
29Audp8BpXRC0+zmmGVOTnhP6oJyS0enExqDryPkBq/zB5JlLfa0liFTgjp5PJyO
up04gQ1hV6h/SHjc7L6SSeFUS1I5CjubldQEHEf8tMKIntjGWkoX8c3gizlC9gxZq
jLTtaHtSR6cBqZzw5SsnbHnsn08UT6D1qm3e32HBAoGADI/of39VnyV4M/fo2KZl
pEvPK/2CL+fSFzV0WhovS2+dZHqnXWQMVRdpqTrGmoziJV8LM0kBhktf/7gm/E
YouRHD3XrQE7vhrn/LAGtJfFqOFCcYcGyHNOlGb5E6hjicZ2ccOgt9ktGboA0K47
CCEbHLQMr3Fm7yAXPZJ/50CgYACAZGid4NXoT0wqpJlKUnkUstg58iGWibYhWkk
6mCiAKUW3ysIZst92vG955XclDc40opadnKk/mbe/hhYEBiNoAiIyp/J0v6Gv8hB
3a+v6mbwi2oZVPYLBni/FAGutakEgP65fRVfSbCgkOFkrNwCsf8zad6fxt1Z5iAf
Us/PgQKBgCY0kaOq4TJK6BJBwXoTIBwaq8DNK+ClxMtABHrGohD3d4hrNWEQ2ARM
```

```
k77rHJ8kYlTR+apbJTWhRsaoovXEsjEQ/2ZHBbi5NsWX/KlpG8tOMFn13wnI9RA
adw0Lmu4tOLTEhHbczXd7Lf50LXDv5PuAFkvNppMlEn0sCOPJZVf
-----END RSA PRIVATE KEY-----
>
1676 bytes
```

Usage: SSL [SHOW/DEL] [CERT/KEY/CA]

Parameter	Description
SHOW/DEL	To display or to delete the item
CERT	SSL Certificate
KEY	SSL Private Key
CA	SSL Certification Authority Certificate (Intermediate CA)

5.7.5.119 <RADIUS [1/2] SECRET>

This command defines common sharing secret for RADIUS server and client.

```
CO_CM>RADIUS 1 SECRET
Enter shared secret:
Repeat shared secret:
-----
Running Network Configuration

<----- cut ----->

Radius servers : 192.168.0.121:1812
Radius secret  : entered          empty
-----
CO_CM>
```

The <RADIUS [1/2] SECRET OFF> command clears sharing secret.

5.7.5.120 <RADIUS [1/2] TEST>

This command test connection with defined RADIUS server and returns access rights or Non-authorized for selected user.

```
CO_CM>RADIUS 1 TEST
Radius #1 Address is 192.168.1.254:1812
User name :ORION3ADMIN
Password  :
Request Accepted
Rights are : ALL
Allowed net : 192.168.0.0
Netmask is : 255.255.0.0
```

5.7.5.121 <RADIUS [1/2] [IP:P/OFF]>

This command adds or removes the IP address of primary or secondary RADIUS server. It is possible to specify a port the client will try to connect to. If port is not defined, the default UDP port 1812 will be used.

```
CO_CM>RADIUS 1 192.168.1.254
-----
New Network Configuration

<----- cut ----->

Radius servers : 192.168.1.254:1812
Radius secret  : empty          empty
-----
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'.
Do not forget to 'CONFIRM' a good working configuration.
CO_CM>
```

The <RADIUS [1/2] OFF> command clears server IP address.

5.7.5.122 <RADIUS RETRIES [0..10]>

This command defines the number of retries, the RADIUS client will try to authenticate at first and second RADIUS server. If the first RADIUS server fails 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_CM>RADIUS RETRIES 2
```

Status	:	Server 1	Server 2
Status	:	Not connected	Not connected
Server IP	:	192.168.1.254	0.0.0.0
Server port	:	1812	0
Server key	:	entered	entered
Retries	:	2	
Timeout, seconds	:	5	

5.7.5.123 <RADIUS TIMEOUT [1..5]>

This command defines the timeout in seconds. If RADIUS server gives no answer within defined period, the RADIUS client initialises next attempt. Default parameter is 2 seconds.

```
CO_CM>RADIUS TIMEOUT 2
```

Status	:	Server 1	Server 2
Status	:	Not connected	Not connected
Server IP	:	192.168.1.254	0.0.0.0
Server port	:	1812	0
Server key	:	entered	entered
Retries	:	2	
Timeout, seconds	:	2	

5.7.5.124 <POECONFIG> Command

This command displays the PoE configuration of the unit.

5.7.5.125 <POEPORT [ON/OFF] [N]> Command

This command switches PoE port ON or OFF on the PoE unit.

Syntax: POEPORT [ON/OFF] [N=1..2], where N is the number of the PoE port.

5.7.5.126 <NETDEFAULT> Command

This command sets default network configurations. Remember, that default network configuration does not set/change IP, netmask and default gateway of the device, as well as servers' IP addresses and RADIUS-settings (highlighted). NETDEFAULT does not affect Security Mode (advanced/basic).

```
CP_NET>NETDEFAULT
```

```
CP_NET>NETCONFIG
```

```
Running Network Configuration
```

Ethernet settings	:	LAN1	LAN2	WAN1	WAN2	WAN3	WAN4	INT
Description	:	LAN1	LAN2	WAN1	WAN2	WAN3	WAN4	INT
Destination	:			DSL1				
Access/Trunk	:	ACC	ACC	Trunk	Trunk	Trunk	Trunk	ACC
Port-based VLAN	:	[A]	[A]	[A]	[A]	[A]	[A]	[A]
VLAN	:	1	1					1
QoS	:	2	2					2
1: VLAN1 VID=1	:			+	+	+	+	
2: VLAN2 VID=2	:			+	+	+	+	
3: VLAN3 VID=3	:			+	+	+	+	
4: VLAN4 VID=4	:			+	+	+	+	
5: VLAN5 VID=5	:			+	+	+	+	
6: VLAN6 VID=6	:			+	+	+	+	
7: VLAN7 VID=7	:			+	+	+	+	
8: VLAN8 VID=8	:			+	+	+	+	

```

OTHER VLANS      :      +      +      +      +
Speed            : AUTO   AUTO
Flow control     : OFF   OFF
System settings
IP address       : 192.168.0.235   MAC address      : 00:0f:d9:15:18:94
Subnet mask      : 255.255.255.0   Management MTU : 1500
Default gateway  : 192.168.0.254
SNMP
SNMP versions    : v1
Allowed pollers  : 192.168.0.121   192.168.0.122
Trap IP/version  :
SNMP v1,v2c community
GET/SET/TRAP     : public/public/public
SET command      : Blocked
Services         : TELNET, SSH(22), HTTP
Syslog servers   : 192.168.0.121   192.168.0.122
SNTP servers     : 192.168.0.121   192.168.0.122           TZ: UTC+00:00
Summer time      : Disabled
Winter time      : Disabled
Radius servers   : 192.168.0.121:1812  192.168.0.122:1812
Radius secret    : entered           empty
-----
CO_CM>

```

5.7.5.127 <FACTORY DEFAULT> Command

This command resets whole configuration to factory default parameters, including IP, netmask and default gateway of the device.

```

CO_CM>FACTORY DEFAULT
Do You really want to setup the Unit to its factory defaults? (Y/N)
Y
The unit will restart

Console is going to be closed now
...

```

6 SOFTWARE DOWNLOAD MINIFLEX SWITCH (MF-MR2N-SW-12ETH,V2 ONLY)

6.1 Using FTP / SFTP servers

Starting from the firmware 2.5 the firmware update and configuration up/download can be executed from CLI commands or by SNMP requests. Fileserver must support FTP or SFTP protocols.



