

GroomerII user guide

Version 10.50 software

MAN1015 Revision 4.50.1



PROPRIETARY INFORMATION

The information contained in this document is the property of Aculab plc and may be the subject of patents pending or granted, and must not be copied or disclosed without prior written permission. It should not be used for commercial purposes without prior agreement in writing.

All trademarks recognised and acknowledged.

Aculab plc endeavours to ensure that the information in this document is correct and fairly stated but does not accept liability for any error or omission.

The development of Aculab's products and services is continuous and published information may not be up to date. It is important to check the current position with Aculab plc.

Copyright © Aculab plc. 2002-2016 all rights reserved.

Document Revision

Rev	Date	By	Detail
1.0.0	10.01.02	DJL	First issue of GroomerII user guide
1.0.1	14.06.02	DJL	Addition of SNMP information
1.0.2	04.10.02	DJL	Revision 7.2.0 software release.
1.0.3	04.11.02	DJL	Additional General Hazard statements
1.0.4	03.01.03	DJL	Addition of CLI authorisation and new backup/restore process
1.4.0	30.01.03	DJL	1U unit, mixed drivers, and SNMP updates
1.5.0	30.03.03	DJL	DDI and Number portability added
1.5.1	12.08.03	DJL	Chassis hardware layout changes
2.0.0	17.11.04	DJL	Addition of IP telephony SIP protocol support
3.0.0	09.05.05	DJL	Updates to support Aculab V6 drivers
3.1.0	13.02.06	DJL	Updated for Windows XP/Server 2003 and IP Telephony
3.2.0	11.08.06	DJL	ETS300 call transfer to SS7 call diversion mapping.
4.0.0	02.10.06	DJL	Updates including Traffic monitor, CDR, and ACT.
4.1.0	27.04.07	INC	Alliance 6U chassis and Prosody X support.
4.1.1	30.04.07	INC	Added earthing connection statement to safety instructions.
4.1.2	05.07.07	INC	Additional safety information. Added Aculab 1U chassis details. Remove Kontron 6U chassis details.
4.1.3	14.11.07	INC	Updated Prosody X card configuration. Clarification of earthing points. Aligned safety appendices. Added Chinese safety appendix.
4.1.4	13.12.07	INC	Gateway lists can now be configured in SIP and H.323 routing screens.
4.1.5	18.07.08	INC	Aculab 8 port 1U chassis. SIP gateway monitoring. Included information from the discontinued Supplementary Information folder, and added System Information pages.
4.1.6	06.01.09	INC	Support for H.323 ID when routing calls to a gatekeeper. Updated for shipping unconfigured systems. Allow PCM conversion to be disabled on systems fitted with PMX modules.
4.1.7	12.01.09	INC	Updated licensed codecs legal notice.
4.1.8	11.02.09	INC	SIP routing fallback and round robin gateway lists.

4.1.9	18.02.09	INC	ETS 300 call transfer to SS7 call diversion mapping.
4.1.10	04.05.09	INC	Configurable VAD on IP telephony codecs.
4.3.0	01.07.09	INC	Full SNMP implementation.
4.4.0	31.07.09	INC	Configurable SS7 CPC and SIP custom headers.
4.5.0	06.10.09	INC	SIP call recovery.
4.6.0	04.11.09	INC	Secure SIP calls.
4.7.0	01.02.10	INC	Updated codec legal notice. Details of grSIPMappings.ini.
4.8.0	06.03.10	INC	Advice of charge mapping between Finnish ISUP and SIP.
4.9.0	05.04.10	INC	Installation instructions for 6U chassis removed. Support for Clear Channel codec.
4.10.0	01.05.10	INC	Routing on subaddress and Aculab-Call-Information SIP header.
4.10.1	16.05.10	INC	Support for carrier grade 1U chassis.
4.12.0	24.05.10	INC	SS7 echo control indication. Support for E1/T1 Digital Access Card discontinued.
4.13.0	01.07.10	INC	Call routing on Nature of Address.
4.14.0	23.07.10	INC	Fallback gateway selection on H.323.
4.15.0	24.08.10	INC	Support for call re-routing and UK ISUP.
4.15.1	06.09.10	INC	Support for setting SS7 charge indicator.
4.15.2	20.10.10	INC	Additional nature of address setting. Support for SIP call hold. SS7 supervisory message throttling.
4.16.0	04.01.11	INC	Routing on CLI presentation indicator. SNMP trap for failed RTP.
4.16.1	23.03.11	EBJ	Updated to corporate fonts
4.17.0	11.05.11	INC	40ms DTMF detection, H.323 call retry and SIP gateway groups.
4.18.0	27.05.11	INC	Configurable location on routing failed clearing, incomplete dialling and ringing timers.
4.18.1	01.07.11	INC	Chapter on installing/uninstalling GroomerII application software removed.
4.19.0	29.07.11	INC	Updated for V10.19 software – no functional changes.
4.20.0	01.08.11	INC	Configurable SIP Aculab-SS7 header production. Instructions for adding/replacing Prosody X cards. Host NIC teaming.
4.22.0	23.01.12	INC	SIP History-Info headers, SIP call redirection, CAMA, silent backup.
4.24.0	11.05.12	INC	Additional SIP headers, SS7 status reporting, TiNG DSP monitoring, chassis monitoring.
4.25.0	23.01.13	INC	Support for CG2100 chassis. SNMP reporting for TiNG DSP status. Hookflash mapping from CAMA to SIP.
4.26.0	07.02.13	INC	H.323 telephony re-introduced. Functional Number Mapping.
4.27.0	07.05.13	INC	Support for R720 chassis.
4.28.0	03.02.14	INC	Support for AC2460 chassis. Removal of H.323 telephony. CNIP/CONP mapping. UUI mapping. MLPP mapping.
4.28.1	24.02.14	INC	Expanded IP telephony network configuration for AC2460 chassis.
4.28.2	10.03.14	INC	Disable SS7 group messaging. Configuration import.

4.29.0	15.08.14	INC	Called party only clearing. SIP gateway routes. Additional supplementary service mapping. SS7 continuity check.
4.30.0	13.02.15	INC	TTY/RTT mapping. SS7 continuity checking. Connected party number mapping.
4.31.0	13.04.15	INC	Hookflash mapping from SIP to CAMA. SIP gateway polling using TCP transport.
4.32.0	15.04.15	INC	Support for R730 chassis.
4.32.1	19.10.15	INC	Support for SNMPv3.
4.33.0	02.12.15	INC	SS7 circuit blocking on layer 1 alarm. Configurable forward call indicator fields.
4.33.1	21.01.16	INC	Status Monitor option to clear error counters on all TDM ports.
4.34.0	22.03.16	INC	Configure ringing timer at route level.
4.50.0	05.05.16	INC & MPL	Support for SIP telephony using IPv6.
4.50.1	10.01.17	MPL	Fix some references to Sections 3.2 and 3.3. Add information to Appendix A. G.729 now royalty free, so cut down Appendix C.

CONTENTS

1	System overview	16
1.1	Chassis installation guides.....	16
1.2	Signalling protocols supported	16
1.3	Activation key mechanism	16
1.4	Principles of operation.....	17
1.5	GroomerII IP telephony principles	18
1.6	2U carrier grade port numbering	19
1.6.1	Dual port breakout adapters	19
1.6.2	Port numbering	19
1.7	System configuration	20
2	System boot-up.....	22
2.1	Overview.	22
2.2	Locking the computer at startup	22
2.3	Initial hardware checks	22
2.4	Basic fault finding.....	24
3	IP telephony network configuration.....	25
3.1	Host network adapter configuration	25
3.1.1	IPv4 configuration.....	25
3.1.2	IPv6 configuration.....	26
3.2	Prosody X card configuration.....	26
3.2.1	Configuring the Prosody X NIC address	27
3.2.1.1	IPv4 configuration.....	27
3.2.1.2	IPv6 configuration.....	28
3.2.2	Configuring the Prosody X media addresses	29
3.2.2.1	IPv4 configuration.....	30
3.2.2.2	IPv6 configuration.....	31
3.2.2.3	Restarting the card	31
3.3	Setting the network connection order	32
3.4	Completing the configuration	32
4	Configuring GroomerII cards	33
4.1	Introduction	33
4.1.1	Restrictions.....	33
4.2	Starting the ACT application	33
4.2.1	Startup messages.....	33
4.3	Overview	34
4.3.1	Card List.....	35
4.3.2	Clocking settings	37
4.3.3	Diagnostics.....	38
4.3.4	IP settings.....	39
4.3.5	Prosody X.....	40
4.3.6	TiNG settings.....	42
4.4	Configuring card TDM port details	43
4.4.1	Protocol selection	45
4.4.2	Protocol configuration (excluding SS7)	46
4.4.3	Protocol configuration for SS7	48
4.4.4	Adding additional switches	52
4.5	Configuring clock settings.....	53
4.6	Running system diagnostics	54

4.7	Flashing a Prosody X card	55
4.8	Prosody X card configuration	57
4.9	TiNG module settings	60
4.10	Completing the configuration	62
5	GroomerII kernel	63
5.1	GroomerII configuration load	65
5.2	Advice of charge configuration load	66
5.3	Address mapping	67
5.4	SNMP reporting	68
5.4.1	Ports tab options	69
5.4.2	Processes tab options	70
5.4.3	System tab options	71
5.4.4	Chassis tab options	73
5.4.5	Call Monitoring tab options	74
5.5	CLI authorisation database selection	76
5.6	DDI authorisation database selection	78
5.7	Number portability database selection	80
5.8	Call data record (CDR)	82
5.9	SIP Authentication	88
5.10	TLS certificates	90
5.11	Port blocking	92
5.11.1	Port blocking for ITU-T, China and UK ISUP	92
5.11.2	Port blocking for ANSI SS7 and non-SS7 TDM ports	93
5.11.3	Port blocking for IP telephony ports	94
5.12	Firmware reload	95
5.13	Port reset	97
5.14	SS7 signalling links	98
5.15	Continuity check	99
6	GroomerII status monitor	101
6.1	Alarms	101
6.2	Events	103
6.2.1	Pausing the log	104
6.2.2	Event filters	104
6.2.2.1	Event categories	104
6.2.2.2	Sample trace	106
6.2.2.3	Event output options	107
6.2.3	Logging events to a disk file	107
6.2.4	Logging events to the serial ports	108
6.3	Diagnose	110
6.3.1	Diagnostics report – E1/T1 trunk port	110
6.3.2	Diagnostics report – IP port	111
6.4	Gateways	113
6.5	SS7	115
6.5.1	Signalling	115
6.5.2	Bearers	116
6.5.3	Routes	117
6.5.4	Destinations	118
6.6	CAS	119
7	GroomerII traffic monitor	120
8	GroomerII configuration	123
8.1	Layout and overview	123
8.1.1	File menu options	123

8.1.2	Configuration	124
8.1.3	Tools	124
8.2	Producing a configuration file	124
8.2.1	Setting the tools options	124
8.2.2	Configuration order	124
8.3	Ports configuration.....	126
8.3.1	Ports.....	127
8.3.2	Setup.....	127
8.3.3	Incoming.....	128
8.3.4	Outgoing.....	131
8.3.5	Alarm handling	131
8.4	Groups configuration	134
8.4.1	Groups	134
8.4.2	Setup.....	134
8.4.3	Advanced	136
8.5	Routing configuration	138
8.5.1	Routes.....	138
8.5.2	Setup.....	139
8.5.3	Routes – Q.931/ISUP	145
8.5.4	Routes – CAS.....	151
8.5.5	Routes – DPNSS.....	153
8.5.6	Routes SIP	154
8.5.7	Routes – general	160
8.6	System configuration	163
8.6.1	Clocks	163
8.6.2	CLI authorisation	164
8.6.3	DDI authorisation.....	165
8.6.4	Number portability	166
8.6.5	Alarm mapping.	167
8.6.6	Timers	169
8.6.7	Protocol Settings	170
8.6.8	Default codecs.....	176
8.6.9	SIP gateways	179
8.6.10	SIP proxy server.....	183
8.7	Cause mapping configuration	185
8.8	Tone generation configuration.....	187
8.9	Advanced configuration options	188
8.10	Comments	190
8.11	Options	190
8.12	Activation key	191
9	Address map editor.....	192
9.1	Creating an address map.....	193
9.2	Using wildcards	193
9.3	Adding and inserting address map entries.....	193
9.4	Editing an entry	196
9.5	Deleting an entry	196
9.6	Maintaining list order.....	196
10	Advice of charge.....	197
10.1	Charge bands.....	199
10.1.1	Adding and removing charge bands	199
10.1.2	Charge band entries	201
10.1.3	Advice of charge parameters	202
10.2	Customers (port groups)	203
10.2.1	Loading available port information.	203

10.2.2 Configuring customers	204
10.2.3 Defining customers	205
10.3 Enabling advice of charge	205
10.4 Tool options	206
10.4.1 Comments	206
10.4.2 Activation key	206
11 Backup and restore	207
11.1 Backup	207
11.2 Restore	209
11.3 Configuration import	210
11.3.1 Host port groups	210
11.3.2 Preparing the backup	211
11.3.3 Preparing the target system	211
11.3.4 Trunk port cabling	212
11.3.5 Importing the configuration	212
11.4 Silent backup	214
12 Call Transfer	216
12.1 Call transfer mapping in GroomerII	216
12.2 ETS 300 Call Transfer to SS7 Call Redirection Mapping	216
12.2.1 Overview	216
12.2.2 Configuration	216
12.2.3 CDR generation	217
12.3 CAMA to SIP Call Transfer Mapping	217
12.4 SIP to CAMA Call Transfer Mapping	217
13 Database connectivity	219
13.1 GroomerII database connectivity	219
13.2 CLI authorisation	219
13.3 DDI authorisation	221
13.4 Number portability mapping	222
14 SIP telephony	224
14.1 IPv4 and IPv6 telephony	224
14.1.1 Incoming call handling	224
14.1.2 Outgoing call handling	224
14.1.3 Call retry and recovery	224
14.2 SIP security	224
14.2.1 Configuration	224
14.2.2 TLS	225
14.2.3 SRTP	225
14.3 SIP call recovery	226
14.4 SIP call hold	227
14.5 SIP call redirection	227
14.6 Functional Number mapping	228
14.7 ISDN subaddress mapping	228
14.8 Interworking with TDM protocols	228
14.8.1 Interworking between SIP and SS7	228
14.8.2 Interworking between SIP and ETS 300	229
14.8.3 Interworking between SIP and CAMA	229
14.9 Additional IETF RFC support	229
15 SS7 telephony	230
15.1 SS7 stack file	230
15.2 SS7 port firmware configuration	236
15.3 Continuity checking	236

16	CAMA telephony	238
16.1	Configuration	238
16.1.1	Signalling firmware configuration	238
16.1.2	GroomerII application configuration	238
16.1.2.1	Port configuration	238
16.1.2.2	Route configuration	239
16.2	Interworking with CAMA	239
16.2.1	CAMA to SIP Interworking	239
16.2.2	SIP to CAMA Interworking	240
16.2.3	Interworking between CAMA and TDM	240
16.3	Disabling incoming CAMA call clearing	240
17	Interworking supplementary services	242
17.1	Name identification supplementary services (CNIP/CONP)	242
17.1.1	Q.SIG	242
17.1.2	SIP	242
17.1.3	Q.SIG to Q.SIG interworking	242
17.1.4	Interworking between Q.SIG and SIP	242
17.1.5	SIP to SIP interworking	243
17.2	User to user signalling (UUS)	244
17.2.1	ETS 300	244
17.2.2	SS7	244
17.2.3	SIP	245
17.2.4	ETS 300 to ETS 300 interworking	245
17.2.5	SS7 to SS7 interworking	245
17.2.6	Interworking between ETS 300 and SS7	245
17.2.7	Interworking between ETS 300 and SIP	245
17.2.8	Interworking between SS7 and SIP	246
17.2.9	SIP to SIP interworking	247
17.3	Multi level precedence and pre-emption (MLPP)	247
17.3.1	ETS 300 and Q.SIG	247
17.3.2	SIP	247
17.3.3	ETS 300/Q.SIG to ETS 300/Q.SIG interworking	247
17.3.4	ETS 300/Q.SIG to SIP interworking	248
17.3.5	SIP to ETS 300/Q.SIG interworking	249
17.3.6	SIP to SIP interworking	249
17.3.7	Interworking to protocols without MLPP support	250
17.3.8	Call diversion and re-routing	250
17.3.9	Call recovery	250
17.4	Additional calling party number	250
17.5	Connected party number (COLP/COLR)	250
17.5.1	Q.931	251
17.5.2	SS7	251
17.5.3	SIP	251
17.5.4	TDM interworking	251
17.5.5	TDM to SIP interworking	251
17.5.6	SIP to TDM interworking	252
17.5.7	SIP interworking	252
18	TTY/RTT mapping	253
18.1	Configuring a TTY system	253
18.2	Operating limits	253
18.2.1	Call capacity	253
18.2.2	Audio codec selection	253
18.2.3	Secure SIP	254

18.3	RTT stream negotiation	254
18.4	T.140 redundancy	254
18.5	Voice and hearing carry over	254
18.6	SIP call retry	254
18.7	SIP call recovery	254
19	Advanced fault finding and maintenance	255
19.1	GroomerII not starting	255
19.2	Kernel errors.....	255
19.2.1	Dongle not present	255
19.2.2	Invalid activation key.....	255
19.2.3	Problem with GRSCHED.DAT	255
19.2.4	CFG FAILED TO LOAD	255
19.3	Status errors.....	256
19.3.1	Openin failed	256
19.3.2	Card clock stopped (TDM ports only).....	256
19.3.3	NO SIGNAL DETECTED (TDM ports only).....	256
19.3.4	DISCONNECTED (IP ports only)	256
19.3.5	REMOTE ALARM INDICATION (TDM ports only)	256
19.3.6	ALARM INDICATION SIGNAL (TDM ports only)	256
19.4	Microsoft Windows error messages.....	256
19.5	Obtaining protocol trace from GroomerII (TDM ports only).....	256
19.6	Using CDRs to monitor system performance	257
19.7	Monitoring a single call through the Groomer.....	257
19.8	Common set-up problems	257
19.8.1	System clock	257
19.8.2	Dedicated timeslots	257
19.9	Aculab technical support.....	258
Appendix A:	SNMP facility.....	259
A.1	Enabling the NuDesign SNMPv3 agent.....	259
A.2	SNMP Alarms.....	260
A.3	SNMP Requests.....	268
Appendix B:	Call data records specifications.....	270
B.1	Fixed format type CDRs.....	270
B.1.1	CDR type A structure	271
B.1.2	CDR type B structure	271
B.1.3	CDR type C structure.....	272
B.1.4	CDR type D structure.....	273
B.1.5	CDR type E structure	273
B.1.6	CDR type F structure	274
B.1.7	CDR type G structure	275
B.1.8	CDR type H structure.....	276
B.1.9	CDR type I structure	277
B.1.10	CDR type J structure	277
B.1.11	CDR type K structure.....	278
B.1.12	CDR type L structure:	279
B.1.13	CDR type M structure	280
Appendix C:	Licensed codecs – legal notice	281
Appendix D:	TDM signalling firmware configuration options.....	282
D.1	-cA/B and X/Y bits configuration (DPNSS only)	282
D.2	-cBBY Backbusy control (CAS only)	282
D.3	-cCA connect acknowledgement (ETS300 only).....	282
D.4	-cCICnnnn circuit identification codes (ISUP only).....	282

D.5	-cCn number of CLI digits (CAS only)	283
D.6	-cDn number of DDI digits (CAS only)	283
D.7	-cDPCnnnnn signalling point code (ISUP only)	283
D.8	-cEn Call Charging Switch (ETS300 only)	283
D.9	-cEX Primary Rate Call Charging (ETS300 only)	284
D.10	-cFD Diversion (QSIG, ETS300, AT&T T1, and NI-2)	285
D.11	-cFF facility (QSIG, ETS300, and NI2)	285
D.12	-cFP MLPP activation (ETS300 only)	285
D.13	-cFR Raw Data (ETS300 and QSIG)	285
D.14	-cFU user to user (QSIG and ETS300)	285
D.15	-cIMP75	285
D.16	-cME	285
D.17	-cNA1 release link trunk (NI-2 only)	285
D.18	-cNCRC disable CRC4 (ISUP only)	286
D.19	-cNE network end configuration (DASS, ETS300, AT&T, and NI2)	286
D.20	-cOPCnnnnn[,i] (ISUP only)	286
D.21	-cQM/S-A/B master/slave priority (QSIG only)	286
D.22	-cRn Default clearing cause (all versions)	286
D.23	-cSLCnn signalling link code (ISUP only)	287
D.24	-cSO disable service message (AT&T and NI2)	287
D.25	-cSP stop call proceeding (ETS300 only)	287
D.26	-cSU stop setup acknowledge (ETS300 only)	287
D.27	-cSW configuration (ETS300 only)	287
D.28	-cTS[I]nn (ISUP only)	287
D.29	-cSPEEDnnk (ISUP only)	287
D.30	-cDAUUS (ETS 300 only)	287
Appendix E: Interpreting GroomerII trace file		288
E.1	Alarms	288
E.2	Layer 1	288
E.3	Data Link	288
E.4	Call Control	289
E.5	Routing	290
E.6	Switching	290
E.7	RTP/RTT	290
E.8	Protocol	291
Appendix F: SIP custom headers		292
F.1	SS7 to SIP mapping headers	292
F.2	SIP call recovery headers	296
F.3	Advice of charge headers	296
F.4	Call information headers	297
F.5	Call control and interworking headers	298
Appendix G: Adding and Replacing Prosody X cards		299
G.1	Adding a Prosody X card	299
G.2	Replacing a Prosody X card	301
Appendix H: Host NIC adapter teaming		303
H.1	Types of teaming	303
H.2	Teaming configuration	303
H.3	Primary and secondary adapter configuration	306
Appendix I: Configuring SIP signalling QoS on Microsoft Windows 7 and Microsoft Windows Server 2008		308
Appendix J: The sip serv.cfg file		312

J.1 Supported parameters.....	312
J.2 Unsupported parameters	313
Appendix K: GroomerII chassis identification	314

Table of Figures

Figure 1-1 Activation key dialog	17
Figure 2-1 GroomerII status monitor alarms tab	23
Figure 2-2 GroomerII Kernel	23
Figure 3-1 IPv4 host port configuration	25
Figure 3-2 IPv6 host port configuration	26
Figure 3-3 Microsoft Windows Network Connection window	27
Figure 3-4 Microsoft Windows network connection Properties window.....	27
Figure 3-5 IPv4 Prosody X NIC address configuration	28
Figure 3-6 IPv6 Prosody X NIC address configuration	28
Figure 3-7 ACT - Prosody X Settings page	29
Figure 3-8 ACT - Prosody X Settings page	30
Figure 3-9 ACT - Prosody X Settings page	31
Figure 3-10 Microsoft Windows Advanced Settings window.....	32
Figure 4-1 ACT splash screen.....	33
Figure 4-2 ACT startup window.....	34
Figure 4-3 ACT card list page	35
Figure 4-4 ACT clocking settings page.....	37
Figure 4-5 ACT diagnostics page.....	38
Figure 4-6 ACT IP settings page	39
Figure 4-7 ACT Prosody X page	40
Figure 4-8 ACT Reset Card dialog	40
Figure 4-9 ACT TiNG settings page	42
Figure 4-10 ACT card details page	43
Figure 4-11 ACT port protocol selection page	45
Figure 4-12 ACT port protocol switch selection page (non SS7)	46
Figure 4-13 ACT switch configuration tab	47
Figure 4-14 ACT port settings confirmation dialog.....	47
Figure 4-15 ACT port protocol configuration page (SS7 Signalling)	48
Figure 4-16 ACT port protocol configuration page (ISUP bearers - hexadecimal)	49
Figure 4-17 ACT port protocol configuration page (ISUP bearers - decimal).....	49
Figure 4-18 ACT additional switches dialog	52
Figure 4-19 ACT configuring clock Settings page.....	53
Figure 4-20 ACT diagnostics page.....	54
Figure 4-21 ACT Flash Card dialog.....	55
Figure 4-22 ACT Add/edit Prosody X card configuration dialog.....	57
Figure 4-23 ACT TiNG module settings page.....	60
Figure 4-24 ACT close dialog.....	62
Figure 5-1 GroomerII Kernel.....	63
Figure 5-2 GroomerII configuration load dialog.....	66
Figure 5-3 AOC configuration load dialog	66
Figure 5-4 Address mapping dialog.....	67
Figure 5-5 SNMP reporting dialog.....	68
Figure 5-6 SNMP reporting – Ports tab dialog.....	69
Figure 5-7 SNMP reporting – Processes tab dialog.....	70
Figure 5-8 Add/Edit Process dialog.....	70
Figure 5-9 SNMP reporting – System tab dialog	71
Figure 5-10 Add/Edit Excluded Process dialog	72

Figure 5-11 SNMP reporting – Chassis tab dialog	73
Figure 5-12 SNMP Reporting – Call Monitoring	74
Figure 5-13 CLI authorisation database connection dialog.....	76
Figure 5-14 DDI authorisation database connection dialog	78
Figure 5-15 Number portability database connection dialog.....	80
Figure 5-16 CDR settings dialog	82
Figure 5-17 SIP authentication dialog	88
Figure 5-18 Add/Edit SIP credentials dialog.....	88
Figure 5-19 TLS Certificates dialog.....	90
Figure 5-20 Port blocking dialog for ITU-T, China and UK ISUP	92
Figure 5-21 Port blocking dialog for ANSI SS7 and non-SS7 TDM ports.....	93
Figure 5-22 Port blocking dialog for IP ports	94
Figure 5-23 Load firmware dialog	95
Figure 5-24 Download firmware progress dialog	95
Figure 5-25 Edit firmware dialog	96
Figure 5-26 Port Reset dialog	97
Figure 5-27 SS7 Signalling Links dialog.....	98
Figure 5-28 Continuity Check dialog	99
Figure 6-1 GroomerII status monitor alarms tab option.....	101
Figure 6-2 GroomerII status monitor events tab option.	103
Figure 6-3 Filter settings dialog.....	104
Figure 6-4 Sample trace for a Euro ISDN to SIP call with Call Control, Routing, Switching and Protocol trace enabled.....	106
Figure 6-5 Disk log settings dialog	107
Figure 6-6 Serial Port Logging dialog.....	108
Figure 6-7 GroomerII status monitor diagnose tab option – E1/T1 trunk.....	110
Figure 6-8 GroomerII status monitor diagnose tab option – IP port.....	111
Figure 6-9 GroomerII Status Monitor Gateways page.....	113
Figure 6-10 GroomerII Status Monitor SS7 Signalling page.....	115
Figure 6-11 GroomerII status monitor SS7 Bearers page	116
Figure 6-12 GroomerII status monitor SS7 Routes page	117
Figure 6-13 GroomerII status monitor SS7 Destinations page	118
Figure 6-14 GroomerII status monitor CAS tab option	119
Figure 7-1 GroomerII traffic monitor dialog	120
Figure 7-2 Alert thresholds dialog	121
Figure 8-1 GroomerII Configuration Editor.....	123
Figure 8-2 Port configuration setup tab option (IP port example)	126
Figure 8-3 Port configuration setup tab option (TDM port example)	126
Figure 8-4 Port configuration incoming tab IP option.....	128
Figure 8-5 Port configuration incoming TDM option	128
Figure 8-6 Port configuration outgoing tab option.....	131
Figure 8-7 Port configuration alarm handling tab option	132
Figure 8-8 Groups configuration setup tab.....	134
Figure 8-9 Groups configuration advanced tab	136
Figure 8-10 Routing configuration setup tab option.....	138
Figure 8-11 Routing configuration Q.931/ISUP - common tab option.....	145
Figure 8-12 Routing configuration Q.931/ISUP – Q.931 tab option	147
Figure 8-13 Routing configuration Q.931/ISUP – ISUP tab option	148
Figure 8-14 Routing configuration CAS tab option	151
Figure 8-15 Routing configuration DPNSS tab option	153
Figure 8-16 Routing configuration SIP incoming codecs tab option.....	154
Figure 8-17 Routing configuration SIP incoming media settings tab option	154
Figure 8-18 Routing configuration SIP outgoing codecs tab option	155
Figure 8-19 Routing configuration SIP outgoing media settings tab option.....	155
Figure 8-20 Type of service selection options	158

Figure 8-21 Routing configuration general tab option	160
Figure 8-22 Add/Edit Re-route cause dialog	161
Figure 8-23 System configuration clocks tab option	163
Figure 8-24 System configuration - CLI authorisation tab option	164
Figure 8-25 System configuration - DDI authorisation tab option	165
Figure 8-26 System configuration – number portability tab option	166
Figure 8-27 System configuration alarm mapping tab option	167
Figure 8-28 System configuration timers tab option	169
Figure 8-29 System configuration Protocol Settings - SIP tab option	170
Figure 8-30 System configuration Protocol Settings - SS7, ANSI tab option	174
Figure 8-31 System configuration Protocol Settings - SS7, UK ISUP tab option	175
Figure 8-32 Add/Edit UK ISUP Priority Number dialog	176
Figure 8-33 System configuration Protocol Settings - CAMA tab option	176
Figure 8-34 System configuration default codec tab option	177
Figure 8-35 SIP Gateways tab – Gateways page	179
Figure 8-36 SIP Gateways tab – Routes page	181
Figure 8-37 SIP Call Gateways tab – Retry/Recovery/Responses page	182
Figure 8-38 Add/Edit SIP Response dialog	182
Figure 8-39 SIP Proxy Server tab	183
Figure 8-40 Add/Edit SIP alias dialog	184
Figure 8-41 Cause mapping configuration	185
Figure 8-42 Tone generation configuration	187
Figure 8-43 Advanced options	188
Figure 8-44 Comments	190
Figure 8-45 Settings option dialog	190
Figure 8-46 Activation key dialog	191
Figure 9-1 GroomerII address map editor dialog	192
Figure 9-2 GroomerII address map editor add record dialog	193
Figure 9-3 Updated GroomerII address map editor dialog	194
Figure 9-4 GroomerII address map editor paste entries	194
Figure 9-5 Paste duplicate DDI prompt	194
Figure 9-6 GroomerII address map editor import entries	195
Figure 9-7 Import duplicate DDI prompt	195
Figure 9-8 Updated GroomerII address map editor dialog	195
Figure 9-9 GroomerII address map editor edit record dialog	196
Figure 10-1 GroomerII advice of charge configuration editor	197
Figure 10-2 Charge band configuration dialog	199
Figure 10-3 Charge band configuration dialog – add bands	200
Figure 10-4 Charge band configuration dialog – copy bands	200
Figure 10-5 Charge band configuration – delete warning dialog	200
Figure 10-6 Charge band configuration dialog – add band entries	201
Figure 10-7 Charge band configuration dialog – copy band entries	201
Figure 10-8 Customer configuration dialog	203
Figure 10-9 Customer configuration – specific GroomerII configuration	204
Figure 10-10 Customer configuration - add a new customer dialog	204
Figure 10-11 Example grshed.dat file configuration	205
Figure 10-12 Advice of charge comments dialog	206
Figure 10-13 Activation key dialog	206
Figure 11-1 GroomerII backup and restore	207
Figure 11-2 Backup destination directory selection dialog	207
Figure 11-3 Backup progress dialog	208
Figure 11-4 Backup successful dialog	208
Figure 11-5 Backup overwrite warning dialog	208
Figure 11-6 Backup read failure warning dialog	208
Figure 11-7 Backup failure dialog	209

Figure 11-8 Restore source dialog	209
Figure 11-9 Restore progress dialog	209
Figure 11-10 Restore successful dialog	209
Figure 11-11 Restore version error dialog	210
Figure 11-12 Restore invalid backup source dialog	210
Figure 11-13 Host port groups	211
Figure 11-14 Import source dialog	212
Figure 11-15 System audit progress dialog	212
Figure 11-16 Unsuitable target system warning dialog	212
Figure 11-17 Prosody X card mapping dialog	213
Figure 11-18 Disconnect source system dialog	213
Figure 11-19 Import progress dialog	213
Figure 11-20 Import complete dialog	213
Figure 12-1 Wait for Transfer Routing Configuration	216
Figure 14-1 User defined ISDN subaddress extension	228
Figure 15-1 Single SS7 link option	234
Figure 15-2 Two SS7 links option	234
Figure 15-3 Single SS7 link looped back option	235
Figure 16-1 CAMA port configuration settings	239
Figure 16-2 CAMA port configured for called party only call clearing	240
Figure G-1 Microsoft Windows Installing device driver software balloon	299
Figure G-2 GroomerII Kernel window showing port blocking message	300
Figure H-1 Device Manager and host adapter properties window	304
Figure H-2 New Team Wizard – Specify team name	304
Figure H-3 New Team Wizard – Select adapters	305
Figure H-4 New Team Wizard – Select team type	305
Figure H-5 New Team Wizard - Finish	305
Figure H-6 Network Connections window	306
Figure H-7 Setting adapter priority	307
Figure I-1 Local Group Policy Editor	308
Figure I-2 Policy-based QoS – Create a QoS policy window	309
Figure I-3 Policy-based QoS – This QoS policy applies to window	310
Figure I-4 Policy-based QoS – Specify the source and destination IP addresses window ..	310
Figure I-5 Setting adapter priority	311
Figure I-6 Local Group Policy Editor	311
Figure K-1 GroomerII Chassis ID dialog	314

1 System overview

1.1 Chassis installation guides

This user guide describes the GroomerII application software packages, and all aspects of system configuration. For a description of the hardware please refer to the appropriate installation guide for your chassis. The installation guides available are:

- MAN1026 GroomerII 2U carrier grade chassis (CG2100) installation guide
- MAN1027 GroomerII 2U carrier grade chassis (R720) installation guide
- MAN1028 GroomerII 1U chassis (AC2460) installation guide
- MAN1029 GroomerII 2U carrier grade chassis (R730) installation guide

Copies of the installation guides will be found on the GroomerII Installation & Utilities CD delivered with your system, or may be downloaded from the Aculab website at <http://www.aculab.com>.

1.2 Signalling protocols supported

GroomerII supports an extensive list of CCS, CAS, and IP Telephony protocols. In some instances, Aculab have developed country or user specific variations of standard protocols. Visit the Aculab web site at <http://www.aculab.com> or contact Aculab support for further details.

A full set of protocol firmware is shipped with GroomerII.

1.3 Activation key mechanism

An activation key is required to run the following programs.

- GroomerII Kernel
- Configuration Editor
- AOC Configuration Editor

The activation key is a 12-character string in the form 58C-3F8-YKQ-G9R, and will be pre-installed when your GroomerII is delivered. Its purpose is to allow a particular revision of software to run on a specific GroomerII chassis. The GroomerII Kernel and configuration editors share the same Activation Key within a single operating system.

If you are using a stand alone PC (support system) to create configurations, your support system will also require a valid activation key.

The activation key will change whenever the major or minor software version number changes. For example, versions 10.32.0 and 10.32.2 will use the same activation key, whilst versions 10.32.0 and 10.33.0 will require different activation keys, as will versions 9.0.0 and 10.0.0.

NOTE

The restricted availability version of GroomerII software uses a different activation key to the standard version.

NOTE

If you are using a support system with multiple versions of the configuration tool loaded, a valid activation key is required for each version.

If the GroomerII chassis for which the activation key was calculated is a GroomerII 1U (AC2460) or GroomerII 2U carrier grade (CG2100) chassis, then the GroomerII Kernel will be prevented from loading any configuration file containing more than maximum number of ports supported by that chassis (9 or 27). Similarly, the Configuration Editors for such systems will be prevented from producing configurations with too many ports.

Using the activation key from a GroomerII 2U carrier grade (R720) or GroomerII 2U carrier grade (R730) system will allow you to prepare configuration files for all system types. Care must be taken when preparing configurations for GroomerII 1U (AC2460) and GroomerII 2U carrier grade (CG2100) systems that you do not define too many ports.

If you try to start a program that requires the activation key, and a valid activation key cannot be found for whatever reason (no key entered or the key is invalid), then the program will display a dialog box similar to that illustrated here. You must enter a valid activation key to proceed.

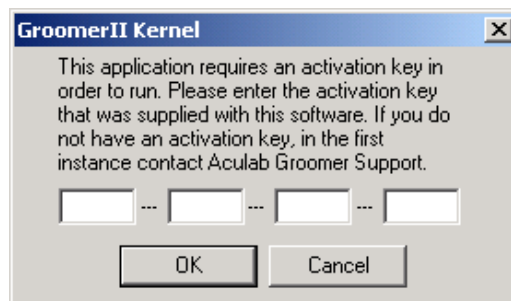


Figure 1-1 Activation key dialog

You will continue to be prompted until the valid activation key for that chassis/software version combination is entered. See section 19.2.2 for guidance on identifying valid activation keys.

Once entered, the system will remember the key, which will be validated each time the Kernel or one of the Configuration applications are started.

1.4 Principles of operation

The primary function of GroomerII is to receive an incoming call, make an outgoing call in response and then connect the voice paths between the two call legs.

Each TDM port in the system can be loaded with any TDM protocol from the Aculab portfolio, with the port being automatically configured for E1 or T1 operation depending upon the protocol in use.

IP telephony ports are automatically enabled for SIP telephony.

At startup GroomerII will automatically listen for incoming calls on every available channel in the system. When an incoming call is detected the Aculab call control software passes the call information up to the GroomerII application software. This call information is used to search the routing table and select a port on which to place the outgoing call. Call control events such as alerting, connect and disconnect are mapped between the calls by the GroomerII application software, and when the far

end answers the call the voice paths are connected, using the H.100 bus for cross-card routes.

GroomerII supports any-to-any protocol conversions. Calls can be routed in either direction between any two ports, with no restrictions on the type of protocol conversions that can be achieved.

1.5 GroomerII IP telephony principles

The principle of operation of GroomerII for routing of traffic from one protocol to another is the same for IP Telephony as it is for all other protocols on GroomerII, the only difference for IP Telephony is that the transmission medium for IP Telephony calls into and out of GroomerII is via an Ethernet digital connection rather than the usual E1/T1 digital trunk.

An E1/T1 trunk is a point to point connection with known end addresses. As the end points are known, data sent out on an E1/T1 port (timeslot) does not need to contain originating and destination address information.

An Ethernet digital connection however does not use a specific timeslot for a call. Call data may take many different routes to reach the destination address. Call data is transmitted over an Ethernet network in packets using the appropriate IP protocol. Each IP packet contains details of the originating and destination IP addresses, allowing the packet to be routed through the network to the correct destination address. To achieve this, GroomerII has to translate standard PSTN call address details into IP address formats that are recognised by the IP protocols, this can be achieved in a number of ways:

1. Route all calls to a specific IP address (gateway).
2. Route calls, or groups of calls, to specific IP addresses based on the information contained in an address map, (local system look up table).
3. Route calls to specific IP addresses via a SIP proxy server.

NOTE

GroomerII currently supports IP call addressing in the format `DDI@IP address`, for example, `123456@192.168.1.18` or `123456@fdac::2998:5000`.

Call set-up

When setting up a call between GroomerII and an IP endpoint (gateway, IP phone etc), the call control signalling is routed via the host NIC on GroomerII. Once the call has been set up, the media is automatically routed via the IP port on the Prosody X card.

Encoding

When interworking between IP and TDM protocols, by default GroomerII will detect the type of connection that is being switched and will use the appropriate encoding.

Pseudo timeslots

IP telephony has no concept of timeslots, however GroomerII assigns a pseudo timeslot to each call for consistency, and to assist with call traffic management.

Codec negotiation

The system can be configured with a default list of available codecs, listed in preference order. Each route can be set to use the default list, or can have its own

list defined with its own preference order. GroomerII uses these lists when negotiating call setup with the remote endpoint.

CAUTION

All Prosody X cards support the G.729AB codec, whose use is subject to license payments. If you are intending to use this codec, please read Appendix C: to establish whether such payments are required.

SIP transport types

SIP is able to use both UDP and TCP for call control signalling. This is implemented in the following way:

- All messages originating from the far end (either an incoming or outgoing call) will use the same protocol as the incoming message for the response.
- All messages originating with GroomerII and sent to an incoming call will use the transport protocol that the far end used to send the incoming INVITE.
- All messages originating with GroomerII and sent to an outgoing call will use the transport protocol configured for the route used.

1.6 2U carrier grade port numbering

Each GroomerII port is assigned a unique number. These numbers are assigned sequentially beginning at zero, with the ports on card zero being assigned their numbers first, followed by the ports on card 1, and so on.

1.6.1 Dual port breakout adapters

Each physical port on a Prosody X card is cabled in a fashion that allows two trunks/IP links to be connected. Your system will be delivered with a set of dual port adapters allowing the ports to be broken out. The chassis installation guide contains a detailed description of the adapters.

NOTE

GroomerII 1U (AC2410) chassis do not require breakout adapters.

1.6.2 Port numbering

The following tables show the port numbering for typical chassis configurations when viewed from the rear.

Card	Port									
	0		1		2		3		4	
	A	B	A	B	A	B	A	B	A	B
0	0		1	5	2	6	3	7	4	8
1	9		10	14	11	15	12	16	13	17
2	18		19	23	20	24	21	25	22	26

2U carrier grade chassis (CG2100) fitted with three cards each having eight TDM ports - these chassis have a serial number in the form G5xxx

Card	Port					Card	Port				
2	0	1	2	3	4	0	0	1	2	3	4
3	0	1	2	3	4	1	0	1	2	3	4

2U carrier grade chassis (R720 and R730) card locations

Card	Port									
	0		1		2		3		4	
	A	B	A	B	A	B	A	B	A	B
0	0		1	5	2	6	3	7	4	8
1	9		10	14	11	15	12	16	13	17
2	18		19	23	20	24	21	25	22	26
3	27		28	32	29	33	30	34	31	35

2U carrier grade chassis (R720 and R730) fitted with four cards each having eight TDM ports - these chassis have a serial number in the form G5xxx

1.7 System configuration

If you did not arrange for your system to be configured by the Aculab Professional Services team prior to delivery, you will need to carry out the following steps to produce a basic configuration. This should be done before attaching any E1/T1 cables to your system.

Power on the system. The GroomerII startup process will run automatically and the configuration used by Aculab to test the system will be loaded. Close down the GroomerII Kernel, GroomerII Status Monitor, and GroomerII Timeslot Monitor applications.

1. Configure the IP telephony network resources:
 - Configure the host IP port as described in section 3.1.
 - Configure the NIC address for each Prosody X card as described in section 3.1.2.
 - Configure the network connection order as described in section 3.3.
2. Start the Aculab Configuration Tool (ACT) and follow the instructions in section 4 to:
 - Select and configure the signalling protocol to be loaded onto each of the TDM ports.
 - Configure the media port settings on each Prosody X card.
 - All other ACT settings should be left as they were delivered.
3. Start the GroomerII Configuration Editor:
 - In the Port Configuration dialog verify that the TDM port settings are appropriate to the protocol in use, as described in section 8.3.
 - In the Groups Configuration dialog configure the groups that you require to route your calls as described in section 8.4.
 - If you will be generating call progress tones configure these using the DSP Configuration dialog as described in section 8.8.
 - In the Clocks page of the System Configuration dialog select your system clock sources as described in section 8.6.1.

- If your GroomerII will be processing IP telephony calls, use the System Configuration dialog to:
 - Select the default codecs to be offered as described in section 8.6.8.
 - Configure how SIP destination addresses will be selected as described in section 8.6.9.
 - Use the Routing Configuration dialog configure the routes that your calls are to use as described in section 8.5.
4. If you will be using address mapping to select SIP destination addresses then you must use the GroomerII Address Map Editor to prepare an address mapping file as described in section 9.

2 System boot-up

2.1 Overview.

The GroomerII start-up process will run automatically at start-up, and will start the GroomerII applications.

2.2 Locking the computer at startup

The startup utility, `grstart.exe`, has a user selectable `-l` switch that locks the computer on start-up using the standard Microsoft Windows lock computer function. The lock computer function prevents any interaction with GroomerII unless a valid login user name and password is entered. GroomerII will continue the start-up process but the process will remain hidden by the Lock Computer screen.

CAUTION

The lock computer option is a standard Microsoft Windows function. Once this option is invoked, maintenance of all login user names and passwords is the responsibility of the user. The default login is Groomer User, with a blank password (Enter).

To set the `-l` switch, go to the Microsoft Windows Start – All Programs – Startup option, right click on GroomerII and then select Properties. You will now be presented with a standard Windows properties dialog.

In the properties dialog, select the `Shortcut` tab and amend the Target field by typing a space followed by `-l` at the end of the existing entry, for example:

From `"C:\Program Files (x86)\Aculab\GroomerII\grstart.exe"`

To `"C:\Program Files (x86)\Aculab\GroomerII\grstart.exe" -l`

Select OK to close the properties dialog, the lock computer function will now operate each time `grstart.exe` is run.

To unlock the lock computer screen, enter a valid login user name and password followed by OK. To re-lock the computer, select `Ctrl+Alt+Del` followed by Lock Computer.

2.3 Initial hardware checks

When GroomerII is powered on, it will go through the boot up sequence and shortly after Microsoft Windows has started the GroomerII Kernel and GroomerII Status Monitor dialogs will be displayed.

From the GroomerII Status Monitor dialog select the Alarms tab, where the status of each telephony port in the system is displayed.

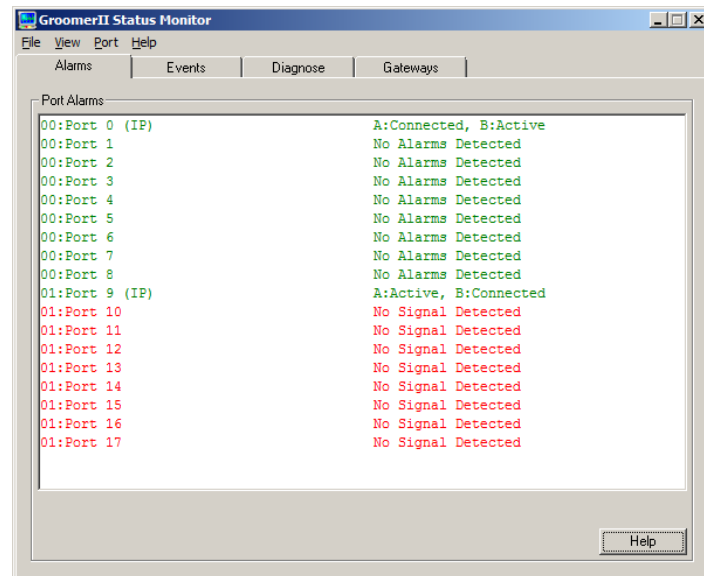


Figure 2-1 GroomerII status monitor alarms tab

The initial state of each port will be `Card Not Started`, and the port will remain in this state until the appropriate Prosody X card is fully started. Once a card has started check that

- The IP telephony link shows one port in the `Active` state,
- Each of the TDM ports shows `No Alarms Detected`.

If any other status is present then either there is no circuit attached (`A:Disconnected`, `B:Disconnected` or `No Signal Detected`), or a fault is present on the network. Faults should be resolved before call passing is attempted.

In the GroomerII Kernel dialog check that the Maintenance Messages panel has no error reports, for example configuration failures, and that there is a `CARD xxxxxx STARTED` message for each card in the system.

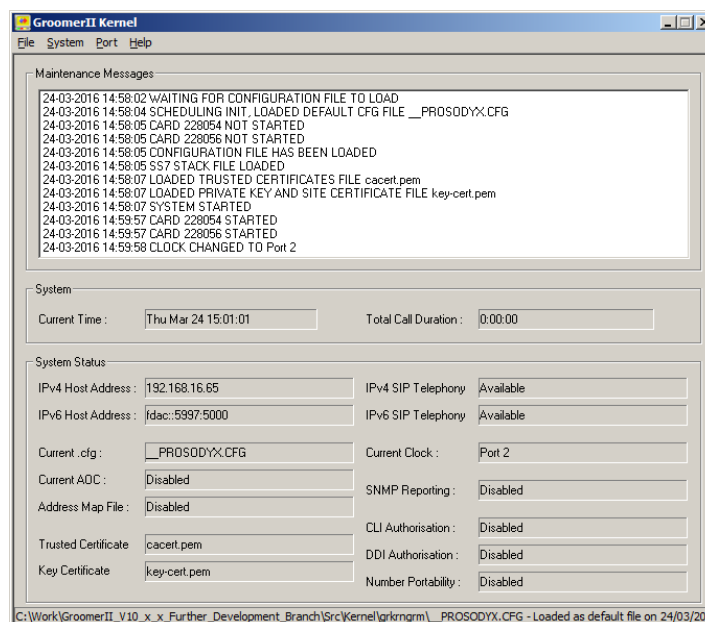


Figure 2-2 GroomerII Kernel

GroomerII is now ready to pass calls.

2.4 Basic fault finding

The following list provides examples of possible reasons for not receiving expected event messages.

Expected message	Possible cause of failure
Layer 1 ready (alarms page)	Check cabling / restart GroomerII or switch.
Layer 2 established	Check if you are using the Net or User ends of the protocol.
Incoming call	Log protocol. If you do not see a large RX string, the switch is not sending the call.
Called number	If there is no number shown you may not be able to route. If you are using CAS, check the digits are in the voice path.
Routing route 0-1	If no routing statement appears you may have a bad Layer 1 state on your outgoing port, or a suitable route could not be found. Check that the incoming group is included in the expected routing table entry.
Outgoing ringing	If you receive a Remote disconnect or call failed message at this point, check that the remote switch is set for incoming calls, or log protocol trace for details. If no message is seen then the call has passed through GroomerII but is waiting for an acknowledgement that a connection is being attempted.
Outgoing connected Incoming connected	The call has not yet switched through and is therefore not yet successful.
Remote disconnect	If you do not receive this message when attempting to clear down the call, use protocol trace to check that the remote switch is sending the disconnect/release.

Refer to section 15.3 for advanced fault finding and maintenance.

3 IP telephony network configuration

Before GroomerII can be used to pass traffic, the IP telephony resources must be configured with settings from your own network. This step must be carried out even if your system will not be making IP telephony calls. GroomerII supports IP telephony using both IPv4 and/or IPv6:

- If IPv4 telephony is to be used the host network adapter and each Prosody X card must be configured with IPv4 addresses.
- If IPv6 telephony is to be used the host network adapter and each Prosody X card must be configured with IPv6 addresses.

NOTE

GroomerII must be configured with static IP addresses. The use of DHCP to obtain dynamic IP addresses is not supported. The use automatically generated IPv6 addresses is not supported. Contact your network administrator to obtain the correct addresses and settings to be used.

3.1 Host network adapter configuration

3.1.1 IPv4 configuration

From the Microsoft Windows Network Connections window open the Internet Protocol Version 4 (TCP/IPv4) Properties window for the Local Area Connection. Configure the IP address, subnet mask, and any other parameters required, and then click the Advanced... button to open the Advanced TCP/IP Settings window.

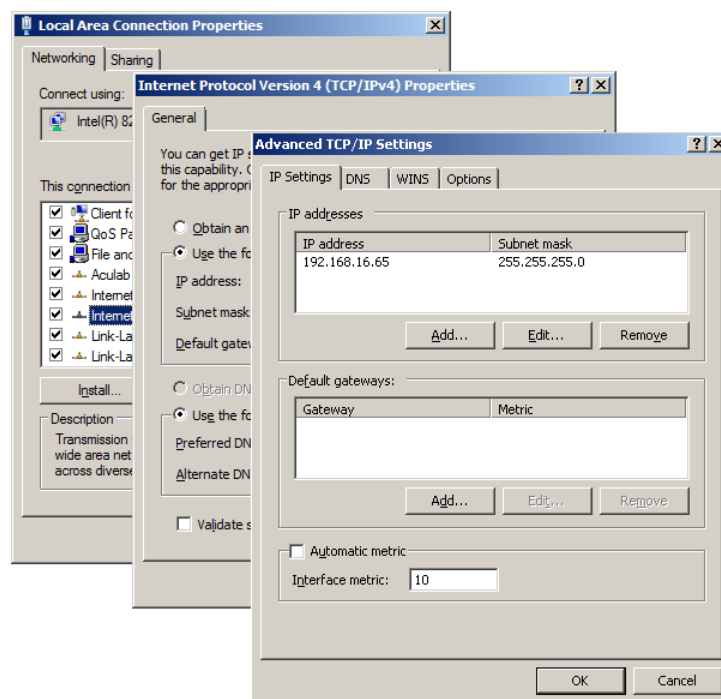


Figure 3-1 IPv4 host port configuration

Uncheck the Automatic metric checkbox, and set the Interface metric value to 10. All other fields should remain at their default settings.

3.1.2 IPv6 configuration

From the Microsoft Windows Network Connections window open the Internet Protocol Version 6 (TCP/IPv6) Properties window for the Local Area Connection. Configure the IP address, subnet prefix length, and any other parameters required, and then click the Advanced... button to open the Advanced TCP/IP Settings window.

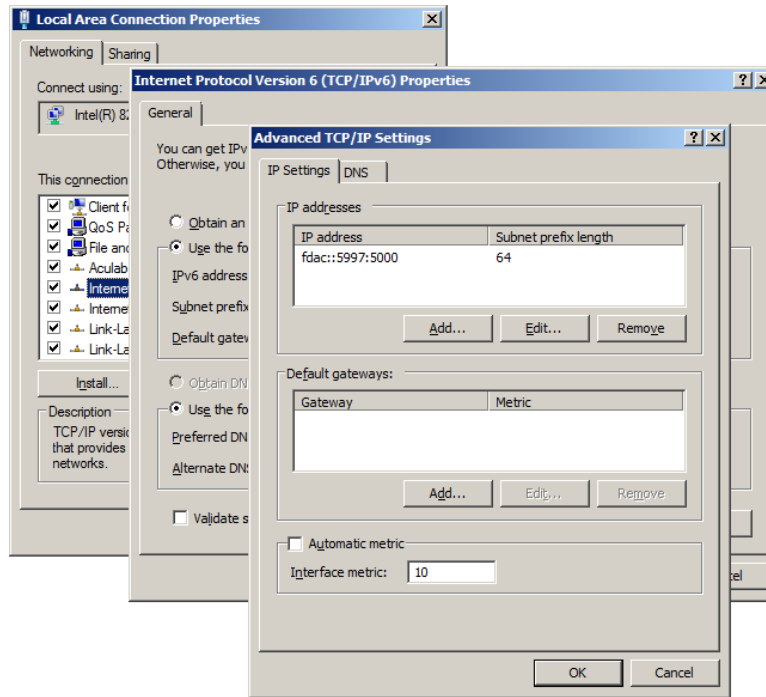


Figure 3-2 IPv6 host port configuration

Uncheck the Automatic metric checkbox, and set the Interface metric value to 10. All other fields should remain at their default settings.

3.2 Prosody X card configuration

The Prosody X card fitted in a GroomerII 1U (AC2460) chassis is configured for remote operation. It requires a single IP address to be assigned to the media port, which is used both to communicate with the host processor and to transmit and receive RTP traffic across the LAN.

In all other types of system each Prosody X card is configured for local operation and requires two IP addresses. When a Prosody X card is fitted a NIC driver is automatically installed to allow communication with the card across the PCIe bus, and each NIC driver must be assigned an IP address. The media port on each Prosody X card must also be assigned an IP address to allow RTP traffic to be received and transmitted across the LAN.

If you are configuring the system for IPv6 telephony, each Prosody X card will require a further IPv6 address for each DSP module fitted to the card.

The following steps must be carried out to configure the Prosody X cards in a system, and it is important that these steps are carried out fully and in the correct order.

- Configure the NIC address and routing metric for each Prosody X card in the system (all systems except GroomerII 1U (AC2460)).
- Configure the media port address for each Prosody X card in the system.
- Configure the DSP addresses for each Prosody X card in the system (IPv6 only).

- Configure the network connection order.
- Power cycle the system.

3.2.1 Configuring the Prosody X NIC address

The NIC address is configured from the Network Connections window. Select Network – Network and Sharing Center – Change adapter settings from the system Start menu to open this window.

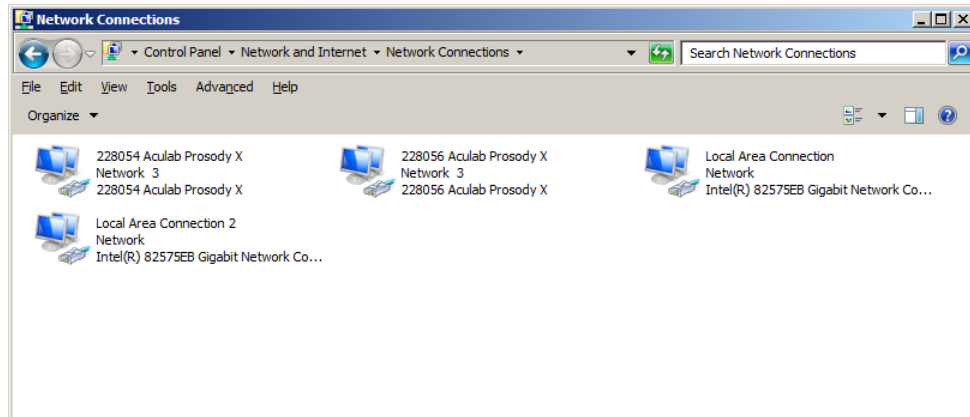


Figure 3-3 Microsoft Windows Network Connection window

Select the required card, identified by serial number, and open its Properties window using File – Properties.

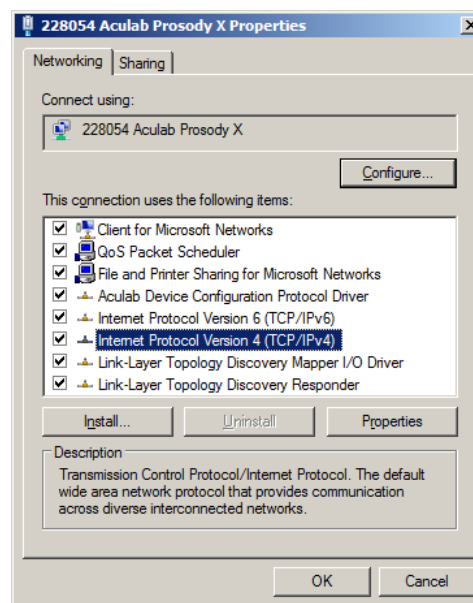


Figure 3-4 Microsoft Windows network connection Properties window

3.2.1.1 IPv4 configuration

In the network connection Properties window, select Internet Protocol Version 4 (TCP/IPv4) and click the Properties button to open the Internet Protocol Version 4 (TCP/IPv4) Properties window. Update the IP address and Subnet mask fields with the values obtained from your network administrator. The Default gateway field should be left blank. Click the Advanced... button to open the Advanced TCP/IP Settings window.

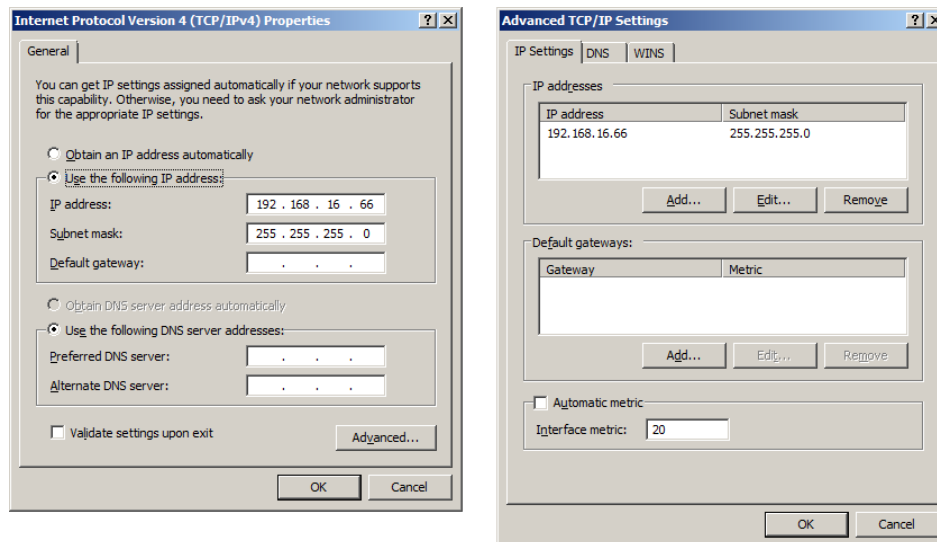


Figure 3-5 IPv4 Prosody X NIC address configuration

Uncheck the Automatic metric checkbox, and set the Interface metric value to 20. All other fields should remain at their default settings.

3.2.1.2 IPv6 configuration

In the network connection Properties window, select Internet Protocol Version 6 (TCP/IPv6) and click the Properties button to open the Internet Protocol Version 6 (TCP/IPv6) Properties window. Update the IPv6 address and Subnet prefix length fields with the values obtained from your network administrator. The Default gateway field should be left blank. Click the Advanced... button to open the Advanced TCP/IP Settings window.

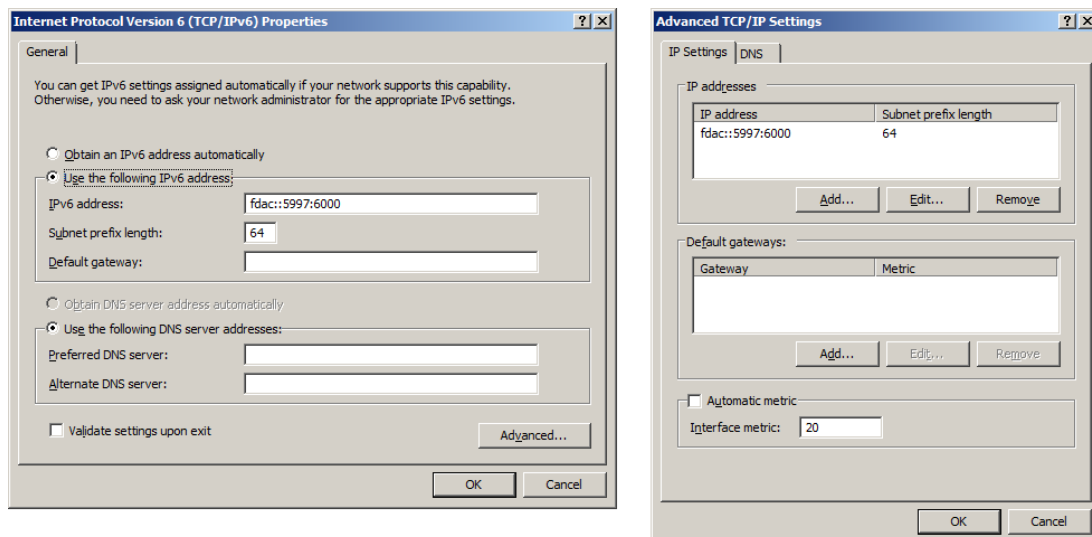


Figure 3-6 IPv6 Prosody X NIC address configuration

Uncheck the Automatic metric checkbox, and set the Interface metric value to 20. All other fields should remain at their default settings.

3.2.2 Configuring the Prosody X media addresses

The media port and DSP addresses are configured using the Aculab Configuration Tool (ACT). Select All Programs – Aculab – V6 - ACT from the system Start menu to open the ACT.