Configuration must be saved after update by `save configuration` command or by SNMP SET NATEKS-MIB|tftpSoftConfirm request.
New firmware will be applied only after system reboot

6.1.1 Command line interface

These commands can be used to download firmware, bootloader or configuration from CLI:

#	Command	Description
1	<code>download [ftp sftp] [bootrom config os] <A.B.C.D> <port> <user> <pass> <filename></code>	The command Download has the following parameters: Protocol: FTP or SFTP Type: config, bootloader or OS image A.B.C.D is an IP address of a server Port: as a port number the server listens to. Default port is 21 for FTP and 22 for SFTP

6.1.2 SNMP

Download and upload parameters are combined into standard maintenance table from Nateks.mib.

tftpInfo (SWU)	
ServerIP	0.0.0.0
SoftFileName	FLEXDSLOS.z
ConfFileName	config.txt
ConnectionTimeout	8
NumRetries	3
TransCmd	noOp
LastOp	noOp
TransferStatus	noOp
LastOpTime	0 days 00:00:00.00
SoftConfirm	readValue
ProtocolVersion	ftp
ServerUserName	
ServerUserPass	
ServerPortNumber	22

The table has the following fields:

#	Field	OID and Description
1	ServerIP	NATEKS-MIB tftpServerIP IP address of FTP/SFTP server
2	SoftFileName	NATEKS-MIB tftpSoftFileName Filename for Software download
3	ConfigFileName	NATEKS-MIB tftpConfFileName Filename for configuration upload and download
4	ConnectionTimeout	NATEKS-MIB tftpConnectionTimeout Server reply timeout in seconds
5	NumRetries	NATEKS-MIB tftpNumRetries Number of attempts to connect server
6	TransCmd	NATEKS-MIB tftpTransCmd Changing this parameter allows the following actions: swDownload(3): download firmware from the server configDownload(4): download config from the server configUpLoad(5): saves config to the server
7	LastOp	NATEKS-MIB tftpLastOp Shows last operation
8	TransferStatus	NATEKS-MIB tftpTransferStatus Shows actual status of file transfer
9	SoftConfirm	NATEKS-MIB tftpSoftConfirm This parameter saves running configuration into startup configuration
10	ProtocolVersion	NATEKS-MIB tftpProtocolVersion FTP or SFTP protocol selection
11	ServerUserName	NATEKS-MIB tftpServerUserName Username to access server
12	ServerUserPass	NATEKS-MIB tftpServerUserPass Password to access server
13	ServerPortNumber	NATEKS-MIB tftpServerPortNumber IP port number the server is running on Standard port numbers are 21 for FTP and 22 for SFTP

7 SOFTWARE DOWNLOAD LINE CARDS, DINRAIL, MF-MR2N-SW-8ETH,V2 AND FLATRACK SWITCHES

The line card & DINrail supports downloading new/old software versions to get some additional features or to protect the device with a released only software version. The download of the software can be performed in following ways:

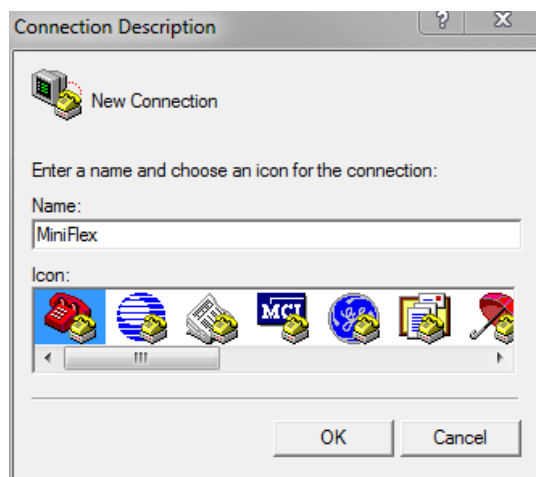
- via the USB port (LCT) by using the X-modem protocol
- via Ethernet (the X-modem protocol)

The Programming of **FXS/FXO/VF** line cards and DINrail units is not under the scope of this User Manual. Please refer to **“UM_FlexDSL_MiniFlex_VoIP_v1-x” User Manual**.

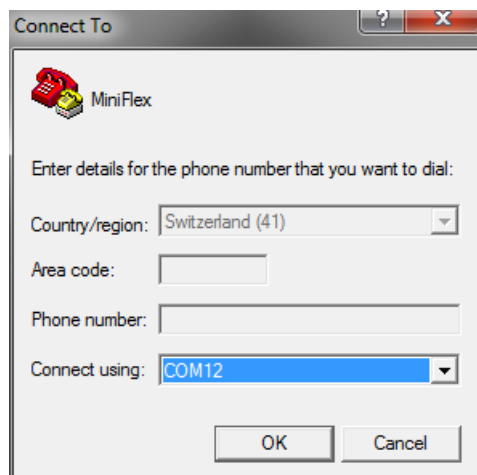
7.1 Software Download via USB Port (LCT) Using Xmodem Protocol

To download the software on any SHDSL line card & DINrail, do the following steps:

1. Power on the device.
2. Connect the USB connector of the device (LCT) with the USB cable 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”.

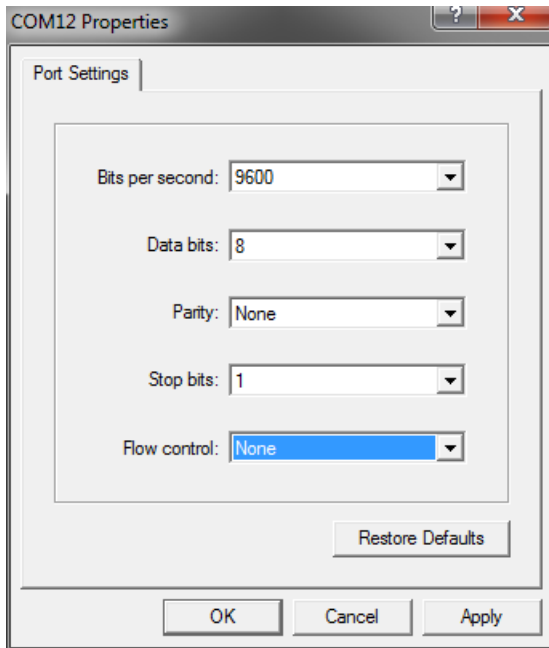


5. Then the “Connect To” window is displayed. Select the COM port connected to the SHDSL line card in the “Connect Using” drop-down menu.
To use the USB interface as local craft terminal, you need to download and install the following driver http://www.flexdsl.ch/extranetfiles/Software/Orion3_USB_Driver.zip. This is an USB to serial driver and allow to have a COM port over USB.
Click “Ok”.

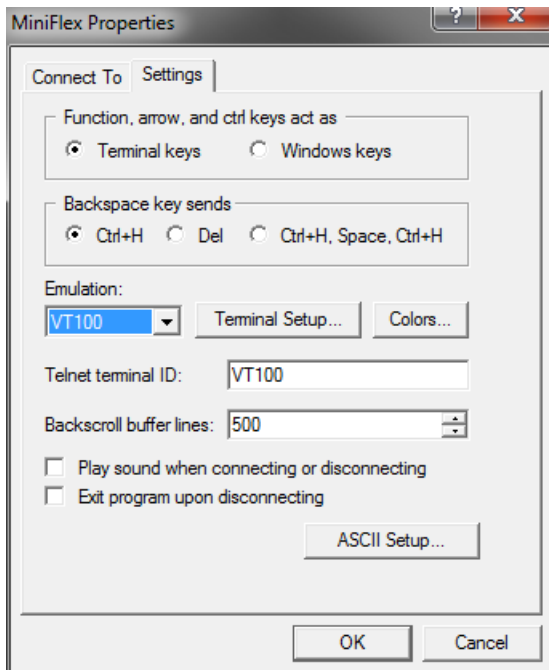


Configure the parameters of the COM port (COM properties). Click “Ok”.