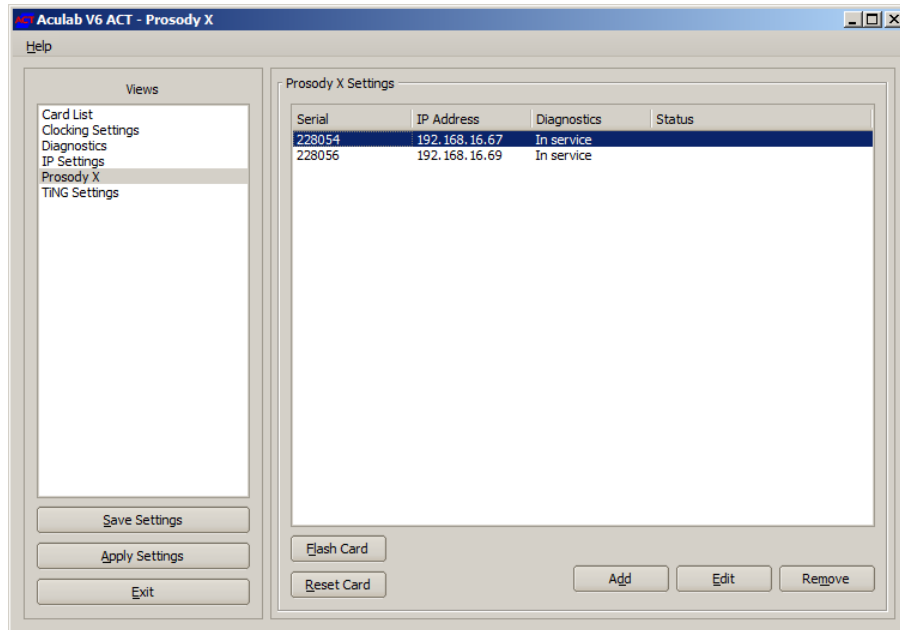


Figure 3-7 ACT - Prosody X Settings page

From the ACT startup window select Prosody X to display the Prosody X Settings page, select the card to be configured, and click the Edit button to open the ACT: Editing Prosody X Card dialog.

NOTE

If you are configuring a GroomerII 1U (AC2460) and the Prosody X card is not listed in the Prosody X Settings page, you must first add the card as described in section 4.8.

For a more detailed explanation of the ACT see section 4.

CAUTION

All Prosody X cards support the G.729AB codec, whose use is subject to license payments. If you are intending to use this codec, please read Appendix C: to establish whether such payments are required.

3.2.2.1 IPv4 configuration

In the ACT: Editing Prosody X Card dialog tick the IPv4 checkbox and select the Static radio button followed by the IPv4 Settings tab. Update the Basecard IP address, Subnet mask and (if required) Default gateway fields with the values obtained from your network administrator.

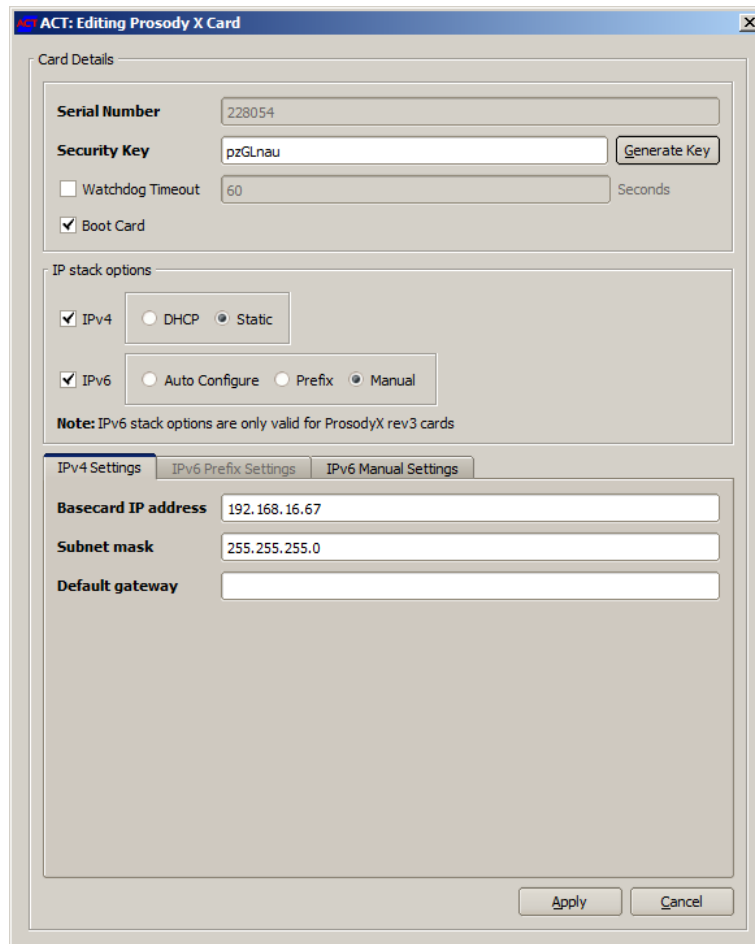


Figure 3-8 ACT - Prosody X Settings page

3.2.2.2 IPv6 configuration

In the ACT: Editing Prosody X Card dialog tick the IPv6 checkbox and select the Manual radio button followed by the IPv6 Manual Settings tab. Use the values obtained from your network administrator to update the Base Card IP address, Subnet prefix length, Default gateway (if required) fields, along with each of the fields in the Speech DSP IP addresses group.

NOTE

If the Prosody X card being configured is fitted with less than four DSP modules, some fields in the Speech DSP IP addresses group will be disabled.

The screenshot shows the 'ACT: Editing Prosody X Card' dialog box. The 'Card Details' section includes fields for 'Serial Number' (228054), 'Security Key' (pzGLnau), a 'Watchdog Timeout' of 60 seconds, and a checked 'Boot Card' checkbox. The 'IP stack options' section shows 'IPv4' checked with 'Static' selected, and 'IPv6' checked with 'Manual' selected. A note states: 'Note: IPv6 stack options are only valid for ProsodyX rev3 cards'. The 'IPv6 Manual Settings' tab is active, showing 'Base Card IP address' (fdac::5997:6010), 'Subnet prefix length' (64), and 'Default gateway'. Below this is the 'Speech DSP IP Addresses' section with four rows: 'DSP 0' (fdac::5997:6020), 'DSP 1' (fdac::5997:6021), 'DSP 2' (fdac::5997:6022), and 'DSP 3' (fdac::5997:6023). 'Apply' and 'Cancel' buttons are at the bottom right.

Figure 3-9 ACT - Prosody X Settings page

3.2.2.3 Restarting the card

When the updates are complete, tick the Boot Card checkbox and close the dialog using the Apply button. The card will restart and the Status column entry will change to Discovering. Wait until the card has cycled through its bootup states and returned to In service before configuring the next card. This may take several minutes.

3.3 Setting the network connection order

The network connection order is configured from the Network Connections window. Select Network – Network and Sharing Center – Change adapter settings from the system Start menu to open this window. Open the Advanced Settings dialog box using the Network Connections – Advanced – Advanced Settings... menu option.

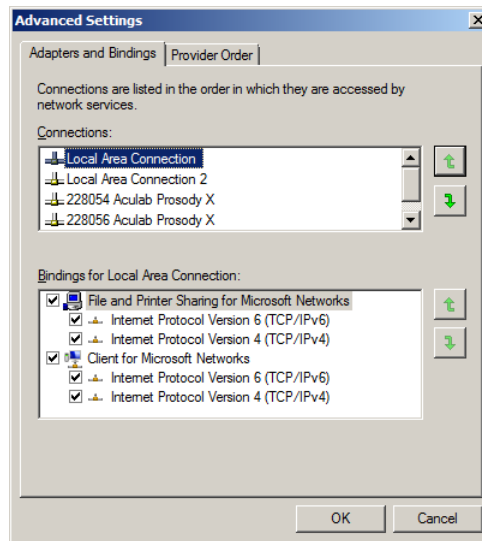




Figure 3-10 Microsoft Windows Advanced Settings window

In the Connections pane use the   buttons to place the network connections in the following order

Local Area Connection

Local Area Connection 2

Local Area Connection 3 (1U (AC2460) and 2U (R720 and R730) systems only)

Local Area Connection 4 (2U (R720 and R730) systems only)

Card 0 : Aculab Prosody X (xxxxxx) (all systems except 1U (AC2460))

Card 1 : Aculab Prosody X (xxxxxx) (when fitted)

Card 2 : Aculab Prosody X (xxxxxx) (when fitted)

Card 3 : Aculab Prosody X (xxxxxx) (when fitted)

Any other connections present should follow the above, with the order in which these are placed being unimportant.

3.4 Completing the configuration

When all cards have been configured and restarted power cycle your system.

4 Configuring GroomerII cards

4.1 Introduction

The Aculab configuration tool (ACT) is a generic Aculab utility program used by GroomerII to configure cards and protocols.

The GroomerII application can only function with cards properly installed and configured in the system.

4.1.1 Restrictions

- You must be logged in as a user with administrative privileges to use the ACT.
- The ACT must never be used to reload firmware or restart cards when GroomerII is running.

4.2 Starting the ACT application

Start the Aculab Configuration Tool by selecting All Programs – Aculab - V6 - ACT from the system Start menu.

4.2.1 Startup messages

A splash screen will be displayed whilst the Aculab Configuration Tool (ACT) is initialising.



Figure 4-1 ACT splash screen

4.3 Overview

Once the configuration tool has started, the application window will appear. The application will now search for installed cards, which will be displayed in the Card List pane. Finding all of the cards and displaying them may take some time.

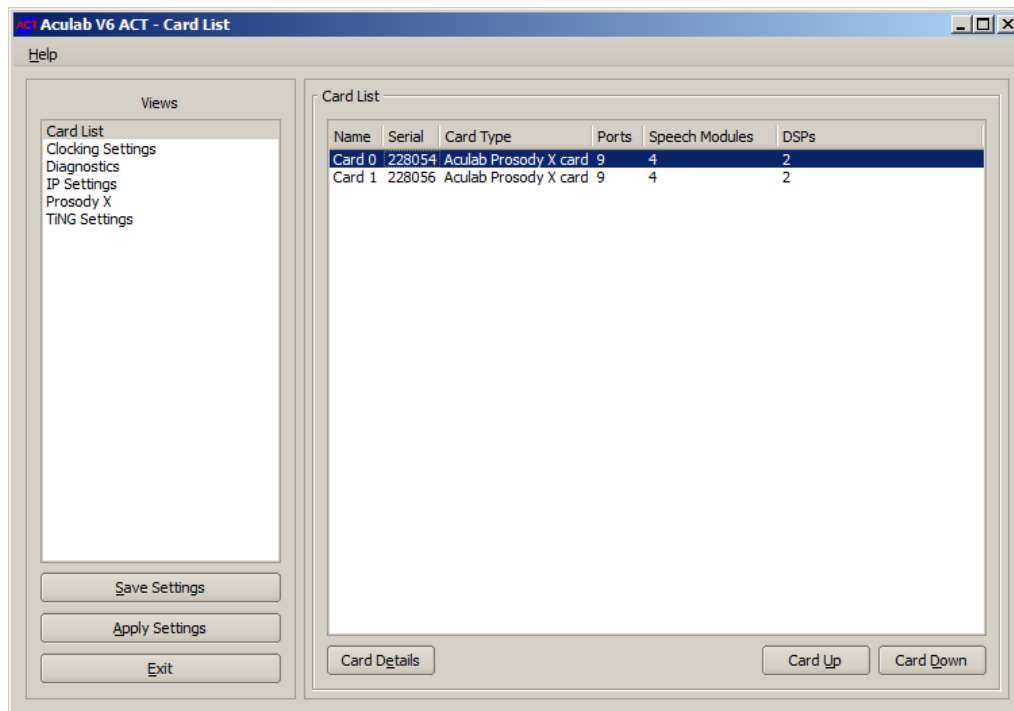


Figure 4-2 ACT startup window

NOTE

A Prosody X card will not appear in this list until it reaches the In Service state.

The following controls are available in the application window.

Views - Use the entries in the Views list to navigate between the top level configuration pages.

Save Settings - Click the Save Settings button to save the current configuration changes without closing the ACT or downloading the changes to the cards.

Apply Settings - Clicking the Apply Settings button will save any configuration changes made, download the configuration to all cards, and close the ACT.

Exit - Click the Exit button to close the application and discard any unsaved changes.

4.3.1 Card List

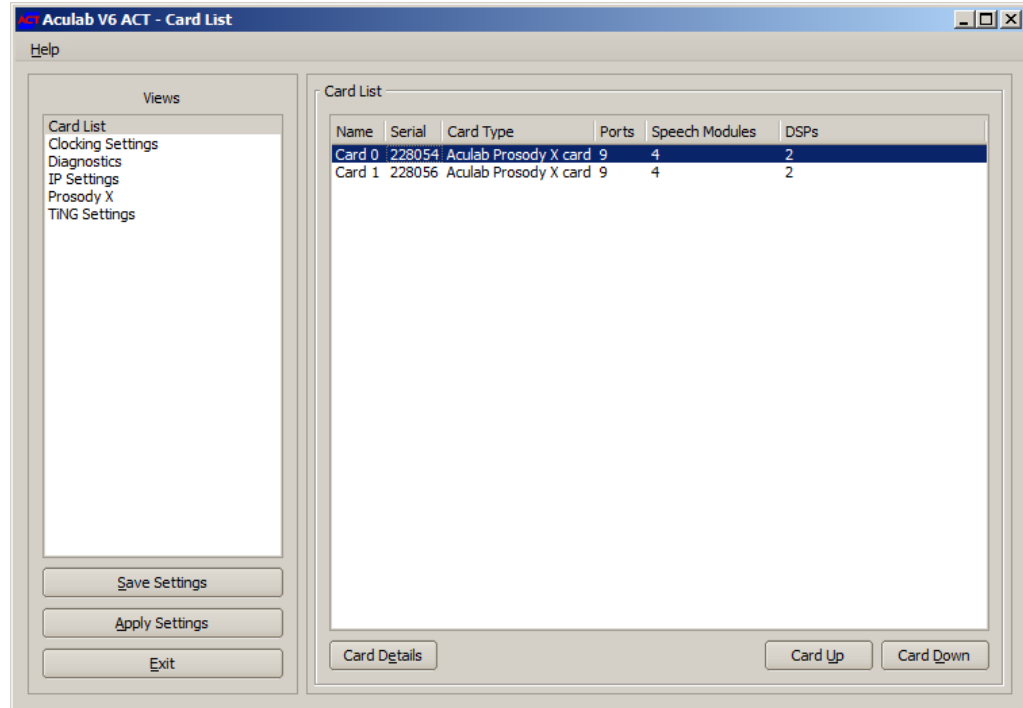


Figure 4-3 ACT card list page

Fields

In this example, when you select Card List, the list shows that two cards have been detected in the system. Each entry shows the hardware configuration details and unique serial number of a specific card.

NOTE

A Prosody X card will not appear in this list until it reaches the In Service state. To reach the In Service state a Prosody X card must have been configured in the Prosody X page.

Buttons

Card Details - Used to configure the TDM ports on a card. Select a card from the list followed by Card Details, or double click on a card entry. This will open a Card Details page for the selected card.

The port firmware and protocol switches will require configuration before the card can be used.

Card Up and **Card Down** – Use these buttons to place the cards into the order that they are installed in the chassis.

NOTE

GroomerII uses this order when assigning port numbers. It is important that the card ordering in this screen remains the same as the physical ordering in the chassis.

When viewing a 2U chassis (CG2100) from the rear the upper card should appear at the top of the list and the lowest card at the bottom of the list.

The table in section 1.6.2 illustrates the card positions for a 2U chassis (R720 and R730).

CAUTION

Changes to the card ordering are saved as they are made. Closing the ACT using the Cancel Changes button will NOT discard any changes made to the order of the card list. Such changes can only be cancelled by manually restoring the original order.

The process for configuring card port details is documented in section 4.4.

4.3.2 Clocking settings

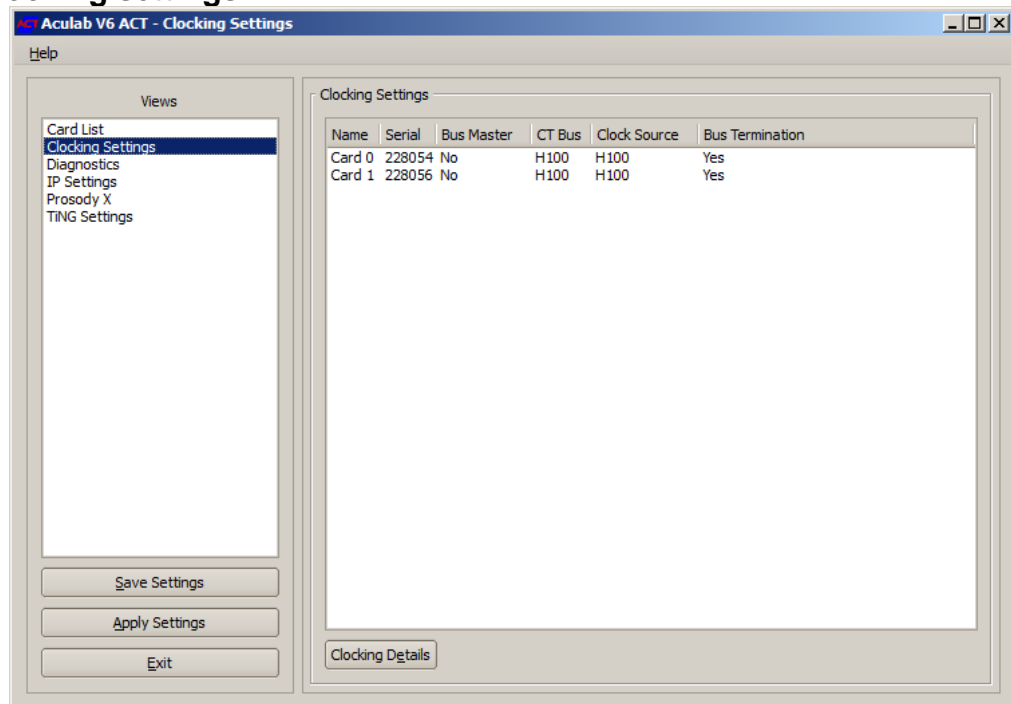


Figure 4-4 ACT clocking settings page

Fields

As with Card List, this selection shows that two cards have been detected in the system. In this instance however, each entry will show the clocking configuration details of each card.

CAUTION

The cards listed in this screen may not be displayed in their installed order.

Buttons

Clocking Details – Used to configure clocking parameters, select a card from the list followed by Clocking Details to open a Clocking Details page for the selected card.

NOTE

Where two or more cards are installed bus termination must be applied to the cards physically located at each end of the H.100 bus, which are the first and last cards in the Card List page.

The exception to this is when a 2U chassis (R720 and R730) is fitted with three or four cards. In this case, bus termination must be applied to the second and third cards in the Card List page.

The process for configuring card clocks is documented in section 4.5.

4.3.3 Diagnostics

The diagnostics option provides the facility to check your system looking at the status of services, current configurations, file versions, and system logs.

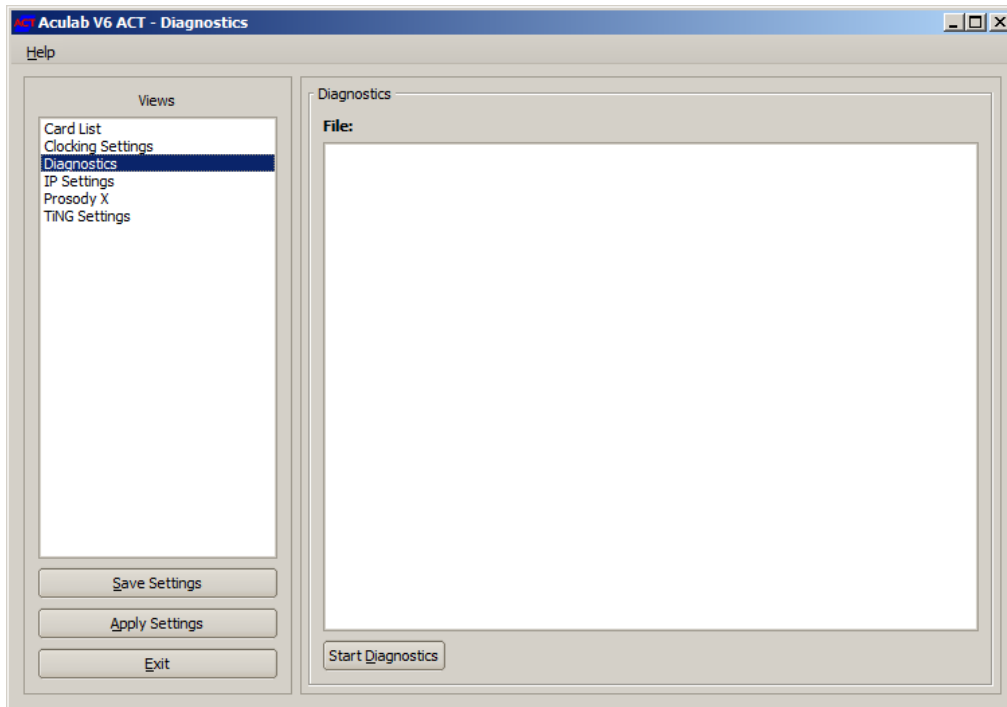


Figure 4-5 ACT diagnostics page

Diagnostics

The dialog area includes:

File: - displays the location of the HTML file that is generated after you run diagnostics, the contents of which will appear in the display area.

Start Diagnostics – select this button to run system diagnostics. A Clear Diagnostics button replaces the Start Diagnostics button once a system diagnosis has been completed.

During diagnostics, the following information is obtained:

Troubleshooting – an optional entry that is only completed if a problem is identified.

Operating System – operating system version, service pack details etc.

System log – log history.

Aculab Path – Aculab root directory.

System Path – path details for key system and Aculab application files.

File Versions – Aculab application files.

Versions – hardware details of Aculab cards detected in the system.

Configuration Files – configuration file details.

IP Telephony – run time IP service configuration details.

Registered Prosody IP Cards – lists the Prosody X cards installed in the system.

OS Specific Output – operating system configuration, devices, running services, etc.

4.3.4 IP settings

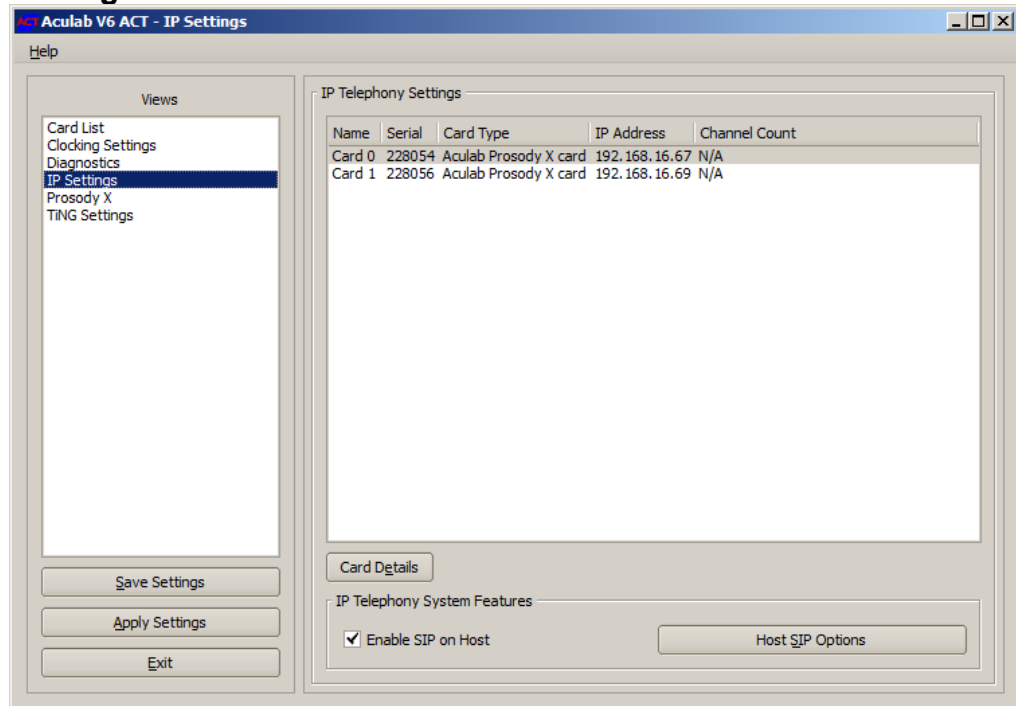


Figure 4-6 ACT IP settings page

Fields

IP Telephony settings - This pane will list the Prosody X cards that have been detected in the system, and includes the IP address assigned to the media port on the card.

CAUTION

The cards listed in this screen may not be displayed in their installed order.

IP Telephony System Features – The controls in this group apply to all Prosody X cards in the system. This group contains a single checkbox:

Enable SIP on Host – Indicates whether the SIP service should be loaded. This box must remain checked at all times.

Buttons

Card Details – This button accesses the configuration parameters for the Aculab IP Telephony card. GroomerII does not support this card, and this button should be ignored.

Host SIP Options – This button is used to open the SIP Protocol Options dialog box.

NOTE

The settings in this dialog box are not used by GroomerII, and should be left at their default values.

4.3.5 Prosody X

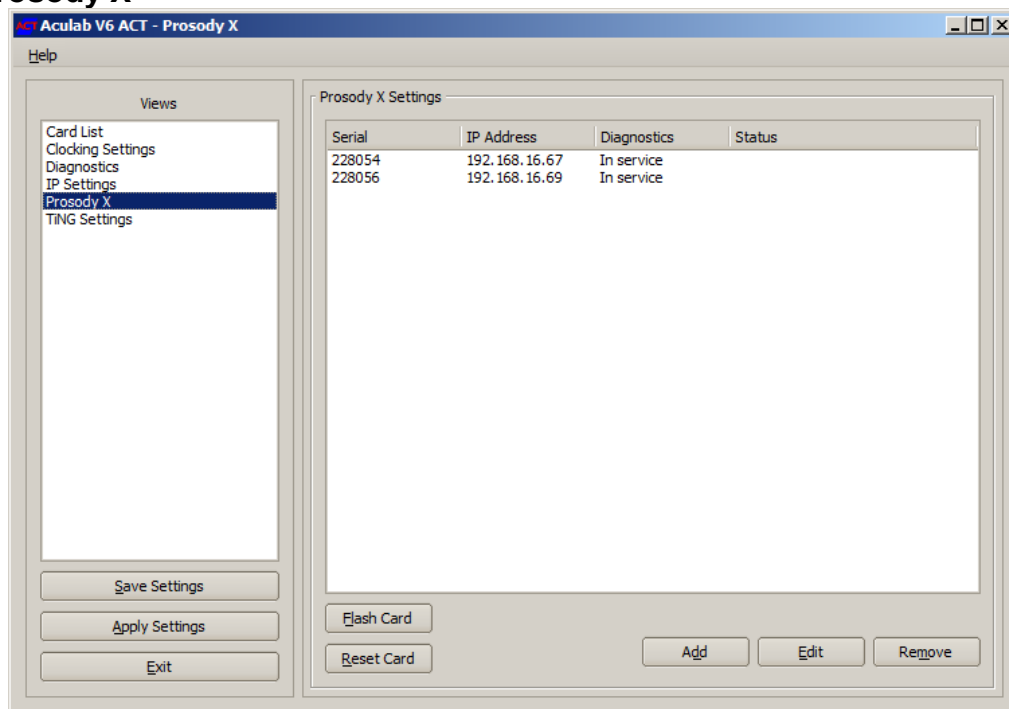


Figure 4-7 ACT Prosody X page

Fields

This page will list all of the Prosody X cards installed in your system. The cards will appear in this screen from system startup. The IP address of the media port, along with the service status is displayed for each card. When a cards status reaches In Service the card will also be listed in the Card List page. The Card List page is documented in section 4.3.1.

CAUTION

The cards listed in this screen may not be displayed in their installed order.

Buttons

Flash Card – This button will display the Flash Card page, which allows the firmware on the Prosody X card to be updated. This operation is detailed in section 4.7.

Reset Card – This button will cause the selected card to be restarted. When the button is pressed a Reset Card countdown dialog will appear. Selecting OK will cause the card to be restarted immediately. Selecting Cancel will prevent the card from being restarted. When the countdown reaches zero the card will be started.

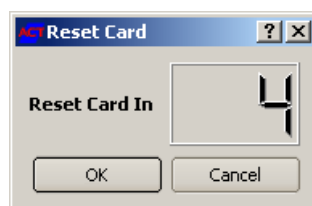


Figure 4-8 ACT Reset Card dialog

CAUTION

If a Prosody X card is restarted all calls in progress will be lost. This is generic ACT functionality, and it is generally not necessary to restart cards in GroomerII. It is recommended that this functionality should only be used under the direction of Aculab support.

Add – This button should be used only when you are configuring a GroomerII 1U (AC2460) chassis, and the Prosody X card is not already listed in the Prosody X Settings pane. If the Prosody X card is already listed in the Prosody X Settings pane use the Edit button to configure the card. This button must not be used when configuring any other type of chassis.

Edit – Used to configure the Prosody X card parameters. Select a card from the list followed by Edit, or double click on a card entry, to open an edit dialog for the selected card.

Remove – Use this button to remove all drivers associated with the card before removing it from the chassis.

NOTE

Should this button be accidentally pressed, it will remove the selected card from the system. To restore the card:

- If your system is a GroomerII 1U (AC2460) use the Add button to add and configure the card.
- For all other types of system, restart the system and configure the card parameters using the Edit button.

The process for configuring Prosody X card parameters is documented in section 4.8.

4.3.6 TiNG settings

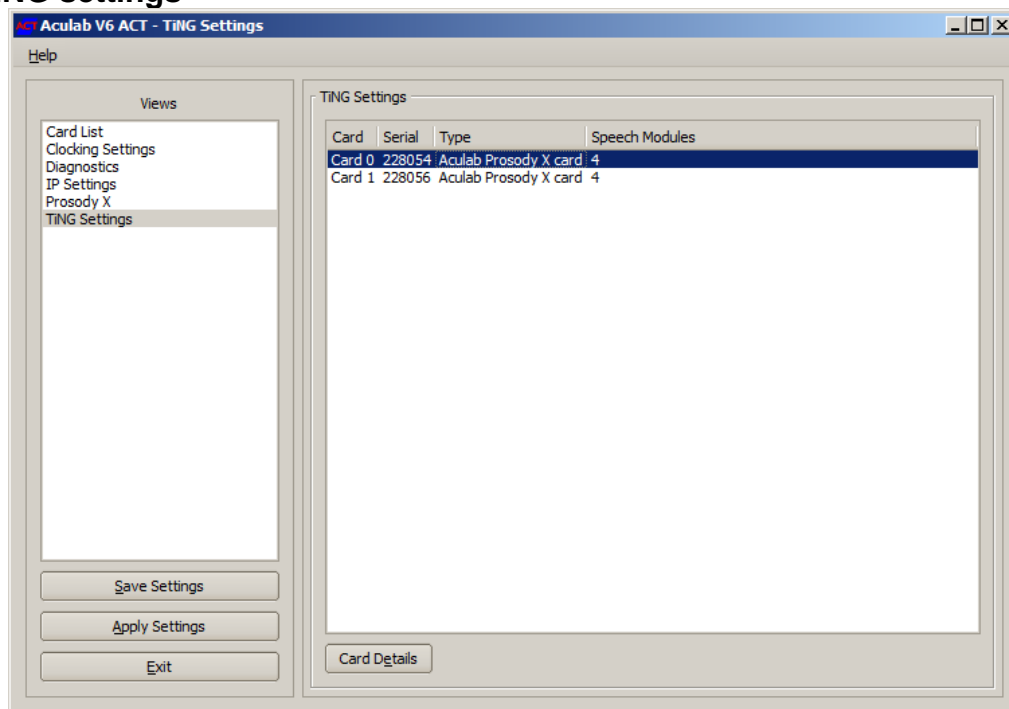


Figure 4-9 ACT TiNG settings page

Fields

This example shows that two Prosody X cards have been detected, and shows the number of DSP modules available on each card.

CAUTION

The cards listed in this screen may not be displayed in their installed order.

Buttons

Card Details – Used to configure the TiNG parameters for each of the Prosody DSP modules. Select a card from the list followed by Card Details, or double click on a card entry, to open a TiNG Firmware Selection dialog for the selected card.

The TiNG Firmware Selection dialog is used to select which TiNG firmware is loaded to each Prosody DSP module on the card. This process is documented in section 4.9.

4.4 Configuring card TDM port details

As detailed in section 4.3.1, select a card from the Card List followed by Card Details, or double click on a card entry from the card list. This will open a Card Details page for the selected card.

Aculab V6 ACT - Card List

Help

Card 228054: Card Details Page

Name: Card 0

Card Type	Aculab Prosody X card	Ports	9
Serial Number	228054	Speech DSPs	4
PM 1 Type	PMX 8 PORT EIT1	Trunk DSPs	2
PM 2 Type	Not Present		

Port Protocols

Port Number	Name	Protocol	Protocol Switches	Port Init
0	228054:P0	ETS 300 User PMX	-s91,1 -s99,224 -s96,0	Yes
1	228054:P1	ETS 300 User PMX	-s91,1 -s99,224 -s96,0	Yes
2	228054:P2	ETS 300 User PMX	-s91,1 -s99,224 -s96,0	Yes
3	228054:P3	ETS 300 Net PMX	-s91,1 -s99,224 -cNE -s96,0	Yes
4	228054:P4	ETS 300 User PMX	-s91,1 -s99,224 -s96,0	Yes
5	228054:P5	ETS 300 User PMX	-s91,1 -s99,224 -s96,0	Yes
6	228054:P6	ETS 300 User PMX	-s91,1 -s99,224 -s96,0	Yes
7	228054:P7	R2T1 PMX	-s59,1 -s14,1 -s96,1 -s1 -s99,224	Yes
8	228054:P8	SIP Port		Yes

Port Details OK Cancel

Figure 4-10 ACT card details page

Subject to the facilities available and the required function of each card, there are a number of options that may need to be set before the card can be fully utilised.

Card detail fields

Name - an optional card details field, used by some systems as a customer specified identifier. Enter a new name as required. GroomerII does not support this option.

Card Type - the product description hard coded onto the card. This will be Aculab Prosody X card.

Serial Number - the unique card identifier hard coded onto the card.

PM 1 Type – indicates the number of TDM ports fitted to the card.

PM 2 Type - this field is not used by GroomerII and will always read Not Present.

Ports - the total number of TDM and IP telephony ports available on the card.

Speech DSPs - this is the number of media DSPs fitted to a Prosody X card.

Trunk DSPs – this is a legacy field and will always read 2.

Port detail fields

Port Protocols - a list of the ports on the card and the current protocol and firmware switch settings of each port. A Prosody X card will list a SIP port in addition to the TDM ports. The SIP port cannot be configured, and the entry cannot be selected.

Buttons

Port Details – used to configure TDM port protocol firmware and switches.

OK – select to confirm any changes and close the card details page.

Cancel – select to discard any changes and close the card details page.

4.4.1 Protocol selection

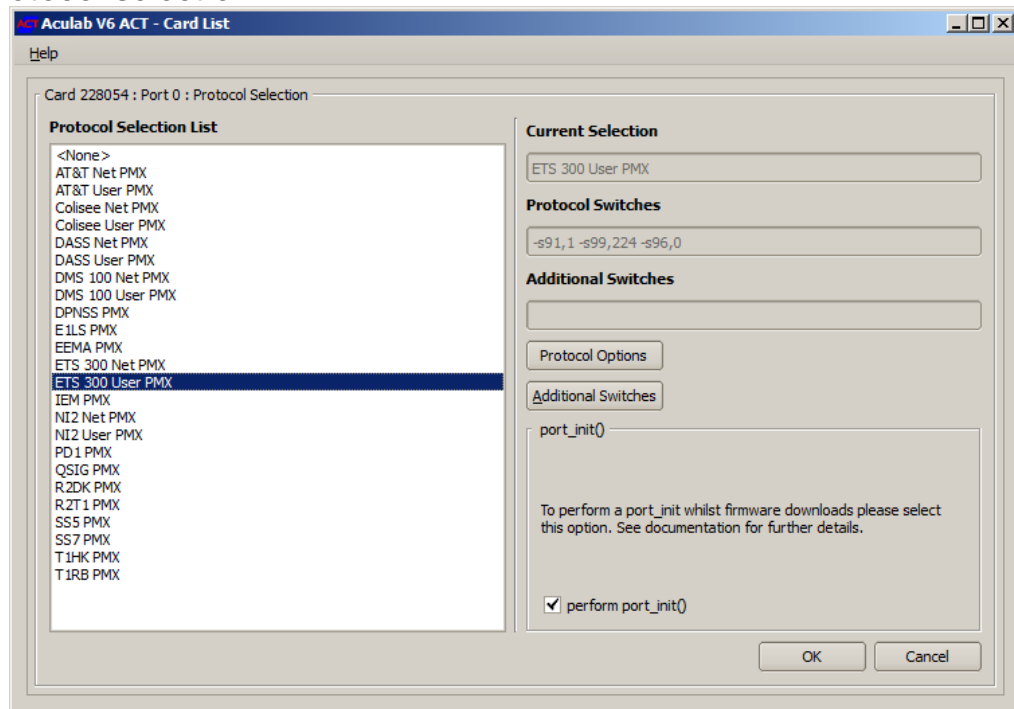


Figure 4-11 ACT port protocol selection page

The Protocol Selection page is used to select and configure the signalling protocol to be loaded onto a TDM port.

The behaviour of the protocol firmware can be modified by the addition of configuration switches. The more commonly used configuration switches can be applied from the user interface that is accessed using the Protocol Options button. These settings will be listed in the Protocol Switches field. Those switches that are not supported by the user interface can be added using the Additional Switches button, and will be displayed in the Additional Switches field.

Details of the configuration switches that can be applied to each protocol are documented in the firmware release notes. Firmware release notes are located in the C:\Program Files (x86)\Aculab\v6\Firmware folder with filenames in the form *_switches.txt. For example the file ets300_switches.txt describes the configuration switches that can be applied to the ETS 300 firmware.

A small number of configuration switches are not included in the firmware release notes, and details of these can be found in Appendix D:.

Select a protocol

Select the required protocol from the Protocol Selection List; this will be displayed in the Current Selection field. Any default switches applied will be displayed in the Protocol Switches field.

The perform port_init() control is not used by GroomerII, its selection will be ignored.

4.4.2 Protocol configuration (excluding SS7)

You can also select and configure switches by selecting Protocol Options to open the Switch Options page for the selected protocol.

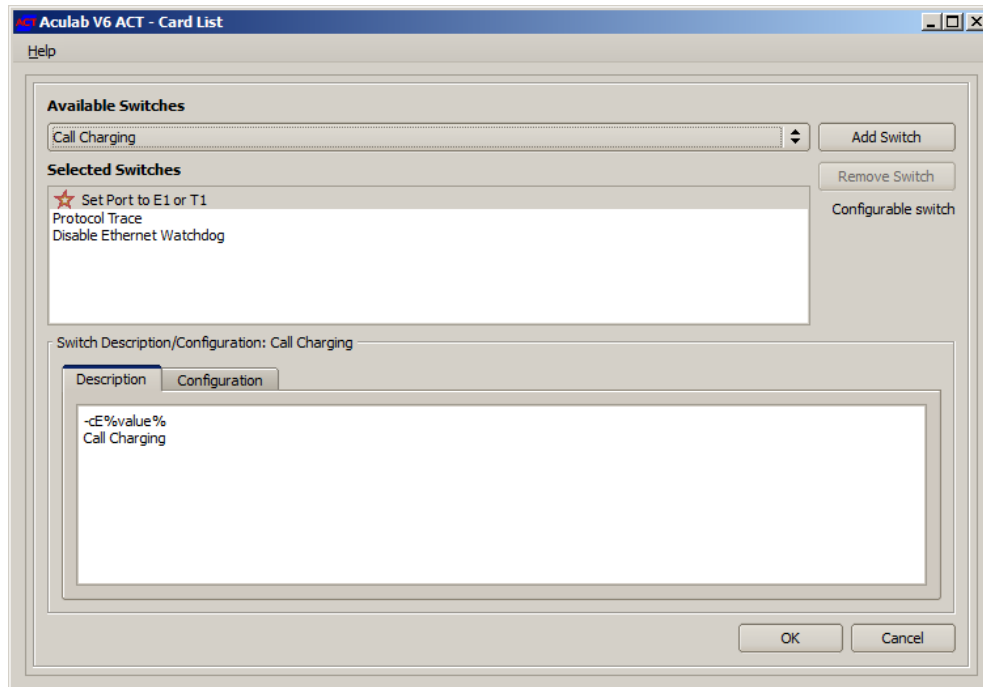


Figure 4-12 ACT port protocol switch selection page (non SS7)

The Available Switches field is a popup list of the switches that may be configured for this protocol.

NOTE

This list is not guaranteed to contain all the switches that may be applied to a protocol.

Any switches already selected will be displayed in the Selected Switches list. A configurable switch will be indicated by a star.

Clicking on a switch in either the Available Switches or Selected Switches lists will display a description of that switch in the Switch Description/Configuration field.

Add a switch

To add a switch to the protocol, select the switch from the Available Switches popup list then click Add Switch. The entry will then be moved from the Available Switches list to the Selected Switches list.

Configuring a switch

To configure a switch select it in the Selected Switches list. Controls that allow the configurable parameters to be set will be displayed in the Switch Description tab. To edit the selection, select the Configuration tab. If a non-configurable switch has been selected, the fields in the Configuration tab will be disabled.

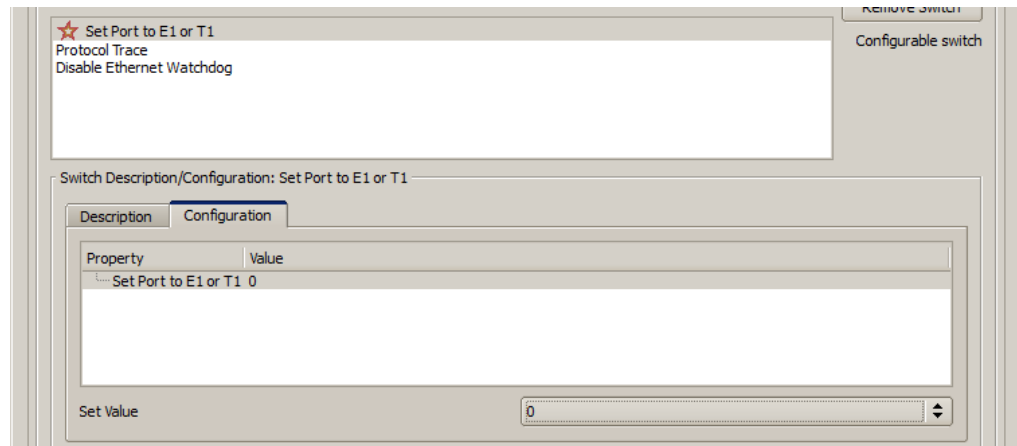


Figure 4-13 ACT switch configuration tab

For details of the valid values, please refer to the firmware release notes for the selected protocol or Appendix D: as required.

To change a value, make a selection from the Set Values popup list.

Remove a switch

To remove an entry from the Selected Switches list, Select the entry followed by Remove Switch.

Once you are satisfied with your switch selections, select OK to return to the Protocol Selection page.

Confirming port details

When you are satisfied with your port configuration, select OK to accept, or Cancel to discard, any changes and return to the Card Details page. You will be prompted to confirm you changes by the Port Settings Dialog.

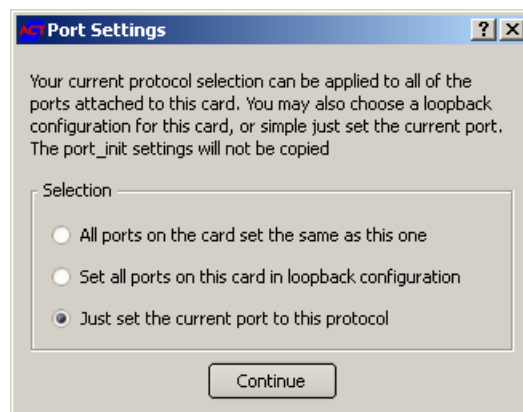


Figure 4-14 ACT port settings confirmation dialog

Make a selection based on the descriptions followed by Continue. You will now be returned to the Card Details Page dialog.

Configure any remaining ports as required.

When you are satisfied with your entire ports configuration, select OK to accept, or Cancel to discard, any changes and return to the Card List dialog.

4.4.3 Protocol configuration for SS7

In the Protocol Selection page, when you select the SS7 PMX protocol followed by Switch Options, you will be presented with an SS7 Protocol Configuration page. This allows you to configure individual port timeslots either as SS7 signalling links or as ISUP bearers.

NOTE

Please refer to section 15 for details on how to configure SS7 links by editing the SS7 stack file `ss7.cfg`

SS7 Signalling tab

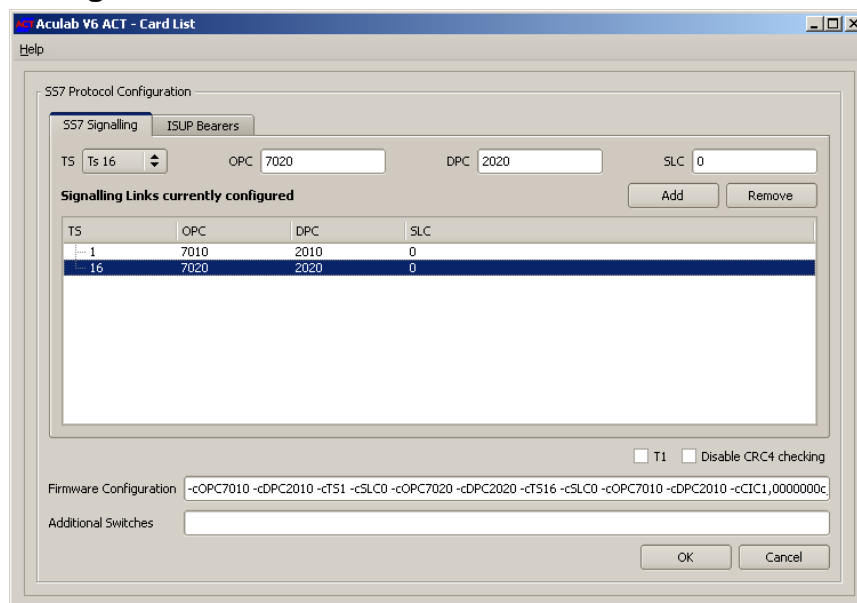


Figure 4-15 ACT port protocol configuration page (SS7 Signalling)

Subject to any system constraints, for example, excluding TS 0 on an E1 port, use the SS7 Signalling tab to define which timeslots on the port are to be used as SS7 signalling links.

To assign a timeslot as a signalling link select the appropriate timeslot (TS), set the appropriate OPC, DPC, and SLC parameters as described below, and then select Add.

TS – Used to select the signalling timeslot to which the settings are to be applied. If the T1 control is checked only timeslot in the range 0-23 will be presented, otherwise timeslots in the range 1-31 will be available.

NOTE

The OPC, DPC and SLC settings are derived from information supplied by your service provider.

OPC – This is point code used to identify GroomerII.

DPC – This will usually be the point code of the SP or STP to which GroomerII is directly connected. Exceptionally, this may be the identity of a distant SP or STP.

NOTE

Point codes will be in the range 1-16383 when using the ITU-T or UK ISUP variants, 1-16777215 when using the ANSI or CHINA variants.

SLC – SLC is a unique numeric Signalling Link Code between zero and fifteen (0 - 15), allowing you to define up to sixteen SS7 signalling timeslots per set of point codes.

Add – Select to add the parameters for the selected timeslot to the Signalling Links currently configured list.

Remove – Select to remove the highlighted entry from the Signalling Links currently configured list.

ISUP Bearers tab

Aculab V6 ACT - Card List

Help

SS7 Protocol Configuration

SS7 Signalling ISUP Bearers

OPC 7010 DPC 2010 CIC Base 1

Map Display Type
☒ Hexadecimal
☐ Decimal

CIC Map ffffffff
 Circuit Map ffffffff

ISUP Bearers currently configured

OPC	DPC	CIC Base	CIC Map	Circuit Map
7010	2010	1	fffffff	fffffff

Add Remove

☐ T1 ☐ Disable CRC4 checking

Firmware Configuration -cOPC7010 -cDPC2010 -cTS1 -cSLC0 -cOPC7020 -cDPC2020 -cTS16 -cSLC0 -cOPC7010 -cDPC2010 -cCIC1,ffffffff,ff

Additional Switches

OK Cancel

Figure 4-16 ACT port protocol configuration page (ISUP bearers - hexadecimal)

Aculab V6 ACT - Card List

Help

SS7 Protocol Configuration

SS7 Signalling ISUP Bearers

OPC 7010 DPC 2010 CIC Base 1

Map Display Type
☐ Hexadecimal
☒ Decimal

CIC Map 2-15:17-31
 Circuit Map 2-15:17-31

ISUP Bearers currently configured

OPC	DPC	CIC Base	CIC Map	Circuit Map
7010	2010	1	2-15:17-31	2-15:17-31

Add Remove

☐ T1 ☐ Disable CRC4 checking

Firmware Configuration -cOPC7010 -cDPC2010 -cTS1 -cSLC0 -cOPC7020 -cDPC2020 -cTS16 -cSLC0 -cOPC7010 -cDPC2010 -cCIC1,2-15:17-31

Additional Switches

OK Cancel

Figure 4-17 ACT port protocol configuration page (ISUP bearers - decimal)

The ISUP Bearers tab is used to define which timeslots on the port you wish to use as ISUP bearers. Each timeslot must be assigned an OPC, DPC and CIC before it can be used as a bearer.

NOTE

The OPC, DPC, CIC Base, CIC Map and Circuit Map settings are derived from information supplied by your service provider.

OPC – This is the point code used to identify GroomerII.

DPC – The point code of the destination SP or STP. This may be the adjacent node, or another distant node on your network via onward SS7 links.

NOTE

Point codes will be in the range 1-16383 when using the ITU-T or UK ISUP variants, 1-16777215 when using the ANSI or CHINA variants.

CIC Base – CIC Base is the number assigned to the first timeslot allocated a Circuit Identification Code on a port/trunk. The CIC number range used on one port/trunk to a given DPC must not overlap with the number range assigned to other ports/trunks to the same DPC. For example, assuming that you are assigning CIC to all timeslots (excluding TS0) to multiple E1 ports/trunks to a single DPC, the CIC Base would typically be 1 for the first port, 33 on the second port and so on in steps of 32. Individual CIC values will be assigned sequentially to each timeslot identified in the CIC map.

Map Display Type – Use the controls in this group to specify whether you wish to enter the CIC Map and Circuit Map using hexadecimal or decimal notation. Changing the selection will convert the current value in each field between the two formats.

CIC Map – The CIC Map value represents the timeslots on the link that are to be assigned a CIC. For details of how to calculate the value for this field, see the timeslot-mapping example below.

Circuit Map – The Circuit map value defines which timeslots are to be used as bearers. For details of how to calculate the value for this field, see the timeslot-mapping example below.

Add – Select to add the parameters for this port to the ISUP Bearers currently configured table.

Remove – Select to remove the selected entry from the ISUP Bearers currently configured table.

Common controls

The following controls are accessible from both the SS7 Signalling and ISUP Bearers tabs.

T1 – Checking the T1 check box will validate the settings for a T1 trunk, otherwise validation will be carried out for an E1 trunk.

Disable CRC4 checking – Checking the Disable CRC4 Checking check box disables cyclic redundancy checking on this port.

Firmware Configuration – Each time you add an SS7 Signalling link or ISUP Bearers to the port, the required switch parameters are added to the string of firmware configuration switches and displayed in this read only field.

Additional Switches – This field allows configuration switches that are not supported by on-screen controls to be added to the port, and performs the same function as the Additional Switches dialog described in section 4.4.4.

OK – Use the OK button to save your changes and return to the Protocol Selection page.

Cancel – Use the Cancel button to discard your changes and return to the Protocol Selection page.

Timeslot mapping

Timeslot mapping is needed to ascertain which timeslots will be assigned a CIC, and which timeslots will be used as bearers.

Specifying hexadecimal timeslot maps

A 32-bit binary hexadecimal code is used to represent the selection of timeslots on an E1 trunk, and a 24-bit hexadecimal code to represent the timeslots on a T1 trunk. A binary zero represents a timeslot that has not been selected; a binary one represents a selected timeslot, the following examples shows timeslots 1 to 31 being selected on an E1 trunk, and 0 to 22 being selected on a T1 trunk:

```

31                                     0      TS/circuit
1111 1111 1111 1111 1111 1111 1111 1110
  f    f    f    f    f    f    f    e

```

```

23                                     0      TS/circuit
0111 1111 1111 1111 1111 1111
  7    f    f    f    f    f

```

A single hexadecimal digit is used to represent 4 timeslots, requiring eight hexadecimal digits (eight hexadecimal codes between 0 and f) per E1 trunk, and six per T1 trunk. The following table shows how to translate each 4 bits of binary into its hexadecimal digit equivalent.

Binary digits	Hexadecimal digit
0000	0
0001	1
0010	2
0011	3
0100	4
0101	5
0110	6
0111	7
1000	8
1001	9
1010	A
1011	B
1100	C
1101	D
1110	E
1111	F

Specifying decimal timeslot maps

Decimal timeslot maps are specified using the timeslot numbers. Each decimal map contains one or more timeslot groups, with the groups being separated by a colon (:). A timeslot group may contain a single timeslot, or a range of consecutive timeslots separated by a dash (-). The following is an example of a decimal timeslot map

1-15:18:20:25-31

This map could be used to assign CICs to timeslots 1 through 15, 18, 20 and 25 through 31.

NOTE

A decimal timeslot map cannot be specified with a single timeslot. A decimal map must contain at least one colon (:) or dash (-), otherwise it will be interpreted as a hexadecimal map by the SS7 driver.

4.4.4 Adding additional switches

You can manually change the switches by selecting **Additional Switches**, this will open an Additional switches dialog.

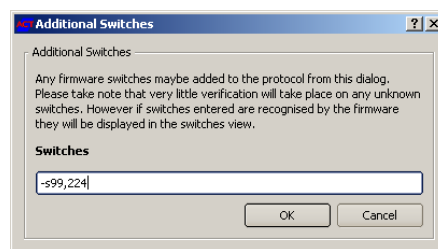


Figure 4-18 ACT additional switches dialog

Edit the Switches field as required. A list of switches for each protocol can be found in the release note for the protocol.

4.5 Configuring clock settings

As detailed in section 4.3.2, select a card from the Clocking Settings list followed by Card Details, or double click on a card entry, to open a Clocking Details page for the selected card.

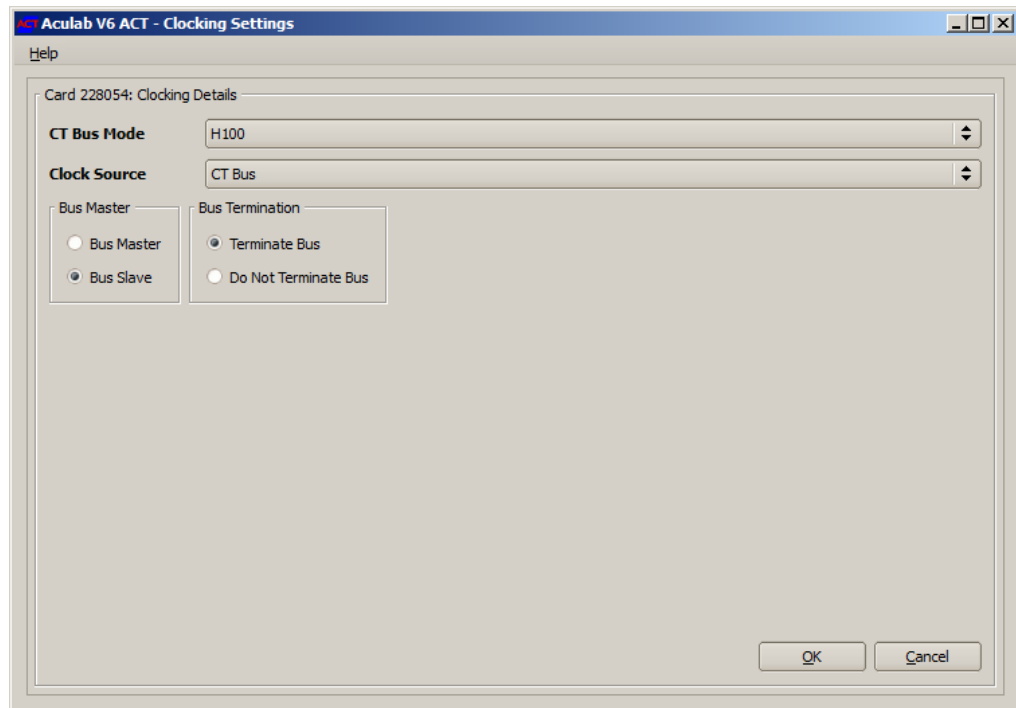


Figure 4-19 ACT configuring clock Settings page

CT Bus Mode – This control must be left at its default setting of H100.

Clock Source – This control must be left at its default setting of CT Bus.

Bus Master – This control must be left at its default setting of Bus Slave.

Bus Termination – select Terminate Bus or Do Not Terminate Bus as appropriate.

NOTE

Where two or more cards are installed bus termination must be applied to the cards physically located at each end of the H.100 bus, which are the first and last cards in the Card List page.

The exception to this is when a 2U chassis (R720 and R730) is fitted with three or four cards. In this case, bus termination must be applied to the second and third cards in the Card List page.

When you are satisfied with your configuration, select OK to accept, or Cancel to discard, any changes and return to the Clocking Settings page. Repeat the process for all other cards as appropriate.

4.6 Running system diagnostics

As described in section 4.3.3, select Start Diagnostics to run a system diagnostics.

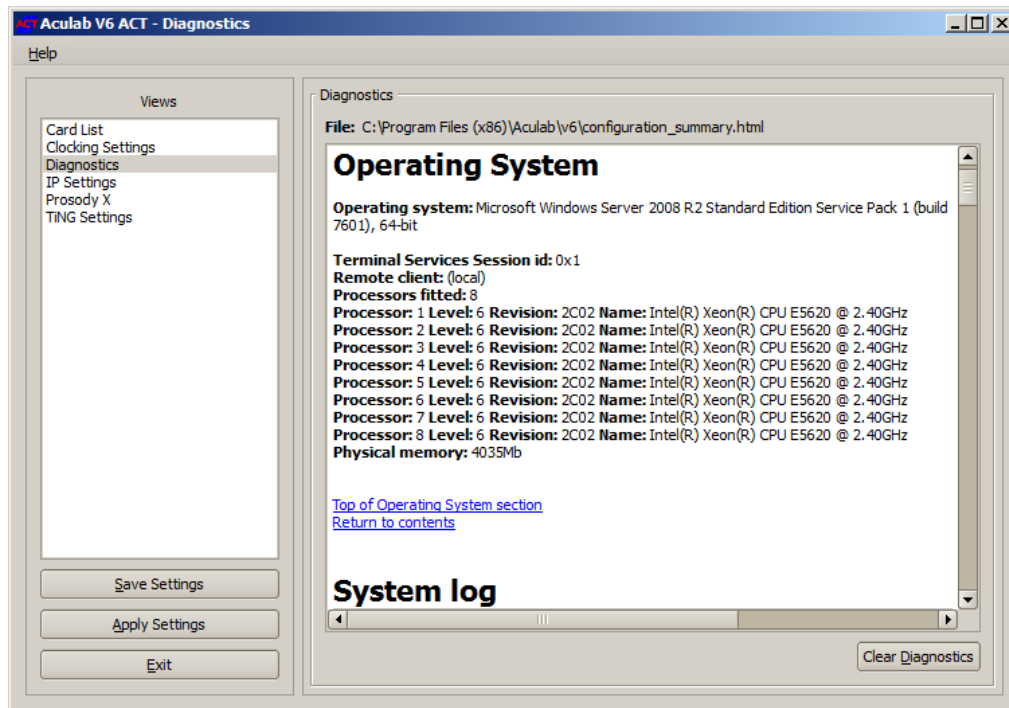


Figure 4-20 ACT diagnostics page

The results of the system diagnostics will appear in the display area. Select Clear Diagnostics to clear the display area.

You can also review the most recent diagnostics report by opening the `C:\Program Files (x86)\Aculab\v6\configuration_summary.html` file.

NOTE

On GroomerII 2U systems, the Troubleshooting section will contain the following report for each card in the system:

Card xxxxxx reports invalid switch clocking. This will cause serious stability problems for firmware running on the card.

It is safe to ignore this message because switch clocking is configured by the GroomerII Kernel application upon startup.

4.7 Flashing a Prosody X card

The Flash Card dialog is used to reload the non-volatile firmware on the Prosody X card. Your GroomerII system will be delivered with the appropriate versions of firmware loaded on the card. If you are installing a new version of GroomerII application software this screen should be used to identify and perform any updates necessary as part of the upgrade process. During normal operation the firmware will not require reloading.

CAUTION

Reloading the firmware to a Prosody X card will cause all calls in progress to be lost. Cards must not be loaded when traffic is passing through the system

As detailed in section 4.3.5, select a card from the Prosody X list followed by Flash Card to open the Flash Card dialog for the selected card.

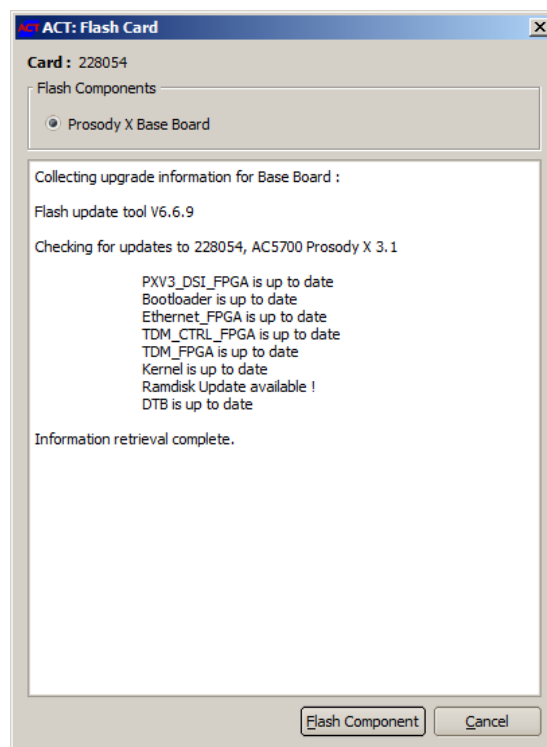


Figure 4-21 ACT Flash Card dialog

The system will compare the versions of firmware files installed on the system hard drive with those downloaded to the card. The individual firmwares on both the Prosody X card will be listed, and each will show whether or not it is up to date.

If any of the firmwares are not up to date then the card should be reloaded.