Bits per second: 9600, Data bits: 8, Parity: None, Stop bits: 1, Flow control: None

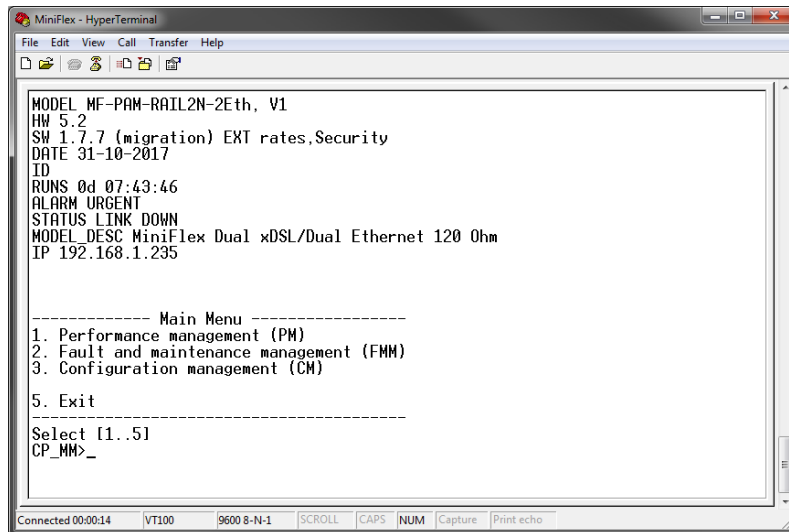


6. Select Properties in the “File” menu of the HyperTerminal program.
7. Select the “Setting” tab. Select the VT100 emulation in the “Emulation” menu. Click “Ok”.

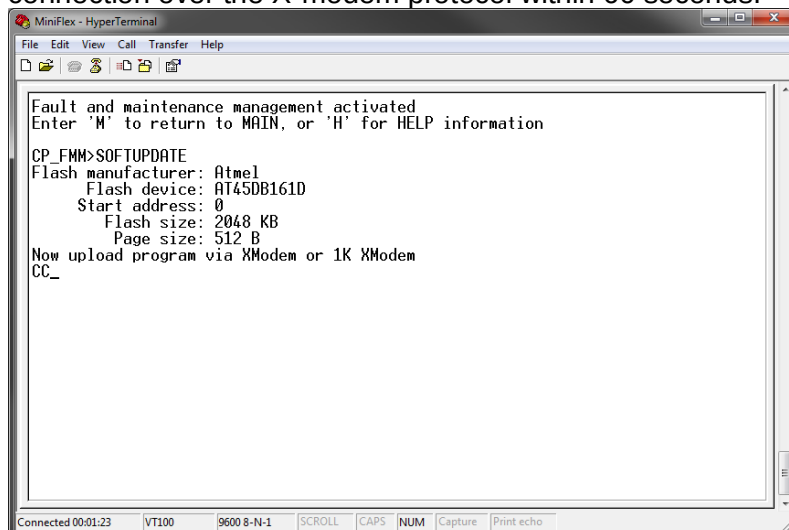


8. Select Call in the “Call” menu. (If the menu is not available, the connection is established automatically. Go to item 9.)

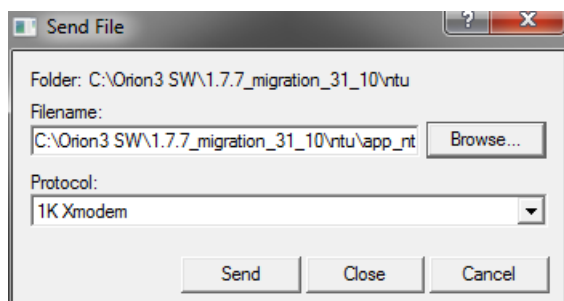
9. Press <Enter>. The main menu of the device will be displayed.



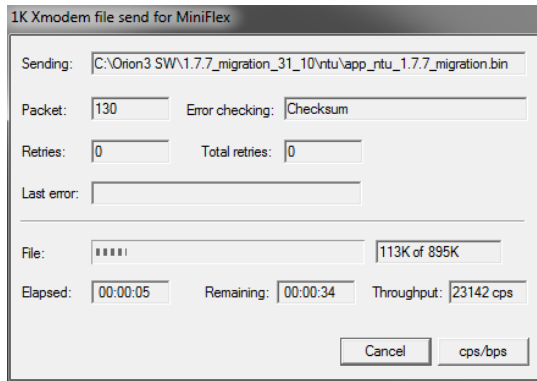
10. Go to the "Fault and maintenance management" menu, means to enter number 2. Enter the <SOFTUPDATE> command. After typing SOFTUPDATE, the device tries to establish connection over the X-modem protocol within 60 seconds.



11. The time counter is started. Select Send File in the "Transfer" menu.

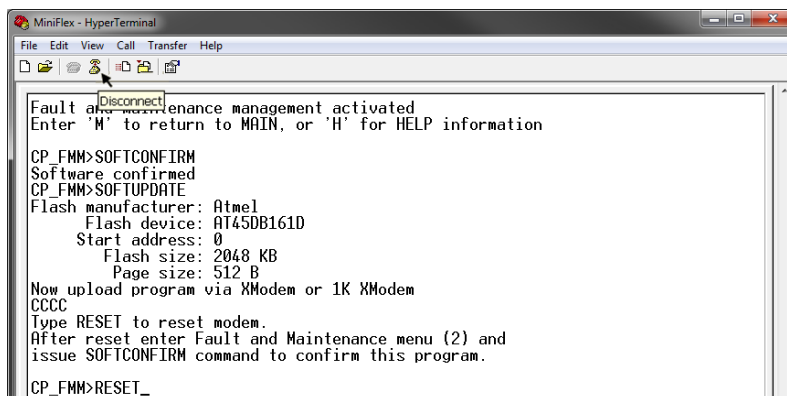


12. Select 1K-Xmodem in the "Protocol" drop-down menu of the "Send File" window. Browse the app.bin file in the "Filename" field (the name of the file depends on the software version). Click "Send". The Hyper Terminal starts downloading the file. After the download is fully completed, the device stores the downloaded file into the memory. After the Send button is clicked, the "1K-Xmodem file send for..." window pops up.

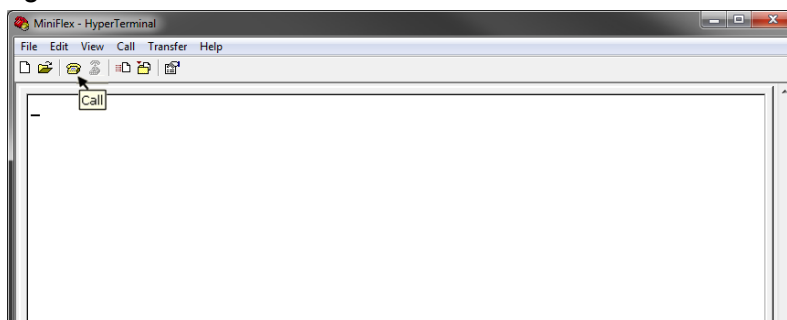


The window displays the software downloading statistics (the name of the file, the number of transmitted packets, the error checking method, the last error, the downloading progress, time, etc.). To cancel downloading, click Cancel.

13. If the software is downloaded, the “1K Xmodem file send for...” window closes automatically.
14. After the software is downloaded completely, enter the <RESET> command in the “Fault and maintenance management” menu. For some computers it is better to disconnect (with the “Disconnect Icon”) the USB interface after the <RESET> command was used, because sometimes the driver does not start correctly after this procedure. The disconnect should be done within 10 seconds after the <RESET> command.



After again around 10 seconds (when the modem started again) connect the USB interface again with the “Connect Icon”.



After this, enter the main menu again. Enter the “Fault and maintenance management” menu and input the <SOFTCONFIRM> command.

15. The software downloading is now completed.

7.2 Software Download via Ethernet (1K-Xmodem and Telnet)

This method of the software downloading is similar to the “Software Download via the USB Port (LCT) Using Xmodem Protocol” described in chapter 7.1. 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.

8 SERVICE INSTRUCTIONS

8.1 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 (18 ... 72 V), please use it with the grounded “+”.
- Before applying primary AC or DC power make sure that equipment properly 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.

8.2 Evaluation of the SHDSL 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 to 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.

9 APPENDICES

9.1 Quick Installation Guide for FlexDSL MiniFlex

9.1.1 Enter a FlexDSL MiniFlex

To enter in a MiniFlex subrack unit, use the Local Craft Terminal (USB) interface with Hyper Terminal (or any equal program) or go with Telnet through the Ethernet interface.