Reloading the firmware

Click the Flash Component button. You will be asked to confirm the operation.

CAUTION

Once the reload operation has been started it cannot be cancelled.

If you proceed then each of the firmwares marked as Update available! will be downloaded in turn, with progress being reported to the screen. When all updates have been completed the card will be restarted and the Cancel button replaced by an Exit button. Click the Exit button to return to the Prosody X page, and wait for the card to return to the In Service state.

4.8 Prosody X card configuration

As detailed in section 4.3.5, either use the Add button to open the Adding Prosody X Card dialog (GroomerII 1U (AC2460 only)) dialog, or select a card from the Prosody X Settings list followed by Edit to open an Editing Prosody X Card dialog for the selected card.

Figure 4-22 ACT Add/edit Prosody X card configuration dialog

Card Details

Serial Number – When using the dialog to add a card, the serial number of the card being added must be entered into this field. For a GroomerII 1U (AC2460) system this will be found on the right hand end of the front panel. When using the dialog to edit a card this field will display the serial number of the selected card.

Security Key – Prosody X cards can be controlled remotely, and this field holds the security key that ensures only authorised applications can access the card. When using the dialog to add a card click the Generate Key button to generate a security key. When using the dialog to edit an existing configuration the value in this field should not be changed.

NOTE

If the security key in an existing configuration is accidentally changed, the system must be power cycled before the card can be used to pass traffic.

Generate Key – pressing the Generate Key button will cause a new security key to be generated, and may prevent your Prosody X card from passing traffic. This button should not be used, except under the direction of Aculab support.

Watchdog Timeout x Seconds – enabling this feature will cause the Prosody X card to reboot itself if it loses contact with the network for longer than the timeout period specified. GroomerII does not support this feature, and this box must be left unchecked. The timeout field will be disabled whilst the box is unchecked.

Boot Card – checking this box will cause the Prosody X card to be rebooted, and any

configuration changes applied, whenever the dialog box is closed using the Add/Apply button. This box should remain checked at all times.

IP stack options

IPv4 – check this box to configure the card with an IPv4 media address, and use the radio buttons to specify the type of address.

DHCP – allows the card to use DHCP to obtain an IP address for the media port. GroomerII does not support the use of DHCP for this purpose, and this option should not be selected.

Static – allows the card to use a static IP address for the media port. When configuring GroomerII to use IPv4 media addresses this option should always be selected.

IPv6 – check this box to configure the card with IPv6 media addresses, and use the radio buttons to specify the type of address.

Auto Configure – allows the card to automatically generate IP address for the media port and DSP modules. GroomerII does not support the use of automatically generated addresses, and this option should not be selected.

Prefix – allows the card to automatically generate each IP address using a common prefix. GroomerII does not support the use of prefix addressing, and this option should not be selected.

Manual – allows static IP addresses to be configured. When configuring GroomerII to use IPv6 media addresses this option should always be selected.

IPv4 Settings tab

This tab is only available when the **IPv4** checkbox is ticked, with the controls on the tab being disabled when the **DHCP** radio button is selected.

Basecard IP address – the IP address of the media port on the Prosody X card is specified here. This is the address to which card control information is directed, and is also the address used by RTP/RTT directed to and from the card.

Subnet mask – the subnet mask for the network the media port is attached to.

Default gateway – the gateway address to be used by the media stream.

IPv6 Prefix Settings tab

This tab is only available when both the **IPv6** checkbox is ticked and the **Prefix** radio button selected. GroomerII does not support the use of prefix addressing, and the controls on this page should be left at their default settings.

IPv6 Manual Settings tab

This tab is only available when both the **IPv6** checkbox is ticked and the **Manual** radio button selected.

Base Card IP address – the IP address of the media port on the Prosody X card is specified here. This is the address to which card control information is directed.

Subnet prefix length – the subnet prefix length for the network the media port is attached to.

Default gateway – the gateway address to be used by the media stream.

DSP x – these are the addresses used by RTP/RTT directed to and from the Prosody X card, and an address must be added for each DSP module fitted. Prosody X cards have different numbers of DSP modules fitted, according to their capacity, and only the fields for the modules fitted to the card will be enabled.

When you are satisfied with the configuration select Add/Apply to save your changes and close the dialog. Selecting Cancel will discard your changes and close the dialog.

4.9 TiNG module settings

As detailed in section 4.3.6, select a card from the TiNG Settings list followed by Card Details, or double click on a card entry, to open a TiNG Module Settings page for the selected card.

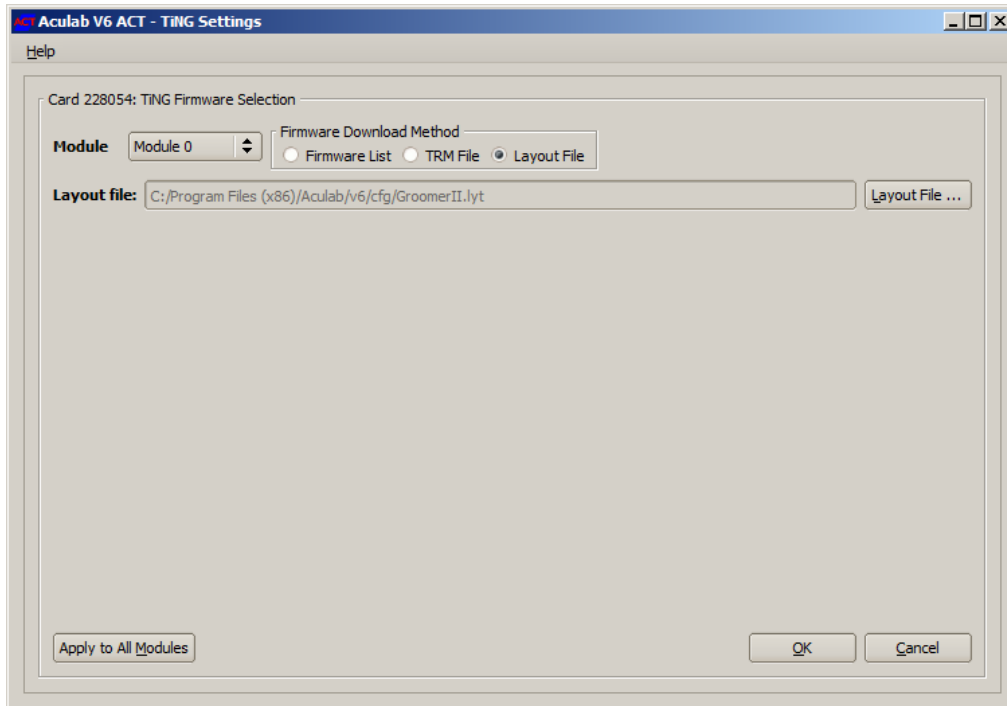


Figure 4-23 ACT TiNG module settings page

TiNG Firmware Selection

A TiNG layout file is used to specify both which firmwares are required by GroomerII, and the order in which they should be loaded. The required layout files are installed with the GroomerII application software.

Module – contains an entry for each TiNG DSP module on the card. Select the module you wish to configure.

Firmware Download Method – The controls displayed will differ depending on which selection is made in the Firmware Download Method groupbox. Select the Layout File radio button to display the layout file controls. GroomerII does not support use of the Firmware List and TRM File controls.

Layout File – specifies the layout file to be loaded. Use the Layout File... button to browse to the folder `C:/Program Files (x86)/Aculab/v6/cfg`, and select the appropriate file.

Layout file	Application
GroomerII.lyt	This is the layout file used for standard GroomerII operation. Unless you have a specific requirement to perform TTY/RTT translation, this file should always be selected.
TTY_GroomerII.lyt	This layout file loads the additional and alternative firmwares that are required to perform TTY/RTT translation. See section 18 for an explanation of TTY/RTT translation.

NOTE

The same layout file must be loaded to each TiNG DSP module in the system.

Apply to All Modules – when the Apply to All Modules button is pressed, the configuration of the currently selected module will be copied to each module on the card.

NOTE

When configuring a Prosody X card for use by GroomerII, the layout file must be loaded to each TiNG DSP module on the card.

When you are satisfied with your configuration select OK to accept, or Cancel to discard, the selection and return to the TiNG Settings page.

4.10 Completing the configuration

Having completed your configuration, select Apply Settings to implement the changes, or Cancel Changes to ignore any changes, and close the ACT application. Selecting Apply Settings will present you with a Firmware Downloading progress and report page.

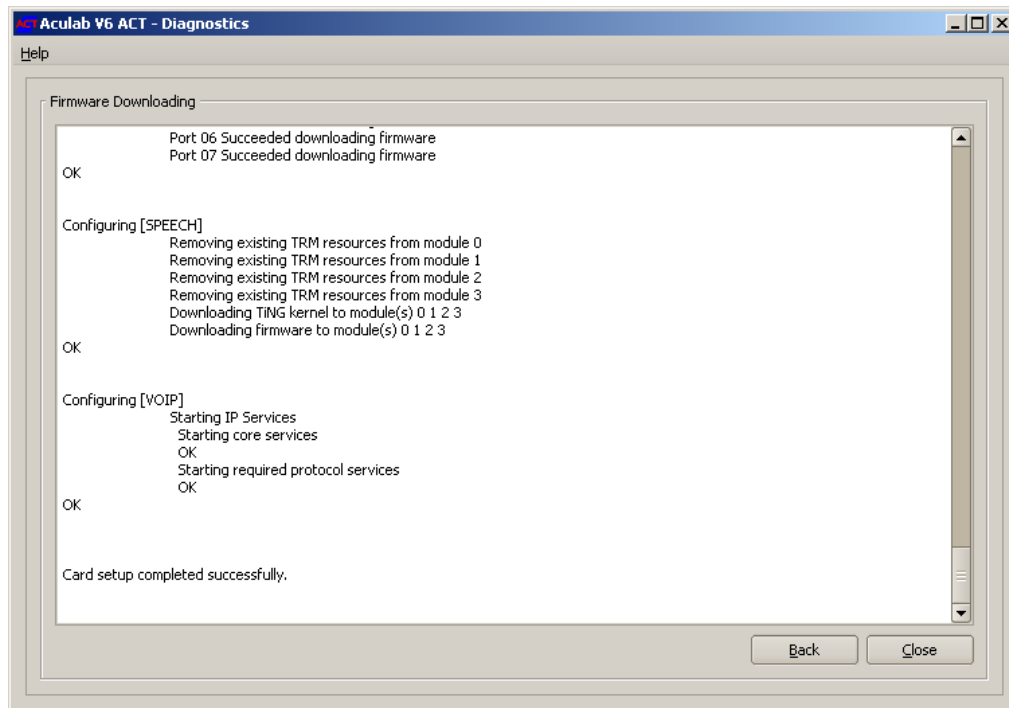


Figure 4-24 ACT close dialog

CAUTION

The ACT must not be used to reload the cards whilst the GroomerII applications are running. Doing so will prevent the Kernel from properly releasing system resources which in turn may prevent the system from processing calls, requiring it to be restarted. Section 5.12 explains how to reload protocol firmware whilst GroomerII is running.

When downloading is complete the Close button will appear. Select Close to complete the configuration and close the Aculab V6 ACT.

5 GroomerII kernel

The GroomerII Kernel is the application program that controls all call routing and handling. When this program is shut down, any calls in progress will be lost and no new calls can be presented to the system.

To ensure that all system resources are properly initialised, the GroomerII Kernel must only be started by powering up the system and logging on to Microsoft Windows.

NOTE

Any attempt to close the application will result in a warning message being displayed giving the option to proceed or cancel.

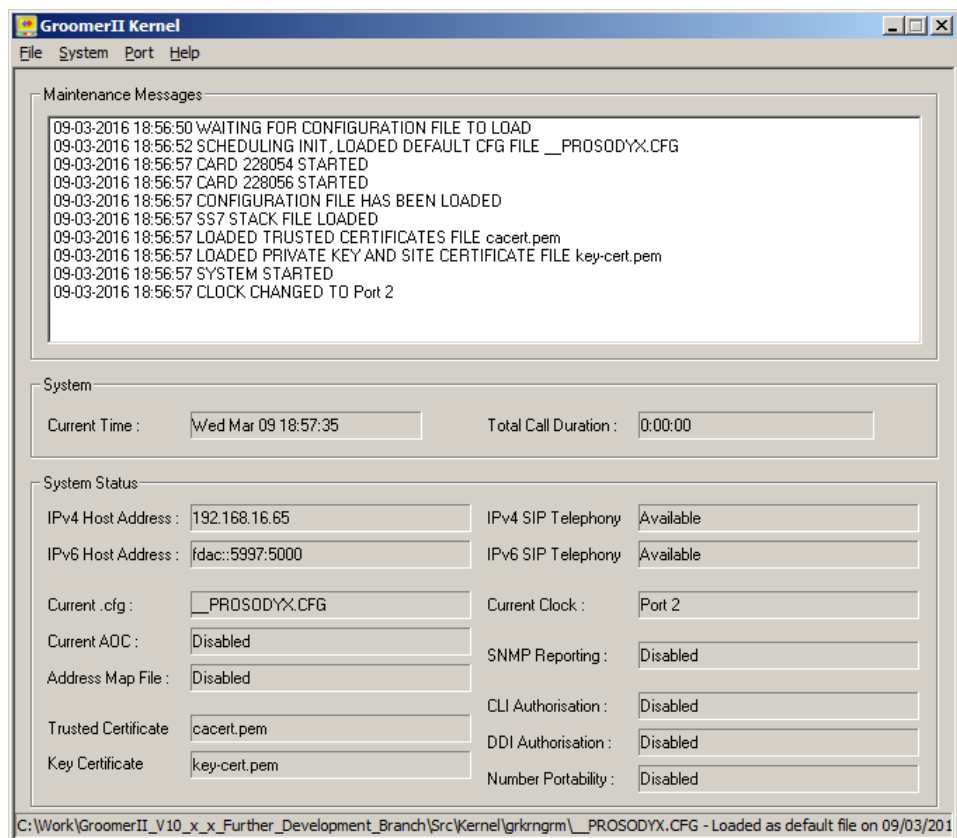


Figure 5-1 GroomerII Kernel

Menu options	See section
File	- Open
	- GroomerII Configuration...
	- AOC Configuration...
	- Address Mapping...
	- Exit
System	- SNMP...
	- Database Connectivity
	- CLI Authorisation...
	- DDI Authorisation...
	- Number Portability...
	- CDR...
	- SIP Authentication...
Port	- Blocking...
	- Load...
	- Reset...
	- SS7 Signalling Links...
	- Continuity Check...
Help	- Contents
	- Search...
	- Index...
	- About GroomerII Kernel

NOTE

The TLS Certificates... menu item will only be available when the restricted availability variant of GroomerII software is in use.

Dialog areas

Maintenance Messages – lists all major changes in the systems operation. The above example shows the type of messages seen when the system starts up successfully.

System – The System group contains the following controls.

Current Time – date and time set in the PC. All Call Data Records and logging information use the PC clock to time stamp the records. The clock can be set or corrected using the standard Microsoft Windows Control Panel – Date/Time option.

Total Call Duration – call duration of all connected calls through the system since the Kernel was started. Total Call duration is only active when CDR Generation is enabled, as described in section 5.8.

System Status – The System Status group contains the following controls.

IPv4 Host Address – the IPv4 address of the host port that will be used for SIP call control signalling, and to which incoming SIP calls should be directed. If no IPv4 host port address has been configured this will read `Not configured`. See section 3.1 for further details.

IPv6 Host Address – the IPv6 address of the host port that will be used for SIP call control signalling, and to which incoming SIP calls should be directed. If no IPv6 host port address has been configured this will read `Not configured`. See section 3.1 for further details.

Current .cfg – the GroomerII configuration file that is being used to process calls.

When no configuration file is being used you will be unable to process any calls. See section 5.1 for further details.

Current AOC – the advice of charge configuration file that is currently in use. When advice of charge is not running, this field will show `Disabled`. See section 5.2 for further details.

Address Map File – the Address Map file currently in use for SIP destination network address selection. When no address map file has been selected, this field will show `Disabled`. See section 5.3 for further details.

Trusted Certificate – the name of the trusted certificate file used when making secure SIP calls. See section 5.10 for further details.

Key Certificate – the name of the key certificate file used when making secure SIP calls. See section 5.10 for further details.

IPv4 SIP Telephony – indicates whether the system is configured to process SIP calls using IPv4 addressing. If IPv4 SIP telephony is configured this field will read `Available`, otherwise it will read `Not configured`. See section 3 for further details.

IPv6 SIP Telephony – indicates whether the system is configured to process SIP calls using IPv6 addressing. If IPv6 SIP telephony is configured this field will read `Available`, otherwise it will read `Not configured`. See section 3 for further details.

Current Clock – indicates which port is currently being used as the clock source for the system. The MASTER clock is the oscillator on an arbitrarily selected Prosody X card. See section 8.6.1 for further details.

SNMP Reporting – this field will show whether SNMP reporting is enabled or disabled.

CLI Authorisation – the name of the ODBC data source if CLI authorisation is currently in use. When CLI authorisation is not running, this field will show `Disabled`. See section 5.5 for further details.

DDI Authorisation – the name of the ODBC data source if DDI authorisation is currently in use. When DDI authorisation is not running, this field will show `Disabled`. See section 5.6 for further details.

Number Portability – the name of the ODBC data source if number portability is currently in use. When number portability is not running, this field will show `Disabled`. See section 5.7 for further details.

5.1 GroomerII configuration load

Selecting **File – Open – GroomerII Configuration...** from the Kernel menu will open the GroomerII Configuration Load dialog. The Filename initially displayed will be for the configuration currently in use. To change or re-load the configuration, either **Browse...** for a file or type the required file name into the Filename field.

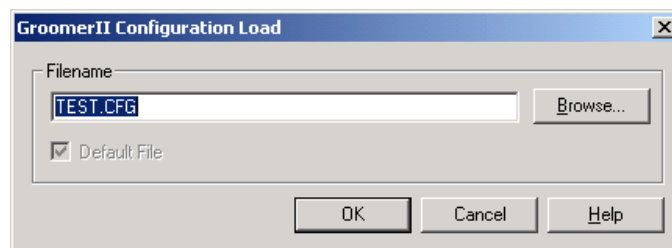


Figure 5-2 GroomerII configuration load dialog

CAUTION

The system will stop running and all calls will be lost if you enter a non-existing file name or use an invalid configuration.

Default File – is enabled once you select a file other than the current default file. The box will initially be unchecked. Check the box only when you wish the file to be the default file used when the GroomerII Kernel is started.

Select OK to load the file or Cancel to ignore any changes and close the dialog.

Changes made to the current/default .cfg file using the GroomerII Configuration Editor can also be loaded using this GroomerII Configuration Load Option.

Reloading a .cfg file will not affect live traffic. Existing calls will continue to use the settings from the previous configuration file, and will remain until normal clearing. All new calls will use settings from the newly loaded file.

5.2 Advice of charge configuration load

Selecting File – Open – AOC Configuration... from the Kernel menu will open the AOC Configuration Load dialog. The Filename initially displayed will be for the configuration currently in use. To change or re-load the configuration, either Browse... for a file or type the required file name into the Filename field.

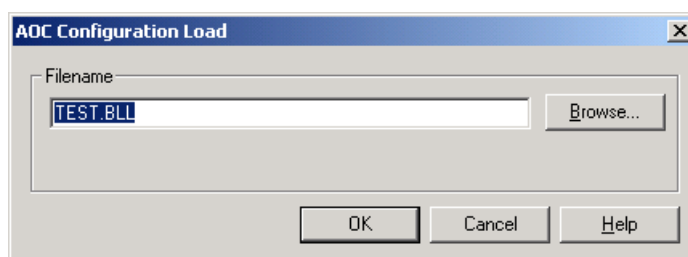


Figure 5-3 AOC configuration load dialog

NOTE

Changes made in this dialog will not be persisted, and the next time GroomerII is started the original AOC configuration file will be loaded. If you wish to make the change permanent the grsched.dat file must also be modified as described in section 10.3.

Select OK to implement any changes or Cancel to ignore any changes and close the dialog.

5.3 Address mapping

Selecting File – Open – Address Mapping... from the Kernel menu will open the Address Mapping dialog. This option is used to select a *.map file and load its configuration into the application. This option can also be used to re-load a *.map file into the application following any updates to the file. The *.map files are created/edited using the Address Map Editor tool.

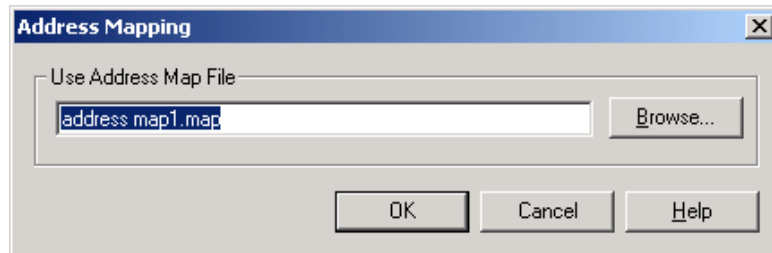


Figure 5-4 Address mapping dialog

Type the required filename into the Use Address Map File field, or select Browse... to browse for the required map file.

CAUTION

Deleting this field will disable address mapping.

Once you have completed your selection, select OK to save the change and load the configuration or Cancel to discard your selection and close the Address Mapping dialog. The newly loaded file will be used as the default file when the system starts.

5.4 SNMP reporting

Select System – SNMP... from the Kernel menu to open the SNMP Reporting dialog. Use this dialog to specify which system faults will be reported using SNMP alarms.

NOTE

The host SNMP service must be installed and suitably configured before SNMP reporting can be used. All new GroomerII systems are delivered with the SNMP service installed. For information on configuring the SNMP service, consult the appropriate vendor documentation.

See Appendix A: for information on the SNMP alarms and reports available.

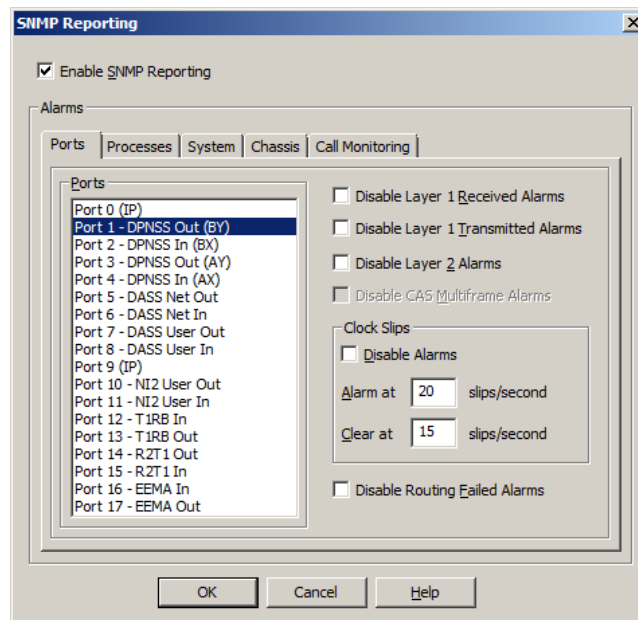


Figure 5-5 SNMP reporting dialog

Enable SNMP Reporting – Check this option to enable the SNMP reporting functions.

Alarms – This group contains the following tab options:

Ports – use this tab to configure the port specific traps:

```
groomerPortIPStatusTrap
groomerTDMRxL1AlarmTrap
groomerTDMTxL1AlarmTrap
groomerTDMLayer2Trap
groomerTDMRxCASMultiframeAlarmTrap
groomerTDMClockSlipsTrap
groomerCallRoutingFailedTrap
```

Processes – use this tab to configure the system process trap:

```
groomerWindowsProcessStateTrap
```

System – use this tab to configure the operating system performance traps:

```
groomerCPUUsageTrap
groomerMemoryUsageTrap
groomerAvailableDiskSpaceTrap
```

Chassis – use this tab to configure the chassis hardware monitoring traps:

`groomerPSUStateTrap`

Call Monitoring – use this tab to configure the call life cycle monitoring trap:

`groomerCallState2Trap`

Having completed any required changes, select OK to accept the changes, or Cancel to discard the changes, and close the SNMP Reporting dialog.

5.4.1 Ports tab options

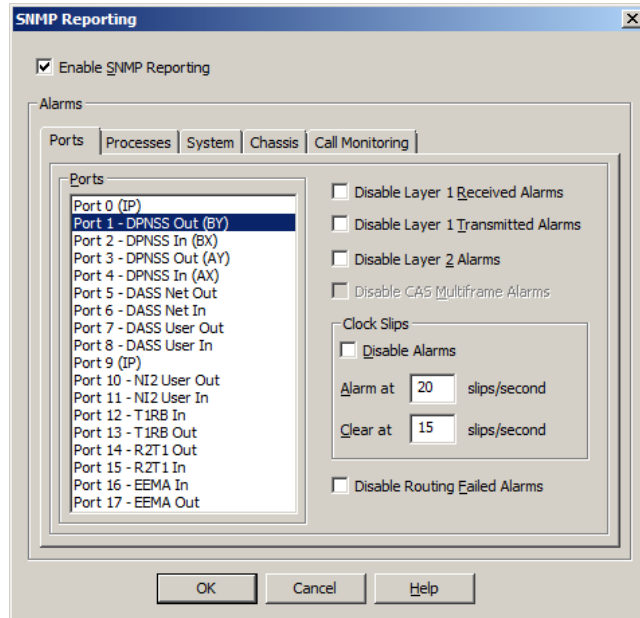


Figure 5-6 SNMP reporting – Ports tab dialog

This dialog is used to configure port specific traps. The dialog options available are:

Ports – A list of all the IP telephony and E1/T1 ports in the system. To disable an SNMP trap for a given port, select the required port from this list then check the appropriate options as detailed below.

Disable Layer 1 Received Alarms – Suppress the `groomerTDMRxL1AlarmTrap` (TDM ports) or `groomerPortIPStatusTrap` (IP telephony ports) for the selected port.

Disable Layer 1 Transmitted Alarms – Suppress the `groomerTDMTxL1AlarmTrap` for the selected port. This option will be disabled if an IP telephony port is selected.

Disable Layer 2 Alarms – Suppress the `groomerTDMLayer2Trap` for the selected port. This option will be disabled if an IP telephony or CAS port is selected.

Disable CAS Multiframe Alarm – Suppress the `groomerTDMRxCASMultiframeAlarmTrap` for the selected port. This option will be disabled if a non-CAS port is selected.

Clock Slips – Use the controls in this group to configure how clock slip alarms will be reported. This control group will be disabled if an IP telephony port is selected.

Disable Alarms – Suppress the `groomerTDMClockSlipsTrap` for the selected port.

Alarm at x slips/second – The number of slips per second at, or above which a slip alarm is generated.

Clear at x slips/second – The number of slips per second at, or below which a slip alarm is cleared.

Disable Routing Failed Alarms – Prevents the `groomerCallRoutingFailedTrap` from being generated when GroomerII fails to route an incoming call arriving on this port.

5.4.2 Processes tab options

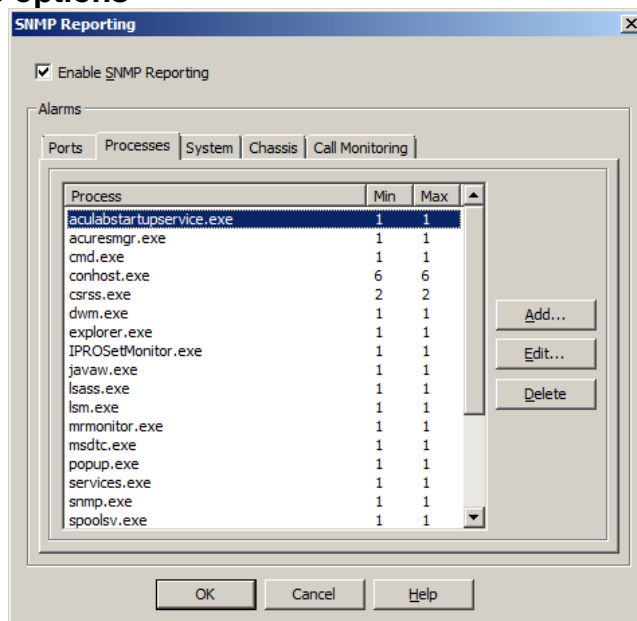


Figure 5-7 SNMP reporting – Processes tab dialog

This dialog is used to manage a list of Windows processes that must be running. It allows a fixed or variable number of instances of each process to be specified. Each process to be monitored is shown in the listbox, which has the following columns:

Process – The name of the process to be monitored.

Min – The minimum number of instances of the process that should be running simultaneously. Anything below this value will generate a `groomerWindowsProcessStateTrap` SNMP trap.

Max – The maximum number of instances of the process that are permitted to be running simultaneously. Anything above this value will generate a `groomerWindowsProcessStateTrap` SNMP trap.

Add... – Use the Add... button to open the Add Process dialog and add a new entry to the list.

Edit... – Use the Edit... button to open the Edit Process dialog and modify the selected list entry.

Delete – Use the Delete button to remove the selected process from the list.

Add/Edit Process dialog

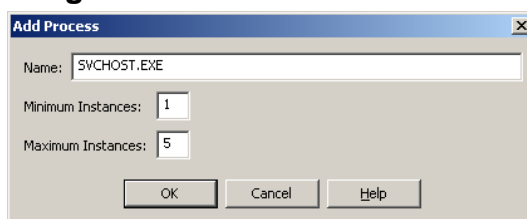


Figure 5-8 Add/Edit Process dialog

Name – The name of the process to be monitored as it would appear in Windows Task Manager.

Minimum Instances – The minimum number of instances of the process that should be running at any time

Maximum Instances – The maximum number of instances of the process that should be running at any time.

Select OK to save, or Cancel to discard, the changes and close the dialog.

5.4.3 System tab options

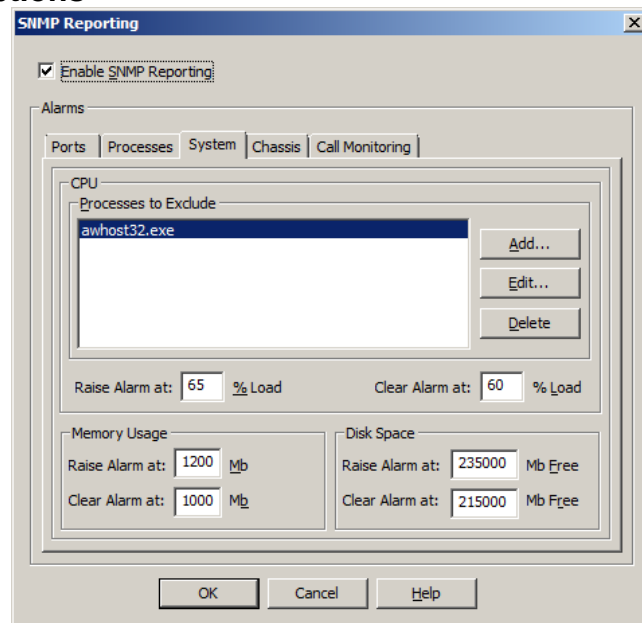


Figure 5-9 SNMP reporting – System tab dialog

This dialog is used to configure system performance alerts relating to CPU usage, memory usage, and disk space availability.

CPU – The controls in the CPU group are used to manage CPU load alarms:

Processes to Exclude – Some processes, for example those associated with remote access to the system, are designed to run at very low priority but will deliberately use all available CPU capacity. Including such processes in the CPU load equation can cause a permanent alarm state, and also mask serious errors. You can exclude such processes from the CPU load equation by entering the process names in this list:

Add... – Use the Add... button to open the Add Excluded Process dialog and add a new process to the list. The Add Excluded Process dialog is described below.

Edit... – Use the Edit... button to open the Edit Excluded Process dialog and modify the list selection. The Edit Excluded Process dialog is described below.

Delete – Use the Delete button to remove the selected process from the list.

Raise Alarm at x % Load – A `groomerCPUUsageTrap` alarm is generated whenever CPU load reaches or exceeds the value entered in this field.

Clear Alarm at x % Load – A `groomerCPUUsageTrap` alarm is cleared whenever CPU usage falls to or below the value entered in this field.

NOTE

CPU load is averaged across several readings to prevent transient spikes from unnecessarily raising or clearing alarms.

Memory Usage – The controls in the Memory Usage group are used to manage memory usage alarms:

Raise Alarm at x Mb – A `groomerMemoryUsageTrap` alarm is generated whenever memory usage reaches, or exceeds, the value entered in this field.

Clear Alarm at x Mb – A `groomerMemoryUsageTrap` alarm is cleared whenever memory usage falls to or below the value entered in this field.

Disk Space – The controls in the Disk Space group are used to manage disk space usage alarms:

Raise Alarm at x Mb Free – A `groomerAvailableDiskSpaceTrap` alarm is generated whenever free disk space falls to or below the value entered in this field.

Clear Alarm at x Mb Free – A `groomerAvailableDiskSpaceTrap` alarm is cleared whenever free disk space rises to or above the value entered in this field.

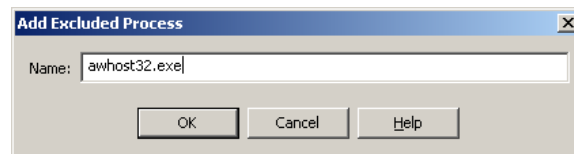
Add/Edit Excluded Process dialog

Figure 5-10 Add/Edit Excluded Process dialog

Name – The name of the process to be excluded from the CPU load calculation as it would appear in Windows Task Manager.

Select OK to save, or Cancel to discard, the changes and close the dialog.

5.4.4 Chassis tab options

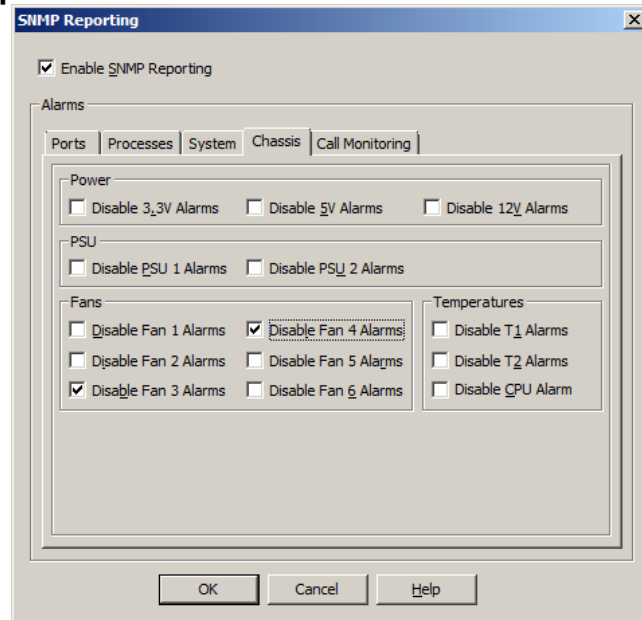


Figure 5-11 SNMP reporting – Chassis tab dialog

The controls on this page allow the production of individual chassis monitoring alarms to be disabled. These controls are provided to allow suppression of spurious alarms generated by known faulty equipment. It is recommended that at all other times the alarms remain enabled.

GroomerII chassis can monitor a variety of system components, although monitoring capabilities vary between individual chassis models. Only those controls applicable to your chassis will be enabled. Where a chassis monitors several components of the same type (for example system fans), you should refer to the installation guide for your chassis to identify specific components.

NOTE

Only those controls that are applicable to the chassis on which the GroomerII Kernel is running will be enabled.

Power – The controls in the Power group are used to suppress the system power rail alarms.

Disable 3.3V Alarms – Use this control to disable the `groomer33VoltStateTrap` alarm.

Disable 5V Alarms – Use this control to disable the `groomer5VoltStateTrap` alarm.

Disable 12V Alarms – Use this control to disable the `groomer12VoltStateTrap` alarm.

PSU – The controls in the PSU group represent each of the power supplies fitted in the chassis.

Disable PSU # Alarms – Check the appropriate Disable PSU # Alarms option to suppress `groomerPSUStatusTrap` alarms relating to that PSU.

Fans – The controls in the Fan group represent each of the system fans fitted in the chassis.

Disable Fan # Alarms – Check the appropriate Disable Fan # Alarms option to suppress `groomerSystemFanTrap` alarms relating to that fan.

Temperatures – The controls in the Temperature group represent each of the internal temperature sensors fitted in the chassis.

Disable T# Alarms – Check the appropriate Disable T# Alarms option to suppress `groomerChassisTemperatureTrap` alarms relating to that temperature sensor.

Disable CPU Alarm – Check the Disable CPU Alarm option to suppress `groomerHBCDeviceTemperatureTrap` alarms relating to CPU temperature.

5.4.5 Call Monitoring tab options

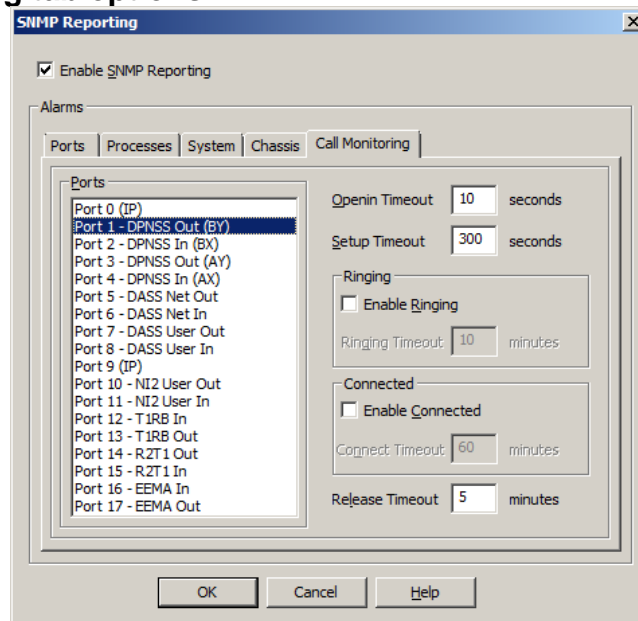


Figure 5-12 SNMP Reporting – Call Monitoring

Call Monitoring provides a mechanism to monitor the life cycle of individual calls and report any faults encountered through SNMP. Faults are reported whenever a call has remained in a state for longer than the period configured by the user by raising a `groomerCallState2Trap` alarm. Any alarms generated will be automatically cleared when the call moves to another state.

Ports – A list of all the IP telephony and E1/T1 ports in the system. To configure the Call Monitoring alarm for a given port, select the required port from this list then modify the appropriate options as detailed below.

Openin Timeout – This is a GroomerII internal process, and represents the time allowed between both legs of a call in progress completing the release procedure, and the timeslot carrying the incoming leg being ready to receive a new incoming call. A timeslot is allowed to remain in the 'listen for incoming' state indefinitely. This alarm, when generated, indicates that GroomerII is unable to accept incoming calls on the particular timeslot.

Setup Timeout – The number of seconds allowed after detecting an incoming call before GroomerII reaches the ringing or connected states. If the ringing or connected state has not been reached within this time an alarm will be generated.

Ringing – Use the controls in this group to manage how alarms will be generated during the ringing stage of the call:

Enable Ringing – Checking this control will cause an alarm to be generated if

GroomerII remains at the ringing stage beyond the specified period. When unchecked the call will be allowed to ring for an indefinite period.

Ringing Timeout – The number of minutes an incoming call is allowed to ring before an alarm is generated. This control will only be enabled when Enable Ringing is checked.

NOTE

Some CAS protocols do not support a ringing stage. In such cases this timer should be set to a sufficient length to allow the outgoing call to be answered.

Connect – Use the controls in this group to manage how alarms will be generated during the connected stage of a call:

Enable Connected – Checking this control will cause an alarm to be generated if the call remains in the connected state beyond the specified period. When unchecked the call will be allowed to remain connected for an indefinite period.

Connect Timeout – The number of minutes a call stays connected before an alarm is generated. This control will only be enabled when Enable Connected is checked.

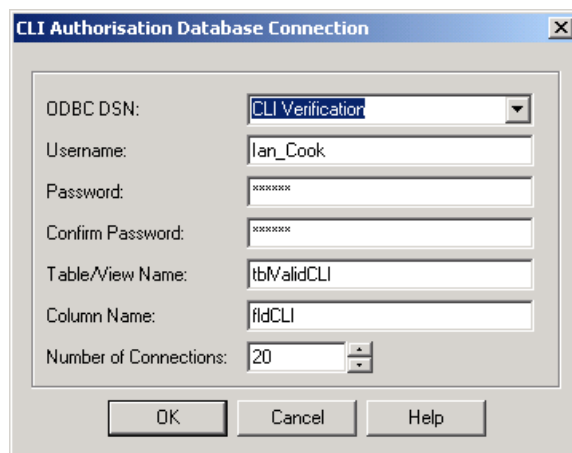
Release Timeout – The number of minutes allowed between receiving a call disconnect and both call legs having completed the release procedure. If the release procedure has not been completed within the specified time then an alarm will be generated.

5.5 CLI authorisation database selection

System – CLI Authorisation

Before using CLI authorisation on an incoming call, you first need to define both a database of CLIs to be used for authorisation, and the maximum number of simultaneous calls (connections), allowed to the database.

Select System – CLI Authorisation... to open the CLI Authorisation Database Connection dialog.



The dialog box titled "CLI Authorisation Database Connection" contains the following fields and controls:

- ODBC DSN:** A pull-down menu currently showing "CLI Verification".
- Username:** A text field containing "Ian_Cook".
- Password:** A password field with masked characters (dots).
- Confirm Password:** A password field with masked characters (dots).
- Table/View Name:** A text field containing "tblValidCLI".
- Column Name:** A text field containing "fldCLI".
- Number of Connections:** A spin box currently set to "20".
- Buttons at the bottom: "OK", "Cancel", and "Help".

Figure 5-13 CLI authorisation database connection dialog

ODBC DSN – a pull down list of Open Database Connectivity Data Source Names as defined in the Microsoft Windows operating system System and User DSN tab option of the ODBC Data Source Administrator dialog. This is located at Control Panel – Administrative Tools – Data Sources (ODBC). Make your required selection from the pull down list.

This field will allow you to select the ODBC data source to be used for CLI authorisation. The names of all the ODBC data sources that are configured on your system will be listed, along with <None>. Selecting a DSN will cause CLI authorisation to be enabled, selecting <None> will cause it to be disabled. The default setting is <None>.

CAUTION

The Microsoft Windows ODBC Manager allows two types of DSN to be configured – System DSNs that are available to all users, and User DSNs that are available to a specific user only. Names can be duplicated between the types. Care should be exercised to ensure that in this situation the correct name is selected. To ensure permanent availability it is recommended that System DSNs only be configured.

Username – must be either a valid user name for the selected ODBC DSN, or left blank when no security authorisation is required.

Use of this field is dependant upon the ODBC data source in use, and how it has been configured. Some data sources offer a login facility as an additional security measure to the system login. Where this facility exists, its use is generally optional. If your data source offers such a facility and you choose to use it, you should enter the data source login username in this field.

Password – must be either a valid password for the ODBC DSN user, or left blank when no security authorisation is required.

Confirm Password – retype the above password in this field. The two fields will be compared to ensure that the password has been entered correctly.

CAUTION

The username and password fields are stored in the `grkernel.dat` file using a simple encryption algorithm only. Appropriate security measures should be adopted to safeguard this data.

Table/View Name – must be a valid table or database view for the selected ODBC DSN.

Your database administrator will provide you with this information. There is no default for this field and it cannot be left blank.

Column Name – must be a valid data field (column) in the selected ODBC DSN. This is the data that will be used to verify authorisation of the CLI.

Your database administrator will provide you with this information. There is no default for this field and it cannot be left blank.

Number of Connections – This is the number of connection threads that will be started. Each connection thread can establish a single connection to the database, and all of the threads can simultaneously perform a CLI authorisation query. The number of connections that your data source can support will have a limit. When this field is configured to exceed that limit, or when sufficient connections to the database are not available, then some of the threads will not be able to connect to the database. A message warning that the database is not fully connected will be issued to the Kernel screen, and an (if enabled) SNMP trap issued. The default value is 5.

For further details on database connectivity, please see section 13.

5.6 DDI authorisation database selection

System – DDI Authorisation

Before using DDI authorisation on an incoming call, you first need to define both a database of DDIs to be used for authorisation, and the maximum number of simultaneous calls (connections), allowed to the database.

Select System – DDI Authorisation... to open the DDI Authorisation Database Connection dialog.

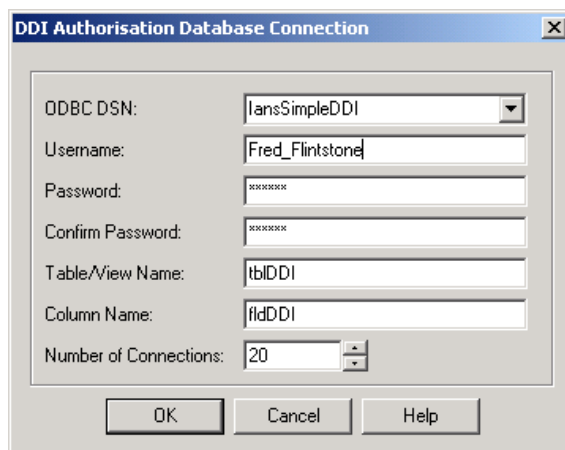


Figure 5-14 DDI authorisation database connection dialog

ODBC DSN – a pull down list of Open Database Connectivity Data Source Names as defined in the Microsoft Windows operating system System and User DSN tab option of the ODBC Data Source Administrator dialog. This is located at Control Panel – Administrative Tools – Data Sources (ODBC). Make your required selection from the pull down list.

This field will allow you to select the ODBC data source to be used for DDI authorisation. The names of all the ODBC data sources that are configured on your system will be listed, along with <None>. Selecting a DSN will cause DDI authorisation to be enabled, selecting <None> will cause it to be disabled. The default setting is <None>.

CAUTION

The Microsoft Windows ODBC Manager allows two types of DSN to be configured – System DSNs that are available to all users, and User DSNs that are available to a specific user only. Names can be duplicated between the types. Care should be exercised to ensure that in this situation the correct name is selected. To ensure permanent availability it is recommended that System DSNs only be configured.

Username – must be either a valid user name for the selected ODBC DSN, or left blank when no security authorisation is required.

Use of this field is dependant upon the ODBC data source in use, and how it has been configured. Some data sources offer a login facility as an additional security measure to the system login. Where this facility exists, its use is generally optional. When your data source offers such a facility and you choose to use it, you should enter the data source login username in this field.

Password – must be either a valid password for the ODBC DSN user, or left blank when no security authorisation is required. Note that the contents of this field are obscured for security purposes.

Confirm Password – retype the above password in this field. The two fields will be compared to ensure that the password has been entered correctly.

CAUTION

The username and password fields are stored in the `grkernel.dat` file using a simple encryption algorithm only. Appropriate security measures should be adopted to safeguard this data.

Table/View Name – must be a valid table or database view for the selected ODBC DSN.

Your database administrator will provide you with this information. There is no default for this field and it cannot be left blank.

Column Name – must be a valid data field (column) in the selected ODBC DSN. This data will be used to verify authorisation of the DDI.

Your database administrator will provide you with this information. There is no default for this field and it cannot be left blank.

Number of Connections – This is the number of connection threads that will be started. Each connection thread can establish a single connection to the database, and all of the threads can simultaneously perform a DDI authorisation query. The number of connections that your data source can support will have a limit. When this field is configured to exceed that limit, or when sufficient connections to the database are not available, then some of the threads will not be able to connect to the database. A message warning that the database is not fully connected will be issued to the Kernel screen, and an (if enabled) SNMP trap issued. The default value is 5.

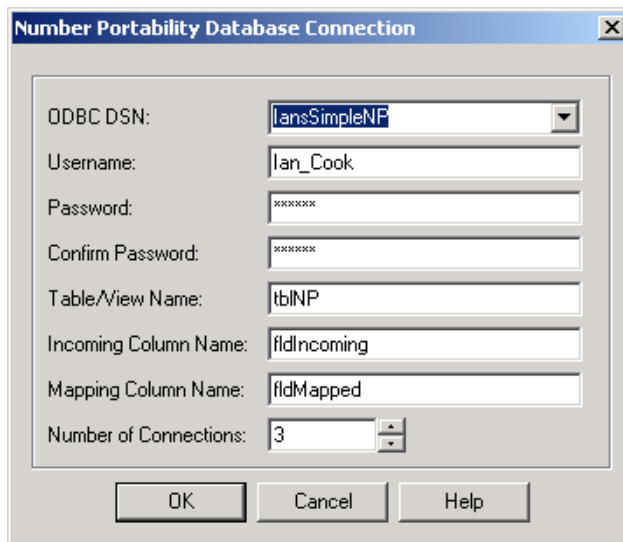
For further details on database connectivity, please see section 13.

5.7 Number portability database selection

System – Number Portability

Before using Number Portability mapping on an incoming call, you first need to define both a database of alternative DDIs to be mapped, and the maximum number of simultaneous calls (connections), allowed to the database.

Select System – Number Portability... to open the Number Portability Database Connection dialog.



The dialog box is titled "Number Portability Database Connection". It contains the following fields and controls:

- ODBC DSN:** A pull-down menu showing "IansSimpleNP".
- Username:** A text field containing "Ian_Cook".
- Password:** A text field with masked characters "XXXXXXXX".
- Confirm Password:** A text field with masked characters "XXXXXXXX".
- Table/View Name:** A text field containing "tblNP".
- Incoming Column Name:** A text field containing "fldIncoming".
- Mapping Column Name:** A text field containing "fldMapped".
- Number of Connections:** A spin box set to "3".

At the bottom are three buttons: "OK", "Cancel", and "Help".

Figure 5-15 Number portability database connection dialog

ODBC DSN – a pull down list of Open Database Connectivity Data Source Names as defined in the Microsoft Windows operating system System and User DSN tab option of the ODBC Data Source Administrator dialog. This is located at Control Panel – Administrative Tools – Data Sources (ODBC). Make your required selection from the pull down list.

This field will allow you to select the ODBC data source to be used for number portability mapping. The names of all the ODBC data sources that are configured on your system will be listed, along with <None>. Selecting a DSN will cause number portability mapping to be enabled; selecting <None> will cause it to be disabled. The default setting is <None>.

CAUTION

The Microsoft Windows ODBC Manager allows two types of DSN to be configured – System DSNs that are available to all users, and User DSNs that are available to a specific user only. Names can be duplicated between the types. Care should be exercised to ensure that in this situation the correct name is selected. To ensure permanent availability, it is recommended that System DSNs only be configured.

Username – must be either a valid user name for the selected ODBC DSN, or left blank when no security authorisation is required.

Use of this field is dependant upon the ODBC data source in use, and how it has been configured. Some data sources offer a login facility as an additional security measure to the system login. Where this facility exists, its use is generally optional. If your data source offers such a facility and you choose to use it, you should enter the data source login username in this field.

Password – must be either a valid password for the ODBC DSN user, or left blank when no security authorisation is required. Note that the contents of this field are obscured for security purposes.

Confirm Password – retype the above password in this field. The two fields will be compared to ensure that the password has been entered correctly.

CAUTION

The username and password fields are stored in the `grkernel.dat` file using a simple encryption algorithm only. Appropriate security measures should be adopted to safeguard this data.

Table/View Name – must be a valid table or database view for the selected ODBC DSN.

Your database administrator will provide you with this information. There is no default for this field and it cannot be left blank.

Incoming Column Name – must be a valid data field (column) in the selected ODBC DSN. This is the data against which the incoming DDI will be matched.

Your database administrator will provide you with this information. There is no default for this field and it cannot be left blank.

Mapping Column Name – must be a valid data field (column) in the selected ODBC DSN. This is the data with which the incoming DDI will be substituted prior to routing the call.

Your database administrator will provide you with this information. There is no default for this field and it cannot be left blank.

Number of connections – This is the number of connection threads that will be started. Each connection thread can establish a single connection to the database, and all of the threads can simultaneously perform a number portability request. The number of connections that your data source can support will have a limit. When this field is configured to exceed that limit, or when sufficient connections to the database are not available, then some of the threads will not be able to connect to the database. A message warning that the database is not fully connected will be issued to the Kernel screen, and an (if enabled) SNMP trap issued. The default value is 5.

For further details on database connectivity, please see section 13.

5.8 Call data record (CDR)

Call Data Records (CDRs) are generated and logged by the Kernel application.

Select System – CDR... to open the CDR Settings dialog.

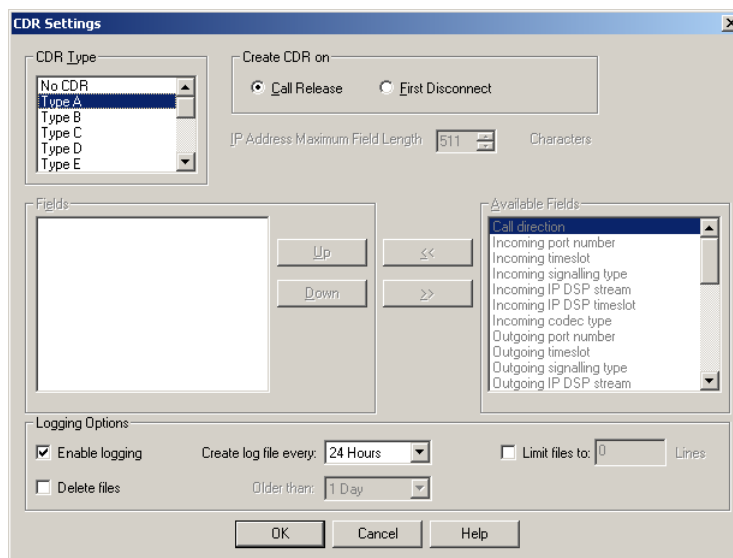


Figure 5-16 CDR settings dialog

CDR Type – a CDR is generated for each call subject to the CDR Type selected. See Appendix B: for definitions of the available CDR types. The initial default for this option is No CDR.

NOTE

CDR types A through M are included for use by legacy TDM systems only, and do not support IP telephony. If you are processing IP telephony calls then only User Defined CDRs should be used.

Create CDR on – By selecting the appropriate radio button, you can create the CDR on either Call Release or First Disconnect.

IP Address Maximum Field Length x Characters – is used to restrict the number of characters reported for any IP network addresses that may appear in user defined CDRs. Any addresses exceeding this length will be truncated.

User defined CDRs – Selecting User Defined in the CDR Type field will enable the controls in this group.

Fields – details the fields that will be included in the user defined CDR. Use the Up and Down buttons to adjust the order in which the fields appear in the CDR.

<< – Use this button to move the selected field from the Available Fields list into the Fields list.

>> – Use this button to remove the selected field from the Fields list back to the Available Fields list.

Available Fields – details the fields that are still available to be added to the user defined CDR when required.

The user defined CDR output is a comma-delimited string in the order of the Fields list. It could look like this depending on which fields are selected:

```
30:10:03,12:08:33,12:09:54,12:15:06,00:05:12,2086764633,906445556
```

Logging Options – CDR records can be logged to a separate file in the CDR directory under the GroomerII installation directory. The following options determine how the GroomerII produces these files.

Enable Logging – Checking this box will enable disk logging. All other controls in the Logging Options frame will be disabled when this box is unchecked.

Create log file every – This specifies the frequency at which the log file is to be closed and a new one started. The datum time is midnight, when a new file will always be started. When there is a limit on the number of lines per file then multiple files per time period may be created.

Limit files to x Lines – When the specified number of lines have been written to a log file, the file will be closed and a new file started when this option is enabled.

Delete files/Older than – When enabled this will cause log files to be automatically deleted when they are older than specified.

User defined CDRs

The fields in the following table can be added to a user defined CDR.

Field	Description
Call direction	A two character field that indicates the type of end to end call made. The first character represents the incoming call leg and the second character the outgoing call leg, for example TI. The following characters are used: T – The call leg was a TDM call. I – The call leg was an IP telephony call. - – No call Leg was made (outgoing position only).
Incoming port number	The port number on which the incoming call leg was received. For IP telephony calls, which receive all incoming calls on the host port, this will be the port selected to carry the media.
Incoming timeslot	The number of the timeslot on which the incoming call leg was received. For IP telephony calls this will be a value assigned by the GroomerII application, and will be the same as that used in the call control trace.
Incoming signalling type	This is a string returned by the Aculab call control software to indicate the protocol used to carry the incoming call leg.
Incoming IP DSP stream	This field is used for fault finding and has no meaning outside of Aculab.
Incoming IP DSP timeslot	This field is used for fault finding and has no meaning outside of Aculab.

Field	Description
Incoming codec type	If an incoming IP telephony call reaches the connected state, this field will contain the codec that was initially negotiated with the remote endpoint, otherwise the field will be empty.
Outgoing port number	The port number on which the outgoing leg of the call was placed. For IP telephony calls this will be the port selected to carry the media.
Outgoing timeslot	The number of the timeslot on which the outgoing call leg was placed. For IP telephony calls this will be a value assigned by the GroomerII application, and will be the same as that used in the call control trace.
Outgoing signalling type	This is a string returned by the Aculab call control software to indicate the protocol used to carry the outgoing call leg.
Outgoing IP DSP stream	This field is used for fault finding and has no meaning outside of Aculab.
Outgoing IP DSP timeslot	This field is used for fault finding and has no meaning outside of Aculab.
Outgoing codec type	If an outgoing IP telephony call reaches the connected state, this field will contain the codec that was initially negotiated with the remote endpoint, otherwise the field will be empty.
Call start date	The date on which the incoming call leg was received in the form dd/mm/yy.
Call start time	The time at which the incoming call leg was received in the form hh:mm:ss. A 24 hour clock is used.
Call answer time	The time at which the outgoing call leg was answered in the form hh:mm:ss. A 24 hour clock is used.
Call end time	The time at which the call was terminated in the form hh:mm:ss. A 24 hour clock is used.
Call duration	The duration for the which the call was in the connected state in the form hh:mm:ss. This is the difference between Call answer time and Call end time.
Call ID	This is the numeric part of the call ID (ID:) used to identify the call in the GroomerII call control trace, for example 0000012345.
Incoming destination address	This is the called party number presented by the incoming call leg. If the incoming call leg is a SIP call this will be the user part of the Request-URI.
Incoming IP network destination	This field is used only when the incoming call leg is an IP telephony call and will be the host part of the SIP Request-URI, typically the IP address of the GroomerII host port. If the incoming call leg is a TDM call then this field will be empty.

Field	Description
Incoming originating address	This is the calling party number presented by the incoming call leg. If the incoming call leg is a SIP call this will be the user part of the URI in the <code>P-Asserted-Identity</code> , if present, or otherwise the <code>From</code> header.
Incoming IP network origin	This field is used only when the incoming call leg is an IP telephony call and will be the host part of the URI in the <code>P-Asserted-Identity</code> , if present, or otherwise the <code>From</code> header. If the incoming call leg is a TDM call then this field will be empty.
Outgoing destination address	This is the called party number sent in the outgoing call leg. If the outgoing call leg is a SIP call this will be the user part of the Request-URI.
Outgoing IP network destination	This field is used only when the outgoing call leg is an IP telephony call, and will be the IP address of the endpoint to which GroomerII has directed the call. If the incoming call leg is a TDM call then this field will be empty.
Outgoing originating address	This is the calling party number sent in the outgoing call leg. If the outgoing call leg is a SIP call this will be the user part of the URI in the <code>P-Asserted-Identity</code> , if present, or otherwise the <code>From</code> header.
Outgoing IP network origin	This field is used only when the outgoing call leg is an IP telephony call. It is the value used in the call control signalling to indicate the endpoint from which the call originated, and will always be the GroomerII host IP address. If the incoming call leg is a TDM call then this field will be empty.
Incoming service indicator code	This indicates the type of line requested by the incoming call, and will be one of <code>3.1KHz</code> , <code>Speech</code> , <code>7KHz</code> , <code>FAX</code> or <code>DATA64K</code> . Protocols that cannot present this information (CAS and SIP) will always report <code>Speech</code> . Line types that are not recognised by GroomerII will be reported as <code>Other</code> . This field is directly related to the SIC control for the incoming call in the Routing Configuration screen (see section 8.5.2 for further information).
Raw call termination cause code	If the remote end disconnects the outgoing call leg before the connected state is reached, then this field will contain the clearing cause returned by the remote end. Raw clearing causes are decimal values that are specific to the signalling protocol in use. If the outgoing call leg is disconnected after reaching the connected state then this field will contain zero.
Generic call termination cause code	This field is used for fault finding and has no meaning outside of Aculab.

Field	Description
Call termination reason	<p>This is a single character field that indicates why the call was terminated, and will be one of the following:</p> <ul style="list-style-type: none"> Y - A successful call was terminated normally. R - Routing failed. O - The Aculab call control software rejected the request to make an outgoing call. E - The outgoing call was rejected with user busy. U - The outgoing call was rejected with number unobtainable. N - The outgoing call was rejected for an unspecified reason. H - The caller hung up before the call reached the ringing stage. I - Terminated by the incomplete dialling timer (see section 8.6.6). M - Terminated by the maximum ringing timer (see section 8.6.6). X - A ringing call was terminated before being answered. L - Terminated by the disconnect calls on layer 1 alarm feature (see section 8.3.5). S - The call was terminated to carry out a firmware download, or because the system is closing down. B - The call was disconnected when a timeslot carrying one of the call legs was blocked (see section 5.11). T - The call was disconnected because the timeslot carrying it was reset (see section 5.13). C - The call was terminated because the service and/or media type requested is not supported. P - The call was terminated due to out of procedure action by the remote endpoint.
Call redirection address Incoming enquiry call port Incoming enquiry call timeslot	<p>When interworking from SS7 to ETS 300, GroomerII supports the mapping of an ETS 300 call transfer request to an SS7 call redirection. Should such a request be processed, Call redirection address will contain the dialled number to which the incoming SS7 call has been redirected. The Incoming enquiry call port and Incoming enquiry call timeslot will contain the port and timeslot numbers used by the outgoing ETS 300 call to make the call transfer request. If no call transfer request has been received these fields will be blank. ETS 300 call transfer to SS7 call diversion mapping is described in section 12.2.</p>

Field	Description
Recovered call	This is a single character field. Y indicates that one or more SIP recovery calls have been made and successfully connected, N indicates that no SIP recovery calls have been connected. SIP call recovery is described in section 14.3.
Total charging units	This is the total number of Advice of Charge (AOC) units mapped from the outgoing call leg to the incoming call leg. AOC units are specific to the signalling protocols in use. AOC mapping is described in section 0.
Re-routing count	This is the number of times a rejected outgoing call was re-routed before either a successful outgoing call was made, or the call was rejected back to the calling party. Call re-routing is described in section 8.5.7.
Connected address	This is the connected party number mapped from the outgoing to the incoming call leg at the connected stage.

CDR call duration

Call duration will always be correct, even when the operating system automatically adjusts its time during a call in progress due to daylight saving. GroomerII uses the underlying system time, which is independent of daylight saving time.

The CDR may however show start or end times that are an hour longer or shorter, for example, in the UK one time may be BST (British summer time) and the other GMT (Greenwich mean time).

NOTE

If the system clock time is manually adjusted, the duration will equal the difference between the recorded start and end times.

5.9 SIP Authentication

This dialog box will allow SIP credential information to be configured, which will be used when making calls to authenticating SIP proxy servers and endpoints. Select System – SIP Authentication... to open the SIP Authentication Settings dialog.

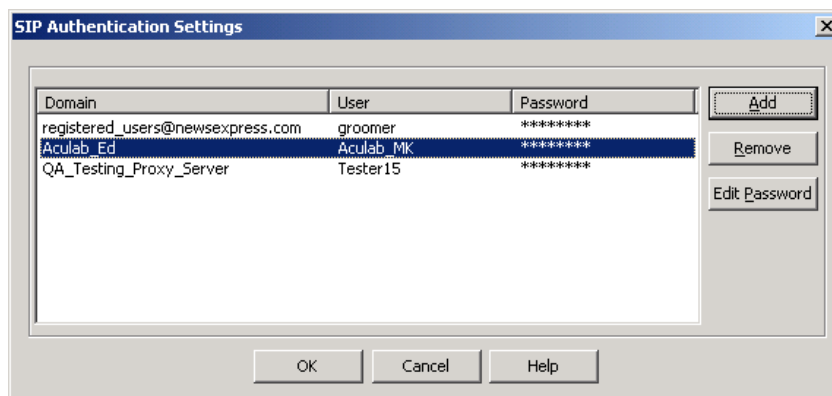


Figure 5-17 SIP authentication dialog

The list will show each authentication record configured, and has the following columns:

Domain – The domain for which the authentication record is valid.

User – The username that GroomerII will return when challenged by that domain.

Password – The password for the above user. This will always be displayed as stars.

Add – Click the Add button to display the Edit SIP Credential Information dialog box and add a new set of authentication credentials.

Remove – Click the Remove button to delete the selected SIP credential information record.

Edit Password – Click the Edit Password button to open the Edit SIP Credential Information dialog box in change password mode and change the password for the selected record.

Click the OK button to close the SIP Authentication Settings dialog and apply your changes, or Cancel to discard the changes.

Edit SIP Credential Information dialog

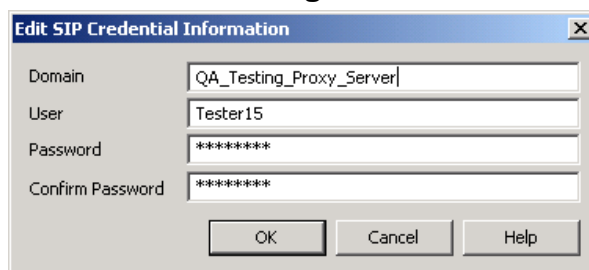


Figure 5-18 Add/Edit SIP credentials dialog

Domain – This is the SIP realm for which the authentication record is to be used, and is the string that will be sent by the remote endpoint to identify itself. This field will be disabled when the dialog box is opened in change password mode.

User – This is the username that GroomerII will return when challenged by the above domain. This field will be disabled when the dialog box is opened in change password mode.

Password/Confirm Password – This is the password that GroomerII will return when challenged by the above domain. These are non-display fields that allow the password to be entered and confirmed. When the entries in the two fields are not identical, the settings will not be accepted.

5.10 TLS certificates

The TLS Certificates window is where the certificate files that will be used when making secure SIP calls are specified. See section 14 for further information on SIP security. Select System-TLS Certificates... from the Kernel menu to open the TLS Certificates dialog.

NOTE

This window is only available when the restricted availability variant of GroomerII software is in use.

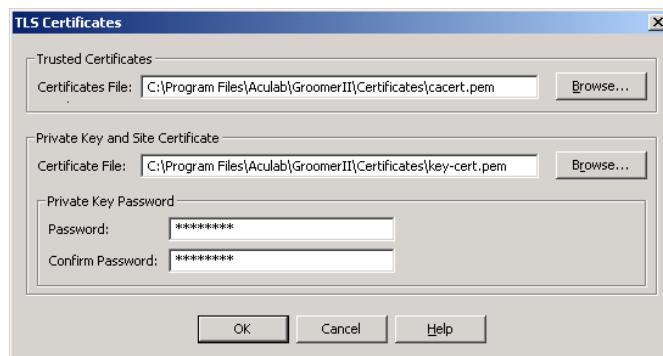


Figure 5-19 TLS Certificates dialog

Trusted Certificates – This file contains the identities of those Certificate Authorities that GroomerII will accept when conducting endpoint authentication.

Certificate File – Enter the path and name of the trusted certificates file, or use the Browse... button to select the file.

Private Key and Site Certificate – This file, which is often referred to as the 'Server Certificate', contains the private key and site certificate that GroomerII will present to remote endpoints during the authentication process.

NOTE

Both the private key and site certificate must be contained in the same file. GroomerII does not support the use of separate files for each.

Certificate File – Enter the path and name of the certificate file in this field, or use the Browse... button to select the file.

Private Key Password – If the private key is password protected then enter the password in both the Password and Confirm Password fields. Asterisks will be displayed when typing into these fields.

If the private key is not password protected then these fields must be left blank.

CAUTION

The password field is stored in the `grkernel.dat` file using a simple encryption algorithm only. Appropriate security measures should be adopted to safeguard this data.

OK – Click the OK button to accept the new settings, close the TLS Certificates dialog and load the new settings. The new settings will be applied to new calls only, calls in progress will continue to use the previous settings.

Cancel – Click the Cancel button to discard any changes made and close the TLS Certificates dialog.

5.11 Port blocking

Port blocking allows individual timeslots on the port to be removed from service so that maintenance operations can be performed.

The current blocking status of all ports is stored, and re-applied on system startup.

If a blocked port is reloaded, its blocking state will be restored following completion of the reload.

GroomerII will not route outgoing calls to blocked timeslots. For SS7, T1 Robbed Bit, AT&T, NI2 and DMS100 this applies equally to both timeslots blocked locally, and timeslots blocked at the far end.

When the GroomerII application is closed down normally, hardware blocking will be applied to any ITU-T, China and UK ISUP ports that are not already blocked. Any shutdown applied blocking will be removed when GroomerII is restarted.

To apply or remove port blocking, select Port – Blocking... to open the Port Blocking dialog.

NOTE

The appearance of the screen will change according to the type of port selected.

5.11.1 Port blocking for ITU-T, China and UK ISUP

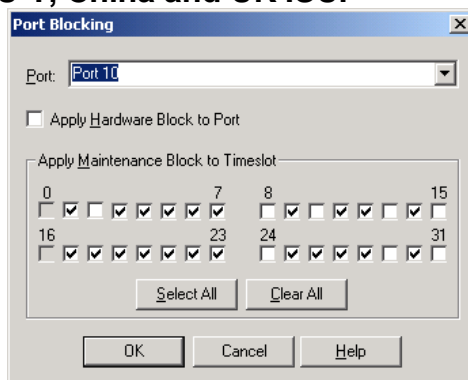


Figure 5-20 Port blocking dialog for ITU-T, China and UK ISUP

Port – Use this option to select the port for which the blocking state is to be configured. Multiple ports may be configured in a single operation. ITU-T, China and UK ISUP ports have a different configuration screen to other TDM ports.

Apply Hardware Block to Port – When checked, hardware blocking will be applied to all bearer timeslots on the port. All calls in progress on the port will be cleared down, and no new calls will be allowed. Un-checking this box will remove hardware blocking and allow calls to be made on the port once again.

CAUTION

Applying a hardware block for SS7 causes all calls on the port to be immediately cleared down, and prevents any further calls from being made on the port until the hardware block has been removed.

Apply Maintenance Block to Timeslot – This group of controls allows maintenance blocking to be applied to individual bearer timeslots, and only those checkboxes that correspond to bearer timeslots will be enabled. When checked, maintenance blocking will be applied to the timeslot. Any call currently in progress on the timeslot will be allowed to complete, but no new calls will be accepted. Un-checking a box will remove the maintenance blocking and allow calls to be made on the timeslot once again.

The Select All and Clear All buttons are aids to typing whose use will cause all timeslot boxes to become checked or unchecked respectively.

As SS7 blocking operations need to communicate with the far end of a link, they are posted for asynchronous execution. When an SS7 blocking operation fails because the far end is unreachable, it is re-posted and executed again.

To determine when an SS7 blocking operation has taken effect, the layer 2 state of the port can be monitored using the Data Link filter. The layer 2 reports contain a (hexadecimal) bitmap of the current layer 2 state of the port. When a timeslot has been successfully blocked, its layer 2 state will be reported as 0.

5.11.2 Port blocking for ANSI SS7 and non-SS7 TDM ports

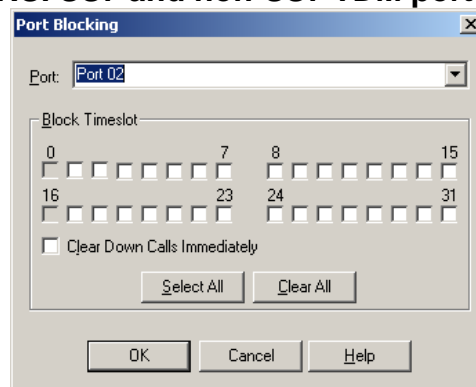


Figure 5-21 Port blocking dialog for ANSI SS7 and non-SS7 TDM ports

Block Timeslot – Only the checkboxes representing the bearer timeslots on the port will be enabled. Check a box to place the corresponding timeslot out of service, and uncheck the box to place it back in service. Once out of service, GroomerII will not allow either incoming or outgoing calls to be made on the timeslot.

When the protocol on the port is T1RB (Robbed Bit), 'Back Busy' will be used to take timeslots in and out of service. This signals the availability of the timeslots to the remote end.

When the protocol is one of AT&T, NI2 or DMS100, SERVICE messages will be used to block or unblock the timeslots. These messages signal the state of the timeslot to the remote end.

When the protocol on the port is ANSI SS7, CIC blocking will be used to block and unblock the timeslots.

Clear Calls Immediately – When checked, if a timeslot on this port that is to be placed out of service is currently carrying a call, that call will be cleared down. When unchecked, any calls currently in progress on blocked timeslots will be allowed to complete, but no new calls will be accepted.

Select All/Clear All – These buttons are aids to typing whose use will cause all timeslot boxes to become checked or unchecked respectively.

5.11.3 Port blocking for IP telephony ports

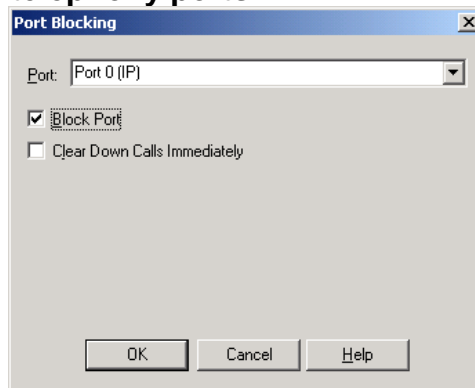


Figure 5-22 Port blocking dialog for IP ports

Block Port – IP telephony has no concept of timeslots, and so the entire port must be placed out of service. Check the box to place the port out of service, and uncheck the box to place it back in service. Once out of service, GroomerII will not allow either incoming or outgoing calls to be made on the port.

Clear Down Calls Immediately – When checked, if the port is to be placed out of service and is currently carrying calls, those calls will be cleared down. When unchecked, any calls currently in progress on the port will be allowed to complete, but no new calls will be accepted.

Closing the dialog using the OK button will (re)apply the configured blocking state to all ports. Closing the dialog using the Cancel button will discard any blocking state changes made.

Blocking operations are reported to the GroomerII Status Monitor using the Data Link events filter; see section 6.2.2 for further details.

5.12 Firmware reload

The firmware reload option is used to re-load the firmware for a selected port, for example, when changing firmware switch options. The information displayed in the Load Firmware dialog is synchronised with the configuration files used by the Aculab Configuration Tool.

The Load Firmware dialog makes it possible to download firmware to an individual port, without closing down GroomerII. It also allows the firmware or switches to be modified before downloading takes place. Changes will persist and will be applied to GroomerII when it is restarted.

Selecting Port - Load... from the menu will open the Load Firmware dialog.

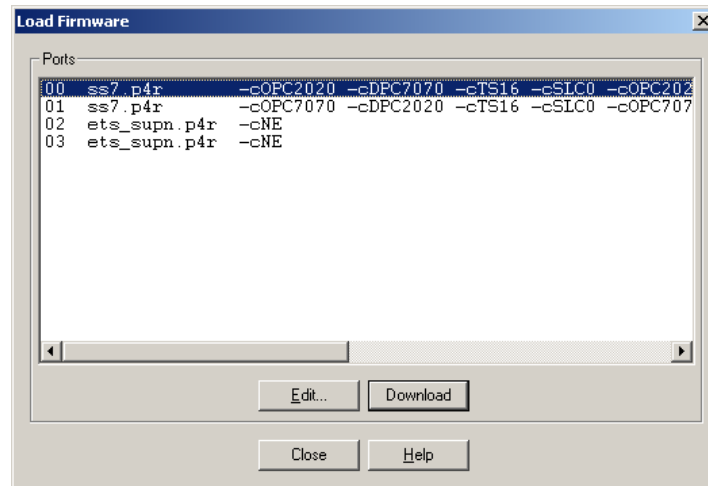


Figure 5-23 Load firmware dialog

To re-load the firmware for a specific port, make your selection from the Ports list, and then select Download. To confirm download progress, the following dialog will be displayed:

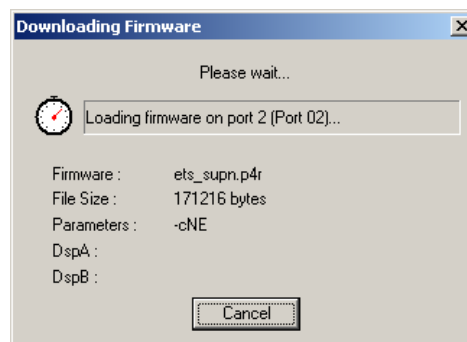


Figure 5-24 Download firmware progress dialog

NOTE

If the type signalling firmware on a port is changed then all timeslots on the port will be blocked following the download operation, and must be unblocked in the Port Blocking screen (see section 5.11) before calls can be passed.

If additional bearer channels are added to SS7 ports then these channels will be maintenance blocked following the download operation, and must be unblocked in the Port Blocking screen (see section 5.11) before calls can be passed.

To modify the firmware for a specific port, make your selection from the Ports list, and then select Edit.... The following dialog will be displayed:

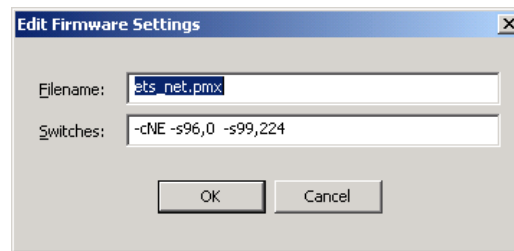


Figure 5-25 Edit firmware dialog

The edit firmware settings function must be used with extreme care, as entering invalid parameters may render a port unable to pass calls.

Filename – This is the filename of the protocol firmware that will be downloaded to the port.

Switches – These are the firmware switches that will be applied when the above file is downloaded to the port. For details of available switches, please see the release note for the selected protocol firmware.

Selecting OK to close the dialog will only save the updated settings; it will not reload the firmware. To reload the firmware, use the Download button.

CAUTION

If the firmware on a port is configured incorrectly it could result in that port not being able to route calls.

GroomerII does not support changing the type of the port from E1 to T1 or from T1 to E1 using the download functionality. GroomerII must be restarted when a port is to be changed in this way.

The reload firmware function will disconnect any calls that are in progress on the port prior to starting the download.

When working with multiple port SS7 links, when the signalling port is reloaded, calls on bearer only ports that are using the reloading port for signalling will not be cleared down. It is strongly recommended that prior to reloading SS7 signalling ports, all other SS7 ports are blocked. See section 5.11 for further details.

5.13 Port reset

The Port Reset dialog is used to reset individual bearer channels. At present only SS7 ports are supported. The dialog can be used to reset bearer channels on multiple ports simultaneously.

Select Port – Reset... to open the Port Reset dialog.

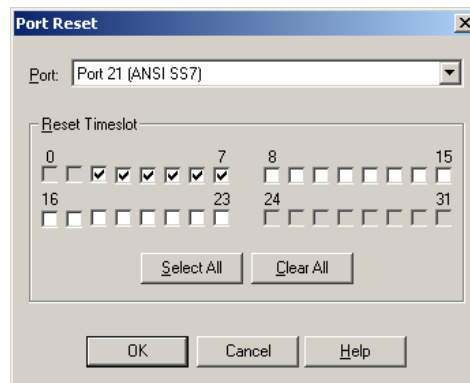


Figure 5-26 Port Reset dialog

Port – Use this control to select the port on which bearer channels are to be reset. Only ports loaded with SS7 firmware will be displayed in this list.

Reset Timeslot – Only those checkboxes representing bearer channels on the selected port will be enabled. Check a box to reset the corresponding timeslot. The Select All and Clear All buttons can be used to check or clear all checkboxes.

NOTE

The reset will not be applied until the dialog is closed using the OK button. When a reset is applied, any calls in progress on the selected timeslots will be cleared and the timeslot will not be available for new calls until the reset is complete.

5.14 SS7 signalling links

The SS7 Signalling Links dialog is used to activate and deactivate SS7 signalling links.

Select Port – SS7 Signalling Links... to open the SS7 Signalling Links dialog.

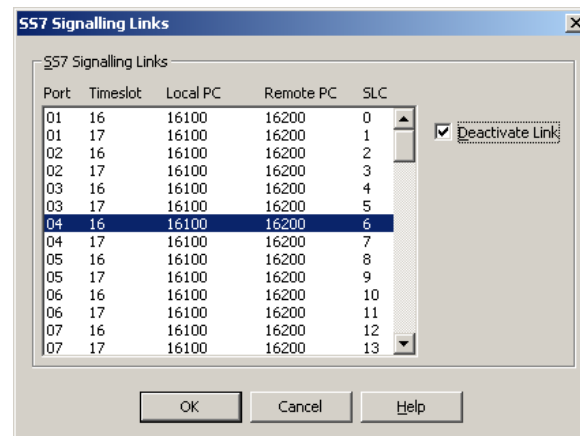


Figure 5-27 SS7 Signalling Links dialog

The listbox contains an entry for each SS7 signalling link that has been configured by a port download (for example, -cOPC2020 -cDPC7070 -cTS16 -cSLC1), and is ordered by Port and Timeslot.

Deactivate Link – Check this control to deactivate the selected signalling link, and uncheck the control to activate it again.

The GroomerII Kernel will maintain signalling link activation/deactivation settings across system shutdown in the following way:

- When the GroomerII Kernel is closed, all deactivated signalling links are activated as part of the shutdown procedure (all SS7 bearer channels are hardware blocked at this point to prevent call delivery).
- When the GroomerII Kernel is restarted, any signalling links that were deactivated prior to running the shutdown procedure will be deactivated again as part of the startup procedure (the configured blocking status of all bearer channels is re-applied at this point to allow call delivery).

Multiple signalling links may be configured at the same time, with all changes being applied when the dialog is closed using the OK button. A warning will be given if the last signalling link to a destination is about to be deactivated, and you will be required to confirm the operation.

5.15 Continuity check

The Continuity Check dialog is used to conduct manual continuity checks on SS7 bearer circuits.

Select Port – Continuity Check... to open the Continuity Check dialog.

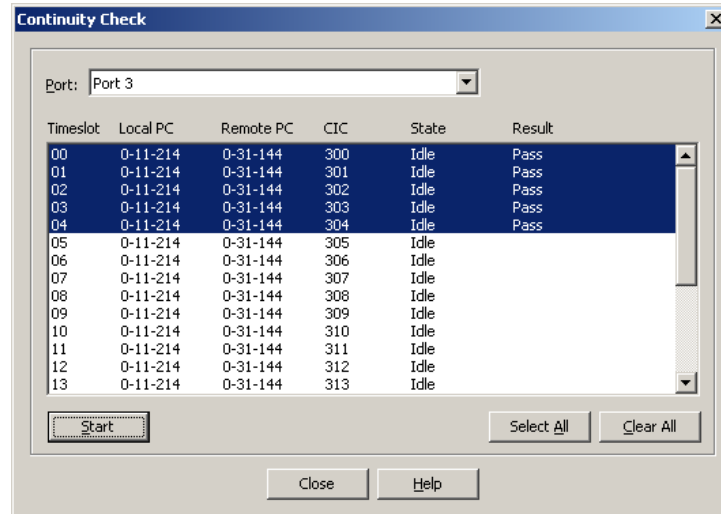


Figure 5-28 Continuity Check dialog

The listbox contains entries for all the SS7 bearer circuits associated with a port. The State column reports the current state of the circuit which may be one of the following:

Idle – The circuit is idle.

Recheck – The circuit is performing periodic continuity rechecks.

Blocked – The circuit is blocked.

Active – A call is present on the circuit.

Testing... – A manual continuity check is in progress.

Stopping... – A manual continuity check is stopping.

The Result column reports the last manual check result of the circuit which may be empty if no check has been carried out, or one of the following:

Pass – The check passed.

Fail – The check failed.

Release cause *n* – The remote end terminated the check with the clearing cause *n*.

No Resources – GroomerII has insufficient resources to run the check.

Circuit Blocked – Circuit was blocked whilst the check was in progress.

Circuit Reset – Circuit was reset whilst the check was in progress.

Circuit Active – An incoming call arrived whilst the check was in progress.

Stopped – The operator has manually stopped the check, or GroomerII stopped the check for an unspecified reason.

Manual continuity checks are carried out by selecting one or more entries from the listbox and clicking the Start button. It is only possible to start manual checks on circuits that are in the Idle or Recheck state. Starting manual checks on a group of circuits will only be permitted if all selected circuits are in the appropriate state.

Port – Use this control to select a port on which to conduct manual continuity checks.

Start – Use this control to start manual continuity checks for the circuits selected in the listbox. While manual continuity checks are running, the Start control changes to a Stop control that may be used to terminate the running checks.

Select All/Clear All – Use these controls to select or deselect all entries in the list box.

NOTE

GroomerII will not place the circuit into the recheck state when a manual continuity check fails. GroomerII will take the circuit out of the recheck state when a manual continuity check passes.

6 GroomerII status monitor

The primary function of the GroomerII Status Monitor is to assist with fault finding. The GroomerII Status Monitor is able to present the current status of the telephony ports in the system, and also has the capability to log system event information.



The status monitor will automatically run when the system is started. Should the status monitor be closed for any reason, it can be restarted by double clicking the GroomerII Status Monitor icon on your desktop.

NOTE

The GroomerII Kernel must be running for the GroomerII Status Monitor to successfully start.

There are six tabs available, the Alarms tab is displayed by default when opening the dialog. The SS7 tab will only be displayed when SS7 firmware is configured on one or more TDM ports. The CAS tab will only be displayed when CAS protocol firmware is configured on one or more TDM ports.

Menu options

- | | |
|------|--------------------------------|
| File | - Exit |
| View | - Events |
| | Alarms |
| | Diagnose |
| | Gateways |
| | SS7 |
| | CAS |
| Help | - Content |
| | Search... |
| | Index... |
| | About GroomerII Status Monitor |

6.1 Alarms

Select the Alarms tab in the GroomerII Status Monitor dialog to view the current received alarm status of each GroomerII telephony port.

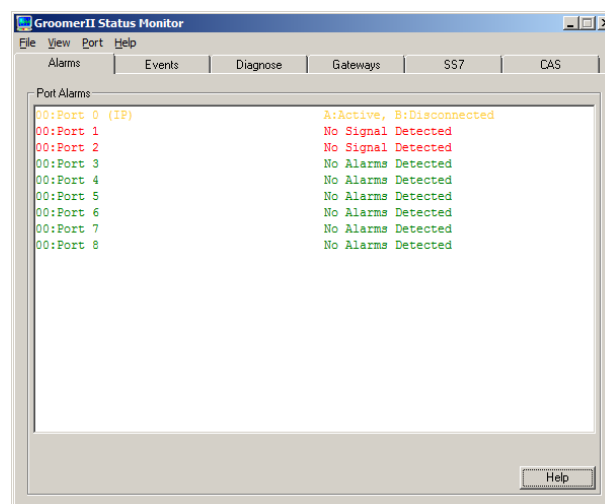


Figure 6-1 GroomerII status monitor alarms tab option

The ports will be displayed in the order that they are declared in the GroomerII Configuration Editor Port Configuration screen, section 8.3 refers. The port will be identified in the form `xx:Port n`, for example `00:Port 2`, where `xx` is the card number on which the port is located, and `n` is the system port number.

The port status may be shown as one of the following:

Card Not Started	This will be seen when GroomerII is first started. It indicates that the Prosody X card is being started and initialised and will remain until initialisation is complete. The port may remain in this state for several minutes.
Card Stopped	This will be seen if the Prosody X card has stopped or restarted for any reason during operation. The port will remain in this state until the system is restarted.

These alarms, when present, will take precedence over link status alarms.

NOTE

GroomerII will not attempt to route calls to ports on a Prosody X card that is not fully started.

In the case of IP ports, the current status of ports A and B is displayed, and each will be either:

Active	the port is connected to a working switch and is currently selected as the one that will be used for RTP traffic.
Connected	the port is connected to a working switch but is not currently selected for use by RTP traffic.
Disconnected	the port is not currently connected to a working switch.

NOTE

The Aculab software will automatically select which port is the `Active` port. Only one port can be active at any time.

To assist in the rapid identification of status, the following colour coded entries are used for IP ports:

Red	both ports are <code>Disconnected</code> , calls will fail.
Yellow	one port is <code>Active</code> and the other <code>Disconnected</code> . The port requires attention.
Green	one port is <code>Active</code> and the other <code>Connected</code> .

NOTE

Providing one port is `Active`, calls can be passed.

In the case of TDM ports only the highest priority alarm on the port is displayed. To view all the alarms for a selected port, use the `Diagnose` tab option. The alarm priorities in descending severity order are:

Layer 1 Stats Failed	The port status could not be read. This is often a transient error caused by timing. If the error persists it will indicate a serious hardware or software failure.
----------------------	---

Card Clock Stopped	This indicates that the protocol firmware on the port is no longer running. Reloading the port firmware may cure this condition.
No Signal Detected	Indicates that the E1/T1 cable is faulty or has been disconnected at one end.
Alarm Indication Signal Detected	Indicates that GroomerII is receiving an Alarm Indication Signal from the far end equipment.
Loss of Synchronisation	Indicates that GroomerII is receiving a Loss of Synchronisation indication from the far end equipment.
Remote Alarm Indication Detected	Indicates that GroomerII is receiving a Remote Alarm Indication from the far end equipment.
CAS Multiframe Alarm Detected	Indicates that GroomerII is receiving a CAS Multiframe Alarm from the far end equipment.
No Alarms Detected	Indicates that GroomerII is not receiving any alarms from the far end equipment.

To assist in the rapid identification of status, the following colour coded entries are used:

- Red failure, a local/received alarm, for example, no received signal detected.
- Yellow indicates remote alarms are being detected (RAI), calls may fail.
- Green OK, no alarm state has been detected.

6.2 Events

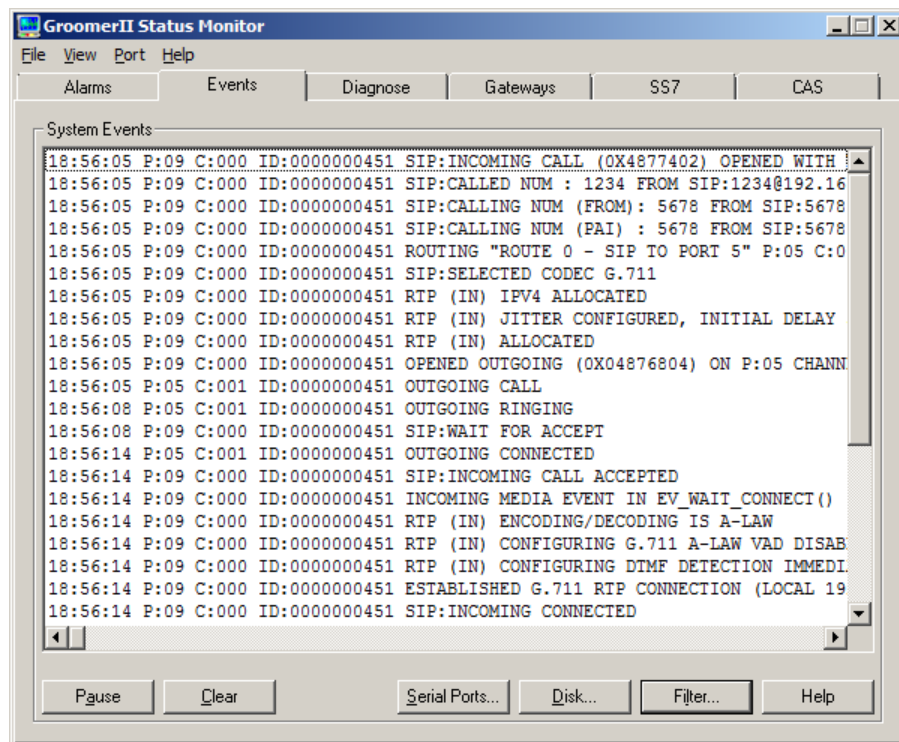


Figure 6-2 GroomerII status monitor events tab option.

Subject to the Filter configuration, time stamped event information is logged to the dialog.

6.2.1 Pausing the log

The System Events list displays the last 100 events. Should you wish to browse these events you will first need to pause the event updates.

Select Pause to stop the updates. The Pause button changes to Resume.

In the paused state, the last 400 lines will be stored in a buffer and sent to the screen when Resume is pressed.

Clear is used to clear the System Events dialog.

If the trace required is larger than 100 lines, you will need to log the trace to disk (file) or output the information to an external device via one of the RS232 (COM) ports.

6.2.2 Event filters

Filters are used to select the type of information to be logged, the ports to be monitored and the destination of the information. Select Filter... to open the Filter Settings dialog.

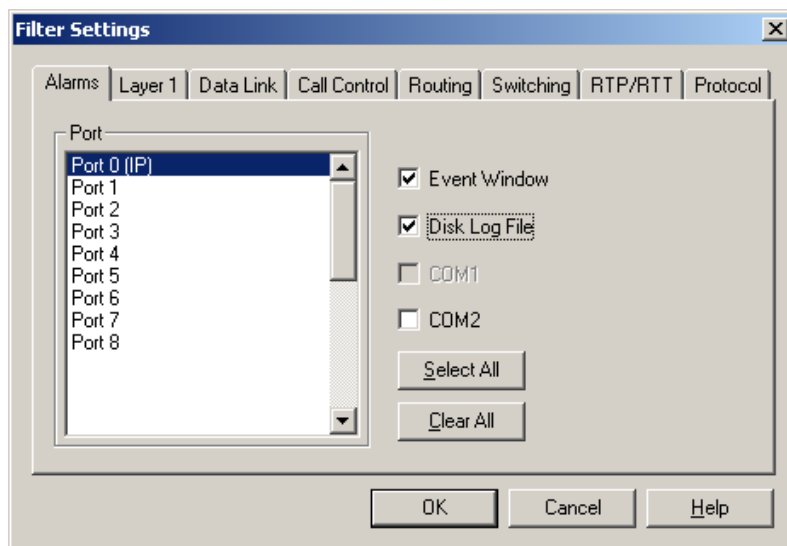


Figure 6-3 Filter settings dialog

Select each event category tab as required, for example, Alarms or Call Control. On each one select the ports to be monitored followed by the destination of the events. In the above example logging will be displayed in the Events dialog as well as being output to a disk log file.

6.2.2.1 Event categories

Alarms – records the alarms generated and cleared by the Alarm Mapping functionality, section 8.6.5 refers.

Layer 1 – logs the status of layer 1 every 2 seconds.

Data link – logs the status of layer 2 every 2 seconds (Not applicable to IP telephony ports).

Call Control – Shows call control events such as incoming call, outgoing call, ringing, connected, disconnect, etc.

Routing – Shows the routing table entry selected by a call passing through the system.

Switching – Shows the H.100 and card switching used in GroomerII. This is for fault finding purposes only and has little meaning outside of Aculab.

RTP/RTT – Shows events associated with the allocation and configuration of RTP and RTT streams (applicable only to SIP ports).

Protocol – Shows protocol trace from the ports. This displays all information sent and received by a port. With the exception of CAS, the trace is a pure hexadecimal dump of the protocol message and is often used by Aculab to identify problems. (Not applicable to SIP ports)

NOTE

When logging protocol trace on an SS7 linkset, the trace will be logged against the port selected by the driver to carry the signalling. This may not be the same port on which the call was placed. Signalling links are selected on a call-by-call basis, so to be sure that you capture the all of the trace for your call, protocol trace should be enabled on all ports carrying SS7 signalling links.

NOTE

Although you can select IP ports in all the options, selecting them in Data Link or Protocol will have no effect. Similarly, selecting TDM ports in RTP/RTT will have no effect.

6.2.2.2 Sample trace

Trace Type	Trace File
CALL	16:26:48 P:02 C:001 ID:0002141615 Incoming Call (0x3b7002), opened ts 1
	16:26:48 P:02 C:001 ID:0002141615 Called Num : 234501
	16:26:48 P:02 C:001 ID:0002141615 Calling Num : 234501
ROUTING	16:26:48 P:02 C:001 ID:0002141615 Routing "Route TDM - SIP" P:00 C:--
	16:26:48 P:00 C:000 ID:0002141615 RTP echo status 0
	16:26:48 P:02 C:001 ID:0002141615 RTP_ALLOCATED (OUT)
	16:26:48 P:02 C:001 ID:0002141615 Opened outgoing (0x00239802) on P:00
	(SIP) to <sip:234501@192.168.16.248>
	16:26:48 P:00 C:000 ID:0002141615 SIP:Outgoing call on st:64, ts:00
SWITCH	16:26:48 P:02 C:001 ID:0002141615 On card bi itoo : sw:00 ist:33
	its:01 ost:64 ots:00
	16:26:48 P:02 C:001 ID:0002141615 On card bi otoi : sw:00 ist:64
	its:00 ost:33 ots:01
CALL	16:26:48 P:00 C:000 ID:0002141615 SIP:Outgoing Ringing
	16:26:48 P:02 C:001 ID:0002141615 Wait for Accept
PROTOCOL	16:26:49 P:02 C:-- TX: 02 01 01 01
	16:26:49 P:02 C:-- RX: 02 01 00 00 08 02 00 2F 05 A1 04 03 80 90 A3
	18 03 A9 83 81 6C 08 00 80 32 33 34 35 30 31
	70 07 80 32 33 34 35 30 31
	16:26:49 P:02 C:-- TX: 02 01 01 02
	16:26:49 P:02 C:-- TX: 00 01 00 02 08 02 80 2F 02 18 03 A9 83 81
	16:26:49 P:02 C:-- RX: 00 01 01 02
	16:26:49 P:02 C:-- TX: 00 01 02 02 08 02 80 2F 01
CALL	16:26:50 P:00 C:000 ID:0002141615 Outgoing Media Event in ev_outgoing()
	16:26:50 P:00 C:000 ID:0002141615 Established G.711 RTP connection (local
	192.168.16.229:16642 remote 192.168.16.248:3084)
	16:26:50 P:00 C:000 ID:0002141615 SIP:Outgoing Connected
	16:26:50 P:02 C:001 ID:0002141615 Incoming Call Accepted
	16:26:50 P:02 C:001 ID:0002141615 Incoming Connected
PROTOCOL	16:26:51 P:02 C:-- RX: 00 01 01 04
	16:26:51 P:02 C:-- TX: 00 01 04 02 08 02 80 2F 07
	16:26:51 P:02 C:-- RX: 00 01 01 06
	16:26:51 P:02 C:-- RX: 02 01 02 06 08 02 00 2F 0F
CALL	16:27:00 P:00 C:000 ID:0002141615 Disconnecting G.711 RTP connection
	(local 192.168.16.229:16642 remote 192.168.16.248:3084)
	16:27:00 P:00 C:000 ID:0002141615 SIP:Stopping RTP (OUT) con_idle
	16:27:00 P:00 C:000 ID:0002141615 SIP:Outgoing Call Gone Idle
	16:27:00 P:02 C:001 ID:0002141615 Incoming Call Disconnected
	16:27:00 P:00 C:000 ID:0002141615 SIP:rtp_release(OUT)
	16:27:00 P:02 C:001 ID:0002141615 Incoming call has gone idle
SWITCH	16:27:00 P:02 C:001 ID:0002141615 Switch Disable : sw:00 ost:33 ots:01
	16:27:00 P:00 C:000 ID:0002141615 Switch Disable : sw:00 ost:64 ots:00
CALL	16:27:00 P:02 C:001 ID:0002141645 Openin from previous call ID:0002141615
	16:27:00 P:02 C:001 ID:0002141645 waiting for incoming
PROTOCOL	16:27:01 P:02 C:-- TX: 02 01 01 04
	16:27:01 P:02 C:-- TX: 00 01 06 04 08 02 80 2F 45 08 02 80 90
	16:27:01 P:02 C:-- RX: 00 01 01 08
	16:27:01 P:02 C:-- RX: 02 01 04 08 08 02 00 2F 4D
	16:27:01 P:02 C:-- TX: 02 01 01 06
	16:27:01 P:02 C:-- TX: 00 01 08 06 08 02 80 2F 5A

Figure 6-4 Sample trace for a Euro ISDN to SIP call with Call Control, Routing, Switching and Protocol trace enabled

Key

CALL	Call control information
PROTOCOL	Protocol Information with TX for data sent by GroomerII and RX for data received by GroomerII.
ROUTE	Routing information. The name of the route selected from the .cfg file
SWITCH	Voice path switching information.
P:XXX	The Port number starting at 00.
C:XXX	The channel (timeslot) number.

ID:XXXXXXXX The unique identifier assigned to the call by GroomerII.

See Appendix E: for a more detailed explanation of GroomerII trace.

NOTE

Protocol and layers 1 and 2 do not have channel references because they apply to the whole port or the D channel.

6.2.2.3 Event output options

Each category of events can be set to output to one or more destinations by checking the required options.

Event Window – outputs events to the status monitor events list.

Disk Log File – logs events to disk. The number of files and lines per file are defined using the Disk... option.

COM1/COM2 – events are output as ASCII text to the systems selected serial communications (COM) ports. The serial port settings are configured using the Serial Ports... option.

NOTE

If you wish to direct output to a serial port, that port must also be enabled for logging in the Serial Port Logging screen.

NOTE

The Status Monitor application will disable the checkbox for any COM port that is not present. The GroomerII 1U (AC2460) chassis does not support serial port logging.

The Select All and Clear All buttons may be used to select or deselect all entries in the Port list, and have no other function.

6.2.3 Logging events to a disk file

If you checked the Disk Log File option for any of the categories in Filter Settings, use the Disk... option to define the size and number of the log files.

Select Disk... from the GroomerII Status Monitor dialog to open the Disk Log Settings dialog.

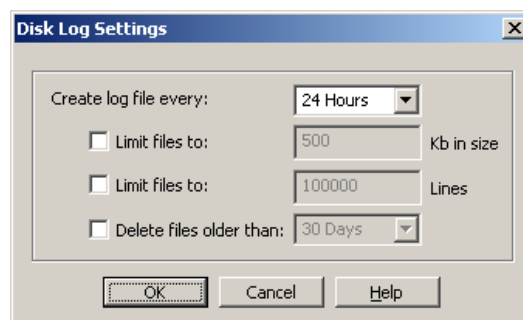


Figure 6-5 Disk log settings dialog

Create log file every – When enabled this option will cause the current trace file to be closed and a new one started after the specified time. The datum time is midnight, when a new file will always be started.

Limit files to x Kb in size – When a trace file reaches the specified size, the file will be closed and a new file started when this option is enabled.

Limit files to x lines – When a specified number of lines have been written to a trace file, the file will be closed and a new file started if this option is enabled.

Delete files older than – When enabled this will cause trace files to be automatically deleted when they are older than specified.

CAUTION

The trace generated by GroomerII is for diagnostic purposes, and it is not expected to be used for long periods. Attempting to log extremely high quantities of trace may result in data being lost.

The trace files will be logged to `C:\Program Files (x86)\GroomerII\Trace`. Filenames are composed of the system name, file start date and file start time in the form `name_yyyymmdd_hhmmss.log`, for example `G5432_20160601_160000.log`.

NOTE

The trace from all filters is written to a single file.

6.2.4 Logging events to the serial ports

If you checked either of the COM1 or COM2 options for any of the categories in Filter Settings, you should ensure that the Serial Ports parameters are correct.

Select **Serial Ports...** from the GroomerII Status Monitor dialog to open the Serial Port Logging dialog.

NOTE

The GroomerII 1U (AC2460) chassis does not support serial port logging, and the **Serial Ports...** button will be disabled.

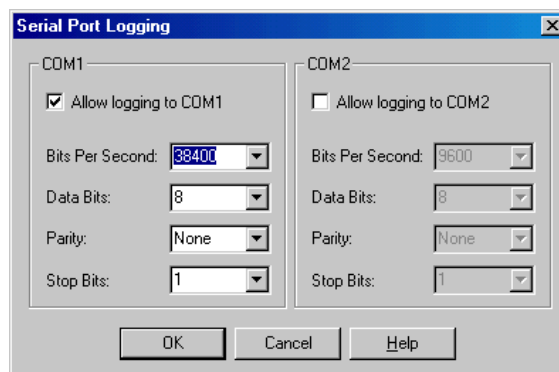


Figure 6-6 Serial Port Logging dialog

NOTE

The Status Monitor application will disable the COM n control group for any COM port that is not present.

Set the serial interface baud rate and data size to the required interface settings.

OK confirms the settings and closes the dialog.

CAUTION

Serial port logging is a legacy feature, and the volumes of data that it is possible for the GroomerII to generate could exceed the serial ports transmission capacity.

6.3 Diagnose

Select the Diagnose tab to view the hardware status of a port, and select the required port from the Port pull down menu.

6.3.1 Diagnostics report – E1/T1 trunk port

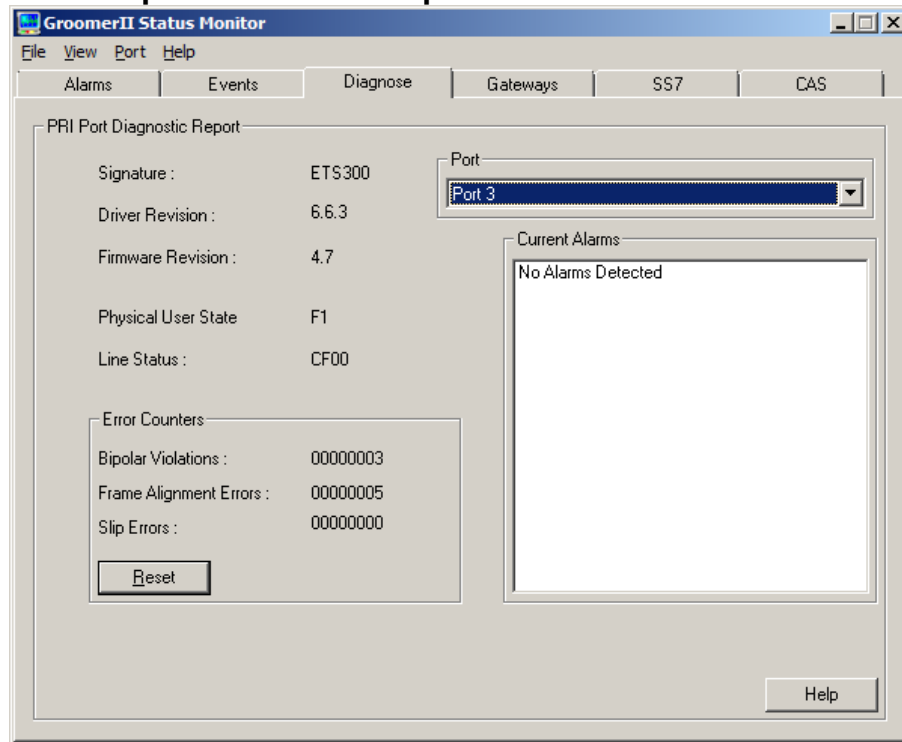


Figure 6-7 GroomerII status monitor diagnose tab option – E1/T1 trunk

Signature – details the name of the firmware running on the card.

Driver and Firmware Revision – detail the revision numbers for the driver and firmware in use on the selected port.

Physical User State and Line Status – are low level hardware monitors and have little meaning outside Aculab.

Error counters – The fields in this group show low-level link information:

Bipolar Violations and Frame Alignment Errors – are low level hardware monitors and have little meaning outside Aculab.

Slip Errors – are a count of the slips received on a port. Use the **Reset** button to zero this count and monitor how long it takes to build up. Slips will occur when the port is in an alarm state. When the ports show ready and are showing slips, the primary clock source should be checked.

Reset – is used to zero the Bipolar Violations, Frame Alignment Errors and Slip Errors counters, and clear any previous alarm indications in the Line Status field.

NOTE

The Port - Reset TDM Error Counters menu option may be used to clear the Line Status and Error Counters indicators on all TDM ports in a single operation.

Current alarms – Details the layer 1 alarms being transmitted and received on the selected port. Unlike the GroomerII Status Monitor Alarm tab, which displays the highest priority received alarm only, this field shows all the alarms being generated on the port.

6.3.2 Diagnostics report – IP port

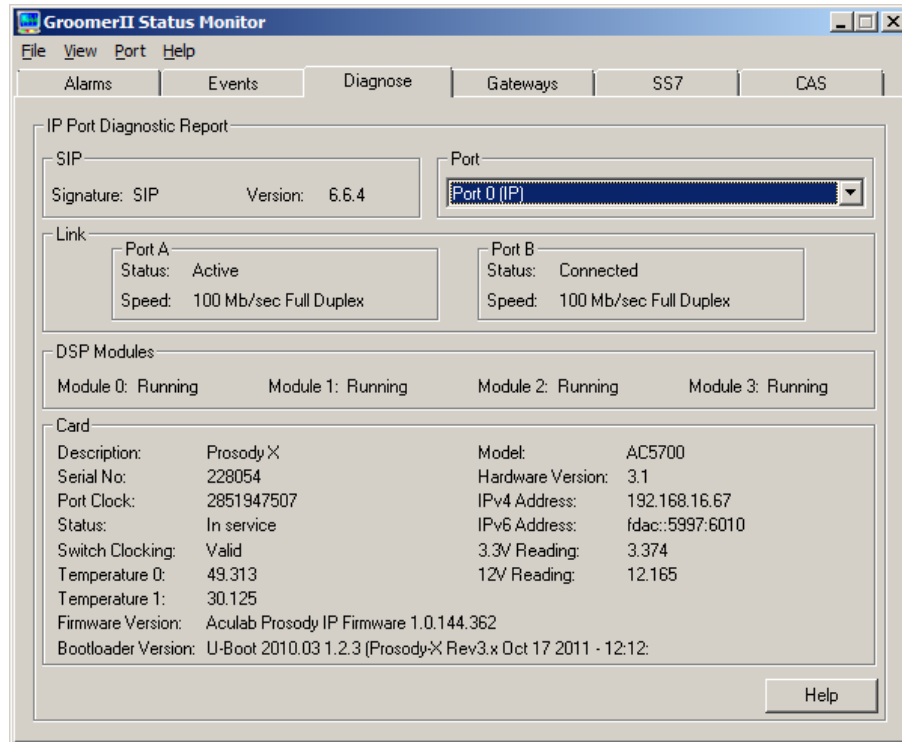


Figure 6-8 GroomerII status monitor diagnose tab option – IP port

SIP – The fields in this group identify the SIP software running on the system:

Signature – displays the signature of the SIP software running on the system.

Version – displays the revision number of the SIP software running on the system.

Link – The fields in this group show the connection status of each of the individual IP ports on the card.

Status – The connection status of the port. This should be one of:

Active – This port is the one on which any traffic passed by the card will be carried.

Connected – There is a cable plugged into the port, but it is currently being used as the fallback port.

Disconnected – There is no cable plugged into this port, the cable that is plugged into it is not connected at the far end, or the equipment at the far end is not running.

Speed – If the port status is Active or Connected, then this field will show the speed and type of the connection. If the status is Disconnected then this field will have no meaning.

DSP Modules – The fields in this group show the current status of each media processing module associated with this port, and will be one of the following.

Starting	The card is carrying the module has not yet started.
Not Fitted	There is no module fitted in this position.
Not Started	The module failed to start when the card started. Modules in this state are unable to process calls, and will be excluded from selection. Should you encounter this state contact Aculab Technical Support.
Running	The module has started, and is available for call processing. This is the normal state.
Stopped	The module was previously in the Running state, but has since stopped. Modules in this state are unable to process calls, and will be excluded from selection. Should you encounter this state contact Aculab Technical Support.

Card – The fields in this group contain information about the card on which the port is located:

Description – the type of card that the port is located on. Currently this will always be Prosody X.

Serial No – displays the serial number of the Prosody X baseboard.

Port Clock – This counter should be constantly changing. If the counter stops, the card is in reset mode and may require re-booting.

Status – displays the current service state of the Prosody X card.

Switch Clocking – indicates the current status of the boards switch clocking. This will be one of Valid, Invalid or Unable to Determine.

Temperature X – these are the temperatures recorded by each of the on card sensors. These values should not exceed 55°C.

Firmware Version – displays the reversion number of the Aculab IP Telephony firmware running on the card.

Bootloader Version – displays the reversion number of the bootloader running on the card.

Model – displays the Aculab model number of the Prosody X baseboard.

Hardware Version – displays the reversion number of the Prosody X baseboard.

IPv4 Address – is the IPv4 address of the media port on the Prosody X card, or Not configured if no IPv4 address has been set.

IPv6 Address – is the IPv6 address that is used for communication between the host and the Prosody X baseboard, or Not configured if no IPv6 address has been set.

3.3V Reading – this is the voltage that the card is detecting on the 3.3V power feed.

12V Reading – this is the voltage that the card is detecting on the 12V power feed.

6.4 Gateways

This page displays the status of each of the SIP gateways to which outgoing calls can be directed.

Address	Status	Current Calls	Monitor	Disabled
192.168.16.65	AVAILABLE	0	Yes	
192.168.16.213	AVAILABLE	15	Yes	
192.168.16.218	AVAILABLE	4	Yes	
192.168.16.224	UNAVAILABLE (TIMEOUT)	0	Yes	
Idac:6a32:1015:5994:5000	AVAILABLE	0		Yes
Idac:6a32:1015:5995:5000	AVAILABLE	0		Yes
Idac:6a32:1015:5996:5000	AVAILABLE	0		Yes
Idac:6a32:1015:5997:5000	AVAILABLE	0		Yes

Figure 6-9 GroomerII Status Monitor Gateways page

There is one entry in the list for each of the gateways configured in the System Configuration – SIP Gateways – Gateways page (see section 8.6.9), and only those gateways configured in that page are reported on this screen.

The Address column will list IPv4 addresses ahead of IPv6 addresses, with each address group sorted in network order.

The Status field shows the current status of the gateway, and will be one of the following:

DISCOVERING – the gateway is waiting to be polled for the first time.

AVAILABLE – the latest poll reported that the gateway was able to accept SIP calls. When monitoring of the gateway is not enabled this status will be shown.

UNAVAILABLE (nnn) – the latest poll reported that the gateway was unable to accept SIP calls, with *nnn* indicating the SIP **OPTIONS** response.

UNAVAILABLE (CALL) – an outgoing call to the gateway has been rejected with one of the responses in the Unavailable Responses list (see section 8.6.9).

UNAVAILABLE (TIMEOUT) – the gateway is not responding and is unreachable.

UNAVAILABLE (SERVER) – an unexpected error occurred when determining the gateway status.

The Current Calls field shows the number of calls in progress to and from the gateway.

The Monitor field will show **Yes** if this gateway monitoring enabled, and will be blank otherwise.

The Disabled field will show `Yes` if the Disable Selection checkbox in the System Configuration – SIP Gateways – Gateways page (see section 8.6.9) is checked, and will be blank otherwise. This field does not report the setting of the Disable Selection checkbox on the System Configuration – SIP Gateways – Routes page.

6.5 SS7

This page is only available when at least one TDM port has been configured to use the SS7 protocol. The following pages provide continuous monitoring of SS7 objects.

6.5.1 Signalling

This page provides continuous monitoring of the SS7 signalling links in the system.

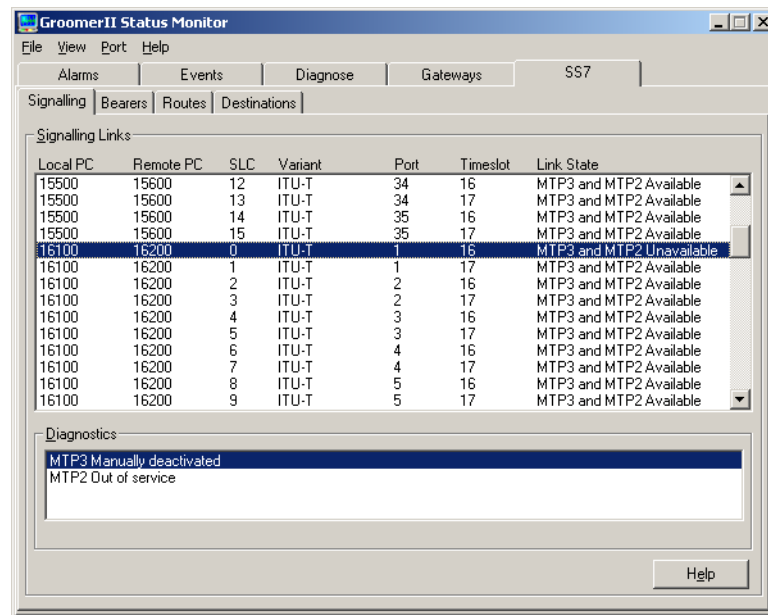


Figure 6-10 GroomerII Status Monitor SS7 Signalling page

The primary listbox is ordered by Local PC, Remote PC, and SLC and contains an entry for each signalling link that has been configured by an SS7 firmware download (for example, -cOPC2020 -cDPC7070 -cTS16 -cSLC1).

The Variant field shows which variant has been declared in the [MTP3] section of the SS7 stack file for that signalling link. See section 15.1 for details of the SS7 stack file.

The State column reports the current state of the link, the normal state being MTP3 and MTP2 Available. When a link is not in the normal state, selecting it will list the reasons in the Diagnostics listbox.

NOTE

Any issues reported in the Diagnostics listbox will prevent traffic from being passed. However, some issues are transient in nature and will only be present whilst a link is being brought into service.

6.5.2 Bearers

This page provides continuous monitoring of the SS7 bearer channels in the system.

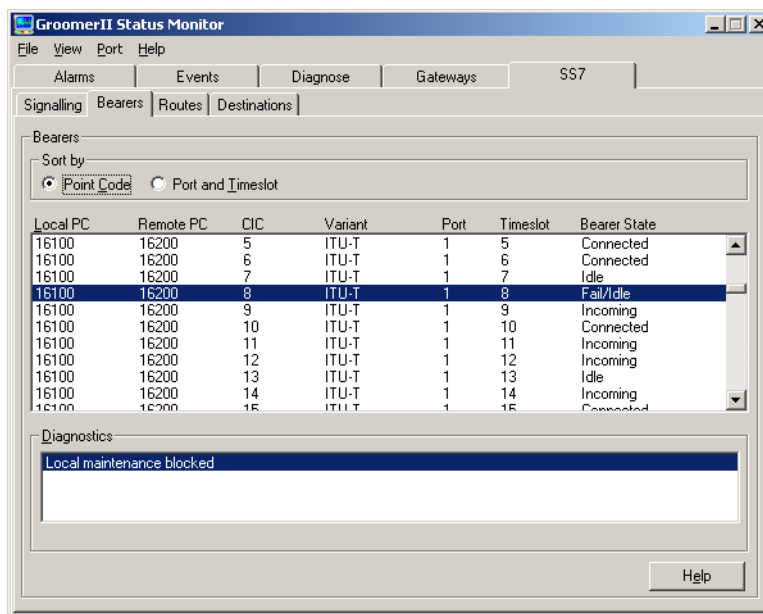


Figure 6-11 GroomerII status monitor SS7 Bearers page

The primary listbox contains an entry for each bearer channel configured by an SS7 firmware download (for example, `-cOPC2020 -cDPC7070 -cCIC1,ffffefffe,ffffefffe`). Use the radio buttons in the Sort by group to order the list either by Local PC, Remote PC, and CIC, or by Port and Timeslot.

The Variant field shows which variant has been declared in the [ISUP] section of the SS7 stack file for that bearer. See section 15.1 for details of the SS7 stack file.

The State column reports the current state of the bearer, the normal states being:

- Idle
- Incoming
- Outgoing
- Connected
- Released
- Free

When a bearer is not in the normal state (this includes any of the above states preceded by `Fail/`), selecting it will list the reasons in the Diagnostics listbox.

NOTE

Any issues reported in the Diagnostics listbox will prevent calls from being passed. However, some issues are transient in nature and will only be present whilst a bearer is being reset or returned to service.

6.5.3 Routes

This page provides continuous monitoring of the SS7 routes that are used by the system.

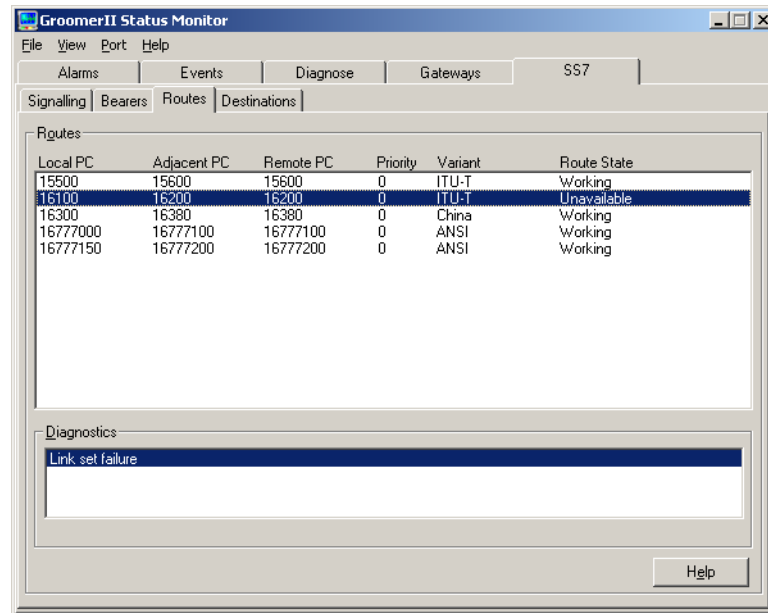


Figure 6-12 GroomerII status monitor SS7 Routes page

The primary listbox contains entries for each destination (for example, -cDPC7070) that has been configured by an SS7 firmware download, with the list ordered by Local PC Adjacent PC, Remote PC and Priority. Two types of route may be reported:

- Direct routes, where a direct connection exists between GroomerII and the destination. For such a route the Adjacent PC and Remote PC fields will be identical, whilst the Priority field will always be set to 0.
- Indirect routes, where the path to the destination passes through a Signalling Transfer Point (STP). For such a route the values in the Adjacent PC and Remote PC fields will differ, whilst the Priority field will indicate the priority assigned to the route in the SS7 stack file.

The Variant field shows which variant has been declared in the [MTP3] section of the SS7 stack file for that destination. See section 15.1 for details of the SS7 stack file.

The State column reports whether the route is currently available for use, the normal state being Working for direct routes and Working or Standby for indirect routes. A route that shows a state of Restricted/Working or Restricted/Standby indicates that a Transfer Restricted (TFR) messages have been received for the route, although the route is still able to carry traffic. When a route is not in the normal state, selecting it will list the reasons in the Diagnostics listbox.

NOTE

Any issues reported in the Diagnostics listbox will prevent traffic from being passed. However, some issues are transient in nature and will only be present whilst a route is being brought into service.

6.5.4 Destinations

This page provides continuous monitoring of the SS7 destinations that are used by the system.

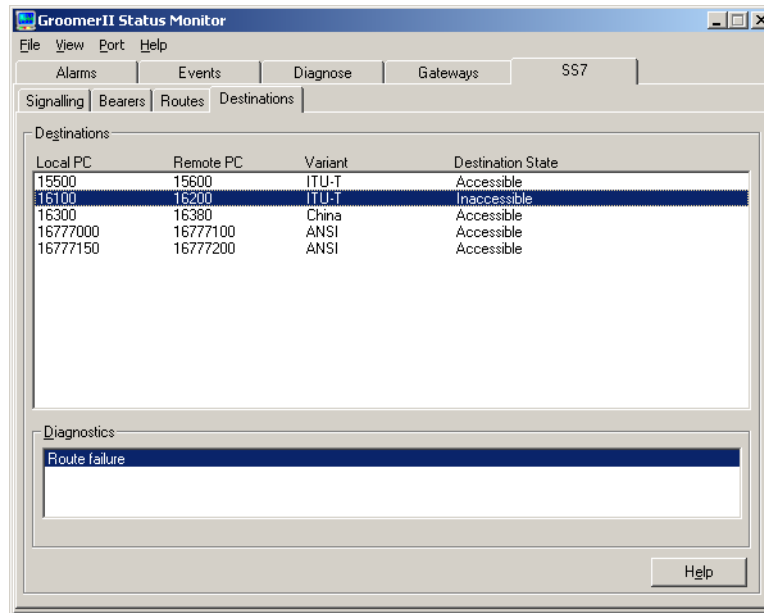


Figure 6-13 GroomerII status monitor SS7 Destinations page

The primary listbox contains an entry for each destination (for example, -cDPC7070) that has been configured by an SS7 firmware download, with the list ordered by Local PC and Remote PC.

The Variant field shows which variant has been declared in the [MTP3] section of the SS7 stack file for that destination. See section 15.1 for details of the SS7 stack file.

The State column reports whether the destination can currently be reached, the normal state being *Accessible*. A destination that remains accessible will show a state of *Restricted* if it can only be reached using restricted routes (i.e. Transfer Restricted (TFR) messages have been received for all routes to the destination). When a destination is not in the normal state, selecting it will list the reasons in the Diagnostics listbox.

NOTE

Any issues reported in the Diagnostics listbox will prevent the destination from being reached. However, some issues are transient in nature and will only be present whilst a restart is in progress.

6.6 CAS

This option will only be available when at least one TDM port has been configured to use a CAS protocol. Select the CAS tab to monitor the transmitted and received ABCD bits on a CAS port. This is useful for checking back-busied and/or seized lines.