Local Craft Terminal (USB) Interface (this must be done on Switch and every SHDSL line card):

- Configure the COM port: Bits per second:9600, Data bits: 8, Parity: None, Stop bits: 1, Flow control: None.
- 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 the Switch in a MiniFlex. All SHDSL line cards have next Ethernet Addresses: Slot1-IP_192.168.0.236 until Slot10-IP_192.168.0.245

After a successful entering the main menu of each device will be displayed. If you enter on Switch, the Switch menu will be displayed, if you enter a SHDSL line card, the line card menu will be displayed.

9.1.2 Configure a FlexDSL MiniFlex

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 two MiniFlex devices over 2 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 pair should continue to work.

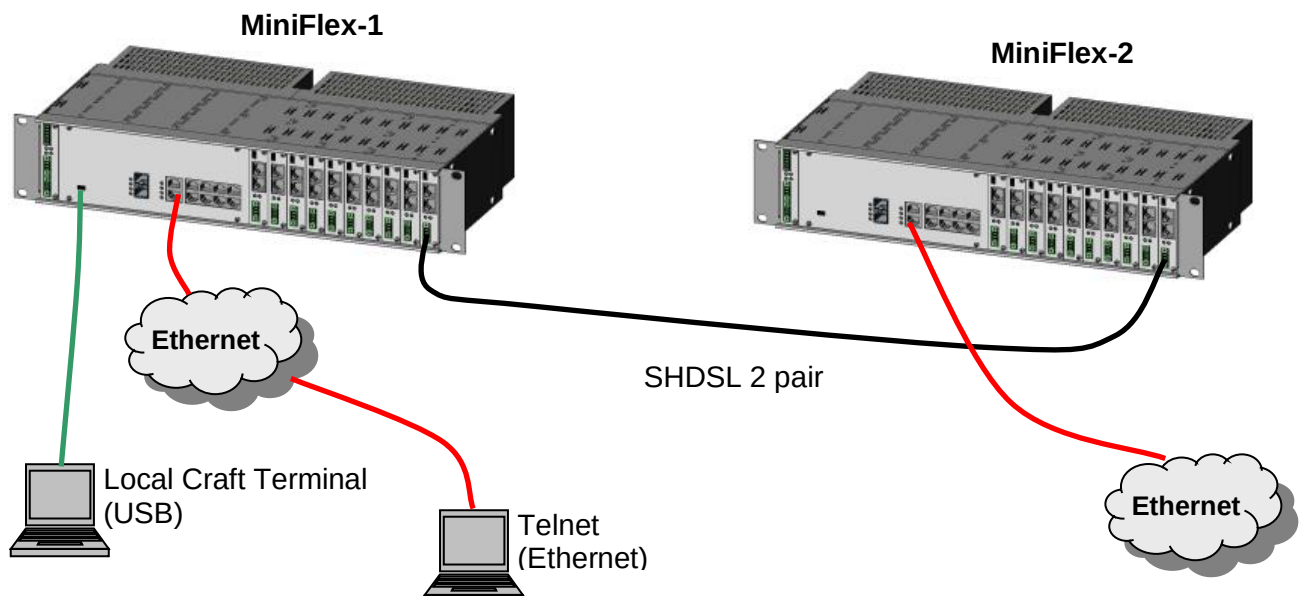


Figure 9.1 Application Example to connect two MiniFlex

MiniFlex-1, Slot10, SHDSL line card: Enter the line card with the LCT (USB) or Telnet interface (IP Address 192.168.0.245).

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
<PAYLOAD WAN 1> <↵>	Configure Ethernet over SHDSL 1
<PAYLOAD WAN 2> <↵>	Configure Ethernet over SHDSL 2
<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_CM>CONFIG

Running Line Configuration

```
-----
xDSL          DSL1          DSL2
Description   : DSL1        DSL2
Mode          : Master (HTU-C) Master (HTU-C)
Extended rates: OFF         OFF
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
-----
```

CO_CM>

MiniFlex-1, Switch card:

Default IP address of MiniFlex Switch is 192.168.0.235; all ports of it are combined in default VLAN. We need to change IP address to prevent address duplication. In MiniFlex switch menu type following commands:

Type following commands	Description
<EN><↵>	Go to privileged mode (login and password are admin)
<IP 10.0.1.1/8 GATEWAY 10.0.0.101><↵>	Enter IP address, Network Mask and default gateway
<SAVE CONFIGURATION><↵>	Save configuration

MiniFlex-2, Slot10, SHDSL line card: Enter the line card with the LCT (USB) or Telnet interface (IP Address 192.168.0.245).

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
<PAYLOAD WAN 1> <↵>	Configure Ethernet over SHDSL 1
<PAYLOAD WAN 2> <↵>	Configure Ethernet over SHDSL 2
<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_CM>CONFIG

Running Line Configuration

```

xDSL          DSL1          DSL2
Description   : DSL1          DSL2
Mode          : Slave (HTU-R) Slave (HTU-R)
Extended rates: OFF          OFF
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
  