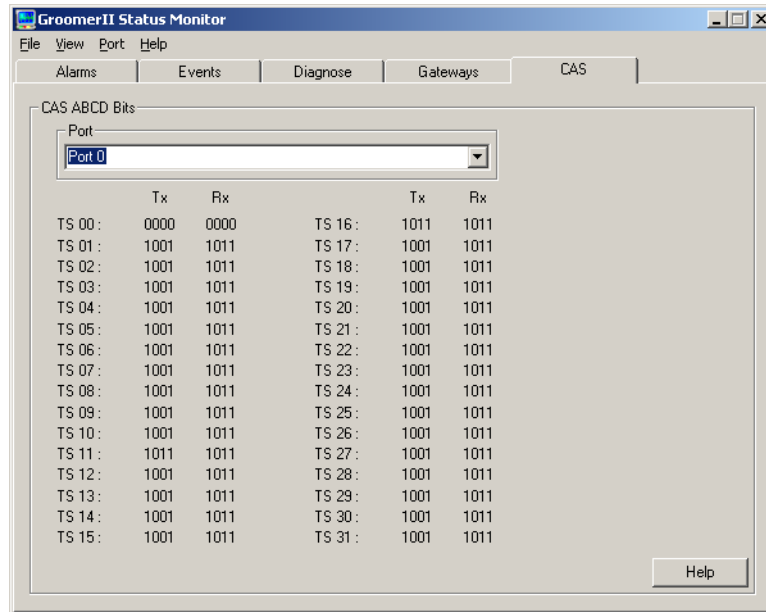


Figure 6-14 GroomerII status monitor CAS tab option

Select the required port from the Port pull down menu.

NOTE

Only CAS ports will be available in the list.

The Tx column shows the transmitted ABCD bits, the Rx shows the received ABCD bits.

With E1 CAS, timeslots 0 & 16 are used as timing and system data channels and not for voice or data calls/traffic. This example shows TS 00 and TS 16 are in a different state from the other timeslots (channels).

7 GroomerII traffic monitor

The GroomerII traffic monitor displays the state of individual timeslots, with visual alerts, within the system.

The traffic monitor will automatically run when the system is started.



Should the traffic monitor be closed for any reason, it can be restarted by double clicking the GroomerII Traffic Monitor icon on your desktop.

NOTE

The GroomerII Kernel must be running for the traffic monitor to successfully start.

The following dialog shows the typical appearance of the traffic monitor when the system is passing traffic.

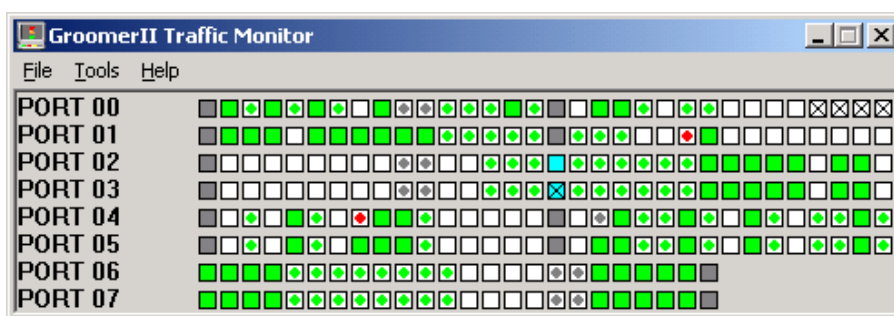


Figure 7-1 GroomerII traffic monitor dialog

Each of the ports present in the GroomerII configuration file will be displayed, and the status of each of its bearer timeslots shown. The following symbols are used to represent timeslot states:



(Black box with grey background)

The timeslot is not a bearer timeslot, but is an HDLC or signalling timeslot.



(Black box with turquoise background)

The timeslot is an SS7 signalling link that is currently in service.



(Black box with turquoise background and black cross)

The timeslot is an SS7 signalling link that is currently out of service.



(Black box with black cross)

The timeslot is currently out of service, and unavailable for calls. Usually this will indicate that the timeslot has been placed out of service in the Kernel port blocking screen. In the case of SS7 timeslots, it can also indicate that the timeslot has had CIC blocking applied by the far end.



(Black box with white background)

The timeslot is currently idle.



(Black box with green circle)

The timeslot is carrying a call in the setup phase.



(Red box with green circle)

The timeslot is carrying a call that has remained in the setup phase beyond the alert threshold.



(Black box with green background)

The timeslot is carrying a connected call.



(Red box with green background)

The timeslot is carrying a call that has remained in the connected state beyond the alert threshold.



(Black box with grey circle)

The timeslot is carrying a call that reached the connected state and is now in the release phase.



(Red box with grey circle)

The timeslot is carrying a call that reached the connected state and has remained in the release phase beyond the alert threshold.



(Black box with red circle)

The timeslot is carrying a call that did not reach the connected state and is now in the release phase.



(Red box with red circle)

The timeslot is carrying a call that did not reach the connected state and has remained in the release phase beyond the alert threshold.



(Black box with white background and black T)

The timeslot is carrying a test call.



(Black box with white background and black R)

The timeslot is an SS7 bearer channel that is currently in recheck mode because it failed an in-call continuity check.



(Red box with white background and black R)

The timeslot is an SS7 bearer channel that is currently in recheck mode because it failed an in-call continuity check, and has remained in recheck mode for more than 30 minutes.

Alerts

The thresholds at which the Traffic Monitor will display visual alerts can be configured using the Alerts dialog. Select Alerts... from the Tools menus to open the Alerts dialog. The configured thresholds apply to all calls in the system.

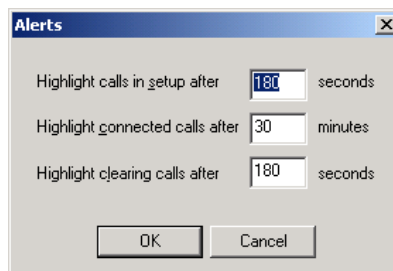


Figure 7-2 Alert thresholds dialog

Highlight calls in setup after x seconds – This is the period, after which calls that are still in the setup phase will be highlighted. The default period is 180 seconds.

Highlight connected calls after x minutes – This is the period, after which calls in the connected state will be highlighted. The default period is 30 minutes.

Highlight clearing calls after x seconds – This is the period, after which calls that are still in the release phase will be highlighted. The default period is 180 seconds.

OK – Closing the dialog using the OK button will apply the changes to both calls currently in the system, and all future calls. The settings will be maintained across system shutdown.

Cancel – Closing the dialog box using the Cancel button will discard any changes made.

8 GroomerII configuration

Double click the GroomerII Configuration Editor icon  on your desktop to open the GroomerII Configuration Editor dialog.

8.1 Layout and overview

- Menus.
- Tool bar.
- File viewer dialog - scrolling text viewer of the current configuration file.
- Status Bar.

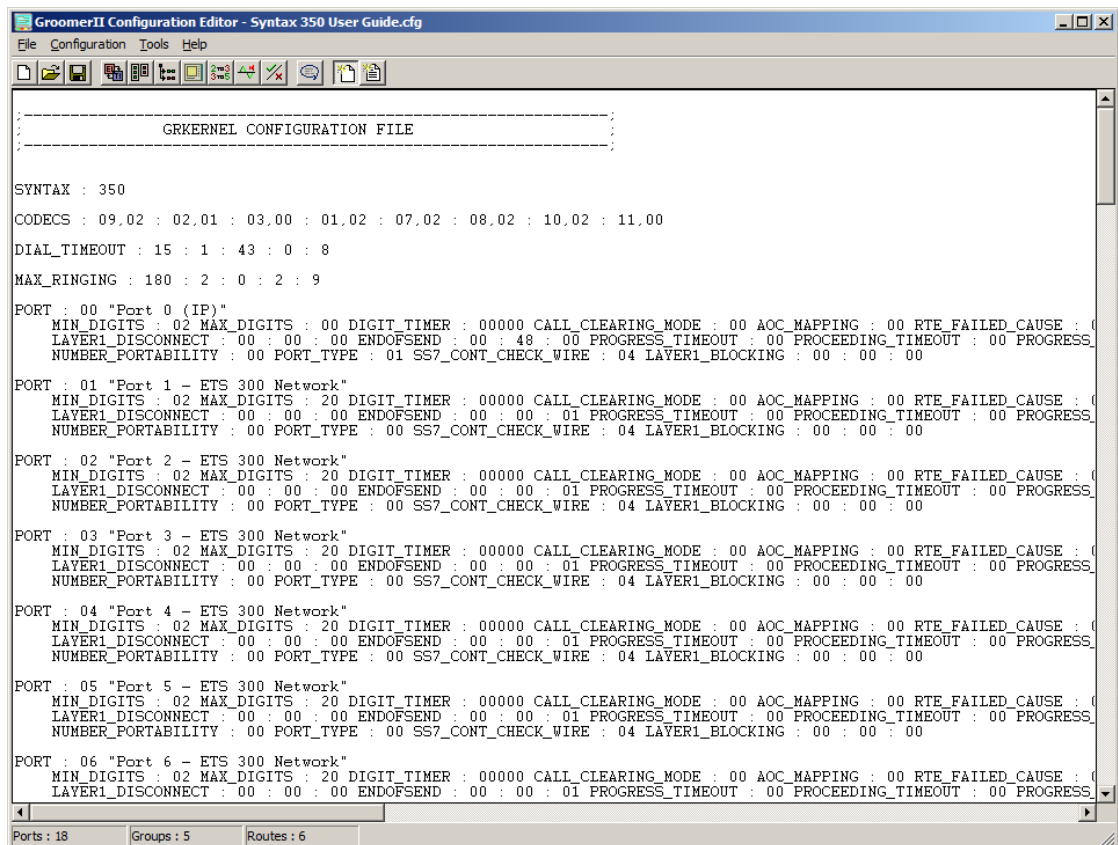




Figure 8-1 GroomerII Configuration Editor

8.1.1 File menu options

The File menu options are used to control the configuration file that is currently being viewed.

New – clears the current configuration data and filename. 

Open – opens an existing configuration file. 

Save – updates the current file with the configuration data. 

Save As... – creates a new/updated file with the configuration data.

History – the last 5 files opened are displayed.


Exit – Closes the application.

CAUTION

If the current configuration has been modified and not saved, then a warning prompt is displayed. For example, when trying to open another file, or closing the program.

8.1.2 Configuration

The Configuration menu options are:


Ports... – Add, Update or Delete ports from the configuration. 


Groups... – Add, Update or Delete Groups from the configuration. 

Routes... – Add, Update or Delete Routes from the configuration. 

System... – setting system parameters, for example, master clock. 

Cause mapping... – set non standard clearing cause translations. 



Tone Generation... – configure call progress tone sets. 

Advanced Options... – enabled or disabled various configuration functions. 

8.1.3 Tools

The Tools menu options are:

Comments... – enter notes or comments into the configuration file. 

Options... – change the add new parameter between use default values,  and use current settings. 

Change Activation Key... – used to change the activation key on a support system.

8.2 Producing a configuration file

You can create a new configuration file, or using the File-Open menu option select to edit an existing file.

8.2.1 Setting the tools options

When you add or insert a port, group or route, the behaviour is subject to the selection made under Tools – Options;

If set to Use Current Values, the new entry will contain a system generated name and a copy of the parameters from the last entry selected.

If set to Use Default Settings, the new entry will contain a system generated name and default values.

8.2.2 Configuration order

Some configuration parameters are dependent on others, for example, Routes depends on Groups which in turn depend on Ports. To avoid problems, a configuration should be built in the following order:

1. Ports.
2. Groups.
3. Tone Generation.
4. Routing.


Followed by the remaining Configuration options as required.

CAUTION

Changes to Ports may change previous settings in Groups, Routes and Tone Generation.

8.3 Ports configuration

A Port is the basic element of the system configuration.

From the GroomerII Configuration Editor, select the  icon or Configuration – Ports... from the menus to open the Port Configuration dialog.

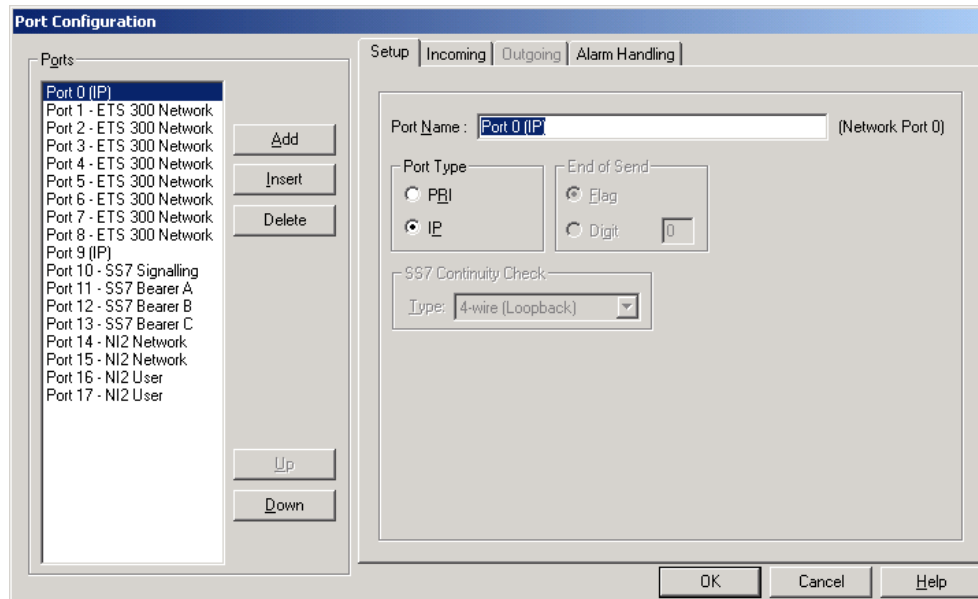


Figure 8-2 Port configuration setup tab option (IP port example)

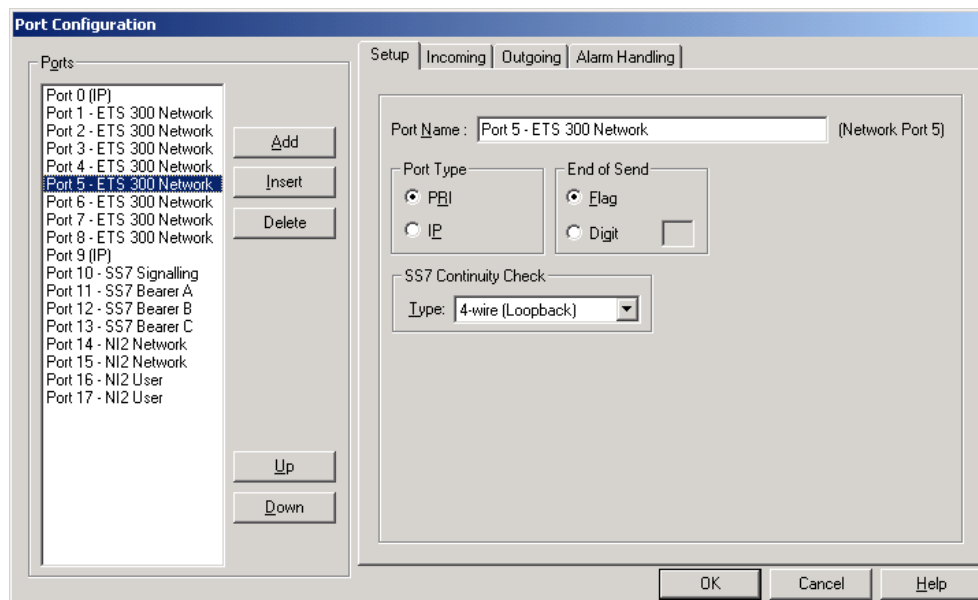


Figure 8-3 Port configuration setup tab option (TDM port example)

This dialog contains two areas, Ports and tab options. The values of the tabs reflect the configuration of a selected port.

Ports must be listed in their order on the card, with those on card 0 listed first, followed by card 1, and so on.

If you add too few or too many ports the GroomerII Kernel will report errors when GroomerII is started, and system operation may be impaired.

8.3.1 Ports

To add a new port select Add. The new port will be added to the bottom of the Ports list.

To insert a new port, highlight the port below the required position in the Ports list, and then select Insert. The new port will now be inserted into the Ports list.

To update an existing port, select the port to be updated and make the required changes.

To remove a port from the Ports list, select the port to be removed followed by Delete.

CAUTION

Deleting a port may cause dependent Groups and Routes to be deleted.

To change the position of a port within the Ports list, select the port followed by either Up or Down .

8.3.2 Setup

The Setup tab option is used to define the parameters associated with a port. This includes:

Port Name – A user defined identification string, which may be up to 63 characters in length. This name will appear within the status application when referencing the port (Ports are only referenced by number from within the GroomerII Kernel). For ease of use it is recommended that you include the port number in this name i.e. DASS (5) etc.

NOTE

There are a number of fields throughout the GroomerII applications that are not of sufficient width to display the entire 63 characters, and the name will be truncated when displayed in such fields. It is recommended that all names are uniquely identified within the first 30 characters.

Port Type – Use the controls in this group to indicate the port type:

PRI – select for an E1 or T1 trunk port.

IP – select for an IP port. The Outgoing tab will be disabled.

End of Send – The controls in this group apply only to TDM ports, and are used to configure how end-of-send is indicated on the selected port. These settings are used to:

- Identify sending complete on incoming calls (when required to do so, for example Route on end of send)
- Append sending complete to out going calls (when required to do so, for example using the [EOS] token during number translation)

End of send is automatically mapped between ports using this parameter, which can be configured to use a flag or digit value as follows:

Flag – select to use the selected ports protocol default sending complete indication.

Digit – select to specify a digit to be used to indicate sending complete.

If for any reason you do not want to map an incoming sending complete indication to an outgoing call, select digit and leave the value blank.

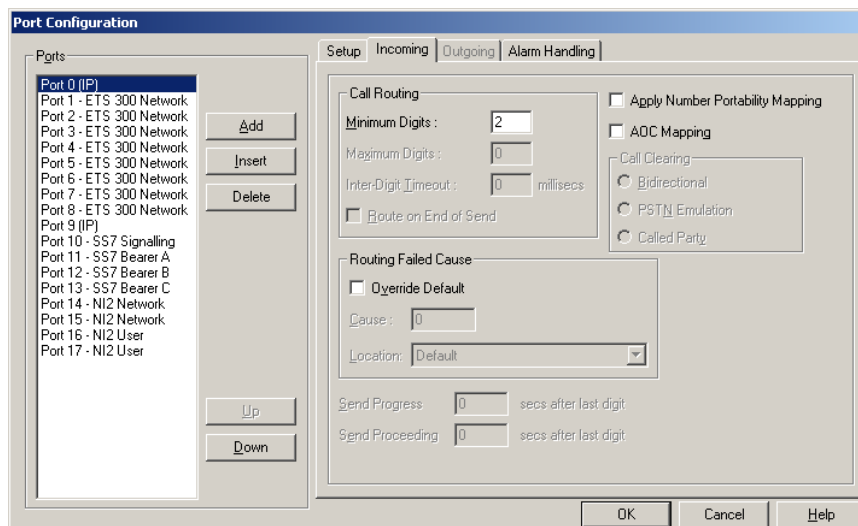
SS7 Continuity Check – This control applies only to SS7 ports, and will be ignored by all other protocols. See section 15.3 for an explanation of SS7 continuity checks.

Type – select the type of continuity check that is to be carried out by this port. The same type will be used for both inbound and outbound continuity checks. The available options are:

- 4-wire (Loopback)
- 2-wire (Transponder)

8.3.3 Incoming

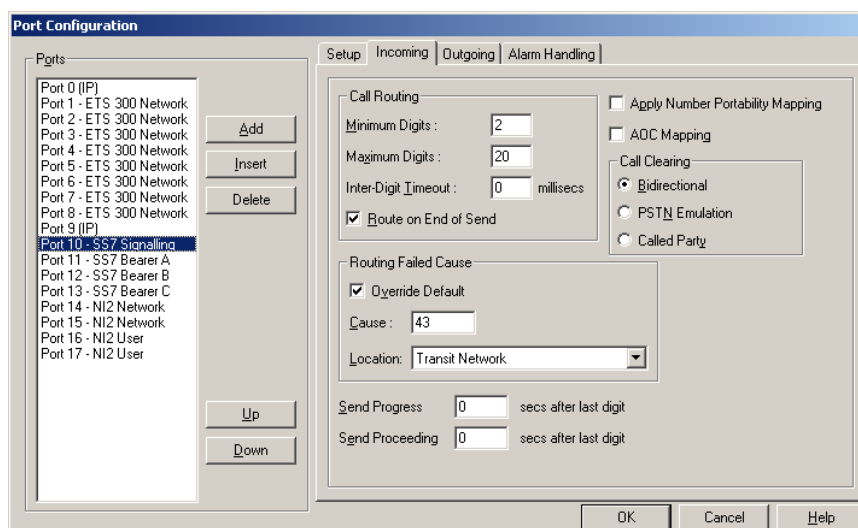
The Incoming tab option is an advanced options page relating to incoming calls on the selected port. The available options will be subject to the type or port selected.



The screenshot shows the 'Port Configuration' dialog box with the 'Incoming' tab selected. On the left, a list of ports is shown, with 'Port 0 (IP)' selected. The main area contains the following settings:

- Call Routing:**
 - Minimum Digits: 2
 - Maximum Digits: 0
 - Inter-Digit Timeout: 0 milliseconds
 - ☐ Route on End of Send
- Routing Failed Cause:**
 - ☐ Override Default
 - Cause: 0
 - Location: Default
- Send Progress:** 0 secs after last digit
- Send Proceeding:** 0 secs after last digit
- Call Clearing:**
 - ☐ Apply Number Portability Mapping
 - ☐ ADC Mapping
 - ☐ Bidirectional
 - ☐ PSTN Emulation
 - ☐ Called Party

Figure 8-4 Port configuration incoming tab IP option



The screenshot shows the 'Port Configuration' dialog box with the 'Incoming' tab selected. On the left, a list of ports is shown, with 'Port 10 - SS7 Signalling' selected. The main area contains the following settings:

- Call Routing:**
 - Minimum Digits: 2
 - Maximum Digits: 20
 - Inter-Digit Timeout: 0 milliseconds
 - ☒ Route on End of Send
- Routing Failed Cause:**
 - ☒ Override Default
 - Cause: 43
 - Location: Transit Network
- Send Progress:** 0 secs after last digit
- Send Proceeding:** 0 secs after last digit
- Call Clearing:**
 - ☐ Apply Number Portability Mapping
 - ☐ ADC Mapping
 - ☒ Bidirectional
 - ☐ PSTN Emulation
 - ☐ Called Party

Figure 8-5 Port configuration incoming TDM option

Call Routing – The controls in this section determine at what point an incoming call will be routed:

Minimum Digits – specifies how many digits must be collected before any attempt is made to route the call. A call will not be routed under any circumstances until this number of digits has been collected. This parameter can be set to zero if no minimum digit check is required. After the minimum required digits have been received, the call will be routed on the first occurrence of any of the following:

Maximum Digits – when enabled (set to a non-zero value), the call will be routed immediately the specified number of digits has been received.

Inter-Digit Timeout – when enabled (set to non-zero), the call will be routed immediately the timer expires.

Route on End of Send – if enabled, the call will be routed immediately the end of send indicator (as defined in the Setup screen) is detected.

The Maximum Digits, Inter-Digit Timeout and Route On End of Send controls are available for TDM ports only.

Apply Number Portability Mapping – When this box is checked and number portability mapping is enabled, then before routing the incoming DDI will be substituted with an alternative retrieved from the Number Portability data source. When there is no alternative present in the Number Portability data source then the incoming DDI will be used to route the call.

If this box is unchecked or number portability mapping is disabled, then the incoming DDI will be used to route the call. The default setting for this control is unchecked.

AOC mapping – When checked any charging messages received from the outgoing leg of an end-to-end call (regardless of the port on which the outgoing call is placed) will be mapped through to the incoming leg.

NOTE

AOC mapping will only be successful when the protocols used for both the incoming and outgoing legs of the call support charge messages. Contact Aculab support for further information on the charge mapping capabilities of the protocols you wish to use.

NOTE

AOC mapping is not supported by CAMA ports.

Call Clearing – Use the controls in this group to configure the behaviour during call clearing.

Bidirectional – This is the default setting and allows either the called or calling party to clear the call.

PSTN Emulation – When an outbound call is made to a busy extension, the call is often rejected with a cause default value. Under normal conditions, this is passed back to the originating port causing the call to disconnect. Once a call is disconnected, it is not possible to send any tones back down the line.

When checked, as the PSTN Emulation requires any call to be cleared forward, it effectively blocks the reject message and holds the voice path open until the originating party clears.

PSTN emulation will be applied to all incoming calls received on this port. It will only be possible to clear the call forward, irrespective of which port the outgoing call is on.

Outgoing calls on this port will only have PSTN emulation applied if the corresponding incoming port has PSTN Emulation applied. Therefore, PSTN emulation may be applied to some outgoing calls, whilst it may not be applied to others.

PSTN Emulation is applicable to TDM calls only.

Called Party – This setting applies to CAMA ports only, and is described in section 16.3. When applied to non-CAMA ports bidirectional call clearing will be used.

Routing Failed Cause – If an incoming call on the selected port cannot be routed, it is cleared by GroomerII. The default clearing cause is user busy. When user busy is not appropriate, subject to the protocol being used, the cause may be manually set to another cause value.

For example, Euro ISDN uses clearing cause 42 to indicate Switching Equipment Congestion. To use this cause instead of the default User Busy, check Override Default to enable the Cause field, then enter 42 into the Cause field.

Override Default – check this box to override the default routing failed cause.

Cause – enter the protocol specific clearing cause to be used by this port. This control is only enabled when Override Default is checked.

Location – this field applies to SS7 and Q.931 calls only, and is ignored by all other protocols. The control allows the location field in the cause parameter to be set. A location of User will be applied when `Default` is selected. This control will be disabled when an IP telephony port is selected.

Send Progress/Send Proceeding – These controls are available on TDM ports only, and are used to trigger the sending of a progress or proceeding message if no digits have been received for # seconds. Both messages have a progress element indicating that in-band tones are available.

Sending progress/proceeding messages in this way can prevent incoming calls from timing out when interworking with very slow far end networks, or can be used to prompt switches to open the voice paths.

NOTE

Some protocols, for example Euro ISDN, send a proceeding message automatically and will not allow a second one to be sent. In such instances use a progress message if you wish to open up the voice path.

8.3.4 Outgoing

The Outgoing tab controls the advanced options relating to outgoing calls on a port.

NOTE

The outgoing tab option is greyed out when an IP port is selected.

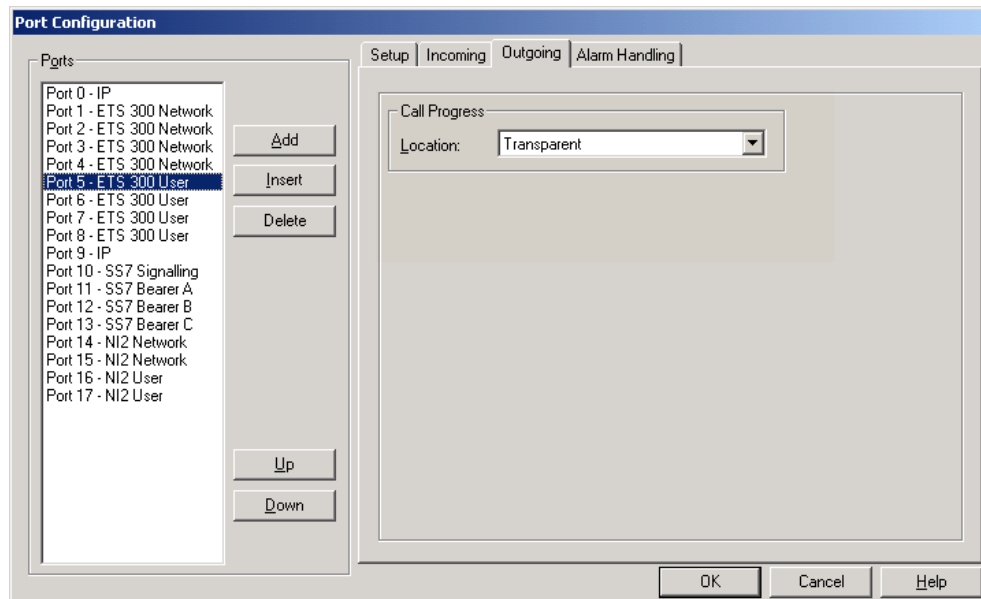


Figure 8-6 Port configuration outgoing tab option

Call Progress – The controls in this group are used to configure how a call progress message received from an outgoing call leg will be mapped to the incoming call leg:

Location – When left at the default setting of Transparent the location field in a call progress message will be mapped between calls unchanged. In the case of, for example, mapping a network port to a network port, or a user port to a user port, it may be necessary to override the default and manually redefine the originator location part of the information. For example, redefining the originating location as a remote user port instead of a network port.

The options available for the progress information element are:

```
Transparent
User
Private Network serving Local User
Public Network serving Local User
Public Network serving Remote User
Private Network serving Remote User
International Network
Network beyond interworking point
Transit Network
```

NOTE

Not all values are supported by every protocol. Refer to the appropriate protocol specification for guidance.

8.3.5 Alarm handling

Use the Alarm Handling tab specify any action that should be taken when a port is in an alarm state.

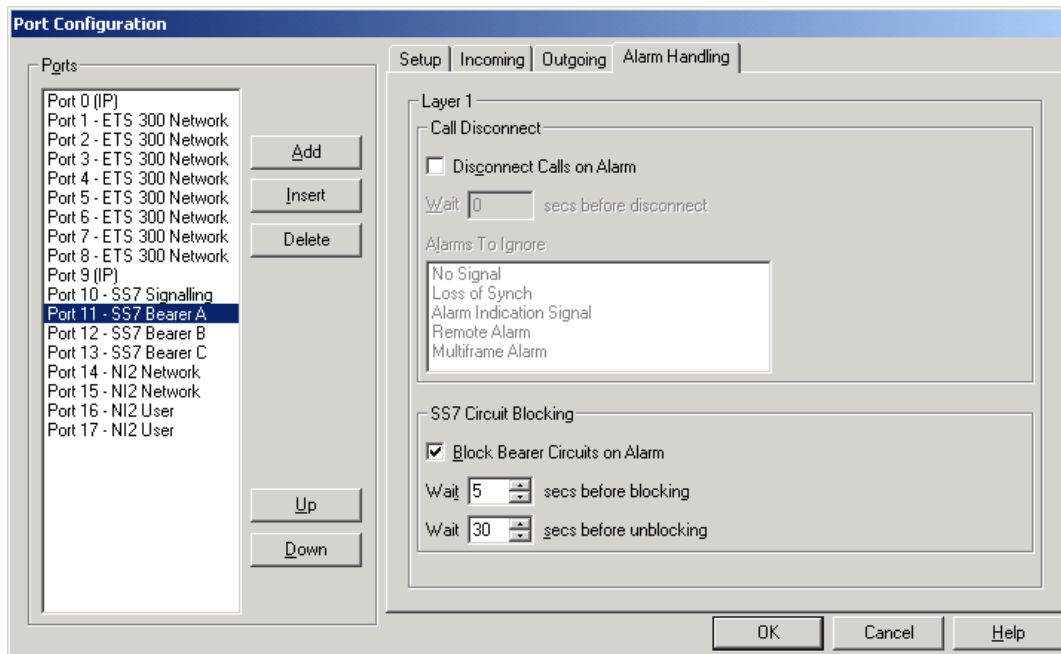


Figure 8-7 Port configuration alarm handling tab option

Call Disconnect – Use the controls in this group to disconnect any calls the port is carrying when an incoming alarm is detected.

Disconnect Calls on Alarm – Checking the Disconnect Calls on Alarm field causes GroomerII to clear calls when a layer 1 alarm is received on the selected port.

Wait x secs before disconnect – The length of time that the port alarm must be continually present before calls will be disconnected.

Alarms to Ignore – As default, disconnect will apply to all of the alarms shown in the Alarms to Ignore field. On some occasions it may be preferable to ignore certain alarms and allow calls to proceed, for example when receiving a Remote Alarm Indication (RAI) that is caused by alarm mapping rather than by a fault. To ignore an alarm, it must be highlighted by selecting it.

NOTE

The Alarms To Ignore field is not applicable to IP ports and is disabled if an IP port is selected.

SS7 Circuit Blocking – The controls in this group are used to apply circuit blocking to any SS7 bearer channels being carried by the port when either an incoming or outgoing alarm is detected.

Outgoing alarms are those applied to the port by the GroomerII alarm mapping feature (see section 8.6.5), and do not include the alarm applied by the port watchdog timer to indicate system failure.

The controls in this group apply to SS7 ports only, and have no effect when configured on ports loaded with other firmwares.

NOTE

Each of the bearer channels on the port must be controlled by at least one available signalling link carried on a separate port. This feature cannot be used to block bearer channels whose only signalling link is being carried on the same port.

Block Bearer Circuits on Alarm – Check the Block Bearer Circuits on Alarm control to enable circuit blocking on the selected port.

Wait x secs before blocking – The length of time that a port alarm must be continually present before circuit blocking will be initiated.

Wait x secs before unblocking – The length of time that the port must be continually free from alarms before circuit unblocking will be initiated.

8.4 Groups configuration

Groups are used as the basic elements for routing of a call. They define a number of resources (ports and timeslots) being used for a common purpose. For example, if any one of a number of Ports can be used to make an outgoing call, then all the Ports can be put into one Group.

From the GroomerII Configuration Editor dialog, select  or Groups... from the Configuration menu to open the Groups Configuration dialog.

8.4.1 Groups

To add a new group select Add. The new group will be added to the bottom of the Groups list.

To update an existing group, select the group to be updated then make the required changes.

To remove a group from the Groups list, select the group to be removed followed by Delete.

CAUTION

Deleting a group will cause any route using that group to be deleted.

8.4.2 Setup

A Group can contain more than one Port.

A Port can belong to more than one Group.

A Group definition can contain one or more subsets of the available timeslots on a Port.

Individual ports can be moved between groups or new ports can be added to groups without affecting any of the routing definitions.

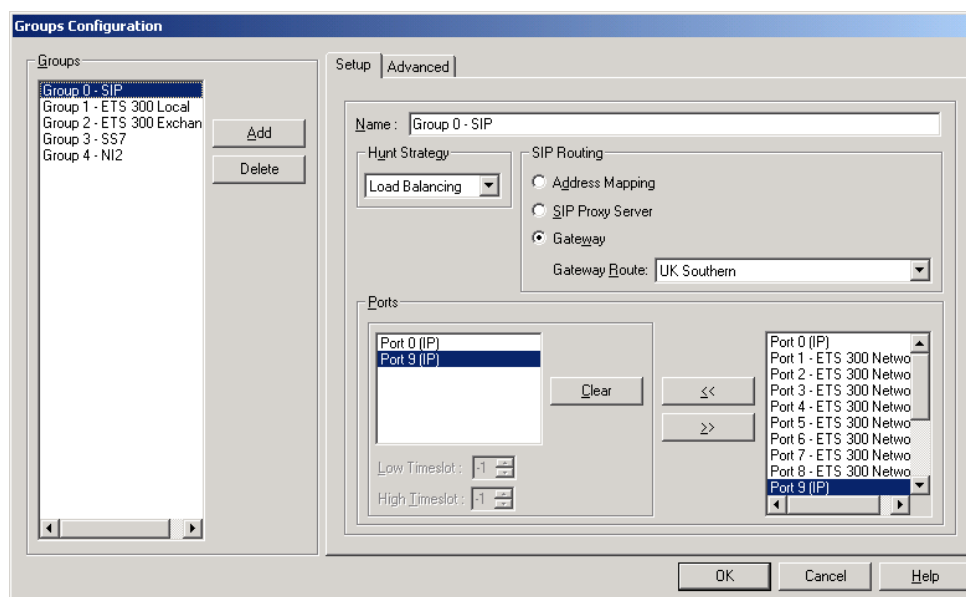


Figure 8-8 Groups configuration setup tab

Name – A unique identification string for user reference only, it is not used within the Kernel itself.

Hunt strategy – Specifies how the outgoing timeslot will be selected from the resources defined for the Group. The options are:

Lowest Available – places the call on the available timeslot that is closest to the beginning of the Group.

Highest Available – places the call on the available timeslot that is closest to the end of the Group.

Follow Input – places the call from the incoming group onto the corresponding port/timeslot in the outgoing port. This hunt strategy can only be used where the incoming and outgoing groups are of identical composition (i.e. contain the same number and type of ports, in the same order, with all bearer timeslots in identical positions). If the corresponding outgoing timeslot is being used, routing will fail.

Random – selects a timeslot at random from those in the Group that are not currently carrying calls.

Cyclic – starts with the first timeslot in the Group, and thereafter selects the next available timeslot following the last one used. When the end of the group is reached the process starts again at the beginning of the Group.

One to One – is similar to Follow Input but only requires the incoming and outgoing groups to have an identical number of bearer timeslots. Corresponding timeslots are determined by counting from the beginning of the group, which allows channel mapping between E1s and T1s. If the corresponding outgoing timeslot is being used, routing will fail.

Load Balancing – is used to balance calls across all ports in a group by looking for the port that is currently carrying the fewest calls.

NOTE

IP telephony has no concept of timeslots, When configuring a group for outgoing IP telephony calls the Load Balancing hunt strategy should always be selected.

NOTE

The hunt strategy only has an effect if the Group is on the outgoing side of a route. The equipment sending the call controls the incoming timeslot.

SIP Routing – These controls will only be enabled if the group contains at least one IP telephony port, and are used to specify how the IP address to which an outgoing SIP call is directed will be selected:

Address Mapping – The called party number presented in the outgoing SIP call will be used to select the destination IP address from the currently loaded address map. Section 9 describes how to create an address map using the GroomerII Address Map Editor. Section 5.3 describes how to load an address map.

SIP Proxy Server – The outgoing SIP call will be directed to the currently configured SIP proxy server for onward routing. Section 8.6.10 describes how to configure a SIP proxy server.

Gateway – The outgoing SIP call will be directed to one of the gateways in the selected gateway route. See section 8.6.9 for a description of gateway routing.

Gateway Route – Select the gateway route to be used by this group from the drop down list. This control will only be enabled when Gateway is selected.

NOTE

SIP routing only has an effect if the Group is on the outgoing side of a route.

Ports – Contains a list of available ports on the right, and a list of ports allocated to the group on the left.

- To remove a port from the group, select the port on the left followed by >>. The Clear button will remove all ports from the group.
- To add a port to the group, select the port on the right followed by <<.

NOTE

When selecting a timeslot for an outgoing call, ports are searched in the order in which they are listed in the allocated ports listbox.

For each port in the group, you must specify the range of timeslots to be used. IP telephony has no concept of timeslots, and the timeslot controls will be disabled if an IP telephony port is selected.

Select the required port from the left hand list (ports included in group)

Low Timeslot Set the low (first) timeslot for the selected port.

High Timeslot Set the high (last) timeslot for the selected port.

NOTE

For simplicity framing and signalling timeslots should be included in the timeslot range, as they will be automatically excluded from selection during operation.

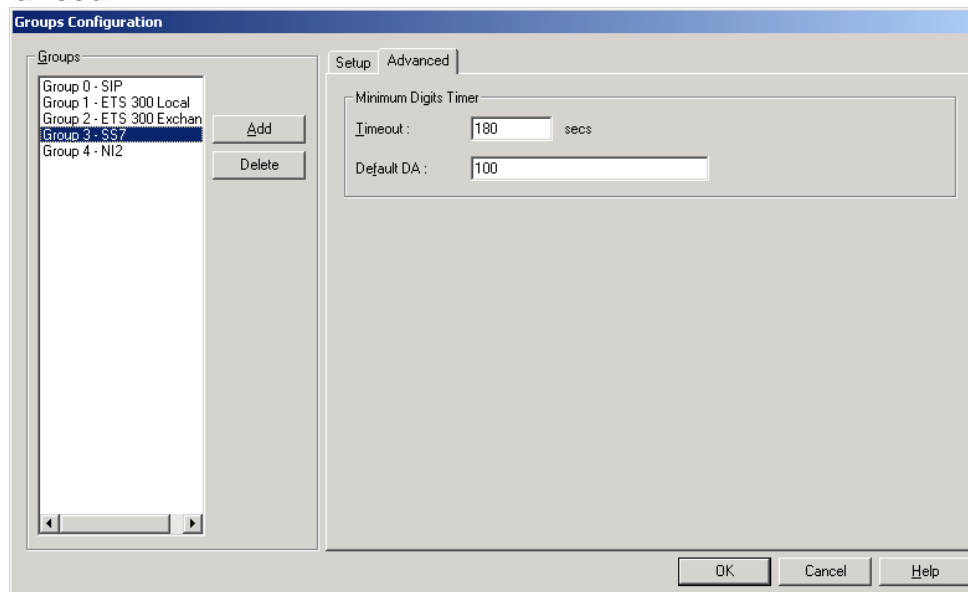
8.4.3 Advanced

Figure 8-9 Groups configuration advanced tab

Minimum Digits Timer – The purpose of the Minimum Digits Timer is to route a call if it arrives with insufficient dialled digits. If the number of digits specified in the Minimum Digits field on the Port Configuration - Incoming page have not arrived within a specified time then the outgoing call will be redirected to a default destination.


Timeout – The time to wait for the minimum number of digits to be dialled.

Default DA – The destination to which the call will be redirected.

The minimum digit timer can be disabled by specifying a timeout of zero seconds.

8.5 Routing configuration

Routing definitions are used to specify how GroomerII will select the port and timeslot to be used for an outgoing call, and to configure settings that are applied on a call-by-call basis.

In the GroomerII Configuration Editor main window select  from the toolbar, or Configuration – Routes... from the menu, to open the Routing Configuration dialog.

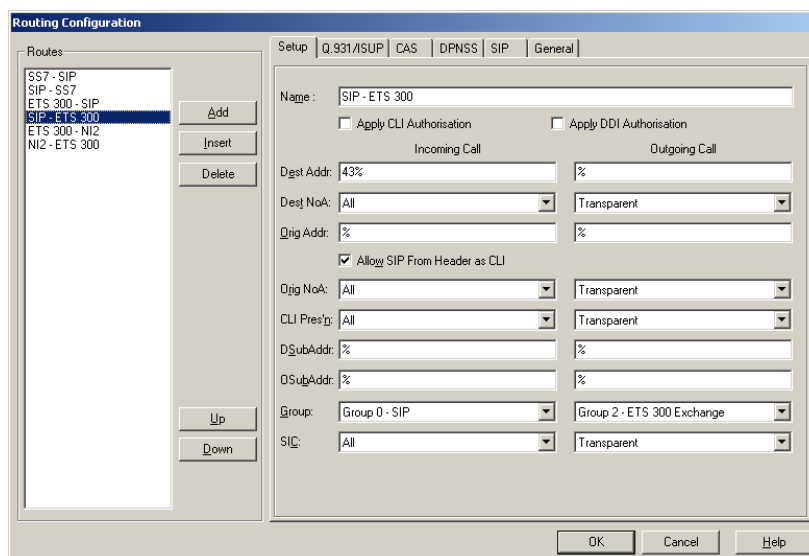


Figure 8-10 Routing configuration setup tab option

8.5.1 Routes

To add a new route, select Add. The new route will be added to the bottom of the Routes list.

To insert a new route, first highlight the route below the required position in the Routes list, and then select Insert. The new route will now be inserted into the Routes list.

To update an existing route, select the route to be updated in the Routes list, and make the required changes.

To remove a route from the Routes list, select the route to be removed followed by Delete.

To change the position of a route within the Routes list, select the required route followed by either Up or Down.

NOTE

The order of the routes is the order that a call searches until it finds a route that meets the required parameters.

8.5.2 Setup

Name – An identification string used for reference only, it is not used within the Kernel itself.

Apply CLI Authorisation – When this box is checked and CLI authorisation is enabled, only calls whose CLI has been authorised will be allowed to use this route. Calls whose authorisation request has been rejected will not be allowed to use the route, and will continue to search for an alternative route. When this box is checked and CLI Authorisation is disabled then all authorisation requests will be rejected and hence no calls will be allowed to use this route. The default is unchecked.

Apply DDI Authorisation – When this box is checked and DDI authorisation is enabled, only calls whose DDI has been authorised will be allowed to use this route. Calls whose authorisation request has been rejected will not be allowed to use the route, and will continue to search for an alternative route. When this box is checked and DDI Authorisation is disabled then all authorisation requests will be rejected and hence no calls will be allowed to use this route. The default is unchecked.

Incoming Call fields

The Incoming Call fields specify the criteria an incoming call must meet in order to use the route.

Dest Addr – The incoming dialled number must match this field. Wildcards may be used to allow the route to handle a range of numbers.

NOTE

The destination address presented by an incoming SIP call may contain a leading '+' and/or embedded '-' characters. When parsed from the SIP headers such characters are discarded, will not be presented to the routing mechanism, and should not be included in the number matching mask. For example to match a dialled number presented as +44-1908-273800 use the mask 441908273800.

Dest NoA – This allows the called party nature of address indicator in the incoming call to be matched. The options available along with their corresponding protocol values are:

```
All
Subscriber (1)
Unknown (2)
National (3)
International (4)
Network Specific (5)
Network Routing (National) (6)
Network Routing (Network Specific) (7)
Network Routing (Called Directory) (8)
Subscriber, Operator Requested (113)
National, Operator Requested (114)
International, Operator Requested (115)
No Number, Operator Requested (116)
No Number, Cut Through (117)
950+ Call (118)
Test Line Test Code (119)
UK Specific Address (126)
```

Select **All** to allow any nature of address setting to be matched.

NOTE

Nature of address is only supported by the SS7 protocol, and some variants may not support all available settings.

Orig Addr – The incoming calling number must match this field. Wildcards may be used to allow the route to handle a range of numbers.

NOTE

The originating address presented by an incoming SIP call may contain a leading '+' and/or embedded '-' characters. When parsed from the SIP headers such characters are discarded, will not be presented to the routing mechanism, and should not be included in the number matching mask. For example to match a calling number presented as +44-1908-273800 use the mask 441908273800.

Allow SIP From Header as CLI – This setting applies to incoming SIP calls only. GroomerII expects an incoming SIP call to present the calling party number in a P-Asserted-Identity header. If the SIP call does not present a P-Asserted-Identity header, the call is considered not to have a calling party number. Ticking this checkbox will allow GroomerII to extract the calling party number from the From header if no P-Asserted-Identity header is presented.

Orig NoA – This allows the calling party nature of address indicator in the incoming call to be matched. The options available along with their corresponding protocol values are:

```
All
Subscriber (1)
Unknown (2)
National (3)
International (4)
Non-Unique Subscriber (113)
Non-Unique National (115)
Non-Unique International (116)
Test Line Test Code (119)
```

Select **All** to allow any nature of address setting to be matched.

NOTE

Nature of address is only supported by the SS7 protocol, and some variants may not support all available settings.

CLI Pres'n – This allows the calling party number presentation indication in the incoming call to be matched. The options available are:

```
All
Allowed
Restricted
Not Available
Reserved
```

Calling party number presentation indication is supported by the SS7 and Q.931 protocols only, and this control will be ignored by all other protocols.

Select **All** to allow any calling party number presentation indication to be matched.

DSubAddr – The incoming destination subaddress must match this field. Wildcards may be used to allow the route to handle a range of numbers.

OSubAddr – The incoming originating subaddress must match this field. Wildcards may be used to allow the route to handle a range of numbers.

NOTE

Subaddresses are supported by SIP, SS7 and Q.931 protocols. Only subaddresses with the Type of subaddress set to User specified and the subaddress information coded using IA5 digits can be pattern matched. Any form of subaddress will be matched against the % wildcard. Section 14.7 describes SIP support for ISDN subaddress.

NOTE

If you wish to match any number to the above fields use the % wildcard. Leaving a field blank will only allow calls that have no associated number to use the route.

Group – The timeslot on which the incoming call arrived must be part of the selected group. The drop down list contains all of the groups defined in the Groups Configuration screen.

SIC – The Service indicator code or Bearer code. This field is used to define what type of calls may use this route. For example, when set to *Speech* the route will only accept voice calls. The default is to accept all call types. This feature is commonly used to identify calls that need to avoid compressed lines, such as 64k data calls. The options available are:

```
All
Speech
64K Data
3.1Khz
Fax
```

NOTE

Some protocols may not support all Service Indicator Codes.

Outgoing Call fields

The Outgoing Call fields specify the parameters that will be used when making an outgoing call on the route.

Dest Addr – is the dialled number to which the outgoing call will be directed. This can be either a fixed number or can be built from the incoming call parameters using number translation features below.

Dest NoA – this sets the called party nature of address indicator in the outgoing call. The options available along with their corresponding protocol values are:

```
Transparent
Subscriber (1)
Unknown (2)
National (3)
International (4)
Network Specific (5)
Network Routing (National) (6)
Network Routing (Network Specific) (7)
Network Routing (Called Directory) (8)
Subscriber, Operator Requested (113)
National, Operator Requested (114)
```

```

International, Operator Requested (115)
No Number, Operator Requested (116)
No Number, Cut Through (117)
950+ Call (118)
Test Line Test Code (119)
UK Specific Address (126)

```

Select `Transparent` to map the incoming call type through to the outgoing call. If the incoming call type does not support the nature of address indicator then a default setting of `International` will be used.

NOTE

Nature of address is only supported by the SS7 protocol, and some variants may not support all settings.

CLI Pres'n – sets the calling party number presentation indication in the outgoing call. The options available are:

```

Transparent
Allowed
Restricted
Not Available
Reserved

```

Calling party number presentation indication is supported by the SS7 and Q.931, and the setting will be ignored by all other protocols.

Select `Transparent` to map the incoming value through to the outgoing call. If the incoming call type does not support calling party number presentation indication then a default setting of `Allowed` will be used.

DSubAddr – is the destination subaddress that will be included in the outgoing call. This can be either a fixed number or can be built from the incoming call parameters using number translation features below.

OSubAddr – is the originating subaddress that will be included in the outgoing call. This can be either a fixed number or can be built from the incoming call parameters using number translation features below.

NOTE

Subaddresses are supported by SIP, SS7 and Q.931 protocols. Only subaddresses with the Type of subaddress set to User specified and the subaddress information coded using IA5 digits can be translated, and the outgoing subaddresses will use this format. Any form of subaddress can be passed through transparently by using the % wildcard in both the Source and Destination field. Section 14.7 describes SIP support for ISDN subaddresses.

Group – the timeslot on which the outgoing call will be made will be selected from this group. The timeslot to be used will be selected according to the hunt strategy defined for the group. If the group has no timeslot available then an alternative route will be sought. The drop down list contains all of the groups defined in the Groups Configuration screen.

The Destination Group field contains the following system entries.

<Wait for Transfer>	This is used when mapping ETS 300 call transfer requests to SS7 call redirection. See section 12.2.
---------------------	---

<Test Call>

When the destination group is set to <Test Call> no outgoing call is made. Instead the user busy tone will be played to the caller until the call is cleared forward (note that some protocols may clear the call automatically after a period of time). If a Tone Generation scheme containing a busy tone has been configured in the General page (see section 8.5.7), then this tone will be used. Otherwise the UK busy tone will be played for to incoming E1 and IP calls, whilst the US busy tone will be used if the incoming call is a T1 call.

SIC – The Service indicator code. This sets the call type of the outgoing call. The options available are:

Transparent
Speech
64K Data
3.1Khz
Fax
Custom

Select `Transparent` to map the incoming call type through to the outgoing call. If the incoming call type is not supported by the outgoing protocol then an appropriate alternative will be used.

The `Custom` option is only available with Q.931 and ISUP outgoing calls and requires the `Custom Bearer` field described in section 8.5.3 to be used.

NOTE

Some protocols may not support all Service Indicator Codes.

Wildcards

When matching an incoming call against the routing entries, the following wildcard characters can be used in the `Dest Addr`, `Orig Addr`, `DSubAddr` and `OSubAddr` fields to allow one routing entry to handle a range of numbers.

? - Single character

% - Any other sequence of characters string (wildcard)

For example, `81%` will match any number beginning with `81`, whereas `8??2` will match any 4 digit number beginning with `8` and ending in `2`.

Number translation

The following characters are used for translating the `Dest Addr`, `Orig Addr`, `DSubAddr` and `OSubAddr` from the incoming call to the outgoing call.

- ? Use next character from incoming string
- x Delete next character from incoming string
- % Use remainder of incoming string, any other incoming characters are sent overlap
- ; Delete remainder of incoming string

E.g. If the incoming called number is `8120` and the outgoing `Dest Addr` is `123x%` the actual outgoing number will be `123120`.

You can transfer information from the incoming Orig Addr field to the outgoing Dest Addr field by putting `[OA] %` in the outgoing Dest Addr field. You can also combine information from incoming Orig Addr and Dest Addr by putting `[OA] ??? [DA] %` in the outgoing field. In our example, following the Orig Addr with four `?`s will take the first 4 digits of the Orig Addr then add the whole Dest Addr value.

NOTE

Placing `%` in the outgoing field signifies the end of the translation, for example, you cannot put `xx??%52` in the outgoing field because the 52 will be ignored.

NOTE

The `[DA]` and `[OA]` tokens are not supported by the DSubAddr and OSubAddr fields.

Customer specific options

Two customer specific options have been created, these are `[RN]`, redirecting number and `[OCN]`, original called number. They may be used in the same way as the `[AO]` and `[DA]` options detailed earlier.

CAUTION

If you use these values but the incoming call does not include them, the call will fail to route.

Tokens

The `[EOS]`, end of send token can be used to append the end of send indicator specified in the Port Configuration screen to the outgoing call at the point when the call is made.

The `[TO n]x`, timeout token can be used to append a terminating sequence to the outgoing call at a specified time after the call has been made. `n` is the time interval specified in one-tenth second increments. `x` is the terminating sequence, which can be either `[EOS]`, which will cause the end of send indicator for the outgoing port to be used, or it can be a literal sequence of digits. For example `[TO 50][EOS]` will cause the end of send indicator to be sent 5 seconds after the outgoing call is made, whilst `[TO 30]*9#` would cause `*9#` to be sent three seconds after making the call.

The `[IN_PORT]` token can be used in both the outgoing DA and outgoing OA fields to insert the incoming port number into the string as a 2 digit field with leading zeroes, for example 00, 05, 32.

The `[IN_TS]` token can be used in both the outgoing Dest Addr and outgoing Orig Addr fields to insert the incoming timeslot number into the string as a 3 digit field with leading zeroes, for example 000, 055, 234.

The `[CALL_ID]` token can be used in both the outgoing Dest Addr and outgoing Orig Addr fields to insert the 10 digit call ID into the string. This token is provided to assist with debugging and fault finding.

NOTE

These fields are case sensitive, for example, `[eos]` will not be recognized but `[EOS]` will.

8.5.3 Routes – Q.931/ISUP

The Q.931/ISUP tab allows outgoing call parameters that are specific to Q.931 and ISUP calls to be configured. Parameters that are common to both protocols appear on the Common page, whilst those that are specific to an individual protocol appear on the Q.931 or ISUP page as appropriate. These parameters should be left at their default settings unless you are familiar with the protocol in use.

When a parameter is set to `Transparent` and the incoming protocol supports that parameter then its value will be passed unchanged from the incoming to the outgoing call. If the incoming protocol does not support the parameter then a suitable default value will be applied to the outgoing call.

NOTE

Some protocols may not support all of the values available.

Common tab options

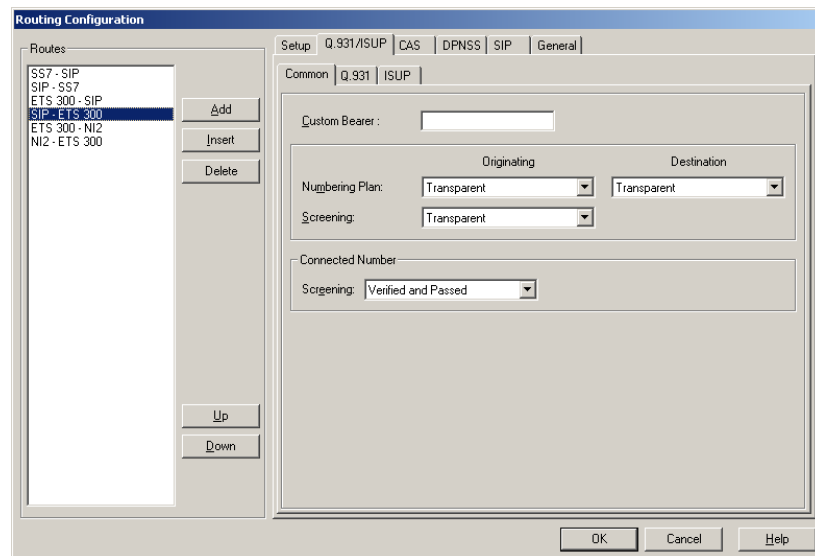


Figure 8-11 Routing configuration Q.931/ISUP - common tab option

Custom Bearer – This field is used when a greater level of control over bearer capability settings is required than that which can be achieved using the Destination SIC field on the Setup page. For example when V.110 rate adaptation is required.

Up to 15 bytes of information can be entered. The information must be entered as a series of hexadecimal numbers, for example 1F 36 CA 01 05 04 1D, and must be in the form of a Q.931 Bearer Capability information element.

When the outgoing protocol is Q.931 the contents of this field will be copied unmodified into a Bearer Capability information element. When the outgoing protocol is ISUP the contents of this field will be used to build a Transmission Medium Requirement parameter.

The Destination SIC field on the Setup page must be set to `Custom` if you wish to use this feature. If the Destination SIC field is not set to `Custom` this field will be ignored.

NOTE

This parameter is used to set the bearer capabilities only. It cannot be used to modify the speech path data.

NOTE

This field can also be used to set the Service Indicator Code (SIC) octets in an outgoing DASS2 or DPNSS call. The first byte must be set to 1 or 2 to indicate how many SIC octets are to be set. The second byte will be written unmodified into SIC octet 1, and the third byte (if specified) into SIC octet 2. Again the Destination SIC field on the Setup page must be set to `Custom`.

Numbering Plan – The `Originating` field sets the calling party numbering plan identification, and the `Destination` field sets the called party numbering plan identification. In addition to `Transparent` the following options are available:

- Unknown
- ISDN CCITT E.164/E.163
- Data CCITT X.121
- Telex CCITT F.69
- National Standard
- Private

Screening – This field sets the calling party number screening indicator. In addition to `Transparent` the following options are available:

- Not screened
- Verified & passed
- Verified & failed
- Network Provided

Connected Number – Use the controls in this group to specify how connected party number information should be sent to an incoming Q.931 or SS7 call using this route. Currently only the screening indicator can be modified, and all other information is passed through unmodified or using suitable default values. See section 17.5 for further information on connected party number interworking.

Screening – This field sets the connected party number screening indicator sent to the incoming side. In addition to `Transparent` the following options are available:

- Not screened
- Verified & passed
- Verified & failed
- Network Provided

NOTE

If the outgoing call does not present a connected party number at the connect stage, no connected party number information will be sent to the incoming call.

Q.931 tab options

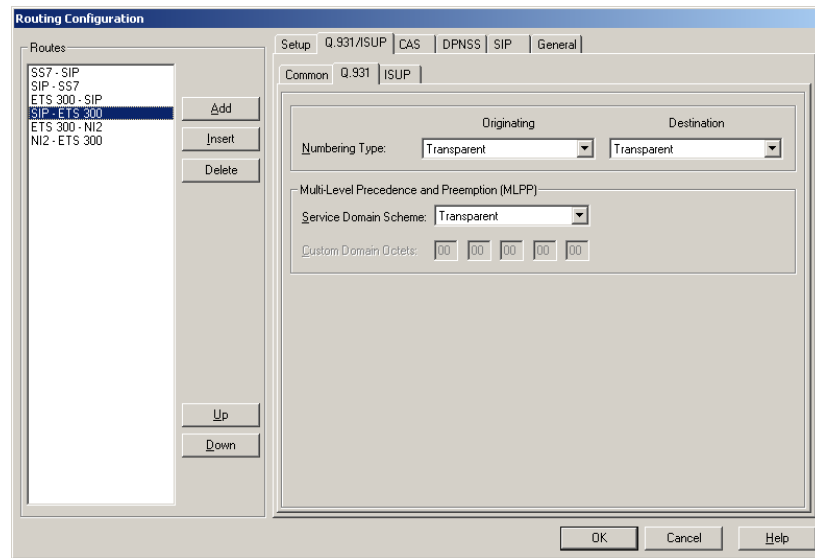


Figure 8-12 Routing configuration Q.931/ISUP – Q.931 tab option

Numbering Type – The Originating field sets the calling party type of number, and the Destination field sets the called party type of number. In addition to `Transparent` the following options are available:

- Unknown
- International
- National
- Network specific
- Subscriber Number
- Abbreviated Number

Multi Level Precedence and Preemption (MLPP) – Use the controls in this group to specify how the Service Domain Scheme should be mapped between an incoming and outgoing call. See section 17.3 for further information on Multi Level Precedence and Preemption.

Service Domain Scheme – Use this control to specify how the Service Domain Scheme parameter will be set in the outgoing call leg. When `Transparent` is selected the setting presented by the incoming call is passed through unchanged. If no Service Domain Scheme is presented by the incoming call a default setting will be applied. When `Custom` is selected any setting presented by the incoming call will be replaced with the content of the Custom Domain Octets control.

Custom Domain Octets – Use this control to specify the five octet Service Domain Scheme parameter to be used in the outgoing call leg, using hexadecimal form. This control will only be enabled when Service Domain Scheme is set to `Custom`.

ISUP tab options

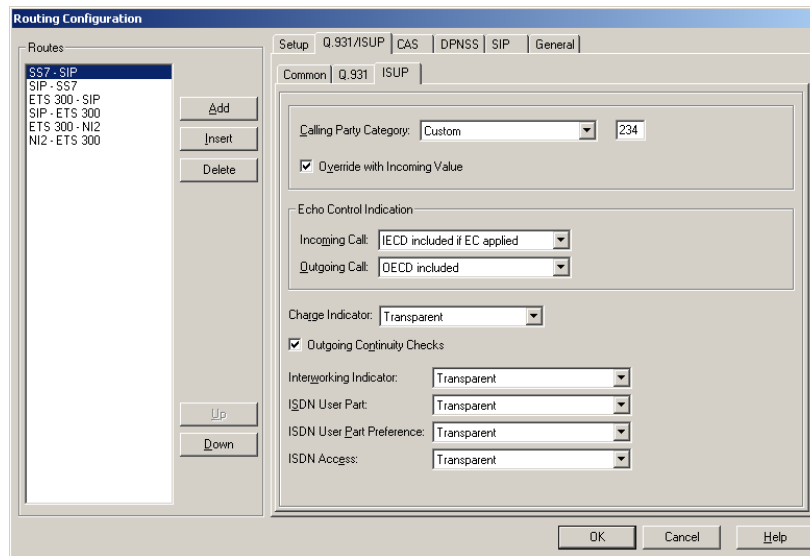


Figure 8-13 Routing configuration Q.931/ISUP – ISUP tab option

Calling Party Category – This field sets the calling party category. In addition to `Transparent` the following options are available:

- Custom
- French operator
- English operator
- German operator
- Russian operator
- Spanish operator
- Ordinary calling subscriber
- Calling subscriber with priority
- Data call
- Test call
- Payphone

When `Custom` is selected the adjacent edit field will be enabled. A decimal value should be entered into this field, this value will be written directly to the Calling Party's category parameter of the outgoing Initial Address Message.

Override with Incoming Value – This field will only be enabled when `Calling Party Category` is set to a value other than `Transparent`.

When `Calling Party Category` is set to `Transparent` a calling party category presented by the incoming call leg will be used in the outgoing call, otherwise a default setting will be used.

When `Calling Party Category` is set to a value other than `Transparent`, then the selected value will be used in the outgoing call leg regardless of whether a value has been presented by the incoming call. Checking `Override with Incoming Value` will modify this behaviour:

- If a calling party category is presented by the incoming call then this will be used in the outgoing call.
- If the incoming call does not present a calling party category then the selected value will be used in the outgoing call.

NOTE

A calling party category will be presented by an incoming SS7 call, or an incoming SIP call that includes an Aculab-SS7-Calling-Party-Category custom header. Refer to Appendix F: for a description of SIP custom headers.

Echo Control Indication – The controls in this group are used to set the Echo control device indicator (ECDI) bit in both the incoming and/or outgoing SS7 call legs.

Incoming Call – This control is used to configure how the ECDI bit in the Backward call indicators returned to an incoming SS7 call will be set. In addition to `Transparent` the following options are available.

IECD not included	The ECDI bit will be set to incoming echo control device not included (0).
IECD included	The ECDI bit will be set to incoming echo control device included (1).
IECD not included if EC applied	If echo cancellation has been applied to the outgoing call leg the ECDI bit will be set to incoming echo control device not included (0), otherwise incoming echo control device included (1) will be used.
IECD included if EC applied	If echo cancellation has been applied to the outgoing call leg the ECDI bit will be set to incoming echo control device included (1), otherwise incoming echo control device not included (0) will be used.

NOTE

The IECD not included if EC applied and IECD included if EC applied options are for use when making outgoing SIP calls only. Other protocols do not support echo cancellation.

Outgoing Call – This control is used to configure how the ECDI bit in the Nature of connection indicators sent in an incoming SS7 call will be set. In addition to `Transparent` the following options are available.

OECD not included	The ECDI bit will be set to outgoing echo control device not included (0).
OECD included	The ECDI bit will be set to outgoing echo control device included (1).

Charge Indicator – This field sets the Charge indicator bits in the Backward call indicators parameter sent to an incoming SS7 call leg. In addition to `Transparent` the following options are available:

No indication
No charge
Charge

Outgoing Continuity Checks – When this box is checked, a continuity check will be carried out before the outgoing SS7 call is made.

Interworking Indicator – This field sets the Interworking indicator bit in the Forward call indicators parameter sent by the outgoing SS7 call leg. In addition to `Transparent` the following options are available:

No interworking encountered
Interworking encountered

ISDN User Part – This field sets the ISDN user part indicator bit in the Forward call indicators parameter sent by the outgoing SS7 call leg. In addition to `Transparent` the following options are available:

- ISDN user part not used all the way
- ISDN user part used all the way

ISDN User Part Preference – This field sets the ISDN user part preference indicator bits in the Forward call indicators parameter sent by the outgoing SS7 call leg. In addition to `Transparent` the following options are available:

- ISDN user part preferred
- ISDN user part not required
- ISDN user part required

ISDN Access – This field sets the ISDN access indicator bit in the Forward call indicators parameter sent by the outgoing SS7 call leg. In addition to `Transparent` the following options are available:

- Originating access non-ISDN
- Originating access ISDN

8.5.4 Routes – CAS

The CAS page contains features intended for use when interworking with or between CAS protocols. Although the features are designed for use with CAS protocols, many are implemented in a protocol independent fashion and can be applied even when both call legs are ISDN.

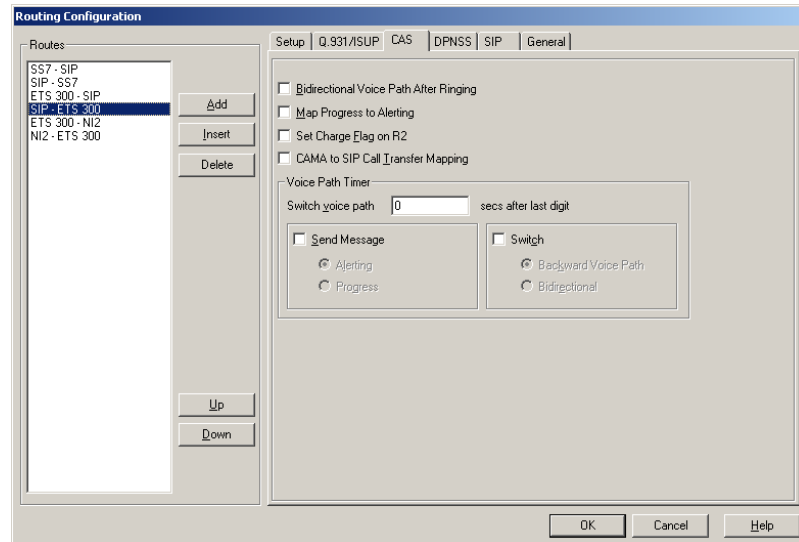


Figure 8-14 Routing configuration CAS tab option

Bidirectional Voice Path After Ringing – When interworking with CAS protocols, by default only the backwards voice path will be opened when the call reaches the ringing state. Selecting this option will open a bi-directional voice path at this stage.

Selecting this option will have no effect if tone generation has been configured to provide a ring tone on this route, or the Voice Path Timer field below has been configured to open up a backwards voice path.

NOTE

This feature is not supported if the incoming call is using the SS5 protocol.

Map progress to alerting – Some ISDN protocols use call progress indication to open up voice paths and allow in-band tones to be passed through. This option provides a way to achieve this when interworking between an outgoing protocol that supports call progress indication, and an incoming protocol which does not. When selected, any call progress messages received on the outgoing side which indicate in-band tones may be available are translated into ringing on the incoming side.

If both the incoming and outgoing protocols support call progress indication, then call progress will be mapped through.

NOTE

Care should be taken when using this option to ensure that it does not cause a calling side switch to generate a local ringing tone in response to a busy or unobtainable announcement.

Set Charge Flag on R2 – By default an accepted call will be charged. Check the Set Charge Flag on R2 option should you wish to indicate that the incoming call should not be charged, for example, when calling a Freephone number. This option is only supported by R2 protocols.

CAMA to SIP Call Transfer Mapping – When enabled a hookflash call transfer request from the outgoing CAMA call leg will be mapped to the incoming SIP call leg using RFC 2833 messaging. See section 12.3 for a description of CAMA to SIP call transfer mapping.

This control applies to CAMA ports only. Enabling this feature for other CAS protocols, or when the incoming call leg is not a SIP call will have no effect.

Voice Path Timer – Voice path switching in GroomerII is based on the protocols used on both ports. This is normally sufficient and copes with most situations encountered, however there may be a time where the default switching needs to be overridden.

With some CAS protocols, it is not possible to know the state of the outbound call, so it may be necessary to switch the voice path and/or send a message to the incoming call to indicate a state change.

Switch voice path x secs after last digit – Using this field to send a switch command and/or call control message a specified time after the last digit was received. Entering 0 will disable the feature.

Send Message – Selecting this option will send a call control message to the incoming call when the timer expires:

Alerting – will send the appropriate call control message for the incoming protocol to indicate that the far end is ringing.

Progress – will send an ISDN call progress message to the incoming call indicating that in-band tones are available.

NOTE

Only selected ISDN protocols support call progress messages.

Switch – Selecting this option will connect the voice paths when the timer expires:

Backward Voice Path – will switch only the backward voice path between the incoming and outgoing calls. This will allow in-band announcements to reach the caller, whilst still allowing the Aculab call control software to pass dialled digits between the calls.

Bidirectional – will switch both the forward and backward voice paths between the incoming and outgoing calls.

8.5.5 Routes – DPNSS

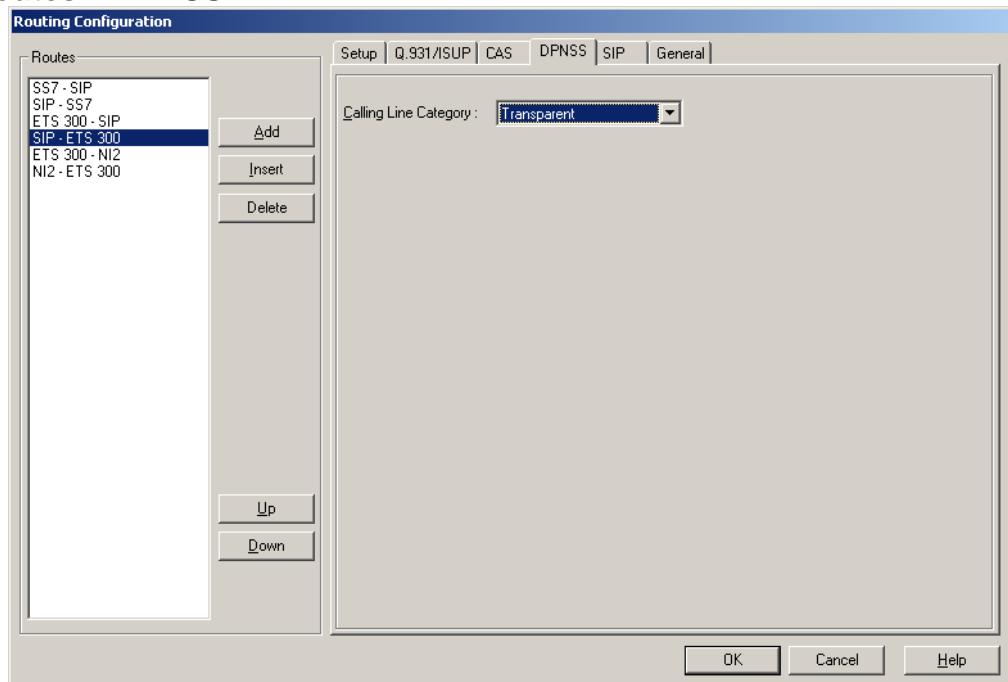


Figure 8-15 Routing configuration DPNSS tab option

Calling Line Category – is used to indicate where the call originated. It is often used to differentiate between calls on a private network and calls that originated in the public network in order to change the ring cadence used by the PBX. The options available are:

- Transparent
- Ordinary
- DASS2
- PSTN
- Decadic
- SSMF5
- Operator
- Network

Unless you are familiar with DPNSS protocols, you should leave this at the default setting of `Transparent`.

8.5.6 Routes SIP

This page allows the media and codec settings for SIP calls using this route to be configured. The settings for incoming and outgoing calls are configured separately using the Incoming and Outgoing pages. Each page contains two further pages:

Codecs – this page is used to specify the codecs to be offered during negotiation.

Media Settings – this page is used to specify protocol specific parameters and media settings.

Each page is shown below:

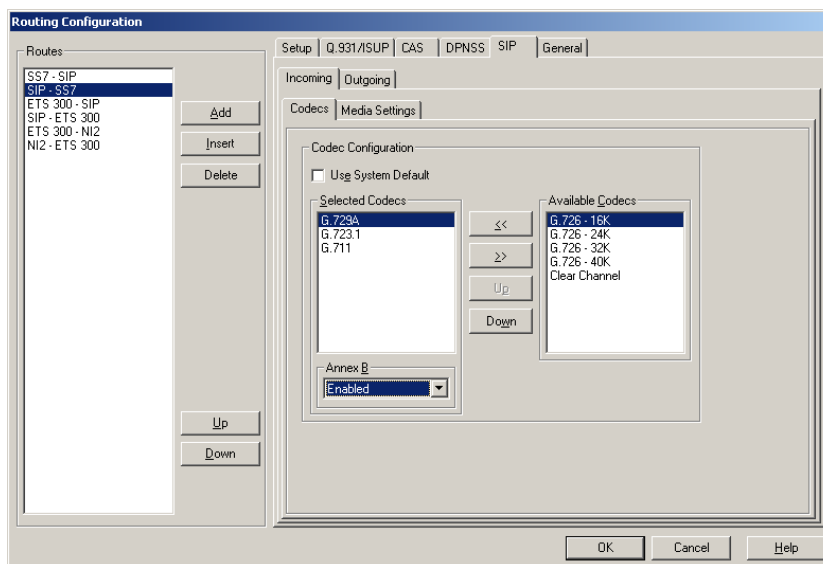


Figure 8-16 Routing configuration SIP incoming codecs tab option

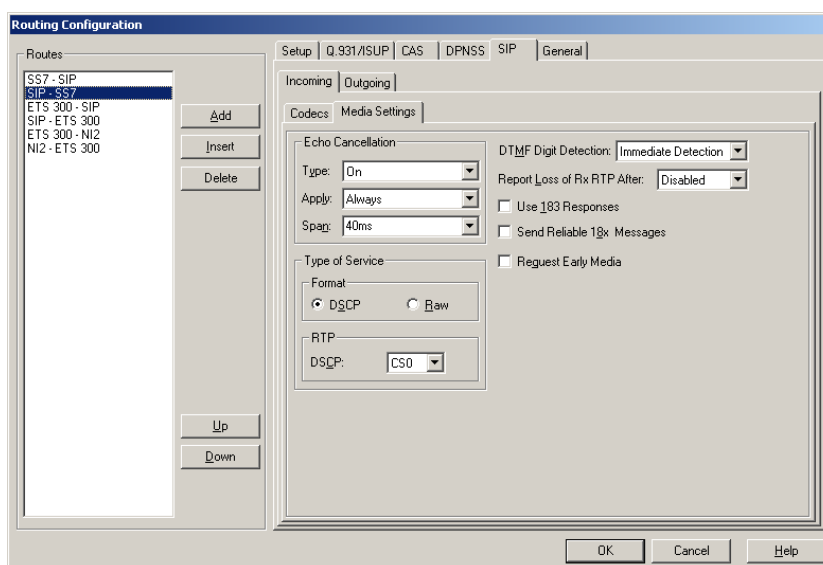


Figure 8-17 Routing configuration SIP incoming media settings tab option

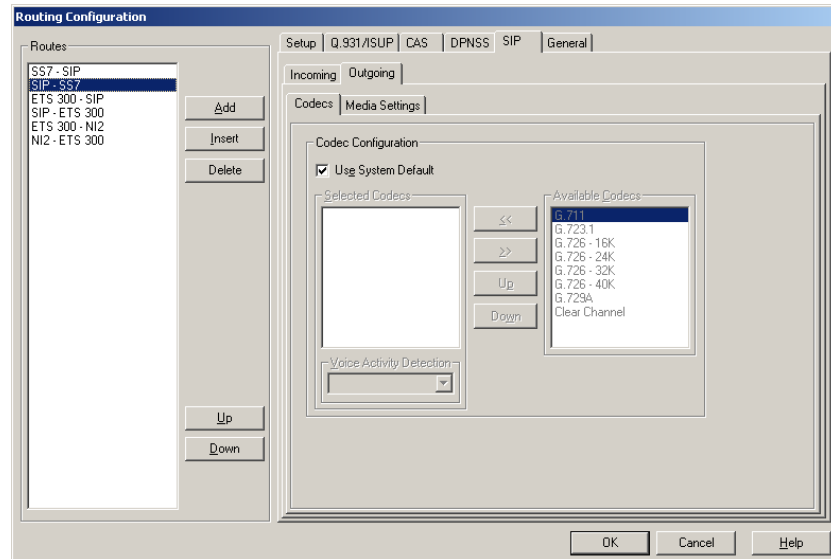


Figure 8-18 Routing configuration SIP outgoing codecs tab option

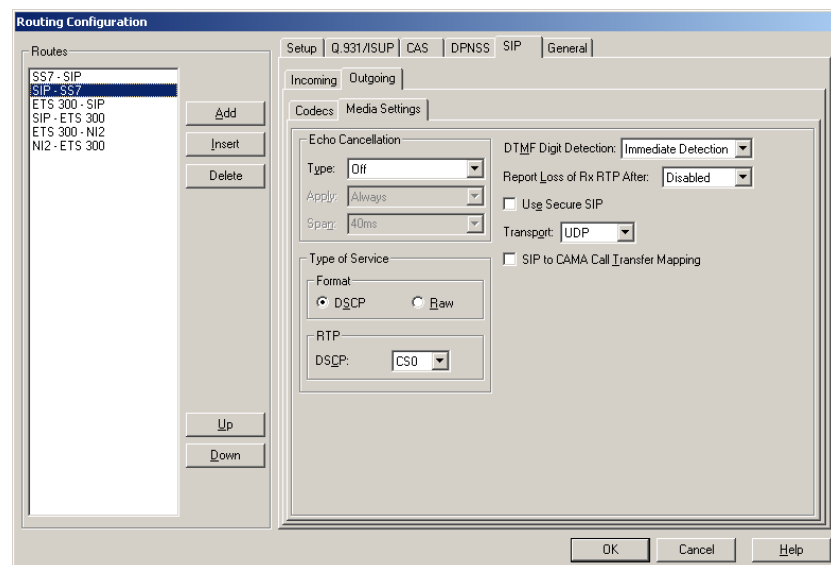


Figure 8-19 Routing configuration SIP outgoing media settings tab option

Codecs page

Use System Default – Check this box if you want the route to offer the system default codec list defined in the System Configuration – Default Codecs page explained in section 0. All other codec configuration controls will be disabled when this option is selected.

NOTE

When Use System Default is selected the codecs offered by this route will change whenever the default codec list is modified.

Uncheck the box if you want the route to offer a different set of codecs to the default list, or if you do not want the set of codecs offered by the route to change when the default list is modified. The codecs to be offered should be placed in the Selected Codecs list in priority order. Use the buttons to manipulate the list:

- To add a codec, select the required codec from the Available Codecs list then click << to move the codec into the Selected Codecs list.
- To remove a codec, select the required codec from the Selected Codecs list then click >> to move the codec into the Available Codecs list.
- To change a codec priority, select the codec in the Selected Codecs list and then use the Up and Down buttons to change the priority order.

NOTE

The G.726 and Clear Channel codecs are not available when making or receiving secure SIP calls.

As the Selected Codecs list is traversed the VAD (voice activity detection) settings applied to the transmitted RTP stream for the selected codec may be configured in the control group below the list.

Voice Activity Detection – This control group is displayed when a G.711 or G.726 codec is selected. The options available are:

Disabled – No silence suppression will be applied. The received audio stream will be packetised and transmitted across RTP

DTX – Discontinuous transmission. The received audio stream will be analysed, and no packets will be sent across RTP when silence is detected.

Comfort Noise – This will offer a comfort noise codec (RFC 3551, payload 13) to the remote endpoint. If this is accepted any silence detected will be replaced by comfort noise packets in the RTP stream. If the remote endpoint does not accept the comfort noise codec then DTX will be used.

When using a G.711 or G.726 codec, if the remote endpoint offers a comfort noise codec this will be accepted by GroomerII regardless of the VAD settings, and any comfort noise packets received decoded into the audio stream.

Silence Compression – This control group is displayed when the G.723.1 codec is selected. The options available are:

Enabled – When selected Annex A silence compression will be applied to the transmitted RTP stream.

Disabled – When selected no Annex A frames will be transmitted in the RTP stream.

When using a G.723.1 codec, any Annex A frames received from the remote endpoint will be accepted and decoded regardless of the setting in this control.

Annex B – This control group is displayed when the G.729A codec is selected. The options available are:

Enabled – When selected the G.729AB codec will be offered to the remote endpoint. If this is accepted the voice activity detector may transmit both 'A' and 'B' frames on the RTP stream, otherwise only 'A' frames will be transmitted.

Disabled – When selected the voice activity detector will generate only 'A' frames on the RTP stream.

When using a G.729A codec, any 'B' frames received from the remote endpoint will be accepted and decoded regardless of the setting in this control.

Media Settings page

Echo Cancellation – The controls in this group are used to configure how echo cancellation will be applied.

Type – Use this control to specify whether echo cancellation should be applied. The options available are:

Off – disables the echo canceller.

On – enables the echo canceller.

On with NLP (Muting) – enables the echo canceller with non-linear processing to suppress the signal whenever echo or background noise are dominant.

This mode of operation is suitable for large-scale conferencing and/or IVR applications, where it is important that the signal is completely muted whenever the caller is not speaking.

On with NLP (CNG) – enables the echo canceller with non-linear processing to replace the signal with comfort noise whenever echo might otherwise be audible. This mode of operation is most appropriate to IP gateway applications where background noise is desirable to maintain the illusion of continuity.

NOTE

If the Clear Channel codec is selected during codec negotiation the setting in this field will be ignored and echo cancellation will not be applied.

Apply – This control is only available when Type is set to On, On with NLP (Muting) or On with NLP (CNG), and is used to specify the conditions under which echo cancellation will be applied. The options available are:

Always Echo cancellation will always be applied.

The following settings should be used only when interworking between SIP and SS7. When interworking with non-SS7 protocols using these settings will result in echo cancellation not being applied.

Backward ECDI = 0 (incoming page only) Echo cancellation will only be applied when the echo control device indicator bit in the Backward call indicators returned by the outgoing SS7 call is set to incoming echo control device not included (0).

Backward ECDI = 1 (incoming page only) Echo cancellation will only be applied when the echo control device indicator bit in the Backward call indicators returned by the outgoing SS7 call is set to incoming echo control device included (1).

Forward ECDI = 0 (outgoing page only) Echo cancellation will only be applied when the echo control device indicator bit in the Nature of connection indicators presented by the incoming SS7 call is set to incoming echo control device not included (0).

Forward ECDI = 1 (outgoing page only) Echo cancellation will only be applied when the echo control device indicator bit in the Nature of connection indicators presented by the incoming SS7 call is set to incoming echo control device included (1).

Span – This control is only available when Type is set to On, On with NLP (Muting) or On with NLP (CNG), and is used to select the length of time for which the echo canceller will monitor the return voice path looking for the forward signal.

NOTE

The echo span may be set to 40ms, 70ms or 104ms. The 70ms and 104ms settings should not be used unnecessarily, as the additional processor requirement may cause echo to be missed during periods of heavy call load.

Type of service – Sets the type of service field within the IP header of real time protocol (RTP) packets transmitted by the board.

Format – Use the radio buttons to select the format in which to specify the Type of Service setting. The available types are:

DSCP – allows the setting to be selected from a list of commonly used named constants.

Raw – the setting is entered as a hexadecimal value, allowing settings for which no DSCP constant is provided to be used.

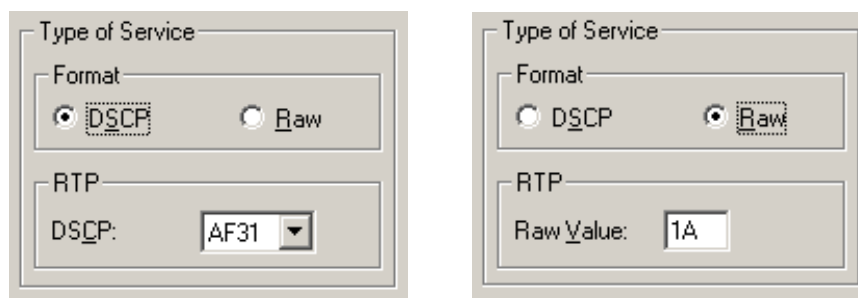


Figure 8-20 Type of service selection options

The controls available are dependent upon the setting in the Format group, as illustrated above.

DSCP – the drop down list contains a list of named constants whose values are based upon the information provided in IETF RFC 4595. The following constants are available, the numbers alongside show their hexadecimal equivalents:

AF11	(0A)
AF12	(0C)
AF13	(0E)
AF21	(12)
AF22	(14)
AF23	(16)
AF31	(1A)
AF32	(1C)
AF33	(1E)
AF41	(22)
AF42	(24)
AF43	(26)
CS0	(00)
CS1	(08)
CS2	(10)
CS3	(18)
CS4	(20)
CS5	(28)
CS6	(30)
EF	(2E)

Raw Value – allows the type of service setting to be specified as an 8-bit value in hexadecimal form.

DTMF Digit Detection – This control specifies whether DTMF digits should be removed from the audio stream and sent out-of-band using RFC 2833 frames. The following settings are available.

Disabled – DTMF digits will not be removed from the audio stream, and no out-of-band frames will be sent.

Immediate Detection – An out-of-band tone will be generated as soon as the appropriate tone has been detected.

40ms Detection – An out-of-band tone will not be generated until the appropriate tone has been detected continuously for at least 40ms.

In most applications Immediate Detection will be the appropriate setting. The 40ms Detection setting is designed for use in environments where high levels of background noise could cause spurious digits to be detected.

Report Loss of Rx RTP After – Setting this control to a value other than <Disabled> will cause a `groomerReceivedRTPStoppedTrap` SNMP alarm to be generated if no RTP packets are received from the remote endpoint for the specified period. The `groomerReceivedRTPStoppedTrap` SNMP alarm is described in Appendix A:.

NOTE

The use of DTX by the remote endpoint may cause silence on the line to be interpreted as loss of RTP.

NOTE

SNMP reporting must be enabled in the GroomerII Kernel for SNMP traps to be produced. See section 5.4 for further details.

Use 183 Response – This option is available for incoming calls only. Enabling this control will cause a 183 message to be sent instead of a 180 message at the ringing stage. This control is provided to overcome interoperability issues. Unless its use is essential, it is recommended that it be left at the default value.

Send Reliable 18x Messages – This option is available for incoming calls only. Enabling this control causes 180 series messages to be sent reliably instead of unreliably. Unexpected behaviour may be experienced if this option is enabled when the caller does not support the protocol extension required for reliable provisional responses.

Request Early Media – This option is available for incoming calls only. This option is primarily intended for use when interworking with protocols such as CAS, which do not themselves support call progress.

Progress information from the outgoing leg of a call will automatically be used to request an early media path from an incoming SIP call if appropriate. Enabling this option will cause an early media request to be made at the ringing stage regardless of what progress information may have been received from the outgoing call.

Use Secure SIP – This option is available for outgoing calls only. When this control is checked all SIP calls made using this route will be secure. See section 14.1 for an explanation of SIP security.

NOTE

This control will only be available when the restricted availability variant of GroomerII software is in use.

Transport – This option is available for outgoing calls only. Sets the IP transport protocol used by SIP to send call control messaging. The default is UDP. Permitted values are:

UDP – User Datagram Protocol.

TCP – Transmission Control Protocol.

This control will be disabled whenever Use Secure SIP is selected.

SIP to CAMA Call Transfer Mapping – This option is available for outgoing calls only. When enabled, an RFC 2833 hookflash call transfer request from the outgoing SIP call leg will be mapped to the incoming CAMA call leg. See section 12.4 for a description of SIP to CAMA call transfer mapping.

This control applies when interworking from CAMA to SIP only. Enabling this feature when the incoming call leg is not a CAMA call will have no effect.

8.5.7 Routes – general

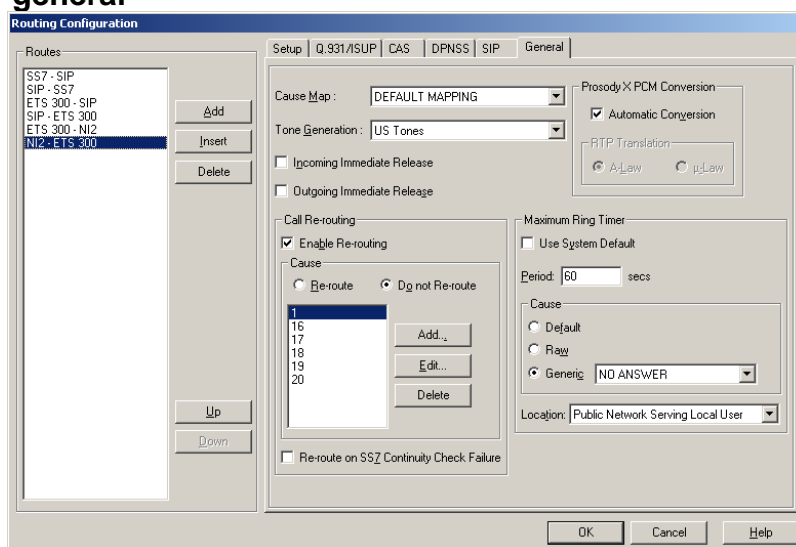


Figure 8-21 Routing configuration general tab option

Cause Map – Used to select between default mapping of clear causes, and a user defined mapping list. The user defined options for Cause Map are created using the Cause Mapping option covered in section 8.7 (Cause mapping).

Tone Generation – Used to select which call progress tone set will be played to the incoming leg of calls using this route. There are four standard tone sets available, and further user defined tone sets can be configured using the Tone Generation option covered in section 8.8 (Tone generation). Select <None> if no call progress tones are to be generated.

Incoming/Outgoing Immediate Release – Under normal conditions, GroomerII does not complete the release of the call until both sides have cleared. This option is used when you have a requirement to clear incoming or outgoing calls as soon a clear request is received. When these fields are checked, GroomerII will not wait for the other part of the call to clear first.

Call Re-routing – The controls in this group allow GroomerII to search for an alternative route should an outgoing call using the selected route be rejected.

NOTE

Call re-routing is not supported in any of the following circumstances:

- The incoming call leg is an ETS 300 call requesting explicit UUS activation,
- The incoming call leg is using the SS5 protocol,
- The outgoing call leg is using any CAS protocol.

Enable Re-routing – Checking this box will allow calls using this route to search for an alternative route should they fail to complete.

Cause – it may not be appropriate to re-route calls under all circumstances (for example when the call returns user busy), and the controls in this group allow a list of protocol specific causes to be defined. The controls in this group will be disabled when Enable Re-routing is unchecked.

Select the Re-route radio button if calls should be re-routed when they fail with a cause in the list, or Do not Re-route to prevent calls from being re-routed when they fail with a cause in the list.

Cause list entries are added and modified using the Add/Edit Re-route Cause dialog. Use the Add... and Edit... buttons to access this dialog.

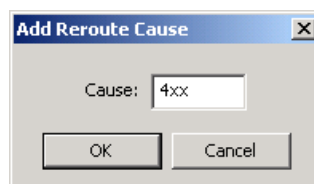


Figure 8-22 Add/Edit Re-route cause dialog

The x wildcard may be used in trailing positions to allow a range of causes to be matched against a single entry.

Entries are removed from the cause list using the Delete button.

Re-route on SS7 Continuity Check Failure – If this box is checked, SS7 calls using this route that fail an outgoing continuity check will be re-routed.

Prosody X PCM Conversion – The controls in this group configure how PCM conversion is applied when routing calls between ports.

Automatic Conversion – The default mode of operation is for GroomerII to detect the type of ports in use (E1/T1/IP) and apply any PCM conversion required automatically. In some instances, for example when E1 links are being used to carry μ -law speech, it may be necessary to disable such conversion. Checking this box will cause PCM conversion to be carried out automatically. Unchecking the box allows the voice path to pass between incoming and outgoing call legs unmodified.

RTP Translation – The controls in this group will be disabled when Automatic Conversion is selected. Use the A-Law and μ -Law radio buttons to select the translation to be applied when passing speech between a TDM port and the RTP stream on an IP telephony port. Incoming RTP will be translated into the selected encoding, whilst outgoing RTP will be translated using the appropriate algorithm for the encoding selected.

NOTE

It is not possible to apply different translations to the incoming and outgoing RTP streams.

Maximum Ring Timer – The control in this group allow the system level Maximum Ring Timer (see section 8.6.6) to be overridden with a route specific setting.

CAUTION

If a Maximum Ring Period is used, the timer should be set to a high value, at least 180 seconds (3 minutes) is suggested. Lower values may cause the call to drop prematurely.

NOTE

The timeout release will not work on most CAS protocols as they do not allow the call to be cleared by the B party.

Use System Default – If this box is checked the system level ring timer will be used and all other controls in the group will be disabled.

Period – The time the outgoing call will be allowed to remain in the ringing state before being cleared. Setting this field to zero will disable the ringing timer.

Cause – Use the controls in this group to specify the cause to be used when clearing the incoming call leg on timer expiry.

Default – When selected the generic clearing cause of NO ANSWER will be used.


Raw – This option allows a protocol specific release code to be used. For example, 17 would be entered to clear an incoming EuroISDN call with User Busy.

Generic – This option allows the clearing cause to be selected from a list of generic causes. This allows an appropriate protocol specific cause to be automatically selected when clearing the incoming call leg. For example, selecting NUMBER BUSY will use the correct busy release cause for the incoming protocol.

Location – The Location field applies to SS7 and Q.931 calls only, and is ignored by all other protocols. This control allows the location field in the Q.850 cause parameter to be set when the timer clears a call. A location of User will be applied when `Default` is selected.

8.6 System configuration

The GroomerII System Configuration dialog is used to configure system wide resources, and settings that will be applied to all calls passing through the system.

In the GroomerII Configuration Editor main window select  from the toolbar, or Configuration – System... from the menu, to open the System Configuration dialog.

8.6.1 Clocks

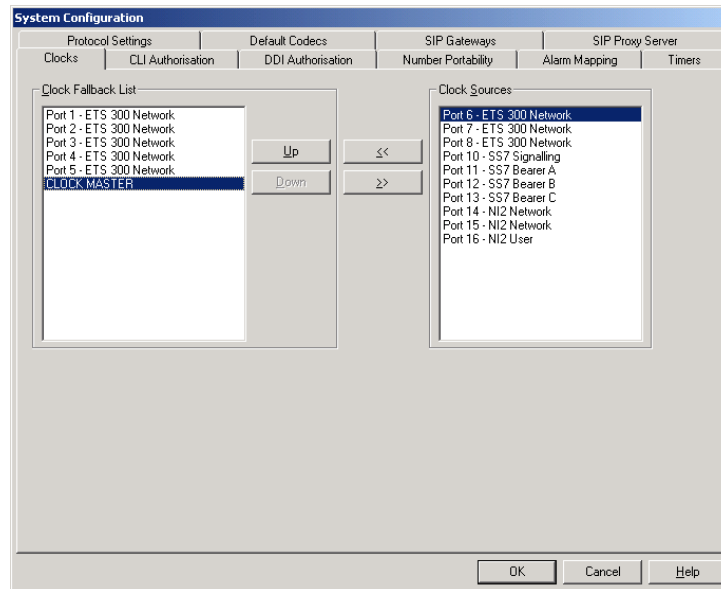


Figure 8-23 System configuration clocks tab option

The Clocks page is used to specify which ports GroomerII will use as the system clock source. The system clock source is used to drive the H.100 bus, which in turn provides clocking to all other ports in the system.

Clock Fallback List – The Clock Fallback List specifies which ports may drive the system clock, and the order in which they should be used. GroomerII will use the first available port in the list to drive the clock, and should this port become unavailable the next available port will be selected. Should a previously failed port become available GroomerII will restore this port as the clock source. The Clock Fallback List must contain at least one entry.

NOTE

Network connections should come before PBX and user connections in the Clock Fallback List.

Clock Sources – Contains a list of the ports available but not selected as a fallback clock source along with the special entry CLOCK MASTER, which uses the oscillator on one of the Prosody X cards to drive the clock. This will be an arbitrary selection based upon which cards are currently started. If none of the equipment connected to the GroomerII can source a clock, then CLOCK MASTER should be the only entry in the fallback list.

NOTE

It is not possible to detect when CLOCK MASTER has failed. If used it should be the last source in the list.

To add a clock source to the Clock Fallback List, select a port from the Clock Sources list, then click <<. The Port will be added to the end of the Clock Fallback List.

To remove a port from the Clock Fallback List, select the port in the list and click >>. The Port will be removed to the Clock Sources list.

The Up and Down buttons are used to re-order the Clock Fallback List.

8.6.2 CLI authorisation

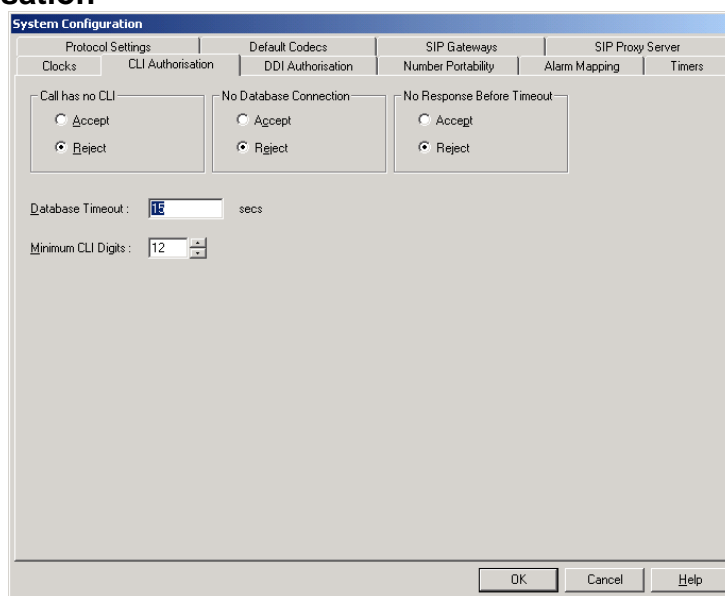


Figure 8-24 System configuration - CLI authorisation tab option

The following settings only apply when you try to use a route that has CLI authorisation enabled. CLI authorisation then looks at the incoming call CLI information and validates the information according to the settings. CLI authorisation is only checked once, so if the first route that has CLI authorisation enabled is rejected, all other routes that have CLI authorisation enabled will also be rejected.

Call has no CLI – Instructs the system what action to take if a call is received that has no CLI. Most CAS protocols do not support CLI, so when using such a protocol you might set this to Accept in order that all calls are authorised. However, ISDN protocols should always contain a CLI, and in this instance you may wish to set this to Reject in order to prevent unauthorised users from accessing a system by hiding their CLI. The default is to reject authorisation.

No database connection – Instructs the system how to authorise a CLI when the request cannot reach the database for whatever reason. This can include both loss of connection to the database, and system errors. The default is to Reject the authorisation request.

No response before timeout – Instructs the system how to authorise a CLI if the database query timeout expires before the query has completed. The default is to Reject authorisation.

Database timeout – This is the database query timeout value, specified in seconds, that applies to the time between the query being initiated and the response being received. It includes time spent waiting in internal system queues. The default value is zero.

CAUTION

If an ODBC data source system timeout has been set to a value that is less than the database query timeout, CLI Authorisation could timeout earlier than the time specified in the Database Timeout field.

Minimum CLI digits – Specifies the minimum number of digits that a CLI must have to be considered valid. The sole purpose of this field is to avoid the expense of sending an invalid CLI to the database for authorisation. When set to zero, this field is disabled and all CLIs will be sent to the database for authorisation. This value defaults to zero.

Calls failing CLI authorisation will be unable to use routes that have CLI Authorisation applied.

8.6.3 DDI authorisation

Figure 8-25 System configuration - DDI authorisation tab option

The following settings only apply when you try to use a route that has DDI authorisation enabled. DDI authorisation then looks at the incoming call DDI information and validates the information according to the settings. DDI authorisation is only checked once, so if the first route that has DDI authorisation enabled is rejected, all other routes that have DDI authorisation enabled will also be rejected.

List type – Defines how the data in the ODBC data source will be interpreted:

Black List – the data source contains a list of DDIs that are prohibited from using routes that have DDI Authorisation enabled. The DDI will only be authorised to use such routes if it is not present in the database.

White List – the data source contains a list of DDIs that are allowed to use routes that have DDI Authorisation enabled. The DDI will only be authorised to use such routes if it is present in the database.

The default is to interpret the data as a Black List.

No database connection – Instructs the system how to authorise a DDI when the request cannot reach the database for whatever reason. This can include both loss of connection to the database, and system errors. The default is to Reject the authorisation request.

No response before timeout – Instructs the system how to authorise a DDI if the database query timeout expires before the query has completed. The default is to Reject authorisation.

Database timeout – This is the database query timeout value, specified in seconds, that applies to the time between the query being initiated and the response being received. It includes time spent waiting in internal system queues. The default value is zero.

CAUTION

If an ODBC data source system timeout has been set to a value that is less than the database query timeout, DDI Authorisation could timeout earlier than the time specified in the Database Timeout field.

Minimum DDI digits – Specifies the minimum number of digits that a DDI must have to be considered valid. The sole purpose of this field is to avoid the expense of sending an invalid DDI to the database for authorisation. When set to zero, this field is disabled and all DDIs will be sent to the database for authorisation. This value defaults to zero.

Calls failing DDI authorisation will be unable to use routes that have DDI Authorisation applied.

8.6.4 Number portability

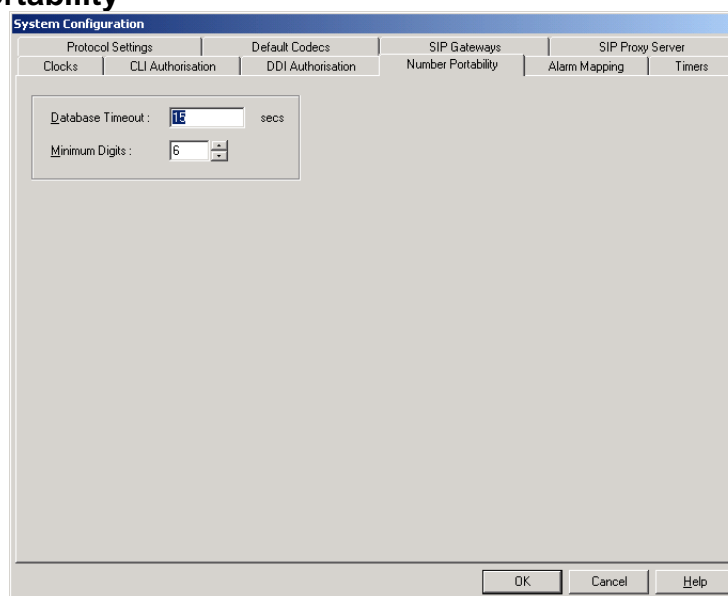


Figure 8-26 System configuration – number portability tab option

The following settings only apply when an incoming call is received on a port that has Number Portability Mapping enabled, and define the system behaviour when submitting a mapping query to the data source.

Database timeout – This is the database query timeout value, specified in seconds, that applies to the time between the query being initiated and the response being received. It includes time spent waiting in internal system queues. The default value is zero.

CAUTION

If an ODBC data source system timeout has been set to a value that is less than the database query timeout, The Number Portability query could timeout earlier than the time specified in the Database Timeout field.

Minimum digits – Specifies the minimum number of digits that a DDI must have in order to be submitted to the data source for mapping. The sole purpose of this field is to avoid the expense of sending an invalid DDI to the database for mapping. When set to zero, this field is disabled and all DDIs will be sent to the database for mapping. This value defaults to zero.

8.6.5 Alarm mapping.

GroomerII can transmit a layer 1 alarm in response to a received layer 1 alarm, for example to warn backward switches that it is no longer able to forward their calls. The Alarm Mapping page is used to define how an incoming alarm on one port should be used to generate outgoing alarms on other ports.

NOTE

Alarms cannot be generated on IP telephony ports.

To add a new alarm map, select Add. The new map will be added to the bottom of the Alarm Mappings list.

To update an existing map, select the map to be updated, and make the required changes.

To remove a map from the Alarm Mappings list, select the map to be removed followed by Delete.

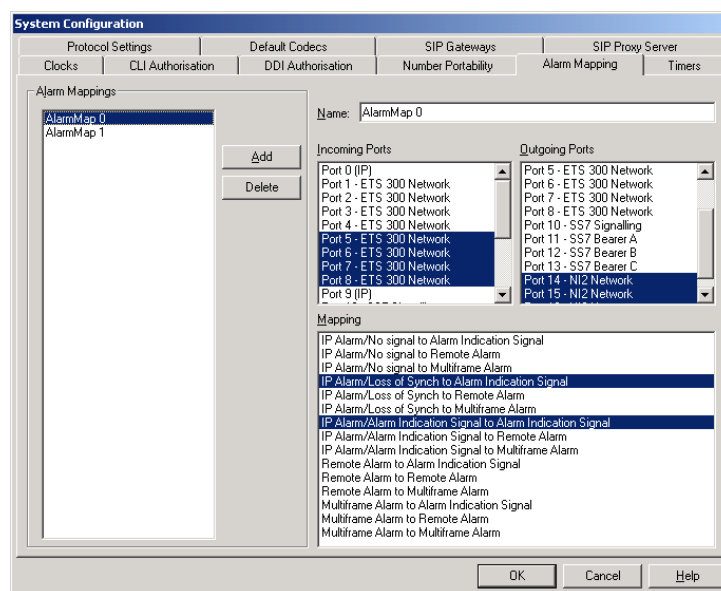


Figure 8-27 System configuration alarm mapping tab option

Name – An identification string for user reference only.

Incoming Ports – Specifies the incoming port(s) to be checked for received alarms. If only one port is selected from the list, then only this port is checked. However, if two or more ports are selected, then all the selected ports must be in an alarm condition for the outbound alarm to be generated.

If you wish to monitor port 0 OR port 1 rather than port 0 AND port 1, then create an alarm map for each port.

Outgoing Ports – Lists the Port(s) on which the mapped alarms should be generated, any number of Ports can be selected from the list.

Mapping – Used to select how alarms should be mapped between the incoming and outgoing ports. Multiple mappings can be selected. Only a single outgoing alarm can be generated on a port at any one time, and this will be the most severe alarm.

Alarm precedence

For the purpose of alarm mapping, when an alarm is received on a port all of the less severe alarms are also considered to be present on that port. The following shows the comparative severity of each alarm, where NOS is the most severe:

- No signal (NOS)
- Loss of synchronisation (LOS)
- Alarm indicator signal (AIS), IP link failure (Ports A and B both Disconnected)
- Remote alarm indication (RAI), Multiframe alarm (MFA)

Only one alarm can be generated on a port at any time. Should the mapping scheme require multiple outgoing alarms to be generated, only the most severe alarm will be applied.

CAUTION

If your PBX has alternative routing, generating alarms to a PBX may force it to re-route calls. Sending Layer 1 alarms to the PTT is highly inadvisable, as this may put the line out of service requiring you to request that the line is returned to service.

8.6.6 Timers

The Timers page is used to configure timeouts that will be applied to all calls passing through the system.

Figure 8-28 System configuration timers tab option

Incomplete Dialling – The Timeout parameter is used to prevent an unfinished call from using up a system resource. When the Timeout value is one or more, then a timer is started when an incoming call is detected.

If an outgoing call has not been made and reached a ringing state when the timer reaches the Timeout value, the call is disconnected with the specified Cause. If ringing is detected within the timeout period, Timeout is cancelled.

Maximum Ring – The Maximum Ring timer is similar to the incomplete dialling timer but starts at the ringing stage and goes on until connect is received or the specified Period is reached. If Period is reached before the outgoing leg is connected, then the call is cleared with the selected Cause.

CAUTION

If a Maximum Ring Period is used, the timer should be set to a high value, at least 180 seconds (3 minutes) is suggested. Lower values may cause the call to drop prematurely.

NOTE

The timeout release will not work on most CAS protocols as they do not allow the call to be cleared by the B party.

Cause values

The operation of the Cause control group is identical for both the Incomplete Dialling and Maximum Ring timers.

Default – When selected will use the generic clearing cause of NUMBER UNOBTAINABLE for incomplete dialling, or NO ANSWER for Maximum Ring.

Raw – This option allows a protocol specific release code to be used. For example, 17 would be entered to clear an incoming EuroISDN call with User Busy.

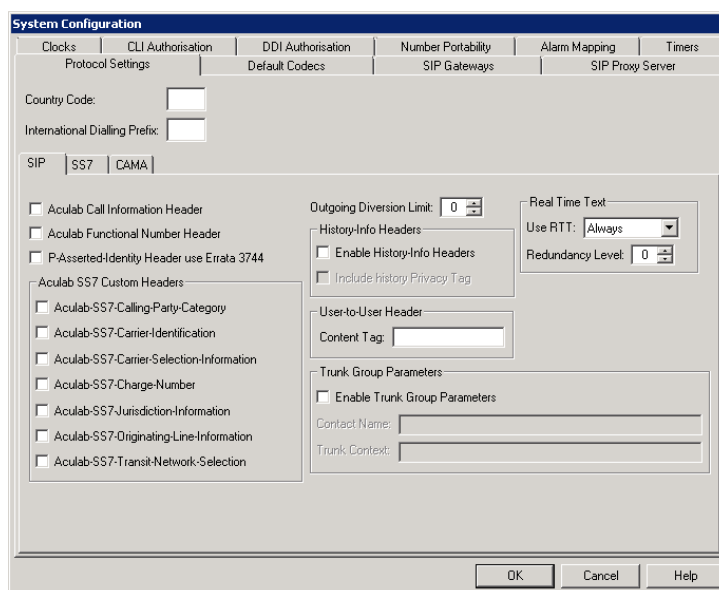
Generic – This option allows the clearing cause to be selected from a list of generic causes. This allows an appropriate protocol specific cause to be automatically selected when clearing the incoming call leg. For example selecting NUMBER BUSY will use the correct busy release cause for the incoming protocol.

Location

The Location field applies to SS7 and Q.931 calls only, and is ignored by all other protocols. This control allows the location field in the Q.850 cause parameter to be set when the timer clears a call. A location of User will be applied when `Default` is selected.

8.6.7 Protocol Settings

The Protocol Settings page is used to configure system level protocol settings.



System Configuration

Clocks | CLI Authorisation | DDI Authorisation | Number Portability | Alarm Mapping | Timers
Protocol Settings | Default Codecs | SIP Gateways | SIP Proxy Server

Country Code:

International Dialling Prefix:

SIP | SS7 | CAMA

☐ Aculab Call Information Header

☐ Aculab Functional Number Header

☐ P-Asserted-Identity Header use Errata 3744

Aculab SS7 Custom Headers

☐ Aculab-SS7-Calling-Party-Category

☐ Aculab-SS7-Carrier-Identification

☐ Aculab-SS7-Carrier-Selection-Information

☐ Aculab-SS7-Charge-Number

☐ Aculab-SS7-Jurisdiction-Information

☐ Aculab-SS7-Originating-Line-Information

☐ Aculab-SS7-Transit-Network-Selection

Outgoing Diversion Limit:

History-Info Headers

☐ Enable History-Info Headers

☐ Include History-Privacy Tag

User-to-User Header

Content Tag:

Trunk Group Parameters

☐ Enable Trunk Group Parameters

Contact Name:

Trunk Context:

Real Time Text

Use RTT:

Redundancy Level:

OK Cancel Help

Figure 8-29 System configuration Protocol Settings - SIP tab option

Country Code – This is the international dialling code for the country in which GroomerII is located. Currently this field is only used when processing UK ISUP calls, and UK ISUP users must set this to 44.

International Dialling Prefix – This is the international dialling prefix used by the country in which GroomerII is located. Currently this field is used when processing UK ISUP calls only, and UK ISUP users must set this to 00.

SIP tab options

The controls on the SIP page (illustrated above) are used to configure settings that are specific to SIP calls.

Aculab Call Information Header – When enabled an Aculab-Call-Information header will be presented to the remote endpoint as described in section F.4.

Aculab Functional Number Header – Enable this control to allow production and processing of an Aculab-Functional-Number header. See section 14.6 for an explanation of Functional Number mapping.

P-Asserted-Identity Header use Errata 3744 – When enabled the P-Asserted-identity header, described in RFC 3325, is populated using Errata 3744 of that RFC. When disabled the header is populated as specified by the original RFC. Disabling this option provides compatibility with older endpoints which, while adhering to the original RFC, are incompatible with the Errata.

Aculab SS7 Custom Headers – Use the controls in this group to manage the production and interpretation of Aculab SS7 custom headers. These headers only apply to calls interworking between SIP and SS7. The Aculab SS7 custom headers are fully described in section F.1.

Aculab-SS7-Calling-Party-Category – When enabled and an Aculab-SS7-Calling-Party-Category header is presented by an incoming SIP call, the information contained will be mapped to an outgoing SS7 call. The calling party category information presented by an incoming SS7 call will be used to generate an Aculab-SS7-Calling-Party-Category header in the outgoing SIP call.

When disabled no mapping is carried out in either direction.

NOTE

When interworking from SIP to SS7, any Aculab-SS7-Calling-Party-Category header present will be overridden by an explicit setting in the routing table.

Aculab-SS7-Carrier-Identification – When enabled and an Aculab-SS7-Carrier-Identification header is presented by an incoming SIP call, the information contained will be mapped to an outgoing ANSI SS7 call. Any carrier identification information presented by an incoming ANSI SS7 call will be used to generate an Aculab-SS7-Carrier-Identification header in the outgoing SIP call.

When disabled no mapping is carried out in either direction.

Aculab-SS7-Carrier-Selection-Information – When enabled and an Aculab-SS7-Carrier-Selection-Information header is presented by an incoming SIP call, the information contained will be mapped to an outgoing ANSI SS7 call. Any carrier selection information presented by an incoming ANSI SS7 call will be used to generate an Aculab-SS7-Carrier-Selection-Information header in the outgoing SIP call.

When disabled no mapping is carried out in either direction.

Aculab-SS7-Charge-Number – When enabled and an Aculab-SS7-Charge-Number header is presented by an incoming SIP call, the information contained will be mapped to an outgoing ANSI SS7 call. Any charge number information presented by an incoming ANSI SS7 call will be used to generate an Aculab-SS7-Charge-Number header in the outgoing SIP call.

When disabled no mapping is carried out in either direction.

Aculab-SS7-Jurisdiction-Information – When enabled and an Aculab-SS7-Jurisdiction-Information header is presented by an incoming SIP call, the information contained will be mapped to an outgoing ANSI SS7 call. Any jurisdiction information presented by an incoming ANSI SS7 call will be used to generate an Aculab-SS7-Jurisdiction-Information header in the outgoing SIP call.

When disabled no mapping is carried out in either direction.

Aculab-SS7-Originating-Line-Information – When enabled and an Aculab-SS7-Originating-Line-Information header is presented by an incoming SIP call, the information contained will be mapped to an outgoing ANSI SS7 call. Any originating line information presented by an incoming ANSI SS7 call will be

used to generate an Aculab-SS7-Originating-Line-Information header in the outgoing SIP call.

When disabled no mapping is carried out in either direction.

Aculab-SS7-Transit-Network-Selection – When enabled and an Aculab-SS7-Transit-Network-Selection header is presented by an incoming SIP call, the information contained will be mapped to an outgoing ANSI SS7 call. Any transit network selection information presented by an incoming SS7 call will be used to generate an Aculab-SS7-Transit-Network-Selection header in the outgoing SIP call.

When disabled no mapping is carried out in either direction.

Outgoing Diversion Limit – Use this control to specify how many times an outgoing SIP call may be diverted before being cleared with an appropriate number changed cause. Setting the control to zero will allow unlimited diversions.

History-Info Headers – The controls in this group are used to manage the production of SIP History-Info headers. History-Info headers are described in IETF RFC 4244 – Request History Information.

Enable History-Info Headers – Use this control to enable the production of History-Info headers. When enabled History-Info headers will be sent in all outgoing SIP call legs, and backwards to any incoming SIP call legs that have presented a Supported header containing the histinfo tag.

Include history Privacy Tag – This control is only available when Enable History-Info Headers is checked. Tick this control to place a Privacy header containing the history tag into any SIP request/response containing History-Info headers.

User-to-User Header – The controls in this group allow the content of the SIP User-to-User header to be set.

Content Tag – The text in this field will be appended to all User-to-User headers included in both incoming and outgoing SIP call legs, using a content tag. If this field is blank then no content tag will be appended to the header. User-to-User headers are described in IETF document draft-ietf-cuss-sip-uu-09.

Trunk Group Parameters – The controls in this group are used to add trunk group parameters to the Contact header in a SIP INVITE. Trunk group parameters are described in IETF RFC 4904 – Representing Trunk Groups in tel/sip URIs.

Enable Trunk Group Parameters – When checked, trunk group parameters will be added to all outgoing SIP calls.

Contact Name – This control is only available when Enable Trunk Group Parameters is checked. The contents of this field will be added as the user part of the sip URI in the contact header.

Trunk Context – This control is only available when Enable Trunk Group Parameters is checked. The contents of this field will be used as the trunk-context parameter in the Contact header.

NOTE

The tgrp parameter in the Contact header will be set to the index of the group on which the incoming call leg arrived.

Real Time Text – The controls in this group define how the SIP RTT stream will be negotiated by systems configured for TTY operation. These controls have no effect on systems configured for standard operation. Section 18 describes TTY operation in GroomerII.

Use RTT – Use this control to specify how media negotiations initiated by GroomerII will be carried out. There are two settings:

Always – Use this option if GroomerII should always request an RTT stream.

On Request – Use this option if GroomerII should not request an RTT stream until a TTY device has been detected on the TDM side.

Redundancy Level – Use this control to specify how many levels of T.140 redundancy will be applied to the RTT stream.

SS7 tab options

The controls on the SS7 page are used to configure settings that are specific to SS7 calls.

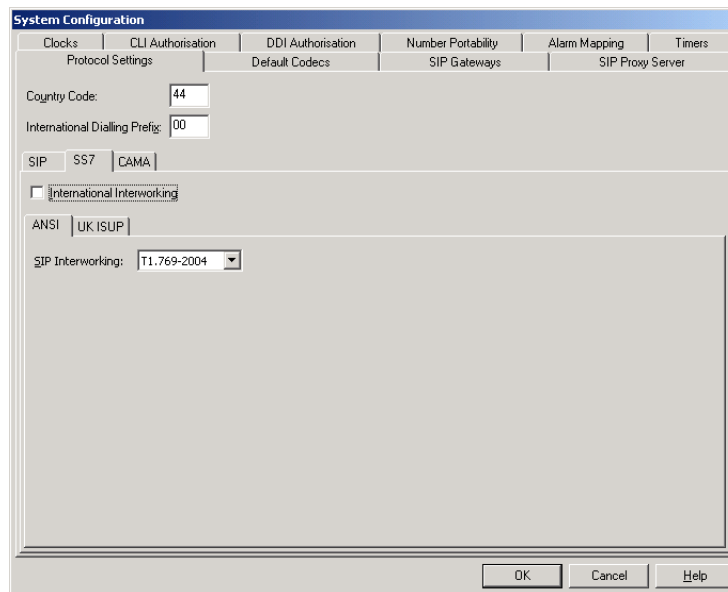


Figure 8-30 System configuration Protocol Settings - SS7, ANSI tab option

International Interworking – Check this control if GroomerII is connected to an SS7 switch using a different country code. This control is currently unused and should be left at its default setting.

ANSI tab options

The controls on the ANSI page (illustrated above) are used to configure settings that will be used by calls placed on ports running the ANSI SS7 variant.

SIP Interworking – Use this control to select the standards to be applied when interworking between ANSI SS7 and SIP. The available options are:

T1.769-2004 – Interworking will be carried out as described in American National Standard T1.769-2004.

NENA i3 – Interworking will be carried out as described in the (American) National Emergency Number Association stage 3 specifications. These specifications are based upon T1.769-2004, but have a number of alternative or additional mappings.

UK ISUP tab options

The screenshot shows the 'System Configuration' window with the 'Protocol Settings' tab selected. Under 'Protocol Settings', the 'SS7' sub-tab is active. The 'UK ISUP' section is expanded, showing the following fields:

- Country Code:** 44
- International Dialling Prefix:** 00
- ANSI / UK ISUP:** UK ISUP is selected.
- Partial CLI:**
 - Type of Switch: 7
 - PNO Identity: 134
 - Switch Number: 16
 - Partial CLI Octets: 30, 35, 35, 39, 32
- Priority Numbers:**
 - Table with 2 entries: 112, 999
 - Buttons: Add..., Edit..., Delete

Figure 8-31 System configuration Protocol Settings - SS7, UK ISUP tab option

The controls on the UK ISUP page are used to configure settings that will be used by calls placed on SS7 ports running the UK ISUP variant.

Partial CLI – These controls are used to configure the settings of the Partial Calling Line Identity (PCLI) parameter presented in an outgoing Initial Address message (IAM). The PCLI parameter will be included in the IAM if there is no Calling Party Number parameter. Your network operator will assign the values entered into the fields in this group.

Type of Switch – This value will be used in the Type of Switch field in the PCLI parameter, and should be a numeric value in the range 0-99.

PNO Identity – This value will be used in the PNO Identity field in the PCLI parameter, and should be a numeric value in the range 0-999.

Switch Number – This value will be used in the Switch Number field in the PCLI parameter, and should be a numeric value in the range 0-999.

Partial CLI Octets – These fields allow octets 5-9 in the PCLI parameter to be configured, one octet per field. The values are entered into the fields in hexadecimal format and should be in the range 00 to FF.

Priority Numbers – The controls in this group are for use when interworking from SIP to UK ISUP. If the incoming SIP call does not present a P-Asserted-Identity header containing a calling party's category, then the Priority Numbers table will be searched using the DDI presented by the SIP call. If the incoming DDI can be matched against one of the entries in the table then the Calling Party's Category parameter in the outgoing Initial Address message (IAM) will be set to 'calling subscriber with priority', otherwise the Calling Party's Category will be set to 'ordinary calling subscriber'.

NOTE

The Calling Party's Category determined by priority number matching can be overridden by the settings in the Routing Configuration screen. Section 8.5.3 refers.

Priority number list entries are added and modified using the Add/Edit UK ISUP Priority Number dialog. Use the Add... and Edit... buttons to access this dialog.

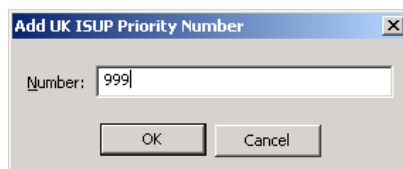


Figure 8-32 Add/Edit UK ISUP Priority Number dialog

The following wildcards are available to allow a range of priority numbers to be matched.

- ? – may appear anywhere within the number and will allow a single digit in the range 0-9 to be matched.
- % - may be used to terminate the number, and will allow zero or more trailing digits in the range 0-9 to be matched.

Entries are removed from the priority numbers list using the Delete button.

CAMA tab options

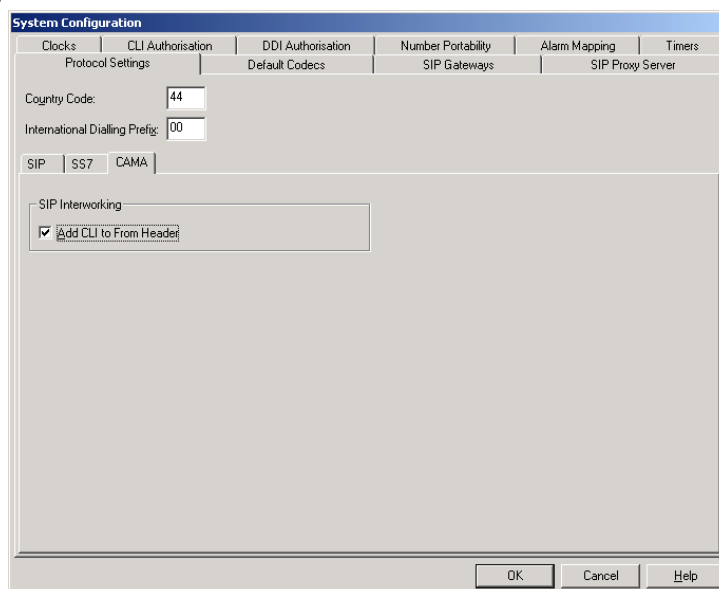


Figure 8-33 System configuration Protocol Settings - CAMA tab option

The controls on the CAMA page are used to configure settings that are specific to CAMA calls.

SIP Interworking – The controls in this group are used to specify how interworking between CAMA and SIP is carried out.