```

CP_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.)
  
```

MiniFlex-2, Switch card:

Default IP address of MiniFlex Switch is 192.168.0.235; all ports of it are combined in default VLAN. We need to change IP address to prevent address duplication. In MiniFlex switch menu type following commands:

Type following commands	Description
<EN><↵>	Go to privileged mode (login and password are admin)
<IP 10.0.1.2/8 GATEWAY 10.0.0.101><↵>	Enter IP address, Network Mask and default gateway
<SAVE CONFIGURATION><↵>	Save configuration

9.1.3 Checking of Correct Working

On every SHDSL line card you have to check the noise margin of the DSL line! 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 every line card.

Type following commands	Description
2 <↵>	Go to Fault and maintenance management (FMM)
<STATUS> <↵>	Displays the actual system status

CO_FMM>STATUS

Status	:	DSL1	DSL2	
I/F mode	:	CO	CO	
SYNC	:	1	1	
SEGD	:	1	1	
Power backoff	:	0.0	0.0	dbm
Far end power backoff	:	0.0	0.0	dbm
Loop attenuation	:	14.0	14.0	dB
NMR	:	7.0	7.0	dB
Bitrate	:	5704	5704	kbit/s
SRU #	:	0	0	
Active sync. source	:	Internal	Internal	
Temperature	:	39.750 C		

CO_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.

9.1.4 Problem with FlexDSL MiniFlex

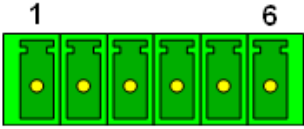
In case you have any trouble with the FlexDSL MiniFlex device, please send following details to your FlexDSL contact:

- Application Description
- Main Menu Picture of every device (Switch and SHDSL line cards)
- Configuration, status and alarms of every device (Please perform with the <DUMP> and <MODEMVIEW> command)

9.2 Connector Description

9.2.1 Alarm Connector (ALARM)

Type – Phoenix Mini Combicom MC 1,5/6-G-3,5 (female), 6 pins.

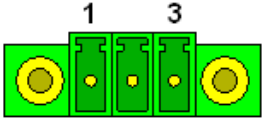
	Pin No.	Description
	1	Non Urgent Alarm, Common Contact
	2	Non Urgent Alarm, Normally Closed
	3	Non Urgent Alarm, Normally Open
	4	Urgent Alarm, Common Contact
	5	Urgent Alarm, Normally Closed
	6	Urgent Alarm, Normally Open

Matching Type for the cable: MC1,5/6-ST-3,5
For AWG 16-28
Area 0.08–1.5 mm² or Diameter 0.32-1.4 mm



9.2.2 DC Power Connector (DC1, DC2)

Type – Phoenix Mini Combicom MC 1,5/3-GF-3,5 (female), 3 pins.

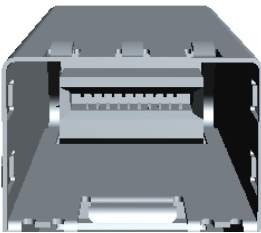
	Pin No.	Description
	1	-PWR (Negative power supply terminal)
	2	FPE, GND (Functional Protective Earth / GND)
	3	+PWR (Positive power supply terminal)

Matching Type for the cable: MC1,5/3-STF-3,5
For AWG 16-28
Area 0.08–1.5 mm² or Diameter 0.32-1.4 mm



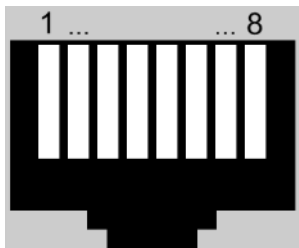
9.2.3 Ethernet SFP Connector

Type – SFP: Tyco 1658391-1 or Amphenol UE75A203000T.

	Pin No	Signal	IO	Description
	1,17,20	TGND		transmit ground
	2	Tx_Fault	O	Transmit fault indication
	3	Tx_Disable	I	transmit disable
	4	SDA	B	SDA line (I2C)
	5	SCL	I	SCL line (I2C)
	6	Mod_ABS	O	Module absent
	7	RS0	I	rate select 0
	8	Rx_LOS	O	Loss of signal indication
	9	RS1	i	rate select 1
	10,11,14	RGND		receive ground
	12	RD-	O	receive data -
	13	RD+	O	receive data +
	15	RX_VCC		receive VCC
	16	TX_VCC		transmit VCC
	18	TD+	I	transmit data +
	19	TD-	I	transmit data -

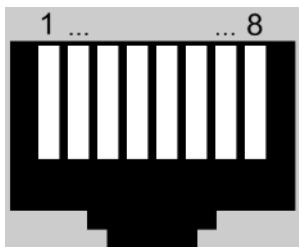
9.2.4 Gigabit Ethernet Connector

Type – RJ-45 (female), 8 pins.

	Pin No.	Description
	1	Bi-directional pair A+
	2	Bi-directional pair A-
	3	Bi-directional pair B+
	4	Bi-directional pair C+
	5	Bi-directional pair C-
	6	Bi-directional pair B-
	7	Bi-directional pair D+
	8	Bi-directional pair D-

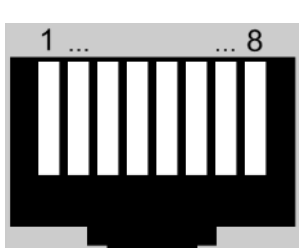
9.2.5 10/100Mbps Ethernet Connector

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)

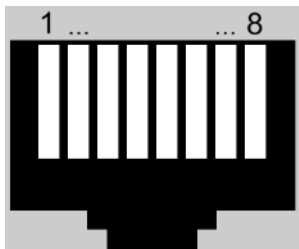
9.2.6 POE Line Card Ethernet Connector

Type – RJ-45 (female), 8 pins.

	Pin No.	Description	PoE, MDI Mode A	PoE, MDI Mode B
	1	Tx+ (transmit data), PoE	+	
	2	Tx- (transmit data), PoE	+	
	3	Rx+ (receive data), PoE	-	
	4	NC (not used), PoE		+
	5	NC (not used), PoE		+
	6	Rx- (receive data), PoE	-	
	7	NC (not used), PoE		-
	8	NC (not used), PoE		-

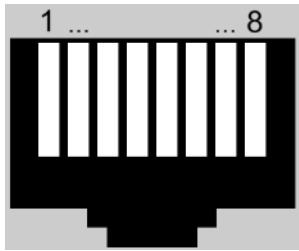
9.2.7 Serial Line Card & DINrail RS-232 & RS-232/422/485 Connector

Type – RJ-45 (female), 8 pins.

	Pin No.	Description RS-232	In-, Output
	1	TxD (transmit data)	Output
	2	RTS (request to send)	Output
	3	RxD (receive data)	Input
	4	GND (Ground)	
	5	GND (Ground)	
	6	CTS (clear to send)	Input
	7	CC (cable connected)	
	8	GND (Ground)	

To detect the cable as connected, connect the CC to GND.

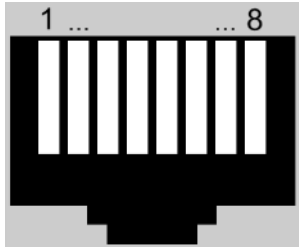
Type – RJ-45 (female), 8 pins.

	Pin No.	Description RS-422/485	In-, Output
	1	Tx+ (transmit data)	Output
	2	Tx- (transmit data)	Output
	3	Rx+ (receive data)	Input
	4	GND (Ground)	
	5	GND (Ground)	
	6	Rx- (receive data)	Input
	7	CC (cable connected)	
	8	GND (Ground)	

To detect the cable as connected, connect the CC to GND.

9.2.8 E1 Line Card & DINrail E1 120 Ohm Connector

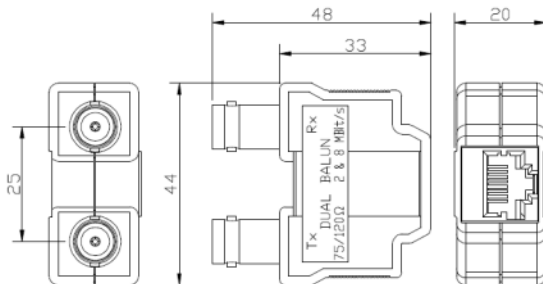
Type – RJ-45 (female), 8 pins.

	Pin No.	Description
	1	E1 Input → Wire A
	2	E1 Input → 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)

9.2.9 E1 75 Ohm Connector

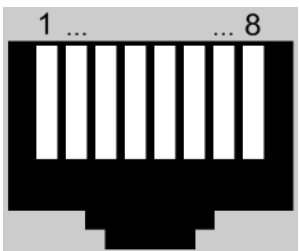
Type - BNC 75 Ω

Please order FG-ADAPT-E1B/E1U to convert RJ-45 connector to BNC.



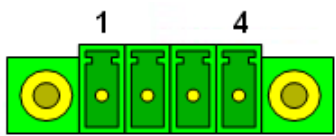
9.2.10 VoIP Line Card & DINrail FXO/FXS/VF Connector

Type – RJ-45 (female), 8 pins.

	Pin No.	Description (FXO/FXS)	Description (VF)
	1	NC (not used)	NC (not used)
	2	NC (not used)	M (E&M Mouth/Magnet)
	3	NC (not used)	R (Analog Input Ring)
	4	RING	RING (Analog Output Ring)
	5	TIP	TIP (Analog Output Tip)
	6	NC (not used)	T (Analog Input Tip)
	7	NC (not used)	E (E&M Ear/Earth)
	8	NC (not used)	SG (E&M Signal Ground)

9.2.11 SHDSL Line Card & DINrail xDSL Connector

Type – Phoenix Mini Combicom MC 1,5/4-GF-3,5 (female), 4 pins.

	Pin No.	Description
	1	SHDSL interface A
	2	SHDSL interface A
	3	SHDSL interface B
	4	SHDSL interface B

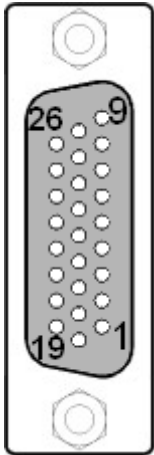
Matching Type for the cable: MC1,5/4-STF-3,5
For AWG 16-28, Screw
Area 0.08–1.5 mm² or Diameter 0.32-1.4 mm

Or: FK-MCP 1,5/ 4-STF-3,5
For AWG 16-26, Push-in
Area 0.14–1.5 mm² or Diameter 0.4-1.4 mm



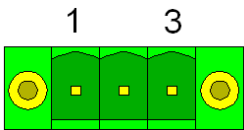
9.2.12 Input / Output Line Card & DINrail Connector

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

9.2.13 DINrail Power Connector

Type – Phoenix Combicom MSTB 2,5/ 3-GF-5,08(male), 3 pins.

	Pin No.	Description
	1	-PWR Negative power terminal or N (Neutral power terminal)
	2	FPE, GND (Functional Protective Earth / GND)
	3	+PWR Positive power terminal or L (Life power terminal)

Matching Type for cable: FKCT 2,5/ 3-STF-5.08
For AWG 12-24
Area 0.2–2.5 mm² or Diameter 0.5-1.75 mm



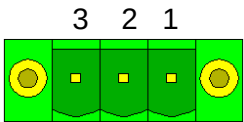
9.2.14 Local Craft Terminal (USB) Connector (LCT)

Type – USB Type Mini-B (female, receptacle), 5 pins.

	Pin No.	Signal	Description
	1	VCC	+5V
	2	D-	Data -
	3	D+	Data +
	4	NC	
	5	GND	SGND

9.2.15 FlatRack Power Connector (Power Supply Module)

Type – Phoenix Combicon MSTB 2,5/ 3-GF-5,08(male), 3 pins.

	Pin No.	Description
	1	-PWR Negative power terminal or N (Neutral power terminal)
	2	FPE, GND (Functional Protective Earth / GND)
	3	+PWR Positive power terminal or L (Life power terminal)

Matching Type for cable: Phoenix 1873210
For AWG 12-24

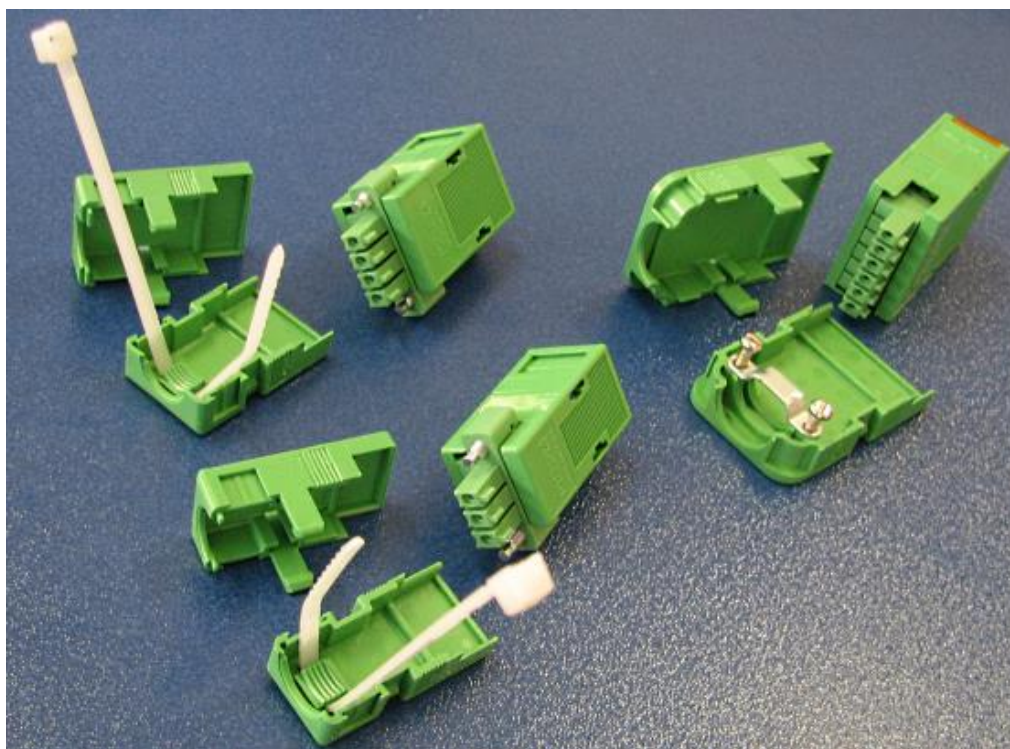
Area 0.25–2.5 mm² or Diameter 0.5-1.75 mm



9.2.16 Connector Hoods and Cord Retaining

For the Phoenix Mini Combicom connector series, there are some hoods available.

Connector	Matching Cable Housing
MC1,5/3-STF-3,5	KGG-MC-1,5/3
MC1,5/4-STF-3,5	KGG-MC-1,5/4
MC1,5/6-ST-3,5	KGG-MC-1,5/6



For the power supply connector on the back of MiniFlex, there is a cable cord retaining kit available.

Connector	Cord Retaining Kit
AC Power	4700.0002



These items, if needed, must be ordered separately!

10 TECHNICAL SPECIFICATION

10.1 Interfaces

10.1.1 1000Base-X Gigabit Ethernet (P1, P2)

Standard:	IEEE-802.3, VLAN IEEE-802.1Q, QoS IEEE-802.1P
Data Rate	1000Base-X, Full/Half Duplex
Protocols	Data, Telnet, SNMP
Connector Type	SFP

Recommended 1.25Gbps SFP Transceiver (1000Base-LX interface):

- EOLS 1312-10D
- HSFP-24-3311S-22F

10.1.2 1000Base-T, Gigabit Ethernet (P3, P4)

Standard:	IEEE-802.3, VLAN IEEE-802.1Q, QoS IEEE-802.1P
Data Rate	1000Base-T, Full/Half Duplex
Protocols	Data, Telnet, SNMP
Signal Level	Ethernet
MDI / MDI-X auto crossover	Supported
Auto Negotiation	Supported
Connector Type	RJ45, 8 pin

10.1.3 10/100Base-T Ethernet (P5-P12, SHDSL, FOM, POE, Serial and Switch)

Standard:	IEEE-802.3, VLAN IEEE-802.1Q, QoS IEEE-802.1P
Standard if POE	IEEE 802.3af (15.4W) or IEEE 802.3at (40.0W)
Data Rate	10/100Base-T, 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

10.1.4 10/100/1000Base-T Ethernet (GFOM, FlatRack, MF-MR2N-SW-8Eth,V2)

Standard:	IEEE-802.3, VLAN IEEE-802.1Q, QoS IEEE-802.1P
Standard if POE	IEEE 802.3af (15.4W) or IEEE 802.3at (40.0W)
Data Rate	10/100/1000Base-T, 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

10.1.5 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 or 2
Bit Rate	192 to 5704kbit/s, Extended: 128 to 15232kbit/s
Connector Type	Phoenix Mini Combicom 4 pin: MC 1,5/4-GF-3,5
Overvoltage Protection	ITU-T Rec. K.20/K.21

10.1.6 100Base-FX Ethernet (FOM, Serial RS-232 Interface)

Standard:	IEEE-802.3, VLAN IEEE-802.1Q, QoS IEEE-802.1P
Data Rate	100Base-FX, Full/Half Duplex
Protocols	Data, Telnet, SNMP, WEB
Connector Type	SFP

Recommended 155Mbps SFP Transceiver (Fast Ethernet, OC-3, STM-1):

- LS38-A3S-TC-N
- XGSF-03-1503-80

10.1.7 100Base-FX / 1000Base-X Ethernet (GFOM)

Standard:	IEEE-802.3, VLAN IEEE-802.1Q, QoS IEEE-802.1P
Data Rate	100Base-FX or 1000Base-X, Full/Half Duplex
Protocols	Data, Telnet, SNMP, WEB
Connector Type	SFP

10.1.8 1000Base-X / 2500Base-X Ethernet (FlatRack, MF-MR2N-SW-8Eth,V2)

Standard:	IEEE-802.3, VLAN IEEE-802.1Q, QoS IEEE-802.1P
Data Rate	1000Base-X, 2500Base-X Full/Half Duplex
Protocols	Data, Telnet, SNMP, WEB
Connector Type	SFP

10.1.9 E1 Line Interface

Specification	ETS 300 166, ITU-T Rec. G.703, G.704
Line Code	HDB3/AMI