Add CLI to From Header – When interworking from CAMA to SIP, the default behaviour is to omit the calling party number from the SIP *From* header, and present it only in a *P-Charge-Info* header. Enabling this option will present the calling party number in both the *From* and *P-Charge-Info* headers.

8.6.8 Default codecs

The Default Codecs page allows the default codec list used by IP telephony calls to be configured. This list will be offered by all IP telephony call legs that do not have an explicit codec list configured in their route. Section 8.5.6 explains route configuration.

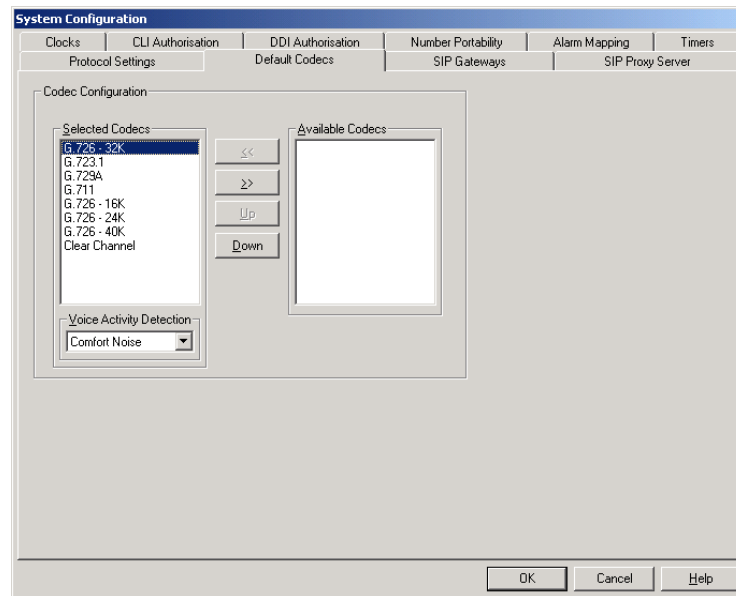


Figure 8-34 System configuration default codec tab option

The codecs to be offered should be placed in the Selected Codescs list in priority order. Use the buttons to manipulate the list:

- To add a codec, select the required codec from the Available Codescs list then click << to move the codec into the Selected Codescs list.
- To remove a codec, select the required codec from the Selected Codescs list then click >> to move the codec into the Available Codescs list.
- To change a codec priority, select the codec from the Selected Codescs list and then use the Up and Down buttons to change the priority order.

NOTE

The G.726 and Clear Channel codecs are not available when making or receiving secure SIP calls.

As the Selected Codescs list is traversed the VAD (voice activity detection) settings applied to the transmitted RTP stream for the selected codec may be configured in the control group below the list.

Voice Activity Detection – This control group is displayed when a G.711 or G.726 codec is selected. The options available are:

Disabled – No silence suppression will be applied. The received audio stream will be packetised and transmitted across RTP

DTX – Discontinuous transmission. The received audio stream will be analysed, and no packets will be sent across RTP when silence is detected.

Comfort Noise – This will offer a comfort noise codec (RFC 3551, payload 13) to the remote endpoint. If this is accepted any silence detected will be replaced by comfort noise packets in the RTP stream. If the remote endpoint does not accept the comfort noise codec then DTX will be used.

When using a G.711 or G.726 codec, if the remote endpoint offers a comfort noise codec this will be accepted by GroomerII regardless of the VAD settings, and any comfort noise packets received decoded into the audio stream.

Silence Compression – This control group is displayed when the G.723.1 codec is selected. The options available are:

Enabled – When selected Annex A silence compression will be applied to the transmitted RTP stream.

Disabled – When selected no Annex A frames will be transmitted in the RTP stream.

When using a G.723.1 codec, any Annex A frames received from the remote endpoint will be accepted and decoded regardless of the setting in this control.

Annex B – This control group is displayed when the G.729A codec is selected. The options available are:

Enabled – When selected the G.729AB codec will be offered to the remote endpoint. If this is accepted the voice activity detector may transmit both 'A' and 'B' frames on the RTP stream, otherwise only 'A' frames will be transmitted.

Disabled – When selected the voice activity detector will generate only 'A' frames on the RTP stream.

When using a G.729A codec, any 'B' frames received from the remote endpoint will be accepted and decoded regardless of the setting in this control.

8.6.9 SIP gateways

The SIP Gateways screen is used to manage the routing of outgoing SIP calls to gateways. You will need to configure the settings in this tab if you wish to direct any outgoing SIP calls to a gateway. The procedure for gateway routing is:

- A pool of the individual gateways to which GroomerII can direct outgoing SIP calls is created.
- Gateway routes are built, each containing one or more gateways from the pool. A gateway may only be used once within an individual route, but can be used in multiple routes.

Each gateway route contains one or more gateway groups that are placed in fallback order, with each group holding one or more gateways.

When GroomerII selects the gateway for an outgoing call the search begins at the first group in the gateway route, with the groups being searched in list order until an available gateway is found. Within a group the gateways are searched in round-robin fashion, with each group maintaining it's own round-robin pointer. This allows the benefits of fallback and round-robin gateway selection to be combined.

To implement a purely fallback strategy place each of your gateways into a group of its own. To implement a purely round-robin strategy, place all of your gateways into a single group.

- In the Groups Configuration screen configure your trunk group(s) to use gateway routing as described in section 8.4.2. Multiple trunk groups can use the same gateway route.

Use the controls on the Gateways, Routes and Retry/Recovery/Responses pages to configure gateway routing.

Gateways page

Use the controls on this page to create a pool of gateways to which outgoing SIP calls can be directed. Up to 100 gateways can be configured.

Address	Port	Capacity	Monitor	Disabled
45.15.16.1			Yes	
45.15.16.2			Yes	
45.15.16.3			Yes	
45.15.16.4			Yes	
47.15.16.1			Yes	
47.15.16.2			Yes	
47.15.16.3			Yes	
47.15.16.4			Yes	
192.168.16.70		100	Yes	
192.168.16.71		100	Yes	Yes
192.168.16.72		100	Yes	
192.168.17.70		200	Yes	
192.168.17.71		200	Yes	
192.168.17.72		200	Yes	
fdac:4a7:2db8:5994:5000			Yes	
fdac:4a7:2db8:5995:5000			Yes	
fdac:4a7:2db8:5996:5000			Yes	
fdac:4a7:2db8:5997:5000			Yes	

Address: 192.168.16.71

Port: 5060 Capacity: 100

☒ Enable Availability Monitoring

☒ Disable Selection Transport: UDP

Figure 8-35 SIP Gateways tab – Gateways page

The Gateways listbox is ordered by IP address, with IPv4 addresses being listed ahead of IPv6 addresses, and contains five columns:

Address – the IP address of the gateway.

Port – the IP port on the gateway to which SIP calls will be directed. For clarity, if the default port number of 5060 is to be used there will be no entry in this column.

Capacity – the call capacity of the gateway. For clarity, if the gateway has an unlimited capacity there will be no entry in this column.

Monitor – indicates whether GroomerII is monitoring the gateway for availability. For clarity, if the gateway is not being monitored there will be no entry in this column.

Disabled – indicates that the gateway is not currently eligible for selection when routing outgoing calls. For clarity, if the gateway is not disabled there will be no entry in this column.

Use the Add button to add a new gateway to the list. Entries are removed from the gateway list using the Delete button.

Address – the IP address of the gateway. All calls made to the gateway will be directed to this address.

Port – the IP port on the gateway to which calls will be directed. The default port number is 5060.

Capacity – the call capacity of the gateway. Leave this field blank to allow unlimited calls to be made to the gateway. When a call capacity has been applied, GroomerII will only make outgoing calls to a gateway when the total number of calls in progress to that gateway (incoming and outgoing) is less than its capacity. Call capacity is not checked when receiving incoming calls from the gateway - these will always be accepted.

Disable Selection – tick this box to prevent GroomerII routing new calls to the gateway. This control can be used to stop calls being routed to a gateway that is temporarily unavailable, for example when the gateway is undergoing maintenance. Calls already in progress to and from the gateway will not be affected. Ticking this box will stop all gateway routes from directing calls to the gateway.

Enable Availability Monitoring – tick this box if you want GroomerII to monitor the availability of the gateway to accept calls. When availability monitoring has been enabled, GroomerII will send a SIP `OPTIONS` method to the gateway at one minute intervals. If the gateway replies with a `2xx` response then GroomerII will continue to direct outgoing calls to the gateway. If the gateway replies with any other response, with the exception of `1xx` which is ignored, then no further calls will be directed to the gateway until a subsequent `OPTIONS` method has received a `2xx` response.

Transport – Use this control to specify whether the UDP or TCP transport protocol should be used when sending a SIP `OPTIONS` method to the selected gateway. This control will only be enabled when Enable Availability Monitoring is checked.

NOTE

The Transport control applies to the SIP `OPTIONS` method only, and does not influence the transport that will be used for SIP call control signalling. See section 8.5.6 for information on configuring the IP transport to be used by SIP call control signalling.

Routes page

Use the controls on this page to create the gateway routes that will be used to select the destination IP address for each call. Up to 40 gateway routes can be created.

Figure 8-36 SIP Gateways tab – Routes page

The Gateway Routes listbox is ordered alphabetically by route name. Use the Add button to add a new route to the list. Entries are removed from the route list using the Delete button.

Route Name – This field allows a descriptive name to be assigned to the route. This name is not used outside the Configuration Editor.

Groups – Use the controls in this group to add gateway groups to the currently selected gateway route.

The Groups listbox displays the gateway route names and is maintained in fallback order. Use the Add button to add a new group to the end of the list, and the Up and Down buttons to re-order the list. The Delete button will remove the selected group from the list.

Group Name – This field allows a descriptive name to be assigned to the group. This name is not used outside the Configuration Editor.

Gateways – Use the controls in this group to add gateways into the currently selected group. A group can contain both IPv4 and/or IPv6 gateways.

Selected – This listbox displays the gateways that have been added to the currently selected gateway group.

Disable Selection – tick this box to prevent the currently selected gateway route from directing calls to the selected gateway. Calls already in progress to and from the gateway will not be affected. This control is intended for use during setup and fault finding. Use the Disable Selection control in the Gateway page if you wish to prevent all routes from directing calls to a gateway.

Available – This listbox displays those gateways in the gateway pool that are not currently in use by any gateway group in the selected gateway route.

Use the << and >> buttons to move gateways between the Available and Selected lists.

Retry/Recover/Responses page

Use the controls on this page to specify what action should be taken when an outgoing call to a gateway fails. The settings are applied globally to all outgoing SIP gateway calls.

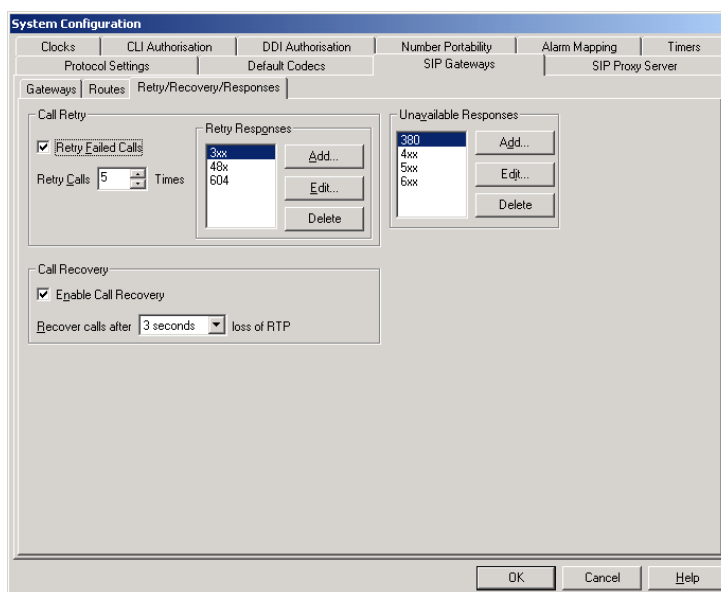


Figure 8-37 SIP Call Gateways tab – Retry/Recovery/Responses page

Call Retry – The controls in this group are used to specify any action that should be taken when an outgoing call to a gateway cannot be connected.

Retry Failed Calls – If this control is checked, any outgoing calls rejected with a response code from the Retry Responses list will be retried using the next available gateway.

Retry Calls X Times – This control is only available when Retry Failed Calls is enabled, and is used to specify the maximum number of times a call may be retried before being rejected back to the caller. If a call cannot be connected after the specified number of retries, then it will be rejected using the last response code returned. If the list of available gateways is exhausted before the maximum number of retries then the call will be rejected with routing failed.

Retry Responses – The controls in this group are only available when Retry Failed Calls is enabled. If a call to a gateway is rejected with one of the response codes in the list then the call will be retried.

Response codes are added and modified using the Add/Edit SIP Response dialog. Use the Add... and Edit... buttons to access this dialog.

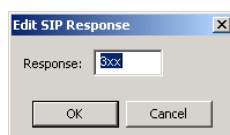


Figure 8-38 Add/Edit SIP Response dialog

The Add/Edit SIP Response dialog has one control:

Response – Enter a SIP response code. Wildcards may be used, and the following are examples of how response codes can be defined:

604 – The specific response code 604,

48x – Any response code between 480 and 489,

3xx – Any response code between 300 and 399.

Entries are removed from the response list using the Delete button.

Call Recovery – The controls in this group are used to configure SIP call recovery. Refer to section 14.3 for an explanation of SIP call recovery.

Recover calls after X loss of RTP – This control is only available when Enable Call Recovery is checked, and is used to select the time that must elapse without receiving an RTP packet from the remote end before call recovery is invoked.

Unavailable Responses – If a call to a gateway returns one of the responses in this list, and the gateway has availability monitoring enabled, then that gateway will be marked as unavailable until such time as it has returned a 2xx response in reply to a SIP OPTIONS method. Use the Add/Edit SIP Response dialog as described above to add, modify and remove list entries.

8.6.10 SIP proxy server

GroomerII can forward outgoing SIP calls to a proxy server for onward routing, and maintain alias registrations with the proxy server. If you wish to route any of your outgoing calls to a SIP proxy server you must configure the settings on this page.

System Configuration

Clocks | CLI Authorisation | DDI Authorisation | Number Portability | Alarm Mapping | Timers

Protocol Settings | Default Codecs | SIP Gateways | **SIP Proxy Server**

☒ Enable SIP Proxy Server Routing

Address : 192.168.1.106

Port : 5060

Transport : UDP

Registration

Alias	Contact
6000@192.168.1.106	6000@192.168.1.11
6001@192.168.1.106	6001@192.168.1.11
6002@192.168.1.106	6002@192.168.1.11
6003@192.168.1.106	6003@192.168.1.11
6004@192.168.1.106	6004@192.168.1.11
6005@192.168.1.106	6005@192.168.1.11

Add... Edit... Delete

OK Cancel Help

Figure 8-39 SIP Proxy Server tab

When directing a call to a SIP proxy server, GroomerII uses the address format:

sip:1234567890@192.168.1.106

1234567890 being the equivalent PSTN DDI number and 192.168.1.106 the proxy server IP address. Subject to how the proxy server is configured, it will either respond with a redirect message to another proxy server or endpoint, or it will pass on your request to another proxy or endpoint. This process will continue until the two call endpoints are identified at which time the call can proceed.

Enable SIP Proxy Server Routing – tick this box if you want to route outgoing calls via a SIP proxy server. Other controls on this page will only be enabled when this box is ticked.

Address – the IP address of the SIP Proxy Server you wish to use. This can be either an IPv4 or IPv6 address.

Port – the IP port that your SIP Proxy Server is using. The default is port 5060.

Transport – the data format to be used to communicate with your SIP Proxy Server. The options available are:

UDP – user datagram protocol format. Connectionless feature of the IP protocol, the exchange of datagrams without acknowledgements or guaranteed delivery.

TCP – transmission control protocol format. End to end IP protocol, the exchange of sequential data between host processes.

Registration – This control group allows a list of contact addresses to be registered with a Proxy Server.

GroomerII maintains these registrations from the point at which the configuration file is loaded into the Kernel, until they are no longer required, for example, until another configuration is loaded or the GroomerII Kernel is closed down.

Registration list entries are added and modified using the Add/Edit SIP Alias dialog. Use the Add... and Edit... buttons to access this dialog.

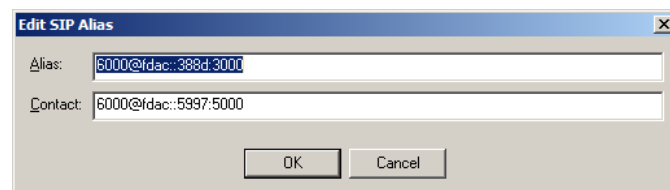


Figure 8-40 Add/Edit SIP alias dialog

The full Alias and Contact must be added in the form `Alias@IPaddress` and `Contact@IPaddress`.


NOTE

To maintain flexibility, IP addresses are not automatically appended.

Entries are removed from the registration list using the Delete button.

8.7 Cause mapping configuration

By default GroomerII automatically maps the call clearing cause presented by the outgoing protocol to the equivalent one for the incoming protocol. Cause mapping allows an alternative mapping to be defined. This is generally not required unless a device such as a PBX acts on a special release code.

In the GroomerII Configuration Editor main window select  from the toolbar, or Configuration - Cause Mapping... from the menu, to open the Cause Mapping Configuration dialog.

NOTE

All Cause Map Sets defined here will be added to the Cause Map pull down options list of the Routing Configuration - General dialog. Section 8.5.7 refers.

Cause maps are added using the Cause Map Sets control group. Each cause map contains one or more individual mapping translations. Any codes that are not defined in the mapping are passed through using standard mapping.

- To add a new cause map, click the Add button in the Cause Map Sets group. The new cause map will be added to the bottom of the Cause Map Sets list. The cause map will be assigned a default name, which can be changed using the Name field.
- To update an existing cause map, select the map to be updated in the Cause Map Sets list and make the required changes.
- To remove a cause map from the list, select the map to be removed and click Delete.

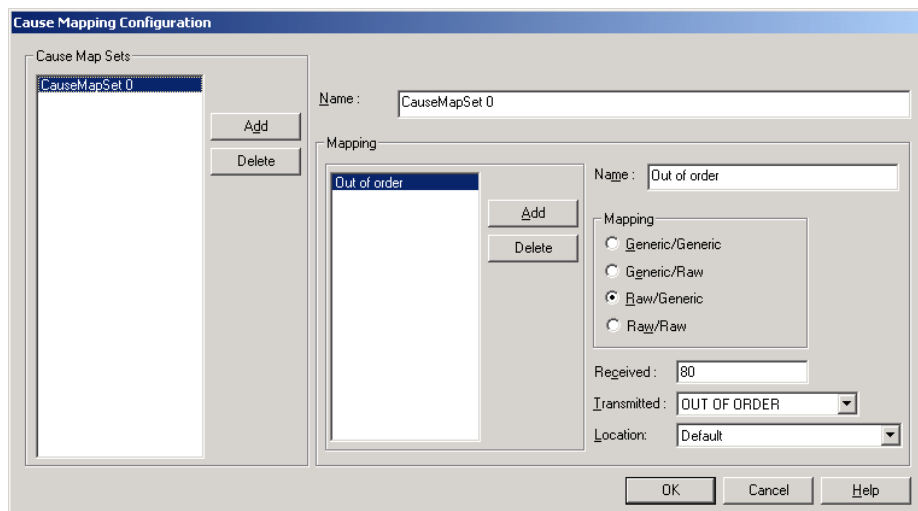


Figure 8-41 Cause mapping configuration

Mapping – Individual mappings are added to the selected cause map using the controls in this group:

Add – Use this button to add a new individual mapping. The new entry will be assigned a default name and added to the bottom of the Mapping list.

Delete – Use this button to remove the selected entry from the Mapping list.

Name – Use this field to modify the default name assigned to the mapping.

Mapping – Translations are in the order of received to transmitted and can be either:

Generic to Generic – the generic cause received from the outgoing call leg will be mapped and passed to the incoming leg using a generic cause.

Generic to Raw – the generic cause received from the outgoing call leg will be mapped and passed to the incoming leg using a raw cause.

Raw to Generic – the raw cause received from the outgoing call leg will be mapped and passed to the incoming leg using a generic cause.

Raw to Raw – the raw cause received from the outgoing call leg will be mapped and passed to the incoming leg using a raw cause.

Received – This is the clearing cause presented by the outgoing call leg.

Transmitted – This is the clearing cause passed to the incoming call leg.

Location – This field is only used when the incoming call leg is using the SS7 protocol, and will be used to set the location field in the release message sent to the incoming call.

Once you are satisfied with the mapping of all the cause translations for your mapping set, either repeat the process to create new mapping sets, select Cancel to ignore any updates or OK to accept any updates and close the dialog.

Cause values

The Received and Transmitted controls will change to reflect the mapping type selected.

When mapping to or from a Raw cause, the decimal value for the release code defined by the protocol being used should be entered into the field. For example, if the protocol is EuroISDN then 17 might be entered to represent User Busy.

When mapping to or from a Generic cause, a drop down list of generic causes will be presented. This can be used to select a cause without needing to know the exact value for that protocol. For example, selecting NUMBER BUSY will set the correct busy release code for the protocol in use.

8.8 Tone generation configuration

This group of controls allows a user to define their own tone sets, and the functionality is provided primarily to ensure backward compatibility with earlier versions of GroomerII application software.

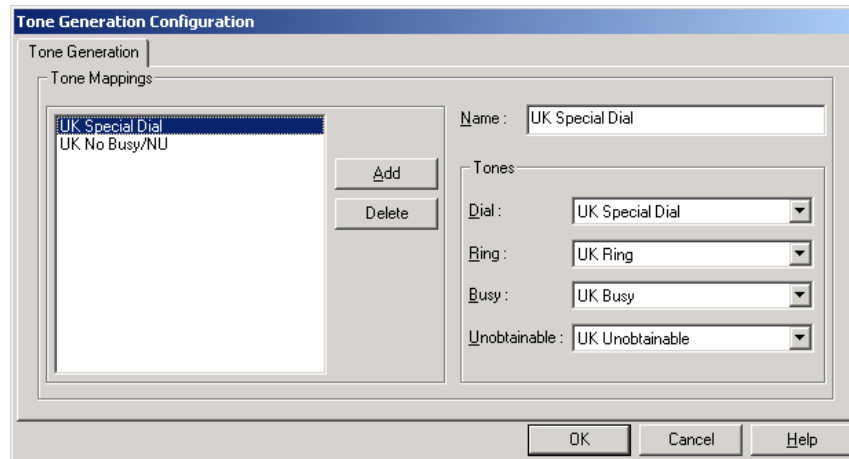


Figure 8-42 Tone generation configuration

NOTE

Tones are encoded in either μ -law or A-law. It is not currently possible to generate both types within one system.

Tone Mappings – Use the controls in this group to add new tone mappings. Four pre-defined tone sets are available

- UK tones,
- EC tones,
- US tones,
- New Zealand tones.

The tone mapping list contains only user defined tone sets, the pre-defined tone sets are not listed and cannot be modified.

To create a new tone mapping click the Add button. The new entry will be assigned a default name and added to the bottom of the Tone Mappings list.

The Delete button can be used to remove entries that are no longer required.

Name – A user name used only within the configuration for the generation settings defined.

Tones – This group of controls allows the individual tones that make up the tone mapping to be selected. If no tone is required for a particular operation select <None>.

Dial – Select the tone that will be played until the first digit is dialled.

Ring – Select the tone that will be played when the destination is ringing.

Busy – Select the tone that will be played if the destination number is engaged.


Unobtainable – Select the tone that will be played if the destination is unreachable.

NOTE

It is recommended that ringback cadence is not included in the tone list as some networks play recorded announcements with an Alerting (ringing) message. The ringback tone provided by GroomerII will overwrite the in-band announcement.

8.9 Advanced configuration options

The Advance Options dialog contains several configuration parameters, which are used to either enable or disable specific functions. The functions are useful in certain specific circumstances or modes of operation.

From the GroomerII Configuration Editor, select  or Advance Options from the Configuration menu to open the Cause Mapping Configuration dialog.

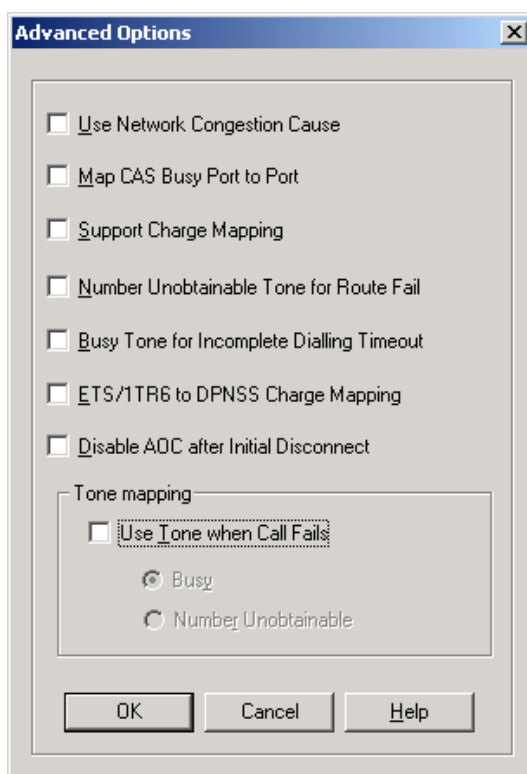


Figure 8-43 Advanced options

These parameters should only be selected when the operator completely understands what is required, and the effect the parameter will have.

Use Network Congestion Cause – When GroomerII cannot route a call, the call is released with a user busy cause. When this option is selected, the release cause is changed to Network Congestion.

Map CAS Busy Port to Port – This option is used when converting between 2 different forms of CAS, for example, a CAS busy (*abcd=1111*) is mapped to the same timeslot on the other side. Please contact Groomer support for advice before using this function.

Support Charge Mapping – This option allows charging information to pass through the GroomerII, however this is restricted to a limited number of protocols. Please contact Groomer support for further information.

Number Unobtainable Tone for Route Fail – Generates number unobtainable tone instead of busy tone when a route failure occurs.

Busy Tone for Incomplete Dialling Timeout – Generates `BUSY` tone instead of `NU` tone when timeout occurs.

ETS/1TR6 to DPNSS Charge Mapping – This option enables the conversion of German meter pulses to meter pulses used on DPNSS.

Disable AOC after Initial Disconnect – This option is used to ensure that AOC pulses/messages are stopped as soon as either of the parties clears down. If this is left unchecked, AOC pulses/messages will only stop when the calling party disconnects.

NOTE


There is usually a delay between a called party clearing and a disconnect message being received, this is due to most called party switches having a delay to allow for called party reconnect, (moving to another phone on the same analogue connection).

Tone Mapping – When converting between CAS and ISDN you often get release causes in the ISDN signalling that cannot be mapped to an appropriate tone, this option causes any call reject except Number Unobtainable and User Busy to generate a selected tone.

Check the `Use Tone when Call Fails` selection box, and then select the appropriate radio button to implement the required tone mapping.

To use tone mapping, tone generation has to be set-up for the route.

8.10 Comments

From the GroomerII Configuration Editor toolbar select , or Comment... from the Tools menu, to open the Comments dialog.

This feature can be used to store notes relating to a configuration file.

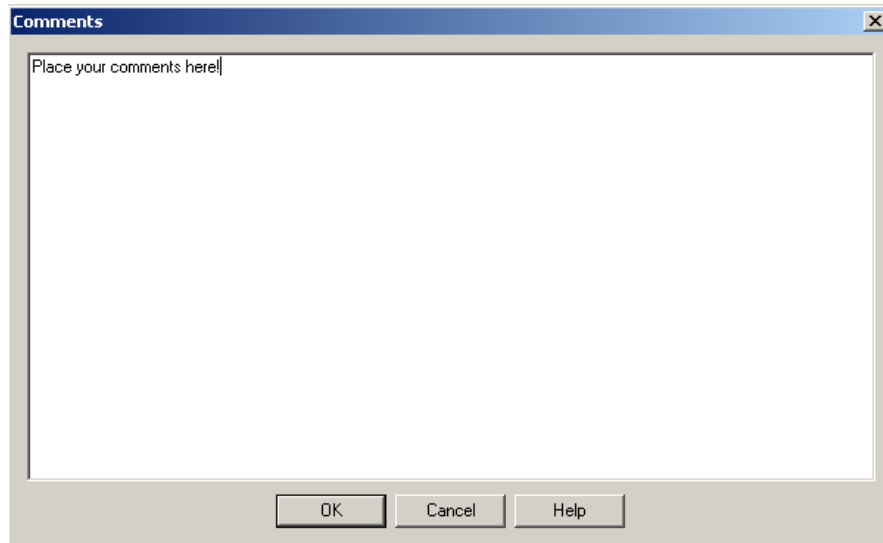


Figure 8-44 Comments

Type the required comment into the dialog area and select OK. All comments are then added to the beginning of the configuration file.

8.11 Options

Select Tools – Options... to open the Options dialog. When you add or insert a port, group or route, the behaviour is subject to the selection made here. When set to Use Current Settings, a new entry will contain a system generated name and a copy of the parameters for the entry selected prior to selecting Add or Insert. When it is set to Use Default Values, the new entry will contain a system generated name and default values.

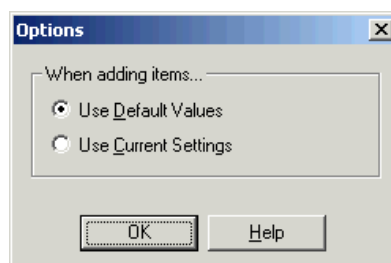




Figure 8-45 Settings option dialog

The following shortcut buttons have been added to the GroomerII Configuration Editor dialog toolbar:

-  use default values
-  use current settings

8.12 Activation key

If you have already entered the activation key for your system, you can change it using the Tools -Change Activation Key... menu option.

CAUTION

This option should only be used on standalone PCs. It is not appropriate on the GroomerII chassis itself as changing the key may prevent the Kernel from working. This option will be disabled (greyed out) if a GroomerII Kernel is detected on the same system.

Selecting the tools menu option to change the activation key, will present the following dialog.

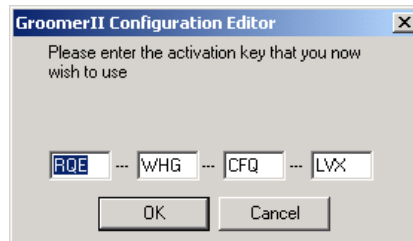


Figure 8-46 Activation key dialog

Enter a valid activation key for the software version being used, for example, RQE-WHG-CFQ-LVX as shown here. You will continue to be prompted until a valid activation key is entered. See section 19.2.2 for guidance on identifying valid activation keys.

NOTE

If you are using a support system with multiple versions of the configuration tools, a valid activation key is required for each.

9 Address map editor

Address mapping can be used to map a PSTN DDI number to an IP network destination address when making an outgoing SIP call. The address map editor is used to create a file of DDI to IP address mappings that is loaded into the GroomerII Kernel when address mapping is in operation.

From the Microsoft Windows Start menu select All Programs – Aculab GroomerII – Address Map Editor to open the GroomerII Address Map Editor dialog.

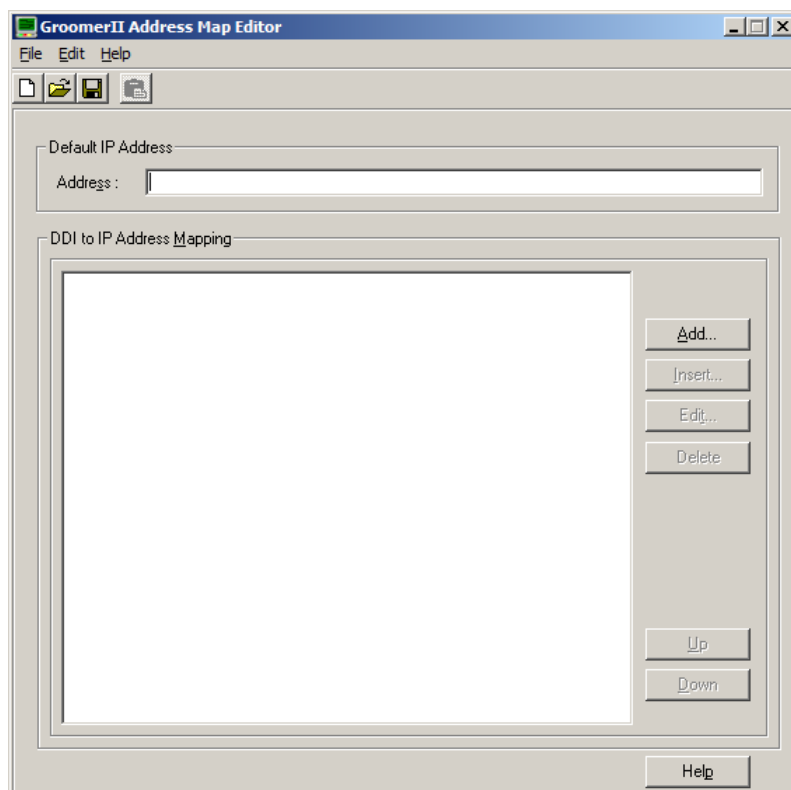






Figure 9-1 GroomerII address map editor dialog

Menu options

File	- New	Ctrl+N	
	- Open...	Ctrl+O	

	- Save	Ctrl+S	
	- Save As...	Ctrl+A	
	- Import...		
	- Exit		
Edit	- Paste	Ctrl+V	
Help	- Contents		
	- Search...		
	- Index...		
	- About GroomerII Address Map Editor		

Dialog Fields

Default IP Address – this is the IP address to which any numbers that are not listed in the DDI to IP Address Mapping list will be directed. This may be an IPv4 or IPv6 address.

DDI to IP Address Mapping – this is the list (look up table) of PSTN DDI numbers and their corresponding destination IP network addresses. Both IPv4 and/or IPv6 addresses can be used.

9.1 Creating an address map

Using the standard dialog selection options, you can create an address map from new or by opening an existing file, editing it and saving it as a new file or to replace an existing file.

9.2 Using wildcards

An address map entry is made up of two parts, the DDI and the IP address, and wildcards may be used in the DDI part. The following wildcards are available:

- ? - Will match a single digit, which must be present.
- % - Will match the remaining 0 or more digits in the DDI. Anything appearing after % will be ignored.

Care should be taken that the correct form of wildcard is used to meet your objective. For example the wildcard string 123??? will match 123456 but will not match 1234567, whilst the string 123% will match both 123456 and 1234567.

9.3 Adding and inserting address map entries

There are three ways that you can add entries to the list:

1. Use the Add... and Insert... buttons – add a single entry at a time
2. Copy and paste from a text file – one or more entries
3. Import from a CSV file – one or more entries

Using the Add and Insert buttons

Select Add... to open the Add Record dialog and add a new entry to the end of the list. Select Insert... to open the Insert Record dialog and add a new entry immediately before the currently selected entry.

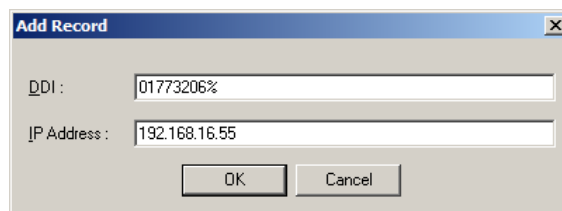


Figure 9-2 GroomerII address map editor add record dialog

The Add Record and Insert Record dialogs have identical controls and functionality. Enter the required DDI and IP Address numbers followed by OK to validate and save the entry or Cancel to discard the entry.

Repeat this process for additional numbers.

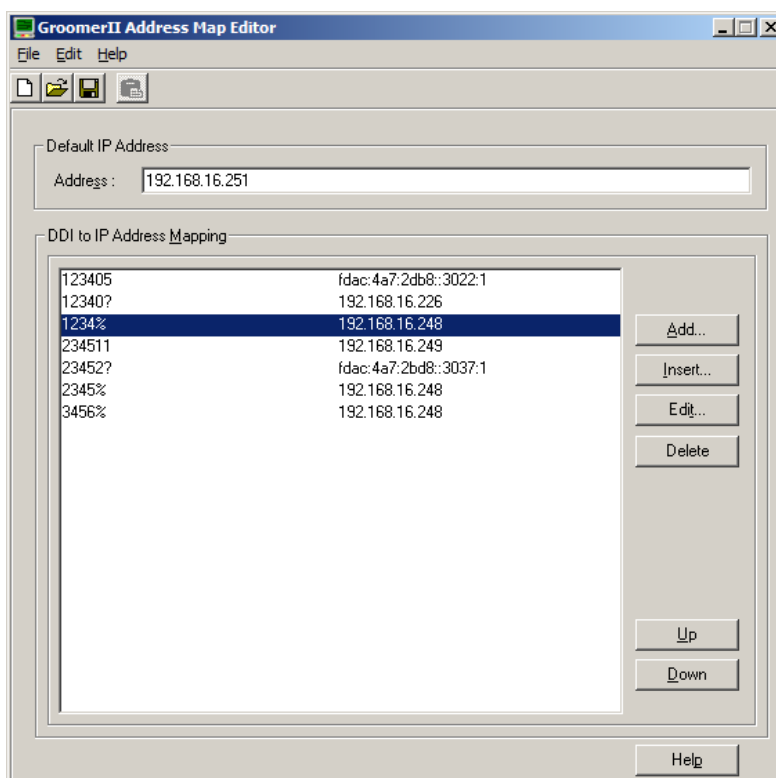


Figure 9-3 Updated GroomerII address map editor dialog

Copy and paste from a text file

You can copy entries from an ASCII text file providing the format of the text is a comma separated list, for example:

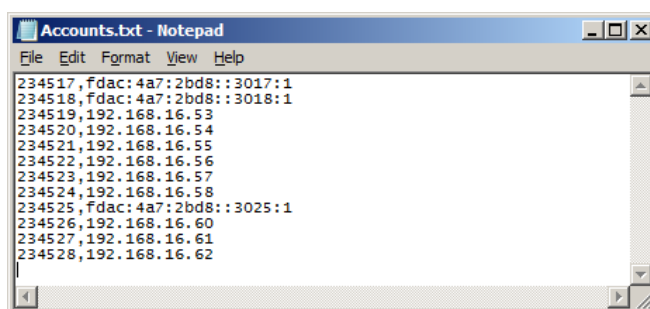


Figure 9-4 GroomerII address map editor paste entries

Highlight the required entries in the ASCII text file followed by Edit – Copy (Ctrl+C). Select the GroomerII Address Map Editor dialog followed by Edit – Paste (Ctrl+V). The data will now be checked, and if free from errors the selected entries will be added to the end of the list. If the data is not valid you will receive a prompt similar to the following:

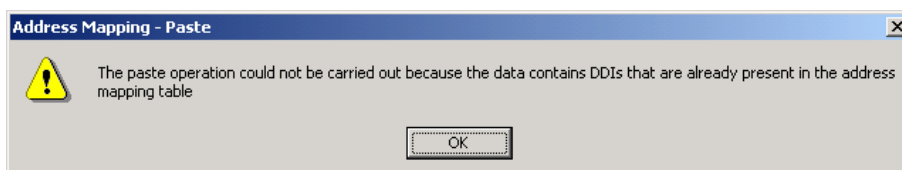


Figure 9-5 Paste duplicate DDI prompt

Import from a CSV file

A CSV file is a comma separated ASCII text file and is usually created as an export from a database, or spreadsheet application such as Microsoft Excel.

To import the data from a CSV file, select File – Import... to open the Open file dialog.

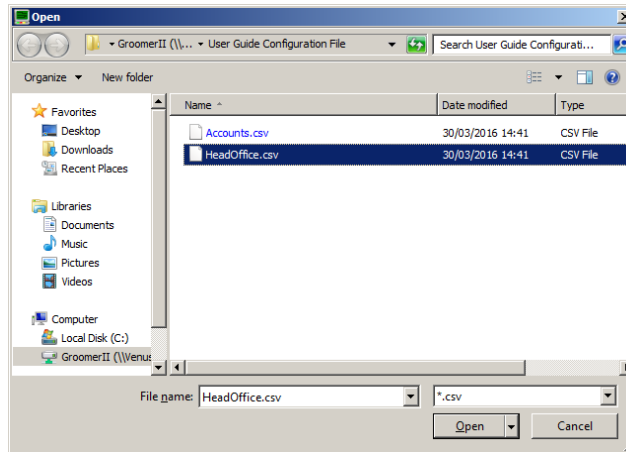


Figure 9-6 GroomerII address map editor import entries

Select the required CSV file followed by Open. The entries from the selected file will now be checked, and if free from errors will be added to the end of the list. If the data is not valid you will receive a prompt similar to the following:

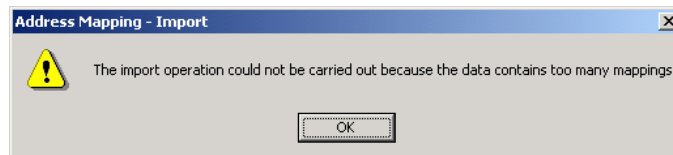


Figure 9-7 Import duplicate DDI prompt

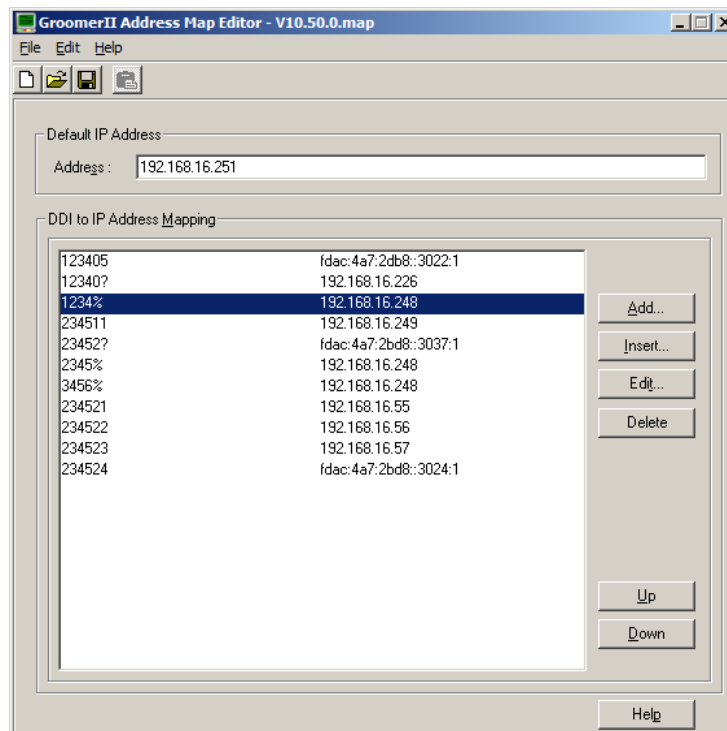


Figure 9-8 Updated GroomerII address map editor dialog

9.4 Editing an entry

Select an entry from the DDI to IP Address Mapping list followed by Edit... to open the Edit Record dialog for that entry.

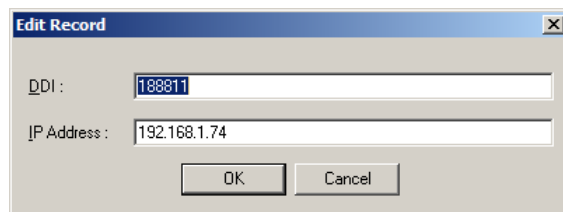


Figure 9-9 GroomerII address map editor edit record dialog

Make the required changes and close the dialog box using OK to save your changes or Cancel to discard your changes.

9.5 Deleting an entry

Select an entry from the DDI to IP Address Mapping list followed by Delete to remove an entry from the list.

9.6 Maintaining list order

The order that the mappings appear in the DDI to IP Address Mapping list is the order in which a call will search the list to find a matching DDI. The list must be maintained in the correct order to avoid calls arriving at an incorrect destination. This is particularly important when wildcard matching is being used. In the following example a call to 01771234 would be directed to 192.168.16.20, not 192.168.16.35 as expected because the DDI will be matched against the wildcard entry 017712% before reaching the explicit entry.

017712%	192.168.16.20
01771234	192.168.16.35
0177123?	192.168.16.37

Re-arranging the list into the following order will ensure that the correct destination address is selected at all times.

01771234	192.168.16.35
0177123?	192.168.16.37
017712%	192.168.16.20

Select an entry and use the Up and Down buttons to move the entry to a different position in the list.

10 Advice of charge

Advice of charge (AOC) is used to define values that can be used when generating CAS meter pulses or advice of charge messages. For example, an R2 CAS protocol would use meter pulses, and an ETS 300 protocol would use AOC messages. For further clarification, please contact Aculab support.

NOTE

Advice of charge is not supported by SIP.

NOTE

Only advice of charge messaging back to the calling party is possible, forward advice of charge messaging to the called party, for example, for reverse charging, is not a feature of GroomerII.

To configure advice of charge, select All Programs – Aculab GroomerII – AOC Configuration Editor from the Start menu. This will open the GroomerII Advice of Charge Configuration Editor.

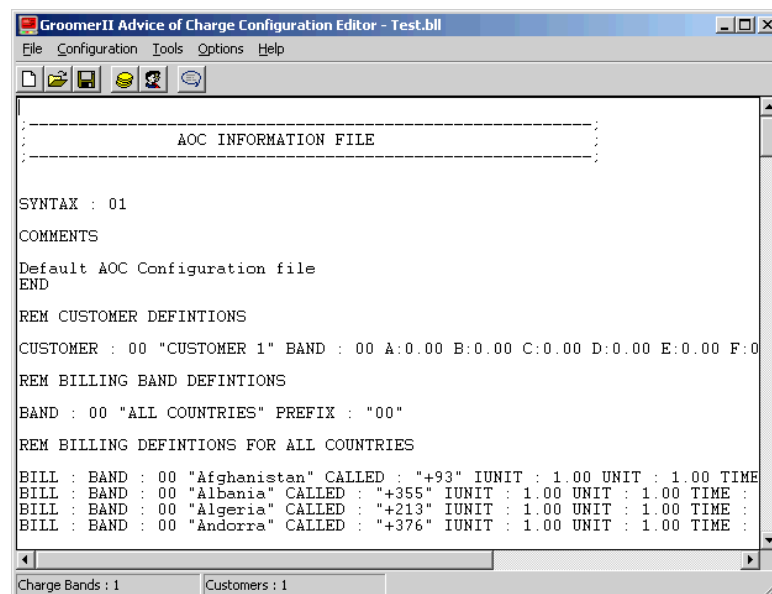








Figure 10-1 GroomerII advice of charge configuration editor

Menu options

File	- New	
	Open	
	Save	
	Save As...	
	Exit	
Configuration- Charge bands...		
	Customers...	
Tools	- Comments...	
	- Change Activation Key...	
Options	- Port Definitions	
		- Load...
		Reset
Help	- Contents	
	Search...	
	Index	
	About GroomerII AOC Configuration Editor	

The configuration editor allows you to define charge bands to individual ports or groups of ports (customers). A configuration is saved in an ASCII text file of the format *.b11

NOTE

Once you have created your *.b11 file, the grshed.dat file will need to be edited to include the configuration. This is covered in more detail at the end of this chapter.


When you first open the Configuration Editor you have the option to create a New file and Save As... a *.b11, or Open and Save an existing *.b11 file. Included with the Configuration Editor is a default configuration file (Test.b11) that includes charges for the most commonly used international dialling codes. This configuration file is used as the example in the following description on Advice of Charge.

To load the example configuration, select File – Open to open a standard Microsoft Windows selection dialog, and then select the Test.b11 file followed by Open. The Test.b11 file configuration will now be loaded and appear in the Configuration Editor dialog.

10.1 Charge bands

Before you can apply an advice of charge to a port or group of ports, you must first set up one or more charge bands.

A charge band is a set of charging information that can be applied to one or more ports in the system. Each charge band can contain individual charging parameters for one or more destinations. This allows different tariffs to be applied to each customer.

Select  or Configuration – Charge Bands... to open the Charge Band Configuration dialog.

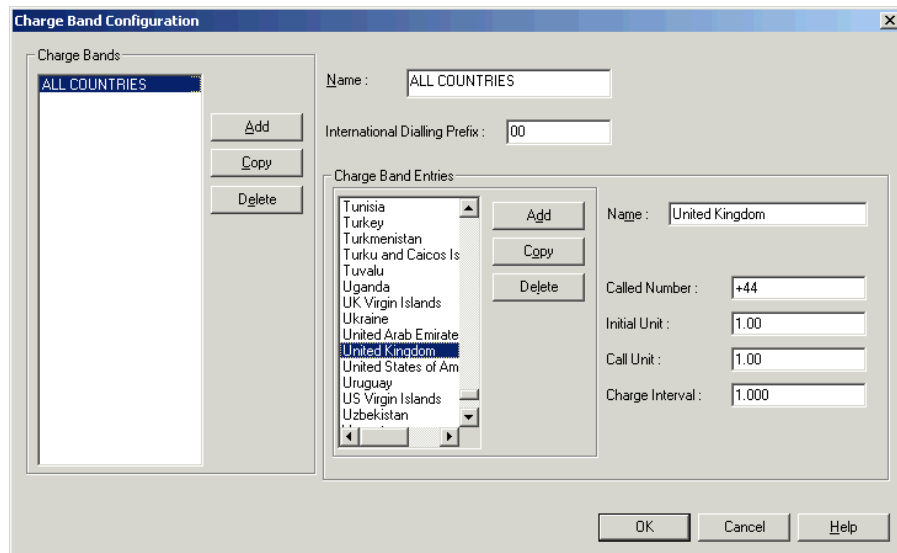


Figure 10-2 Charge band configuration dialog

For a new configuration, all the fields by default would be blank or disabled. This example shows the configuration that exists for the previously loaded `Test.bll` file. You now have the option to Add a new charge band, make a Copy of a selected charge band or Delete a selected charge band.

10.1.1 Adding and removing charge bands

Charge Bands – Use the controls in this group to add and remove charge bands:

Add – creates a new system generated name in the Charge Bands list with blank Charge Band Entries.

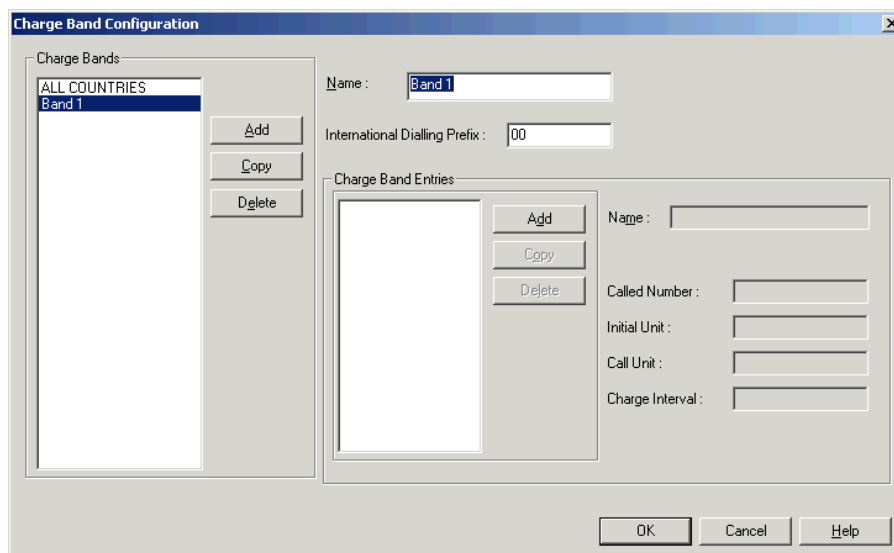


Figure 10-3 Charge band configuration dialog – add bands

Copy – creates a new system generated name in the Charge Bands list with a copy of the currently selected charge band and charge band entries.

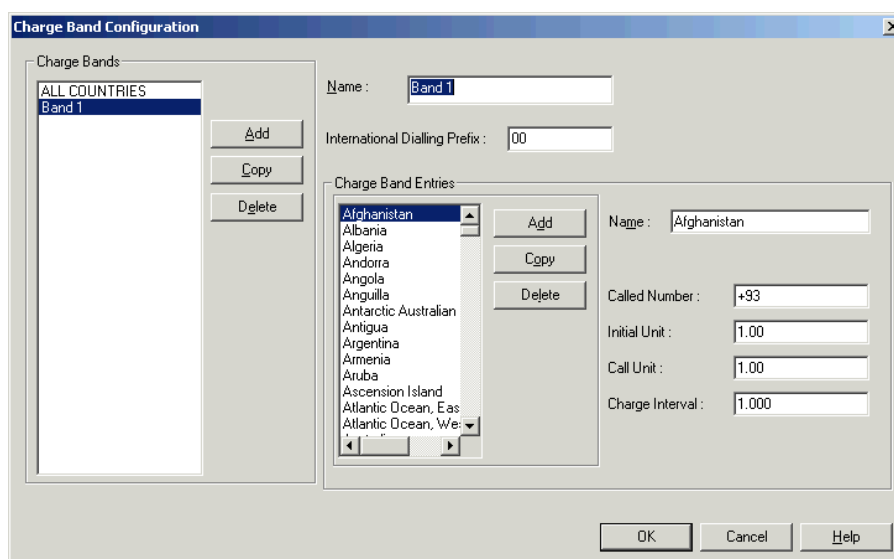


Figure 10-4 Charge band configuration dialog – copy bands

Delete – deletes the selected charge band from the Charge Bands list. To delete a charge band, you must first ensure that it is not allocated to a customer in the Customer Configuration dialog. You will be presented with a warning dialog should you try to delete a charge band that is still associated with port or group of ports (customers).

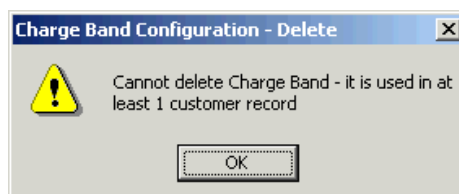


Figure 10-5 Charge band configuration – delete warning dialog

Name – is not system dependent and may be any unique alpha/numerical identity you choose to assign as the identifier of a charge band.

International Dialling Prefix – can be left blank or can contain a number of digits that are to prefix a called number. This field will be ignored unless a + has been entered as the first digit in the Called Number field.

10.1.2 Charge band entries

Use the controls in the Charge Band Entries group to add charging parameters for individual destinations to the charge band.

Add – creates a new entry to the Charge Band Entries list. The entry will contain system default entries for the associated fields.

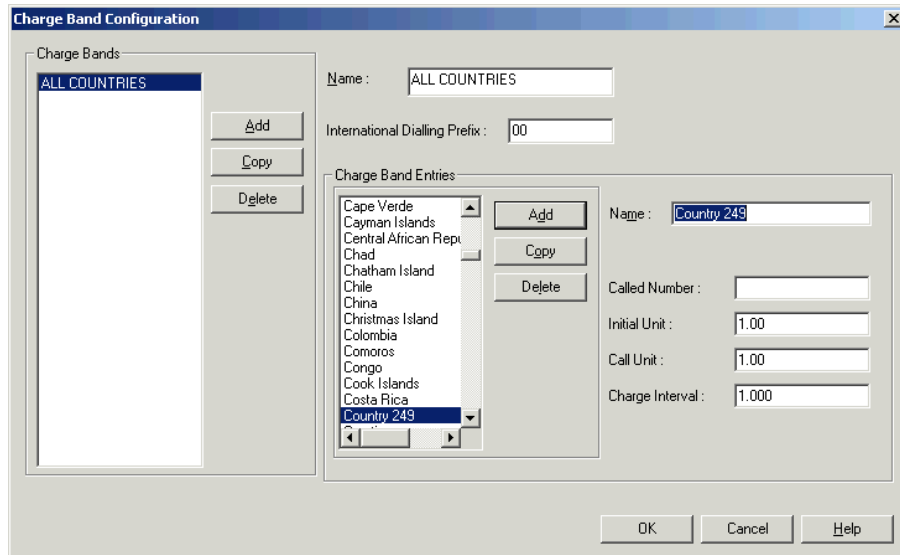


Figure 10-6 Charge band configuration dialog – add band entries

Copy – creates a new entry to the Charge Band Entries list. This entry will contain a copy of the currently selected charge band entry in the associated fields.

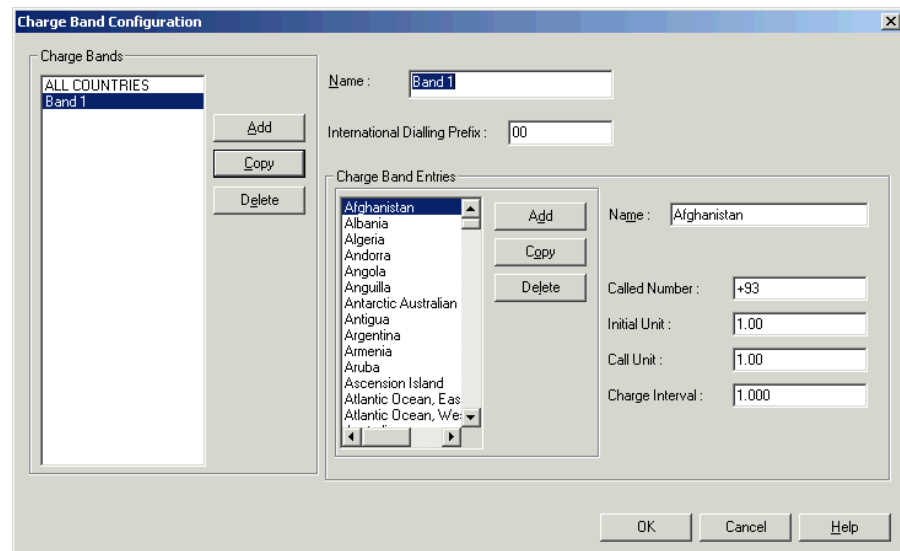


Figure 10-7 Charge band configuration dialog – copy band entries

Delete – deletes a selected charge band entry from the Charge Band Entries list.

Name – is not system dependent and may be any unique alpha/numerical identity you choose to assign as the identifier of a charge band entry.

Called Number – this field contains a prefix that precedes a called number; in our example the called number is the country code. If the field also contains a + as the first digit, then any digits entered in the International Dialling Prefix must precede the digits entered in the Called Number field. For example, an International Dialling Prefix of 00 and a Called Number of +93, will result in the advice of charge parameters being applied to any called number starting with 0093.

10.1.3 Advice of charge parameters

There are three advice of charge parameters:

Initial Unit – the first advice of charge indicator. The system default is one unit.

Call Unit – subsequent advice of charge indicators. The system default is one unit.

Charge Interval – the period in milliseconds (expressed in seconds) between advice of charge indicators. The system default is one second.

How these three values are used is subject to the signalling protocols being used, for example:

For CAS protocols such as R2, if a unit field is zero then the associated pulse will not be generated. In the case of Initial Unit or Charge Interval being zero, then there is no advice of charge as no meter pulses or messages will be sent. When the fields contain non-zero values, then a single pulse will be generated irrespective of the actual non-zero value.

For Non-CAS, such as ETS300 or DASS, the values in the fields may be used in association with advice of charge messages. For example, DASS advice of charge messages periodically report the accumulative values of the initial unit and call units for a call in progress. Therefore if the initial unit is 1, the call unit is 3 and the charge interval is 1, then a value of 1 would be sent on call connect. One second later 4 will be sent, and then another second later 7 will be sent and so on until call disconnect.

For further advice on the use of Advice of Charge messaging, please contact Aculab support.

NOTE

How advice of charge values are used for call charging is subject to the calling party exchange and is not a function of the GroomerII.

Once you have completed the set up of all required charge bands, select OK to accept any charges, or Cancel to ignore any changes, and return to the GroomerII Advice of Charge Configuration Editor dialog.


CAUTION

The ordering of the charge records within the AOC file is important to the correct operation of GroomerII. The AOC Editor will maintain the correct ordering automatically. You should not therefore modify the AOC configuration (*.blf) file outside the AOC Editor. Doing so may cause GroomerII to generate AOC incorrectly.

CAUTION

If GroomerII cannot find a charging record that matches the called number, then the call will be connected (subject to an appropriate route being present) but AOC will not be generated. Your AOC configuration files should therefore be thoroughly tested before being loaded onto a live system.

10.2 Customers (port groups)

To apply an advice of charge to a port or group of ports (customer), select  or Configuration – Customers... to open the Customer Configuration dialog.

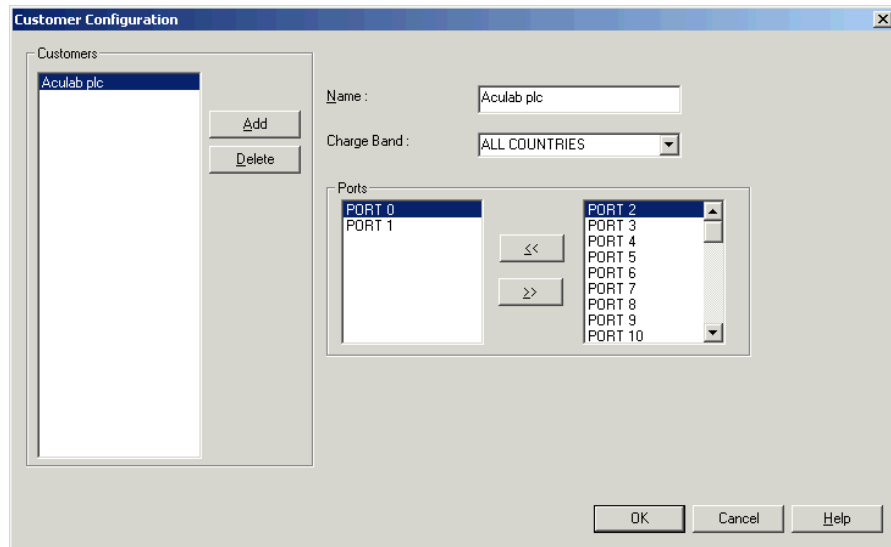


Figure 10-8 Customer configuration dialog

For a new configuration, all the fields, except the system default available ports list, will be blank. By default GroomerII can have up to 45 ports (PORT 0 to PORT 44). As it is possible to re-name the ports using the GroomerII configuration tool, the facility has been provided to allow you to load the actual available ports configuration information for the GroomerII configuration file associated with this advice of charge configuration.

10.2.1 Loading available port information.

Close the Customer Configuration dialog and return to the GroomerII Advice of Charge Configuration Editor dialog. Select Options – Port Definitions – Load... to display a Microsoft Windows Open dialog. Browse for and select the required *.cfg file followed by Open. This will load the associated GroomerII configuration ports list.

To continue customer configurations, return to the Customer Configuration dialog.