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)

10.1.10 Serial RS-232 / RS-232/422/485 Interface

Standard:	ITU-T Rec V.28 or RS-232/485
Bit Rate	75, 150, 300, 600, 1200, 2400, 4800, 9600, 14400, 19200, 28800, 38400, 56000, 57600, 115200, 230400 bps
MF-FOM-RAIL2N-SER-xx	
MF-FOM-SR2L-SER/Eth,Vx	
Bit Rate	75, 1200, 2400, 9600, 19200, 38400, 57600, 115200, 230400 bps
MF-FOM-RAIL2N-2V24-xx	
MF-SER-SRL-4V24,Vx	
Format RS-232/485	Bits: 5...8
	Stop bits: 1/1.5/2
	Parity: odd/even/mark/space
Connector Type	RJ45, 8 pin

10.1.11 FXO Interface

Type	Exchange isolated interface for CO connection
Specification	ITU-T Q.552
Coding	ITU-T G.711
Relative Input Level	-3dB nominal
Input Impedance	600 Ohm, active
Ringing Frequency detection	15 to 50 Hz
Ringing Voltage	35..110 Vrms
Ringing Detector Impedance	$ Z \geq 2 \text{ kOhm}$
Loop Current in off-hook state (normal operation)	10...40mA
On-hook resistance	$\geq 100 \text{ kOhm}$
Dialing Mode	DTMF/Pulse
Connector Type	RJ45, 8 pin

10.1.12 FXS Interface

Type	Subscriber non-isolated interface
Specification	ITU-T Q.552
Coding	ITU-T G.711
Relative Input Level	0dB nominal
Input Impedance	600 Ohm, active
Ringing Signal Specification (@Z@25Hz $\geq 2 \text{ kOhm}$)	Signal form: sine (THD $\leq 3,5\%$) Frequency: 25 ± 1 Hz Vpeak-to-peak: 136 ± 6 V Vrms: 48 ± 2 Vrms No DC offset
On-hook loop current	25 ± 2 mA
Off-hook voltage	48 ± 3 V
Maximum Loop resistance (including phone)	2 FXS interfaces used: 800Ohm 1 FXS interface used: 1500Ohm
Dialing Mode	DTMF/Pulse
Connector Type	RJ45, 8 pin

10.1.13 Voice Frequency (Analog) Interface

Description	Voice Frequency 4-wire interface
Coding	ITU-T G.711
Relative Input Level	-13.0 ... +7 dBm (SW adjustable)
Relative Output Level	-17.0 ... +4 dBm (SW adjustable)
Max. Overload:	+3.14 dBm0
Frequency Range	300 ... 3400 Hz
Amplitude Frequency Mask	ITU-T G.712
Input Impedance	600 Ohm, balanced
Squelch Threshold Level	-40.0 ... -10.0 dBm (SW adjustable)
Connector Type	RJ45, 8 pin

10.1.14 E&M Interface

E&M Type	5 (other types available by request), carrier side
E-wire	output ON state: current source, 8...12mA@-4...-72VDC OFF state: $R_{off} \geq 1M\Omega$ Max. allowed voltage: +/-72VDC
M-wire	input ON state detection current: max. 3.11mA ON state detection resistance to GND: min. 7.5k Ω Max. short to GND current: 18.6mA OFF state detection current: min. 1.00mA OFF state detection resistance to GND: max. 17k Ω Open circuit voltage: min. -43.2Volts
Connector Type	RJ45, 8 pin

10.1.15 Digital Input / Output Interface

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

10.1.16 Local Craft Terminal (USB) Interface

Specification	USB V2.0 full and low speed
Data Rate	12Mbit/s
Protocol	Master/Slave, Uses the USB communication device class (CDC) drivers to take advantage of the installed PC RS-232 software to talk over the USB
Connector Type	USB Type Mini-B female connector

10.1.17 Alarm Interface

Specification	Isolated Relay Output
Load	1A @ 24VDC, 0.5A @ 125VAC
Max. Operation Voltage	60VDC, 125VAC
Max. Operation Current	1A
Max. Switch Capacity	62VA, 30W
Connector Type	Phoenix Mini Combicom 6 pin: MC 1,5/6-G-3,5

10.2 Power Supply

10.2.1 MiniFlex Mini DSLAM (Subrack)

Specification	ETSI ETS 300 132-2
MF-PS48, V1	
Input Voltage	18-72VDC
Connector Type	Phoenix Mini Combicom 3 pin: MC 1,5/3-GF-3,5
MF-PS110/230, V1	
Input Voltage	90-264VAC, 47-63Hz
Connector Type	IEC 60320-1, C14, 10A/250VAC UL 498, CSA C22.2 no. 42
Power Consumption (All DSL links up, Ethernet on)	Max. 18W for MiniFlex without SHDSL Line Cards Max. 4.0W for MF-PAM-SR2L-2Eth,V1 Max. 2.2W for MF-FOM-SRL,V1 Max. 3.7W for MF-FOM-SR2L-2Eth,V1 Max. 3.8W for MF-FOM-SR2L-SER/Eth,V1 Max. 3.5W for MF-SW-SRL-8Eth,V1 Max. 42.0W for MF-POE-SRL-2Eth,V1 Max. 2.2W for MF-SER-SRL-4V24,V1 Max. 2.7W for MF-TDM-SRL-4E1B, V1 Max. 7.1W for MF-VOIP-SRL-2Eth/2FXS, V1* Max. 2.6W for MF-VOIP-SRL-2Eth/2FXO, V1* Max. 5.1W for MF-VOIP-SRL-2Eth/2VF, V1* Max. 2.5W for MF-IO-SRL-4I4O/Eth, V1 Max. 5.5W for MF-GFOM-SR2L-2Eth,V1
*Note for VoIP cards: All units: Both Ethernet Active @ 10Mbps FXS: - One call active with $R_{loop}=320\Omega$ 2nd channel ringing @ $Z_{25Hz}=2k\Omega$ FXO: 2 calls in progress VF: both connections established, M lines to ground, E-lines in ON state	

10.2.2 MiniFlex FlatRack

Specification	ETSI ETS 300 132-2
MF-PS48-FR05N,V1	
Input Voltage	18-72VDC
Connector Type	Phoenix Mini Combicom 3 pin: MC 1,5/3-GF-3,5
MF-PS230-FR05N,V1	
Input Voltage	170-264VAC / 200-370VDC
Connector Type	Phoenix Mini Combicom 3 pin: MC 1,5/3-GF-3,5
MF-PS120-FR05N,V1	
Input Voltage	85-132VAC
Connector Type	Phoenix Mini Combicom 3 pin: MC 1,5/3-GF-3,5
Power Consumption (All DSL links up, Ethernet on)	Max. 5.8W for Integrated Switch without Line Cards Max. 4.0W for MF-PAM-SR2L-2Eth,V1 Max. 2.2W for MF-FOM-SRL,V1 Max. 3.7W for MF-FOM-SR2L-2Eth,V1 Max. 3.8W for MF-FOM-SR2L-SER/Eth,V1 Max. 3.5W for MF-SW-SRL-8Eth,V1 Max. 42.0W for MF-POE-SRL-2Eth,V1 Max. 2.2W for MF-SER-SRL-4V24,V1 Max. 2.7W for MF-TDM-SRL-4E1B, V1 Max. 7.1W for MF-VOIP-SRL-2Eth/2FXS, V1* Max. 2.6W for MF-VOIP-SRL-2Eth/2FXO, V1* Max. 5.1W for MF-VOIP-SRL-2Eth/2VF, V1* Max. 2.5W for MF-IO-SRL-4I4O/Eth, V1 Max. 5.5W for MF-GFOM-SR2L-2Eth,V1
*Note for VoIP cards: All units: Both Ethernet Active @ 10Mbps FXS: - One call active with $R_{loop}=320\Omega$ 2nd channel ringing @ $Z_{25Hz}=2k\Omega$ FXO: 2 calls in progress VF: both connections established, M lines to ground, E-lines in ON state	

10.2.3 MiniFlex MiniRack

Specification	ETSI ETS 300 132-2
Input Voltage	18-72VDC
Connector Type	Phoenix Mini Combicom 3 pin: MC 1,5/3-GF-3,5
Power Consumption (All DSL links up, Ethernet on)	Typ. 16W for MiniRack with SHDSL Line Cards

10.2.4 MiniFlex Dual Unit

Specification	ETSI ETS 300 132-2
-12V Models	
Input Voltage	9-36VDC
Connector Type	Phoenix Combicom 3 pin: MSTB 2,5/ 3-GF-5,08(male)
-24V Models	
Input Voltage	18-72VDC
Connector Type	Phoenix Combicom 3 pin: MSTB 2,5/ 3-GF-5,08(male)
-230V Models	
Input Voltage	85-264VAC, 120-370VDC, 47-63Hz
Connector Type	Phoenix Combicom 3 pin: MSTB 2,5/ 3-GF-5,08(male)
Power Consumption (All DSL links up, Ethernet on)	Max. 20W with any Line Cards except PoE Max. 35W with any Line Cards including PoE

10.2.5 MiniFlex DINrail

Specification	ETSI ETS 300 132-2
-12V Models	
Input Voltage	9-18VDC
Connector Type	Phoenix Combicom 3 pin: MSTB 2,5/ 3-GF-5,08(male)
-24V Models	
Input Voltage	18-72VDC
Connector Type	Phoenix Combicom 3 pin: MSTB 2,5/ 3-GF-5,08(male)
-230V Models	
Input Voltage	85-264VAC, 100-370VDC, 47-63Hz
Connector Type	Phoenix Combicom 3 pin: MSTB 2,5/ 3-GF-5,08(male)
Power Consumption (All DSL links up, Ethernet on)	
Max. 4.8W for MF-PAM-RAIL2N-2Eth-12V, V1	Max. 4.5W for MF-PAM-RAIL2N-2Eth-230V, V1
Max. 5.3W for MF-PAM-RAIL2N-2Eth-24V, V1	Max. 2.7W for MF-FOM-RAILN-Eth-230V, V1
Max. 3.7W for MF-FOM-RAILN-Eth-24V, V1	Max. 4.4W for MF-FOM-RAIL2N-2Eth-230V, V1
Max. 5.0W for MF-FOM-RAIL2N-2Eth-24V, V1	
Max. 42.0W for MF-POE-RAILN-Eth-24V, V1	
Max. 4.1W for MF-SW-RAIL-4Eth-24V, V1	Max. 3.5W for MF-SW-RAIL-4Eth-230V, V1
Max. 5.0W for MF-FOM-RAIL2N-2V24-24V, V1	Max. 4.5W for MF-FOM-RAIL2N-2V24-230V, V1
Max. 5.3W for MF-FOM-RAIL2N-SER/Eth-24V, V1	Max. 4.6W for MF-FOM-RAIL2N-SER/Eth-230V, V1
Max. 3.9W for MF-TDM-RAILN-4E1B/2Eth-24, V1	Max. 3.3W for MF-TDM-RAILN-4E1B/2Eth-230, V1
Max. 6W for MF-VOIP-RAILN-2Eth/2FXS-24V, V1*	Max. 5.6W for MF-VOIP-RAILN-2Eth/2FXS-230V, V1*
Max. 2W for MF-VOIP-RAILN-2Eth/2FXO-24V, V1*	Max. 1.8W for MF-VOIP-RAILN-2Eth/2FXO-230V, V1
Max. 4.4W for MF-VOIP-RAILN-2Eth/2VF-24V, V1*	Max. 4W for MF-VOIP-RAILN-2Eth/2VF-230V, V1*
Max. 2W for MF-IO-RAILN-4I4O/Eth-24V, V1	Max. 3W for MF-IO-RAILN-Eth-4I4O/Eth-230V, V1
Max. 7.0W for MF-GFOM-RAIL2N-2Eth-24V, V1	Max. 8.0W for MF-GFOM-RAIL2N-2Eth-230V, V1

***Note for VoIP DINrail:**

All units: Both Ethernet Active @ 10Mbps

FXS: 1 call in progress with $R_{loop}=320\Omega$, 2nd channel ringing with load $Z_{@25Hz}=2k\Omega$

FXO: 2 calls in progress

VF: both connections established, M lines to ground, E-lines in ON state

10.3 Environment

10.3.1 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)
Operation (Dual Unit):	ETS 300 019-1-3 Class 3.2 ext	(-40°C ... +70°C)
Operation (FlatRack):	ETS 300 019-1-3 Class 3.2 ext	(-20°C ... +60°C)
Higher Operation Temperature range available on request (-25°C ... +80°C)		

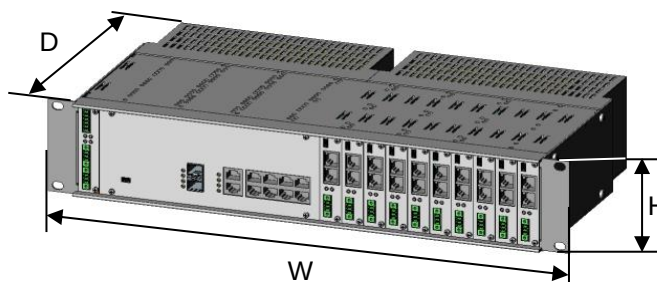
10.3.2 EMC and Safety Standards

Safety	IEC 60950-1:2005/A2:2013 EN 60950-1:2006/A2:2013
EMC	EMC emissions: EN 300 386 V1.6.1 EN 55022:2010/AC:2011 EN 50121-4:2006/AC:2008 EN 61000-3-2:2014 EN 61000-3-3:2013 EMC immunity: EN 300 386 V1.6.1 EN 55024:2010 EN 50121-4:2006/AC:2008 EN 61000-4-2:2009 EN 61000-4-3:2006/A1:2008/A2:2010 EN 61000-4-4:2012 EN 61000-4-5:2014 EN 61000-4-6:2014 EN 61000-4-11:2004
RoHS	RoHS2 Directive 2011/65/EU
WEEE	WEEE Directive 2012/19/EU

10.4 Physical Dimensions and Weight

10.4.1 MiniFlex Mini DSLAM (Subrack)

Dimension with Power Supply:
482(W)x248(D)x89(H) mm
19" (W), 2U (H)

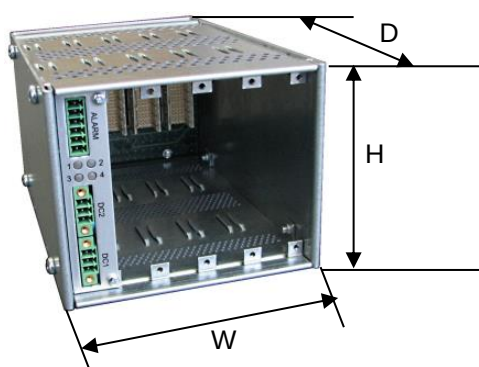


Weight without Line Cards
Weight with 10 Line Cards

< 4.4kg
< 5.5kg

10.4.2 MiniFlex MiniRack

Dimension with Power Supply:
110(W)x181(D)x88(H) mm
with Clip
2U (H)



Weight without Line Cards
Weight with 4 Line Cards

< 1.1kg
< 1.7kg

10.4.3 MiniFlex Dual Unit

Dimension:
50(W)x190(D)x87(H) mm
with Clip
2U (H)



Weight without Line Cards
Weight with 2 Line Cards

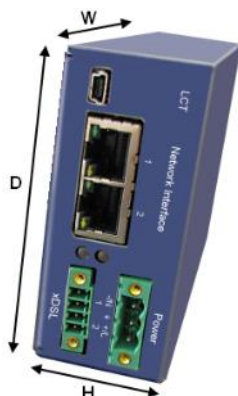
< 0.55kg
< 0.90kg

10.4.4 MiniFlex SHDSL, Single FOM, POE DINrail

Dimension:

143(W)x87(D)x37(H) mm

153(W)x87(D)x37(H) mm with Clip



Weight

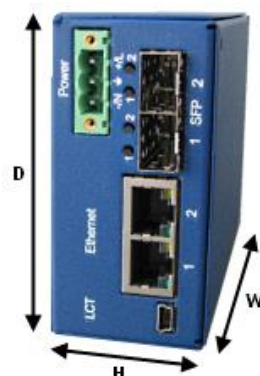
< 0.5kg in Metal DIN-Rail Enclosure

10.4.5 MiniFlex Dual FOM, GFOM, Switch, Serial, E1, VoIP, IO DINrail

Dimension:

143(W)x87(D)x43(H) mm

153(W)x87(D)x43(H) mm with Clip



Weight

< 0.5kg in Metal DIN-Rail Enclosure

10.4.6 FlatRack

Dimension:

482(W)x293(D)x24(H) mm

19" (W), 1½U (H)

Weight without Line Cards < 3.0kg

Weight with 5 Line Cards < 3.5kg