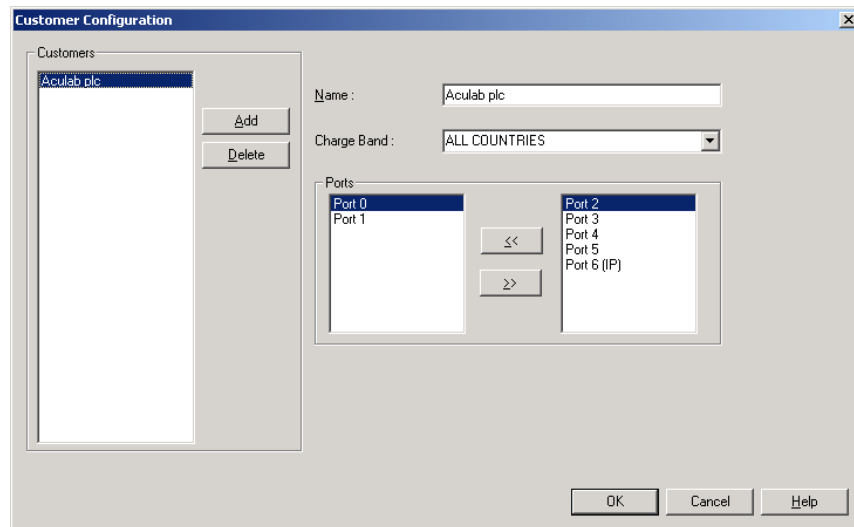


Figure 10-9 Customer configuration – specific GroomerII configuration

The configuration will remain associated with the GroomerII Advice of Charge Configuration Editor until either the current session is closed and a new session is started, another *.cfg file is loaded or you select Options – Port Definitions – Reset to return to the system default ports list.

10.2.2 Configuring customers

The following example shows the configuration that exists for the previously configured and loaded Test.bl1 file. You have the option to add a new customer, or remove an existing customer.

Add – selecting this option will add a new entry, with a default system name, to the Customers list. No Ports will yet have been selected and the Charge Band will be <None>.

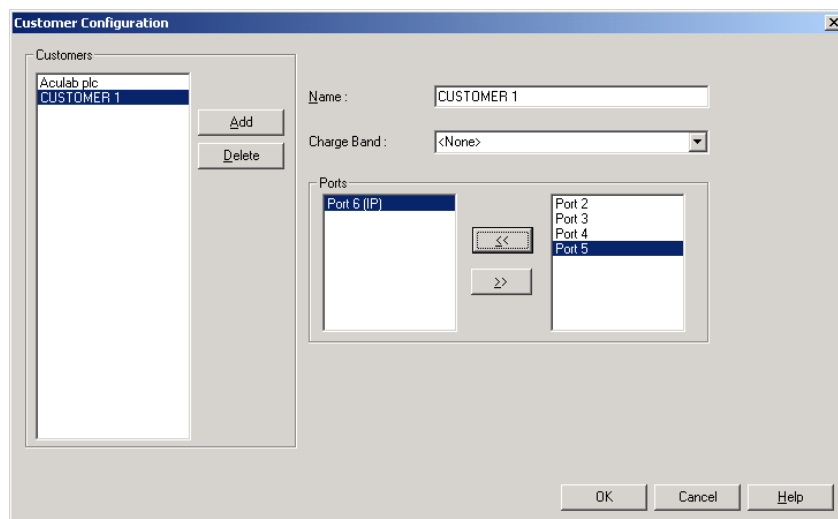


Figure 10-10 Customer configuration - add a new customer dialog

Delete – click to delete the selected entry from the Customers list.

10.2.3 Defining customers

Name – is not system dependent and may be any unique alpha/numerical identity you choose to assign as the identifier of a customer.

Charge Band – this pull down menu contains a list of all charge bands previously defined in the Charge Band Configuration dialog. Select the required charge band for the highlighted customer.

Ports – contains two lists, on the right a list of available ports and on the left a list of ports included in the charge band for the selected customer.

- Highlight a port in the right hand list then select << to include the port in the customer charge band list.
- Highlight a port in the left hand list then select >> to remove the port from the customer charge band list.

Once you have completed the set up of all required customers, select OK to accept any charges, or Cancel to ignore any changes, and return to the GroomerII Advice of Charge Configuration Editor dialog.

10.3 Enabling advice of charge

Once you have created and saved your advice of charge configuration, changes need to be made to the system `grshed.dat` file to include it when the GroomerII Kernel is started. The three parameters that need to be specified are `BILLING`, `DEF_BLL` and `UPDATE_BILLING`.

<code>BILLING:</code>	<code>ENABLE</code>	Use scheduled file
	<code>DISABLE</code>	Use default file
<code>DEF_BLL:</code>	<code>*.bll</code>	A default configuration file. This file will be used if there is no scheduled file found or <code>BILLING</code> is set to <code>DISABLE</code> . If no default file is defined, then advice of charge is switched off.
<code>UPDATE_BILLING:</code>	<code>ENABLE</code>	When a new <code>*.bll</code> file is loaded, the configuration will be applied to both new calls and calls in progress.
	<code>DISABLE</code>	When a new <code>*.bll</code> file is loaded, the configuration will be applied to new calls only. Calls in progress will continue to use the previous configuration parameters.

Example `grshed.dat` file:

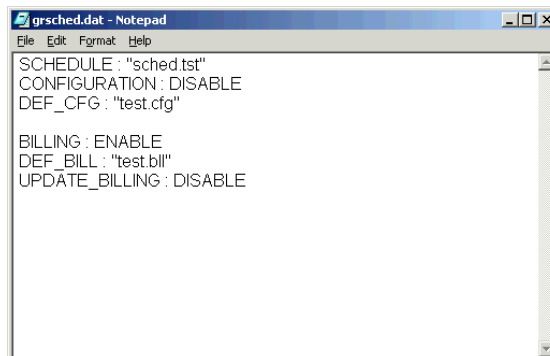


Figure 10-11 Example `grshed.dat` file configuration

10.4 Tool options

10.4.1 Comments

Select Tools - Comments... from the menu to add notes to the Advice of Charge configuration file. You will be presented with Comments notes dialog:

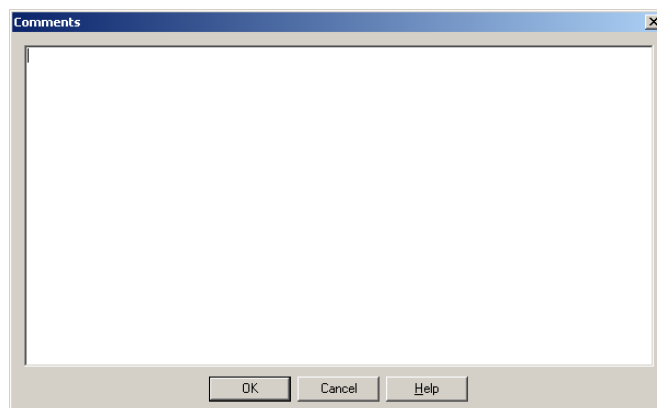


Figure 10-12 Advice of charge comments dialog

Enter any required comments followed by OK.

10.4.2 Activation key

If you have already entered the activation key for your system, you can change it using the Tools -Change Activation Key... menu option.

CAUTION

This option should only be used on standalone PCs. It is not appropriate on the GroomerII chassis itself as changing the key may prevent the Kernel from working. This option will be disabled (greyed out) if a GroomerII Kernel is detected on the same system.

A valid reason for changing the activation key may be due to a change of major revision to the GroomerII software.

Selecting to change the activation key, will present the following dialog.

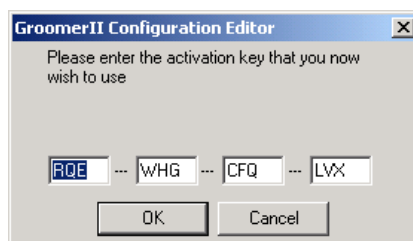


Figure 10-13 Activation key dialog

Enter a valid activation key for the software version being used, for example, RQE-WHG-CFQ-LVX as shown here. You will continue to be prompted until a valid activation key is entered. See section 19.2.2 for guidance on identifying valid activation keys.

NOTE

If you are using a support system with multiple versions of the software, a valid activation key is required for each.

11 Backup and restore

An option has been provided with the GroomerII software to enable the backup and restoration of key GroomerII registry, data and configuration files.

Select All Programs – Aculab GroomerII – Utilities – Backup and Restore from the Start menu to open the GroomerII Backup and Restore application.

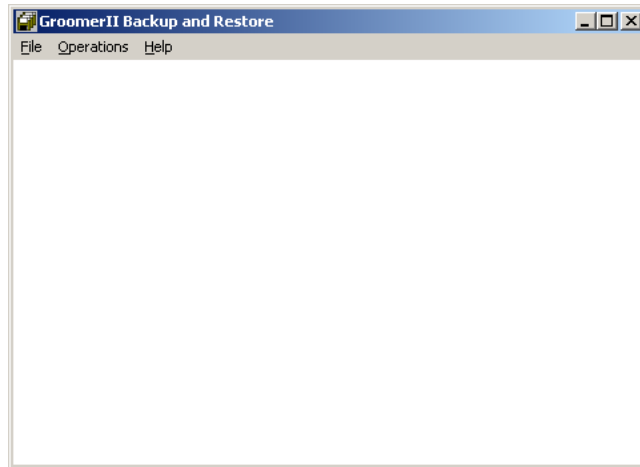


Figure 11-1 GroomerII backup and restore

Menu Options

File	- Exit
Operations	- Backup...
	Restore...
	Import...
Help	- Content
	Search...
	Index
	About GroomerII Backup and Restore

11.1 Backup

Use the Operations-Backup... menu option to backup all the important system and configuration files to a secure location.

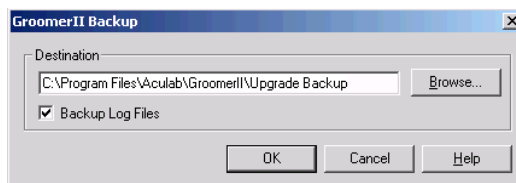


Figure 11-2 Backup destination directory selection dialog

Defining a location followed by OK will back up all configuration files detailed in the `grsched.dat` file along with the Aculab call driver configuration files and the following system files:

```
grsched.dat
grstatus.dat
```

grkernel.dat

The Backup Log Files checkbox allows call control trace files to be included in the backup. This control should only be checked if you are producing a backup that will be sent to Aculab Technical Support, and should be unchecked at all other times. Call control trace files will extend the time taken to produce the backup, and these files are neither deleted when the GroomerII applications are uninstalled, nor are they restored by a Restore operation.

A progress dialog will be displayed during backup.

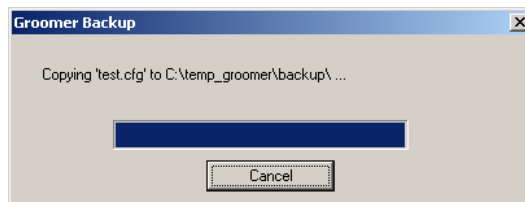


Figure 11-3 Backup progress dialog

And the following prompt on successful completion of the backup.



Figure 11-4 Backup successful dialog.

Backup error prompts

Should the selected backup destination contain existing backup files, you will receive the following prompt, select OK or Cancel as appropriate.

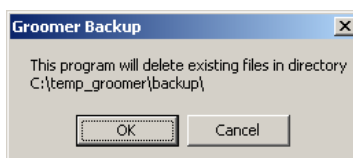


Figure 11-5 Backup overwrite warning dialog

Should the backup process fail to read the `grsched.dat` file for details of configuration files to back up, you will receive the following prompt:



Figure 11-6 Backup read failure warning dialog

Should the backup process fail to backup some or all of the default system files, you will receive the following type of prompt:



Figure 11-7 Backup failure dialog

11.2 Restore

Use the Operations-Restore... menu option to restore system and configuration files from a backup location.

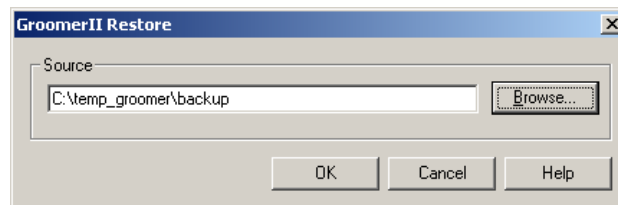


Figure 11-8 Restore source dialog

Make your required source selection followed by OK.

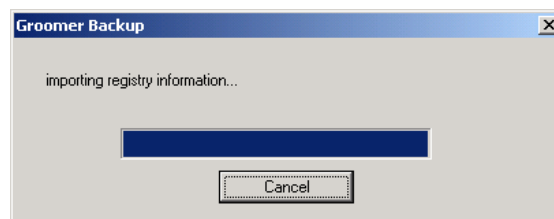


Figure 11-9 Restore progress dialog

You will be presented with a progress dialog followed by a restore completed successfully dialog.

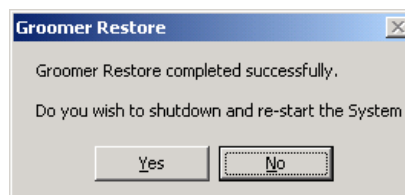


Figure 11-10 Restore successful dialog

Select Yes to re-boot the system or No to continue to use the current system.

Restore error prompts

Should there be any problems during restore, you will be presented with an appropriate prompt, for example, should the `_GroomerII.bak` file show a different GroomerII version to that currently installed, you will receive the following type of prompt:

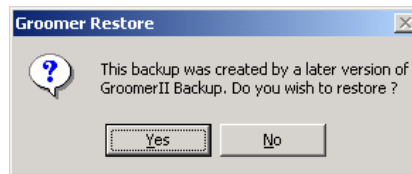


Figure 11-11 Restore version error dialog

Should the `_GroomerII.bak` file be missing from the source directory, you will receive the following prompt.



Figure 11-12 Restore invalid backup source dialog

11.3 Configuration import

The configuration import utility allows a backup taken from one system to be imported onto another. The import feature can be used in two ways:

- To duplicate the configuration from one system onto a second identical system. This form of import would be used when installing a new chassis with a universal configuration. It will copy the configuration of the Prosody X cards in the source system to those in the target system, whilst retaining the existing IP configuration of the target system.
- To copy the configuration from a failed system onto a replacement. This form of import will copy both the Prosody X configuration and the IP configuration from the source to the target system, allowing disconnect/reconnect replacement of the failed unit.

NOTE

Only backups produced by GroomerII application software version 10.28.0 or later can be used for import.

11.3.1 Host port groups

When producing and importing backups GroomerII uses host port groups to transfer the host adapter IP configuration between systems. A host port group is one or more network adapters sharing a common IP address and configuration parameters. This approach allows configurations to be moved between systems that have different numbers of IP adapters.

An example of this might be when replacing a failed GroomerII 2U (R730) system that has four host adapters configured into two teams with a standby GroomerII 2U (CG2100) system having two host adapters configured as single ports. The host port groups concept allows the configuration from the two teams to be imported onto the two single port adapters, thereby maintaining full system functionality (the redundancy provided by the source teams will however be lost).

The following diagram illustrates a system with four host port adapters, two of which (Local Area Connection and Local Area Connection 2) are formed into a team (Local Area Connection 5).

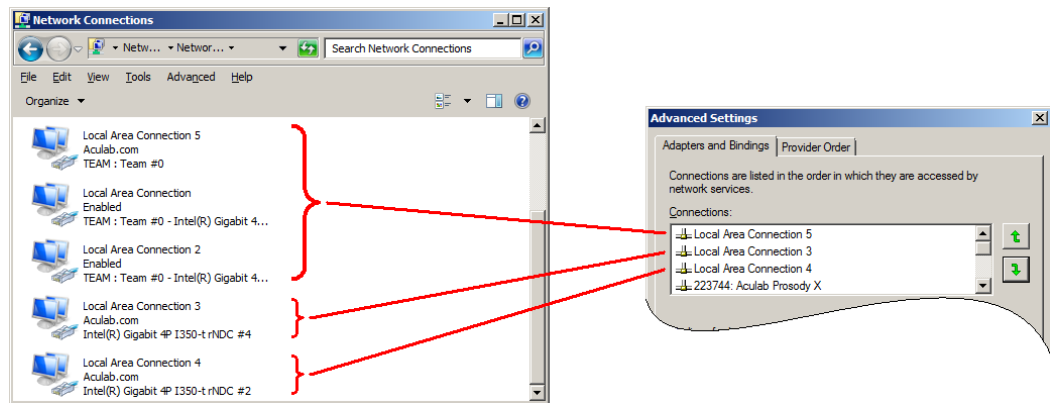


Figure 11-13 Host port groups

NOTE

The above diagram is for illustrative purposes only and is not representative of a properly configured system. When enumerating the host port groups, the backup software will automatically exclude any Prosody X cards interleaved with the host adapters, along with any individual host ports that are included in a team.

When a backup of this system is produced, the IP configuration of the three host port groups present will be stored in the order that they are listed in the Advanced Settings dialog. When the backup is imported, these configurations will be restored to the first three host port groups listed in the Advanced Settings dialog on the target system.

If the source system contains more host port groups than the target system, the excess groups will be discarded.

If the target system contains more host port groups than the source system, the excess groups will be configured for DHCP operation.

11.3.2 Preparing the backup

The following rules must be observed when producing a backup that will be used as a configuration import source.

- All host network ports on the source system must be connected to a network switch before the backup is taken, otherwise it will not be possible to detect the IP configuration of the port.
- All Prosody X cards on the target system must be in the In service state.

It is not necessary to check the Backup Log Files control when producing the backup, as these files will not be imported onto the target system.

11.3.3 Preparing the target system

The following rules must be observed when importing a configuration backup.

- The target system must have an identical number Prosody X cards to the source system. The target cards must be of equivalent type (having the same number of TDM ports and DSPs) to the source cards, and the physical ordering of the cards in the chassis must be the same.
- The target system must be installed with the same or later version of GroomerII application software as the source system, and the software activated with the appropriate activation key.
- If the IP configuration is to be imported onto the target system, the host port groups must be correctly ordered in the Advanced Settings dialog.

- All Prosody X cards on the target system must be in the In service state.

11.3.4 Trunk port cabling

When using the configuration import to replace a failed system, it may be necessary to connect the trunk port cables to the substitute chassis in a different order. An example of this would be when replacing a GroomerII 2U (TIGH2U) chassis with a GroomerII 2U (R730) chassis, where each chassis has a different trunk port numbering scheme.

Refer to section 1.6 for further information on trunk port numbering.

11.3.5 Importing the configuration

Ensure that all GroomerII applications on the target system are closed.

Use the Operations-Import... menu option to begin the import procedure, and you will be prompted to select the location from which to import the backup.

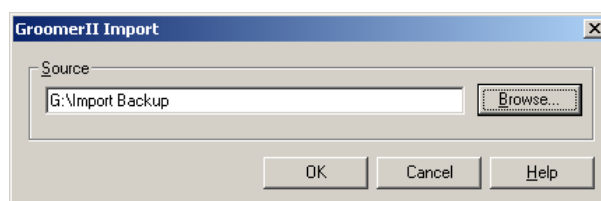


Figure 11-14 Import source dialog

When you have selected your source backup an audit will be performed to verify that the hardware configuration of the target system is suitable, during which time a number of progress dialogs will be seen.

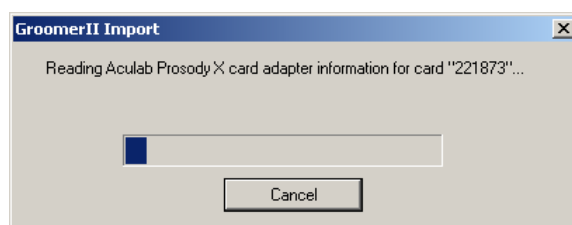


Figure 11-15 System audit progress dialog

If the target system is not suitable for the import, a warning dialog will be displayed and you will be returned to the GroomerII Backup and Restore main window.

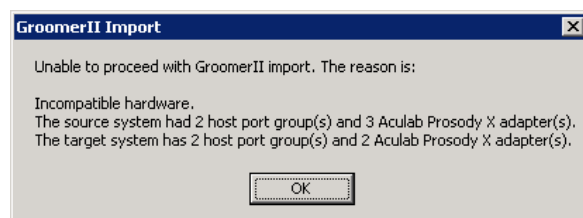


Figure 11-16 Unsuitable target system warning dialog

You will now be taken to the Prosody X card mapping dialog.

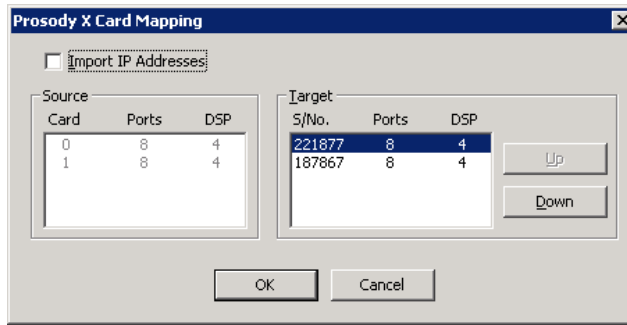


Figure 11-17 Prosody X card mapping dialog

Import IP – Tick this checkbox to copy the IP configuration from the backup to the target system. Both IPv4 and/or IPv6 configurations can be imported. Leaving the checkbox unticked will preserve the existing IP settings on the target system.

Source – The list contains one entry for each card present in the backup, listed in the order they were installed in the source chassis.

Destination – The cards detected in the target chassis are displayed in the list. Use the Up and Down buttons to place these cards in their installed order. It is important that the card in each position is equally matched between the Source and Destination list.

If you checked the Import IP tickbox you will be prompted to disconnect the source system from the network.

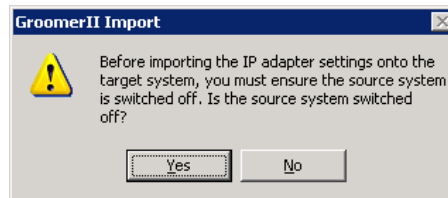


Figure 11-18 Disconnect source system dialog

The source configuration will now be copied to the destination system, during which time a number of progress dialogs will be seen.

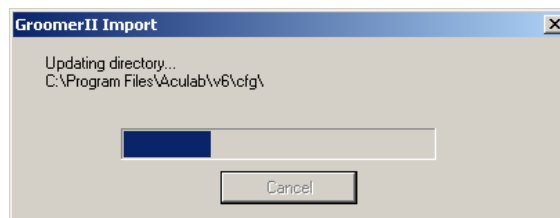


Figure 11-19 Import progress dialog

When the configuration has completed copying, the following dialog will appear.

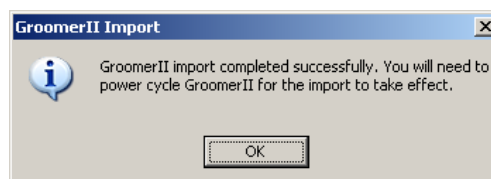


Figure 11-20 Import complete dialog

You should now power cycle the target system, which will start ready to process calls.

11.4 Silent backup

The GroomerII Backup and Restore utility will allow a silent backup to be performed. When started in silent mode no user interaction is required, and any reporting will be written to a log file. This will allow a GroomerII backup to be performed periodically using a utility such as Microsoft Windows Scheduled Tasks. For details of the Scheduled Tasks utility consult the appropriate Microsoft documentation.

To start the GroomerII Backup and Restore utility in silent mode execute

`grBackupAndRestore.exe -silent` at the command line, adding the appropriate parameters from the list below.

<code>-help</code>	If the program is started with this switch anywhere on the command line, then a description of the available switches will be displayed and the program will terminate.
<code>-silent</code>	<p>If the program is started with the <code>-silent</code> switch then no user interface will be displayed. An unattended backup will be performed automatically using the values specified by other parameters as input, and when complete the program will terminate.</p> <p>If the <code>-silent</code> switch is not present when the program is started then the user interface will be displayed and all other switches will be ignored.</p>
<code>-dest <path></code>	This specifies the destination folder in which the backup is to be archived, for example <code>-dest F:\G4321\Backup</code> . If no destination is specified then a default location of <code>C:\Program Files (x86)\Aculab\GroomerII\Backup</code> will be used. The specified folder will be created if not already present.
<code>-overwrite</code>	<p>If the <code>-overwrite</code> switch is specified, any existing files found in the destination folder will be removed and replaced with the new backup.</p> <p>If <code>-overwrite</code> is not used and existing files are found in the destination folder, then the program will terminate and no backup will be taken.</p>
<code>-noimport</code>	By default a configuration import file will be generated by the backup. Using this switch will stop the file from being generated, and you will not be able to export the backup to another system.
<code>-nokernel</code>	By default the <code>kernel.log</code> file is included in the backup. Using this switch will exclude <code>kernel.log</code> from the backup.
<code>-notrace</code>	By default the backup includes any call control trace files found in the <code>C:\Program Files (x86)\Aculab\GroomerII\Trace</code> folder that have been generated during the preceding 24 hours. Using this switch will exclude such files from the backup.

`-logfile <pathname>` This is the path and name of the file in which the results of the unattended backup will be recorded, for example `-logfile F:\G4321\Backup.log`. If no logfile is specified a default pathname of `C:\Program Files (x86)\Aculab\GroomerII\grBackup_YYMMDD_HHMMSS.log` will be used, where YYMMDD and HHMMSS represent the date and time at which the backup was started.

The specified folder and/or file will be created if not already present. If the specified file already exists the results will be appended to the end of the file.

Logging will only be produced for unattended backups.

NOTE

The log file must not be placed in or below the folder specified by the `-dest` parameter, as this will cause the backup to fail.

Switches may appear in any order on the command line. Unrecognised switches will be ignored.

The results of the unattended backup will be logged to disk, in either the specified or default location, as dictated by the command line parameters. The following is an illustration of a backup log showing both a successful and failed backup.

```
=====
Backup started 31/03/16 02:00:00
grBackupAndRestore V10.50.0
Switches: -dest F:\Groomer_Backups\G4321\Backup
          -overwrite
          -notrace
          -logfile F:\Groomer_Backups\G4321\grBackup.log
Unrecognised switches: -nokenrel
Backup successful
=====
Backup started 01/04/16 02:00:00
grBackupAndRestore V10.50.0
Switches: -dest F:\Groomer_Backups\G4321\Backup
          -overwrite
          -nokernel
          -notrace
          -logfile F:\Groomer_Backups\G4321\grBackup.log
ERROR: Unable to copy grBackup.dat
ERROR: Unable to copy grStatus.dat
Backup failed
```

12 Call Transfer

12.1 Call transfer mapping in GroomerII

GroomerII is able to map call transfer requests from the called side through to the calling side. At present only the mapping of ETS 300 call transfer requests to SS7 call redirection requests is supported.

12.2 ETS 300 Call Transfer to SS7 Call Redirection Mapping

12.2.1 Overview

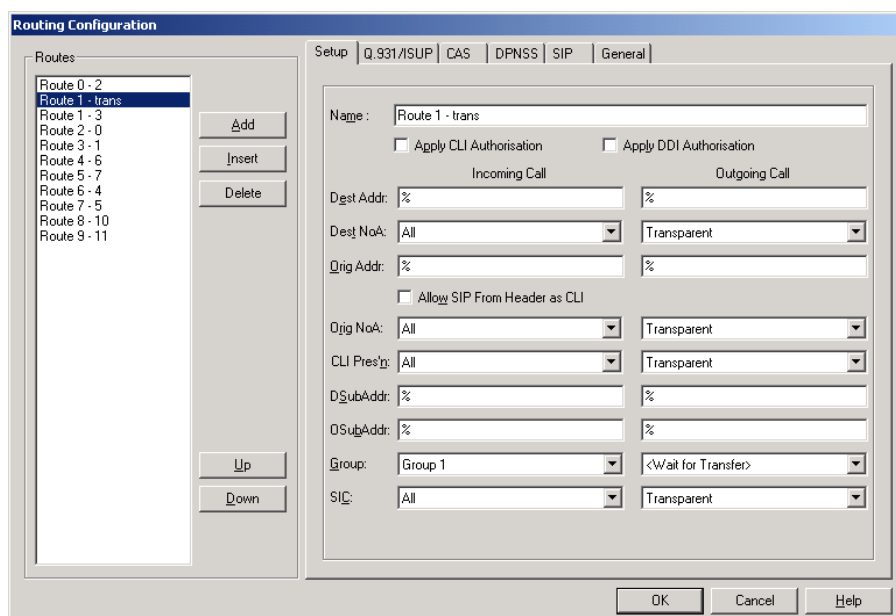
When performing protocol conversions in the direction SS7 to ETS 300, GroomerII will automatically map an explicit call transfer request received from the ETS 300 side into a call redirection request on the SS7 side. If an ETS 300 call transfer request is received when the incoming call leg is not SS7, then the request will be rejected.

12.2.2 Configuration

NOTE

The `-cFF` firmware switch must be applied to all ETS 300 ports that will be involved in call transfer operations.

The called party will initiate a transfer by making a new enquiry call into GroomerII, and this call must be made on a separate timeslot from the original call. A separate route is configured to receive this call, where the destination group is set to the system entry of <Wait for Transfer>, as illustrated below.



The image shows a 'Routing Configuration' dialog box with a 'Routes' list on the left containing 'Route 0 - 2', 'Route 1 - trans', 'Route 2 - 0', 'Route 3 - 1', 'Route 4 - 6', 'Route 5 - 7', 'Route 6 - 4', 'Route 7 - 5', 'Route 8 - 10', and 'Route 9 - 11'. The 'Route 1 - trans' is selected. The main configuration area has tabs for 'Setup', 'Q.931/SUP', 'CAS', 'DPNSS', 'SIP', and 'General'. The 'General' tab is active. It contains fields for 'Name' (Route 1 - trans), 'Apply CLI Authorisation' (unchecked), 'Apply DDI Authorisation' (unchecked), 'Incoming Call' and 'Outgoing Call' sections with fields for 'Dst Addr', 'Dest NoA', 'Orig Addr', 'Orig NoA', 'CLI PresId', 'DSubAddr', and 'OSubAddr'. The 'Group' dropdown is set to 'Group 1' and the 'SIC' dropdown is set to 'All'. The 'Wait for Transfer' option is selected in the 'Group' dropdown.

Figure 12-1 Wait for Transfer Routing Configuration

When a call is received on this route, no outgoing call will be made. The call will be progressed to the ringing stage, and will remain in this state until cleared down. Whilst in this state the call will respond to a Link ID request, which the original called party should return to the original outgoing ETS 300 call in a call transfer execute request. At this point GroomerII will:

- Clear down the original ETS 300 call leg in an appropriate fashion,

- Clear down the ETS 300 enquiry call in an appropriate fashion,
- Redirect the SS7 call by releasing it with a fixed cause value of 23.

The same incoming group can be used, in separate routes, to receive both call transfer requests and normal incoming calls as long as the calls can be differentiated during route selection, for example by using a Destination Address mask.

12.2.3 CDR generation

The following fields in the Used Defined CDR may be used to report the call transfer mapping

- Call redirection address – this is the dialled number to which the original call has been redirected.
- Incoming enquiry call port – this is the number of the port on which the enquiry call requesting the transfer was received.
- Incoming enquiry call timeslot – this is the timeslot on the above port used by the enquiry call.

12.3 CAMA to SIP Call Transfer Mapping

NOTE

The `-s26` firmware switch must be applied to all CAMA ports that will generate hookflash call transfer requests. The recommended setting is `-s26, 30`.

When performing protocol conversions in the direction SIP to CAMA, GroomerII can be configured to map a hookflash call transfer request from the CAMA side to the SIP side. The following procedure is invoked if a hookflash is detected on the CAMA side whilst the call is in the connected state:

- The hookflash is mapped to the SIP side using the RFC 2833 event 16 (Flash).
- The US dial tone is played to the CAMA side.
- When the first DTMF dialled digit is detected on the CAMA side, the dial tone will be discontinued. This digit and all subsequent DTMF dialled digits will be mapped to the SIP side using RFC 2833 digits.

CAMA to SIP call transfer mapping is configured using the Routing Configuration window in the GroomerII Configuration Editor, and must be enabled separately for each route on which mapping is required. The configuration procedure is:

- On the CAS page select the CAMA to SIP Call Transfer Mapping checkbox (see section 8.5.4),
- On the SIP – Incoming – Media page, enable RFC 2833 event generation by setting the DTMF Digit Detection control to either Immediate Detection or 40ms Detection (see section 8.5.6).

12.4 SIP to CAMA Call Transfer Mapping

NOTE

The `-s25` firmware switch must be applied to all CAMA ports to which hookflash call transfer requests will be mapped. The recommended setting is `-s25, 15`.

When performing protocol conversions in the direction CAMA to SIP, GroomerII can be configured to map an RFC 2833 hookflash (event 16) call transfer request from the SIP side to the CAMA side. The following procedure is invoked if a hookflash is detected on the SIP side whilst the call is in the connected state:

- The hookflash is mapped to the CAMA side.
- The US dial tone is played to the SIP side.
- When the first DTMF dialled digit is detected on the SIP side, the dial tone will be discontinued. This digit and all subsequent DTMF dialled digits will be mapped to the CAMA side in the normal fashion.

SIP to CAMA call transfer mapping is configured using the Routing Configuration window in the GroomerII Configuration Editor, and must be enabled separately for each route on which mapping is required. Navigate to the SIP – Outgoing – Media page (see section 8.5.6) and:

- Enable RFC 2833 event generation by setting the DTMF Digit Detection control to either Immediate Detection or 40ms Detection,
- Tick the SIP to CAMA Call Transfer Mapping checkbox.

13 Database connectivity

13.1 GroomerII database connectivity

Database connectivity allows GroomerII to retrieve information from an external source (typically a remote database) to use when routing a call, and is achieved by connecting to an ODBC data source. The installation and configuration of ODBC data sources, ODBC drivers, and DBMS software is beyond the scope of this document, and the reader should refer to the user documentation for that product.

The following aspects will be the responsibility of the customer:

- Provision, configuration, and population of the database
- Supply, installation, and configuration of an appropriate ODBC driver
- The resolution of any security issues that may arise from storing database connection and login information in GroomerII configuration files
- The resolution of any performance issues that may result from the use of a remote database.

GroomerII database connectivity has been designed and implemented in a fashion that will allow a user to access any corporate data source to retrieve information. This is achieved by issuing a simple SQL query to the ODBC data source in order to retrieve the required data. If the required data cannot be retrieved by directly accessing a table, or if it is stored across a number of different tables, then your DBA (Database Administrator) can define a view that will present the data in the required form. For assistance in configuring database connectivity, in the first instance contact your DBA. Separate ODBC data sources may be used for each of the three connectivity functions.

The mechanism will monitor all connections to the database, with changes in the connection state being reported to the Kernel main dialog. When a database connection is lost, GroomerII will automatically attempt to re-establish the connection at regular intervals.

GroomerII currently supports database connectivity for:

- CLI authorisation
- DDI authorisation
- Number Portability Mapping

13.2 CLI authorisation

CLI authorisation can be applied to individual routes, and allows the CLI for an incoming call to be validated against a data source.

The CLI authorisation connectivity is configured using the CLI Authorisation Database Connection screen. This screen is located under the GroomerII Kernel dialog, Options menu, and CLI Authorisation... selection.

Subject to any limitations imposed by the data source, up to 25 simultaneous connections to the database can be established. The CLI is authorised using the following query:

```
SELECT <column name>
FROM <object name>
WHERE <column name> = '<CLI>'
```

For example:

```
SELECT fldCLI
FROM vwCLI_Validation
WHERE fldCLI = '01908273800'
```

The CLI will be authorised if the query returns one or more rows, otherwise it will be rejected. No checking is performed on the content of any rows returned. <object name> may be either the name of a table that physically exists in the database, or the name of a view specially prepared for this purpose. The object will have a column (<column name>) of type `varchar(32)`, which will contain the CLI. Both <object name> and <column name> are configurable so that corporate naming conventions may be observed. The contents of the <CLI> field will be taken from the incoming call details.

CLI authorisation is reported to the Events screen in the Status Monitor via the Call Control filter using the following messages:

```
CLI 01908273800 - Requested authorisation
CLI 01908273800 - Authorisation accepted (<info>)
CLI 01908273800 - Authorisation rejected (<info>)
```

Where <info> takes one of the following formats:

```
<time1>:<time2>
<time1>:<cause>
<cause>
```

Where:

<time1> is the number of milliseconds that the request waited for a connection to the database to become available. If this value is considered excessive, assigning more connections to the database can usually reduce it.

<time2> is the number of milliseconds taken to execute the round trip to the database. If this value is considered excessive, improvements to your networking and/or database server performance will be necessary to reduce it.

<cause> can be one of the following values:

disabled	CLI Authorisation is not enabled because the ODBC DSN field in the CLI Authorisation Database Connection dialog is set to <None>.
length	The CLI contained fewer than the minimum number of digits as specified in the System Configuration dialog in the Configuration Editor.
queue	The request could not be placed in the internal queue pending processing. This type of failure is treated as if there was no connection to the database.
no connection	The request could not be processed as there was no connection to the database. The default action is applied as specified in the System Configuration dialog in the Configuration Editor.
timeout	The request could not be completed before the timeout expired.
error	The request could not be completed due to a database error. This type of failure is treated as if there was a lost connection.

13.3 DDI authorisation

DDI authorisation can be applied to individual routes, and allows the DDI for an incoming call to be validated against a data source.

The DDI authorisation connectivity is configured using the DDI Authorisation Database Connection screen. This is located under the GroomerII Kernel dialog, Options menu, and DDI Authorisation... selection.

Subject to any limitations imposed by the data source, up to 25 simultaneous connections to the database can be established. The DDI is authorised using the following query:

```
SELECT <column name>
FROM <object name>
WHERE <column name> = '<DDI>'
```

For example:

```
SELECT fldDDI
FROM vwDDI_Validation
WHERE fldDDI = '01908273800'
```

<object name> may be either the name of a table that physically exists in the database, or the name of a view specially prepared for this purpose. The object will have a column (<column name>) of type varchar(32), which will contain the DDI. Both <object name> and <column name> are configurable so that corporate naming conventions may be observed. The contents of the <DDI> field will be taken from the incoming call details.

The system may be configured to use the information in the database as a black list (rejecting a call if the query returns one or more rows) or as a white list (accepting the call if the query returns one or more rows). No checking is performed on the content of any rows returned.

DDI authorisation is reported to the Events screen in the Status Monitor via the Call Control filter using the following messages:

```
DDI 01908273800 - Requested authorisation
DDI 01908273800 - Authorisation accepted (<info>)
DDI 01908273800 - Authorisation rejected (<info>)
```

Where <info> takes one of the following formats:

```
<time1>:<time2>
<time1>:<cause>
<cause>
```

Where:

<time1> is the number of milliseconds that the request waited for a connection to the database to become available. If this value is considered excessive, assigning more connections to the database can usually reduce it.

<time2> is the number of milliseconds taken to execute the round trip to the database. If this value is considered excessive, improvements to your networking and/or database server performance will be necessary to reduce it.

<cause> can be one of the following values:

disabled	DDI Authorisation is not enabled because the ODBC DSN field in the DDI Authorisation Database Connection dialog is set to <None>.
----------	---

length	The DDI contained fewer than the minimum number of digits as specified in the System Configuration dialog in the Configuration Editor.
queue	The request could not be placed in the internal queue pending processing. This type of failure is treated as if there was no connection to the database.
no connection	The request could not be processed as there was no connection to the database. The default action is applied as specified in the System Configuration dialog in the Configuration Editor.
timeout	The request could not be completed before the timeout expired.
error	The request could not be completed due to a database error. This type of failure is treated as if there was a lost connection.

13.4 Number portability mapping

Number Portability mapping can be applied to individual ports, and allows the DDI for an incoming call to be substituted with an alternative (typically the same number with a prefix attached) to allow the call to be routed in a cost effective fashion. It is most often used to route calls to mobile phones in situations where the customer has moved between networks and the dialling prefix cannot be used to identify the provider.

The Number Portability mapping is configured using the Number Portability Database Connection screen. This is located under the GroomerII Kernel dialog, Options menu, and Number Portability... selection.

Subject to any limitations imposed by the data source, up to 25 simultaneous connections to the database can be established. The mapping is carried out using the following query:

```
SELECT <mapping column name>
FROM <object name>
WHERE <incoming column name> = '<Incoming DDI>'
```

For example:

```
SELECT fldMappedDDI
FROM vwNumberPortability
WHERE fldIncomingDDI = '07953123456'
```

<object name> may be either the name of a table that physically exists in the database, or the name of a view specially prepared for this purpose. The object will have two columns. One column (<incoming column name>) of type varchar(32) will contain the incoming DDI, whilst the other (<mapping column name>) of type varchar(32) will contain the number that is to be used in its place. Both object name and the column names are configurable, so that corporate naming conventions may be observed. The contents of the <Incoming DDI> field will be taken from the incoming call details.

If one or more rows of data are returned, the contents of <mapping column name> in the first row will be used to route the call, otherwise <Incoming DDI> will be used to route the call.

NOTE

If the incoming DDI is appended with an EOS (end of send) character, the EOS character will not be included in the number that is sent to the database for mapping. For example if the incoming DDI is 01234!, only 01234 will be sent to the database. If the incoming DDI was appended with an EOS character and the mapped DDI is less than 31 characters in length, the EOS character will be appended to the mapped DDI. If the mapped DDI is longer than 31 characters, the EOS is not appended.

Number Portability mapping is reported to the Events screen in the Status Monitor via the Call Control filter using the following messages:

```
NUMBER PORTABILITY - Requested mapping for DDI 07953123456
NUMBER PORTABILITY - DDI 07953123456 mapped to 307953123456 (<info>)
NUMBER PORTABILITY - Default mapping used for DDI 07953123456 (<info>)
NUMBER PORTABILITY - No mapping available for DDI 07953123456 (<info>)
```

Where <info> takes one of the following formats:

```
<time1>:<time2>
<time1>:<cause>
<cause>
```

Where:

<time1> is the number of milliseconds that the request waited for a connection to the database to become available. If this value is considered excessive, assigning more connections to the database can usually reduce it.

<time2> is the number of milliseconds taken to execute the round trip to the database. If this value is considered excessive, improvements to your networking and/or database server performance will be necessary to reduce it.

<cause> can be one of the following values:

disabled	Number portability is not enabled because the ODBC DSN field in the Number Portability Database Connection dialog is set to <None>.
length	The DDI contained fewer than the minimum number of digits as specified in the System Configuration dialog in the Configuration Editor.
queue	The request could not be placed in the internal queue pending processing. This type of failure is treated as if there was no connection to the database.
no connection	The request could not be processed as there was no connection to the database. The default action is applied as specified in the System Configuration dialog in the Configuration Editor.
timeout	The request could not be completed before the timeout expired.
error	The request could not be completed due to a database error. This type of failure is treated as if there was a lost connection.

14 SIP telephony

14.1 IPv4 and IPv6 telephony

SIP telephony supports the use of IPv4 and/or IPv6 addresses, with both IPv4 calls and IPv6 calls being handled at the same time. GroomerII must be configured for IPv4 and/or IPv6 telephony as described in section 3.

The call handling procedures applied by systems configured to use both IPv4 and IPv6 are described in the following sections.

14.1.1 Incoming call handling

The following procedure will be applied when handling incoming SIP calls:

- When the incoming INVITE is accompanied by an SDP, GroomerII will select a media stream that matches the signalling address whenever possible. For example an IPv4 media stream will be selected for a call signalled using IPv4. If this is not possible then any suitable media stream will be chosen which may result in, for example, a call signalled using IPv4 selecting an IPv6 media stream.
- When the incoming INVITE does not present an SDP, GroomerII will initiate media negotiation at an appropriate point:
 - If the incoming call was signalled using an IPv4 address GroomerII will present an IPv4 media offer.
 - If the incoming call was signalled using an IPv6 address GroomerII will present an IPv6 media offer.

14.1.2 Outgoing call handling

When making an outgoing call GroomerII will always match the media offer to the signalling type:

- When directing a call to an IPv4 endpoint, the INVITE will be accompanied by an SDP offering IPv4 media only.
- When directing a call to an IPv6 endpoint, the INVITE will be accompanied by an SDP offering IPv6 media only.

It is not possible to direct a call to an IPv4 endpoint and offer IPv6 media, or vice versa.

14.1.3 Call retry and recovery

When a SIP call is retried or recovered GroomerII may direct the replacement call to a different type of endpoint (for example, the original call might have been directed to an IPv4 endpoint whilst the replacement call is directed to an IPv6 endpoint). In this situation a new SDP will be created following the rules in section 14.1.2 above.

14.2 SIP security

GroomerII is able to make secure SIP calls using Transport Layer Security (TLS) for call control signalling and Secure RTP (SRTP) for the media stream.

14.2.1 Configuration

GroomerII will not be able to make or receive secure SIP calls until the appropriate RSA certificate files have been loaded. See section 5.10 for further details.

NOTE

It is the responsibility of the customer to provide the appropriate certificate files.

Once the appropriate certificate files have been loaded both secure and non-secure incoming calls will be handled automatically.

Outgoing calls must be explicitly configured to use SIP security on a route-by-route basis. See section 8.5.6 for details.

The G.726 codec cannot be used with secure SIP calls.

14.2.2 TLS

TLS negotiation will be conducted on port 5061. Incoming secure calls may be identified using either the `sips:` prefix in the `To:` header (for example `To: <sips:1234@10.11.12.13>`), or by the `transport=tls` parameter in the `Contact:` header (for example `Contact: <sip:1234@10.11.12.13;transport=tls>`).

If the TLS layer refuses an incoming SIP call this will **NOT** be reported by the GroomerII application.

14.2.3 SRTP

Support for Secure RTP is in accordance with IETF RFC 4568.

Media transport type

Incoming calls using the `RTP/SAVP` transport type will be negotiated in accordance with IETF RFC 4568.

NOTE

In some instance incoming calls may arrive that request SRTP but use the RTP/AVP transport type. Such calls are outside of specification. GroomerII will attempt to negotiate a secure media stream on such occasions, although success cannot be guaranteed.

All outgoing secure calls will use the `RTP/SAVP` transport type.

Crypto suites and key parameters

The following Crypto-Suites are supported, and will be offered in the order listed

AES_CM_128_HMAC_SHA1_80

AES_CM_128_HMAC_SHA1_32

F8_128_HMAC_SHA1_80

Key parameters

Each crypto suite offered will use a different key, and new keys will be generated for each call. GroomerII does not support the use of multiple keys, and only a single inline key is permitted.

GroomerII does not support the key lifetime parameter. It will not be present in a media offer, and will be ignored if received in a media proposal.

GroomerII does not support the master key identifier (MKI) parameter. It will not be present in a media offer, and will be ignored if received in a media proposal.

Session parameters

GroomerII will not include any session parameters in a media offer. Session parameters included in an offer from a remote endpoint will be processed in the following manner:

KDR –	This parameter is not supported by GroomerII and will be ignored.
UNENCRYPTED_SRTCP –	GroomerII does not support RTCP processing. If this parameter is offered it will be included in the media answer.
UNENCRYPTED_RTP –	GroomerII will use unencrypted RTP.
UNAUTHENTICATED_RTP –	GroomerII will use unauthenticated RTP.
FEC_ORDER –	This parameter is not supported by GroomerII and will be ignored.
FEC_KEY –	This parameter is not supported by GroomerII and will be ignored.
WSH –	This parameter is not supported by GroomerII and will be ignored.

14.3 SIP call recovery

SIP call recovery is a customer specified feature. Its purpose is to identify when an outgoing SIP call leg has failed and re-establish the call automatically via an alternative gateway. This feature is independent of the protocol used by the incoming call leg.

Call recovery is only available when outgoing SIP calls are being routed to a gateway. It is configured on a system wide basis, and once enabled all new outgoing SIP calls will be monitored. Section 8.6.9 describes enabling SIP call recovery.

NOTE

Call recovery can only be used when a gateway list containing two or more gateways is in operation.

Call failure is detected by monitoring the RTP stream received from the remote endpoint, and monitoring begins when the outgoing SIP call reaches connected state. Call recovery cannot be used with a remote endpoint that is performing discontinuous transmission (DTX).

NOTE

When a SIP call is placed on hold by the remote endpoint, RTP monitoring is suspended. RTP monitoring is resumed when the call is taken off hold.

When call failure is detected the failed SIP call leg is released and a replacement call made. The call attributes (for example called party number, calling party number) of the failed call will be used when making the recovery call. The following gateways will be excluded from the search for an alternative destination:

- The gateway to which the failed call was directed,
- Any gateway that is currently marked as unavailable,

- Any gateway whose call capacity has been reached.

Failed call retry will be applied to the recovery call if enabled. Once the recovery call has reached the connected state it may be recovered a second and subsequent time.

Call recovery is reported using the Call Control filter, and will be reported using the Call ID of the failed call leg.

A SIP custom header is used to identify a recovery call. See Appendix F: for details.

14.4 SIP call hold

When a SIP call is in the connected state GroomerII will acknowledge a call hold request from a remote endpoint and discontinue the transmitted RTP stream. The received RTP stream will continue to be processed to accommodate features such as music on hold.

To place a call on hold the remote endpoint should send a REINVITE with an SDP whose media description contains the `sendonly` or `inactive` attribute. To remove the call from hold the remote endpoint should send a further REINVITE with an SDP whose media description contains the `sendrecv` or `recvonly` attribute. Whilst a call is on-hold, any REINVITE received that is not an off-hold instruction will be processed in the normal way.

GroomerII is resilient to changes in the session ID of a call whilst it is on-hold. A call will not be removed from hold unless the session ID of the off-hold instruction matches that of the on-hold instruction.

NOTE

GroomerII can only place a call on hold in response to a request from the remote endpoint. GroomerII cannot make a call hold request.

14.5 SIP call redirection

GroomerII will redirect a call when an outgoing INVITE is cleared with a 300, 301, 302 or 305 response before reaching the connected stage. The INVITE response must present a `Contact` header, as described in RFC 3261 section 20.10, with the URI containing both a DDI and an IP Address, for example `Contact:`
`<sip:12345@192.168.1.10>.`

If the IP address in the `Contact` header matches the GroomerII host port IP address, then the DDI will be extracted and the call will be passed back through the routing table to establish the new destination. All other routing parameters will be taken from the original incoming call. This allows an outgoing SIP call to be redirected to the TDM network.

If the IP address in the `Contact` header does not match the GroomerII host port IP address, then a new SIP call will be made to the destination specified. All other call parameters will be those used for the original outgoing call. If GroomerII is configured to use a SIP proxy server for outgoing calls then the new call will be directed to that SIP proxy server for onward routing.

The 300 - Multiple Choices response may present multiple `Contact` headers to facilitate analysis and selection. No such analysis and selection will be carried out, and the first `Contact` header encountered in the response will be used.

The requirement that local directories should be updated on receipt of a 301 - Moved Permanently response is not supported.

All other 3xx responses (including specifically 380 – Alternative Service) will be treated as rejected calls and will not be redirected.

14.6 Functional Number mapping

GroomerII supports the mapping of a Functional Number between an ITU-T SS7 call leg and a SIP call leg by means of the `Aculab-Functional-Number` header.

If an ITU-T SS7 call presents a Functional Number in the User-to-user information parameter of the incoming IAM, the number will be placed unmodified into an `Aculab-Functional-Number` header in the outgoing SIP INVITE.

If a SIP call presents an `Aculab-Functional-Number` header in the incoming SIP INVITE, the number will be placed unmodified into a User-to-user information parameter in the outgoing ITU-T SS7 IAM.

The presentation of a functional number in the User-to-user information parameter of an SS7 call is described in section 5.1 of ETSI TS 102 610 V1.1.0 (2008-01), whilst the format of the `Aculab-Functional-Number` header is described in section F.5.

To enable Functional Number mapping refer to section 8.6.7.

14.7 ISDN subaddress mapping

GroomerII supports mapping of called, calling and connected party ISDN subaddresses using the `isub` URI parameter. The `isub` parameter is described in IETF RFC 3966, and is extended by the addition of the `isub-encoding` parameter described in IETF RFC 4715.

RFC 4715 does not support the user specified subaddress type, and a private extension of has been implemented to accommodate these. When transporting a user defined subaddress the `isub-encoding` parameter is set to `acu-user`. The first character in the `isub` parameter must be 0 or 1 to indicate the setting of the odd/even indicator bit in octet 3, with the remaining characters being hexadecimal digit pairs containing the settings of octet 4 onwards. This is illustrated in the following diagram using the calling party subaddress as an example. The called and connected party subaddresses are coded in an identical way.

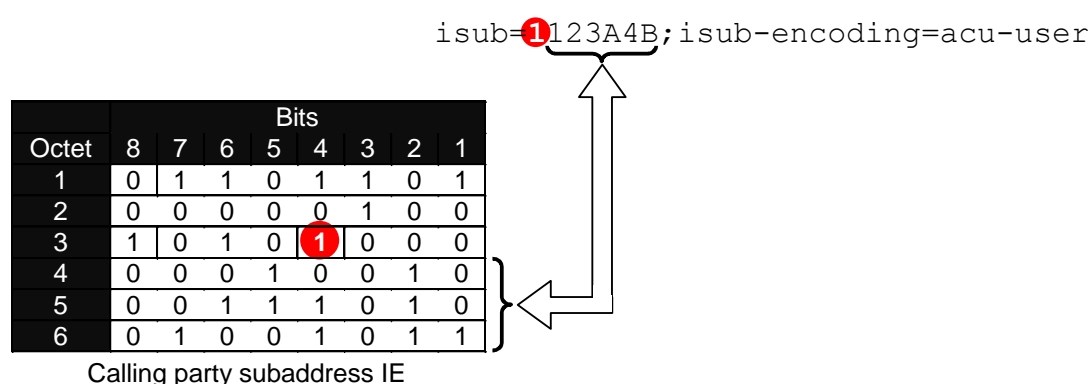


Figure 14-1 User defined ISDN subaddress extension

14.8 Interworking with TDM protocols

14.8.1 Interworking between SIP and SS7

Interworking between SIP and SS7 is carried out as described in the following specifications.

SS7 variant	Interworking specification
ANSI (1995 and 2005 variants)	ANSI T1.769-2004. The NENA i3 modification may be applied using the configuration option in the Protocol Settings screen, section 8.6.7 refers.
ITU-T	ITU-T Recommendation Q.1912.5.
China	ITU-T Recommendation Q.1912.5.
UK ISUP	NICC Document ND1017:2006/07

14.8.2 Interworking between SIP and ETS 300

Interworking between SIP and ETS 300 is based upon ETSI TS 183 036. This includes:

- Mapping of the calling party number to/from the `P-Asserted-Identity` header, including support for the `Privacy` header.
- Mapping of the additional calling party number (when present).
- Mapping of clearing causes to/from the `Reason` header.

14.8.3 Interworking between SIP and CAMA

Interworking between SIP and CAMA is described in section 16.2.

14.9 Additional IETF RFC support

GroomerII supports the production and/or interpretation of optional headers specified in the following IETF RFCs.

- RFC 3891 The Session Initiation Protocol (SIP) “Replaces” Header.
- RFC 4244 Request History Information, see section 8.6.7 for further information.
- RFC 4412 SIP Resource Priority, see section 17.3 for further information.
- RFC 4715 The Integrated Services Digital Network (ISDN) Subaddress Encoding Type for tel URI. RFC 4715 has been extended by Aculab, see section 14.7 for details. RFC 4715 carries implied support for the `isub` parameter described in RFC 3966.
- RFC 4904 Representing Trunk Groups in tel/sip URIs, see section 8.6.7 for further information.

When interworking with ANSI SS7, GroomerII also supports the `P-Charge-Info` header as described in IETF Internet Draft draft-york-sipping-p-charge-info-08. Information is automatically mapped between the `P-Charge-Info` header and the SS7 Charge Number parameter.

GroomerII also uses the `Remote-Party-ID` header described in IETF Internet Draft draft-ietf-sip-privacy-04 to carry name identification information. See section 17.1 for further information.

GroomerII supports the transfer of user-to-user information with the `User-to-User` header specified in IETF Internet Draft draft-ietf-cuss-sip-uui-09. See section 17.2 for further information.

15 SS7 telephony

If you are using SS7 on your GroomerII, you will need to configure:

- The SS7 links using the SS7 stack file
- The SS7 link protocol firmware timeslot usage.

The SS7 stack file is named `ss7.cfg`, and is located in the directory `C:\Program Files (x86)\Aculab\v6\bin`. It can be modified, as described in section 15.1 below, using any standard text editor such as notepad.

Making SS7 protocol selections for SS7 Signalling and ISUP Bearer timeslot usage is documented in section 4.4.3.

15.1 SS7 stack file

The SS7 stack file will be loaded by the Kernel at startup, and cannot be reloaded without restarting GroomerII. The stack file will always be loaded, even if SS7 is not in use. Unless your GroomerII was supplied pre-configured with SS7 – in which case a suitably configured stack file will be included – then an empty stack file will be provided, which will be loaded whenever GroomerII is started.

When the stack file is loaded, in order to identify the success or failure of the operation, the message `SS7 STACK FILE LOADED` or `SS7 STACK FILE FAILED TO LOAD`, will be written to the Maintenance Messages screen in the Kernel main dialog.

A number of the optional stack file settings are essential for GroomerII to operate correctly. All such parameters are pre-configured to their required settings in the file `GroomerII.cfg`, located in the directory `C:\Program Files (x86)\Aculab\v6\ss7`. This file must be imported into `ss7.cfg` by using the following as the first non-comment line

```
include "..\ss7\GroomerII.cfg"
```

NOTE

If you are upgrading your GroomerII application software from an earlier version it will be necessary to add this line to your existing `ss7.cfg` file if it is not already present. New systems will be shipped with this line already present in the file.

Many of the entries in the SS7 stack file replace firmware switches that were previously present, and as such the stack file can become very complicated. In most cases however, only a very simple stack file is required. This section shows the stack files that would be required for the most popular GroomerII SS7 configurations. Should you need to write a stack file for a different configuration, or need to use additional parameters, contact Aculab support for assistance.

A stack file contains one [SP] section for each unique OPC/DPC pair

```
[SP]
  LocalPC=aaaaa
  NI=x
  [ISUP]
    variant=vvv
  [EndISUP]
  [MTP3]
    variant=vvv
    [DESTINATION]
      RemotePC = bbbbb
    [EndDESTINATION]
  [EndMTP3]
[EndSP]
```

Two mandatory and two optional parameter are required

Mandatory

LocalPC=aaaaa

specifies the point code used by GroomerII for the particular signalling link.

RemotePC=bbbbbb

specifies the point code of the remote SP or STP to which GroomerII is physically connected.

Optional

NI=x

This is the SS7 network indicator, and will be in the range 0 to 3. If this parameter is omitted the default of NI=0 will be applied. The value to be used in this parameter must be obtained from you service provider, and in most instances will be either:

0 - International network

2 - National network

variant=vvv

This is the protocol variant used by ISUP and MTP3, and must be specified separately in each section. The combination of values currently supported is shown in the following table.

[ISUP] section	[MTP3] section
ITU_UKISUP_2001	ITU
ITU	ITU
CHINA	CHINA
ANSI	ANSI
ANSI_2005	ANSI

If this parameter is omitted the default of variant=ITU will be applied.

Unsupported parameters

GroomerII does not support use of the following stack file parameters.

<code>default_cpc=n</code>	This parameter specifies the value that will be used in the Calling party's category parameter if no setting is provided by application program. The GroomerII application always sets the Calling party's category and so using this parameter will have no effect.
<code>auto_inf=y</code>	This setting instructs the SS7 driver to respond to an INR with an INF. The GroomerII application will respond to all INR messages. The behaviour if this parameter is included is undefined.
<code>report_non_q931_cause=n</code>	This setting instructs the SS7 driver to convert any non ITU-T standardised causes to ITU-T cause 127 (Interworking, unspecified). This will prevent GroomerII from mapping and reporting non ITU-T standardised causes correctly.
<code>continuity_defer_event=y</code>	This setting prevents the GroomerII application from being notified of in-call continuity checks until they have been completed. If this parameter is included continuity checks will not be reported to the call control log.
<code>apply_continuity_loop=y</code>	This setting instructs the SS7 driver to apply a voice path loop to incoming continuity checks. This may override the switching carried out by the GroomerII application and cause the continuity check to fail.
<code>continuity_check_output_value</code>	This setting is associated with the use of <code>apply_continuity_loop</code> . The behaviour should this parameter be set to a value other than <code>none</code> is undefined.
<code>ccr_application=n</code>	This setting instructs the SS7 driver not to inform the GroomerII application when an inbound CCR is received. If the parameter is included, the GroomerII application will be unable to process inbound CCR messages.
<code>ccr_auto_lpa=y</code>	This setting is only applicable to ANSI SS7, and instructs the SS7 driver to automatically send an LPA upon receipt of a CCR. The GroomerII application will send an LPA in response to a CCR. The behaviour if this parameter is included is undefined.

System X interworking

Some versions of System X exhibit problems if large numbers of ISUP circuit related housekeeping messages are received simultaneously. GroomerII can be configured to throttle delivery of such messages by using the `system_x_throttle_rate` and `system_x_throttle_limit` parameters in the `[ISUP]` section of the stack.

When throttling is enabled the delivery rate of the following messages will be restricted

UPT User part test

BLO	Blocking
UBL	Unblocking
CGB	Circuit group blocking
CGU	Circuit group unblocking
RSC	Reset circuit
GRS	Circuit group reset

Throttling is implemented by accumulating credits into a buffer at the rate of one per millisecond. The maximum value of this buffer (which is also the initial value) is configured using the `system_x_throttle_limit` parameter. A message credit value is configured using the `system_x_throttle_rate` parameter. Each time a throttled message is dispatched the credit buffer is decremented by the message credit value. The credit buffer is checked continuously and a message dispatched whenever its value is zero or greater. Sending a message when the credit buffer has a value of zero will cause the buffer to be decremented to a negative value, and no further messages will be sent until the buffer has been incremented back to zero.

The following example will send five messages immediately upon startup (one each at 200, 150, 100, 50 and zero), or after a period of idle, and thereafter one message every 50 milliseconds.

```
[SP]
...
[ISUP]
    variant=ITU_UKISUP_2001
    system_x_throttle_rate=50
    system_x_throttle_limit=200
[EndISUP]
...
[EndSP]
```

Using the settings `system_x_throttle_rate=50` and `system_x_throttle_limit=0` will avoid a burst of messages at startup/idle, and will dispatch each message at 50ms intervals.

Removing the `system_x_throttle_rate` and `system_x_throttle_limit` parameters from a stack will disable throttling.

Disabling group messages

Some SS7 switches can be configured to refuse group reset and/or blocking messages. GroomerII can be configured to send a series of individual circuit messages in place of a group message in such circumstances by using the `send_group_reset_messages` and `send_group_block_messages` parameters. The following example illustrates how to use these parameters.

```
[SP]
...
[ISUP]
    send_group_reset_messages=never
    [DESTINATION]
        send_group_block_messages=never
        RemotePC=7070
    [EndDESTINATION]
[EndISUP]
...
[EndSP]
```

Placing the parameter in the `[ISUP]` section will cause it to be applied to all destination point codes in that section, whether implicitly or explicitly declared.

Placing the parameter inside a [DESTINATION] section will apply the setting to that destination point code only.

The `send_group_reset_messages` parameter will replace a GRS with a series of RSC messages.

The `send_group_block_messages` parameter will replace a CGB with a series of BLO, and a CGU with a series of UBL. Hardware blocking (ITU-T/UK ISUP/China) and blocking with immediate release (ANSI) must be signalled using a CGB, even when only a single circuit is being blocked. The procedure applied here is for the CGB to be replaced by an appropriate series of BLO, and on any circuit carrying an active call the BLO will be preceded by an RSC.

Example 1

GroomerII uses one link (one or more trunks) to connect to a Signalling Point (SP) or Signalling Transfer Point (STP)

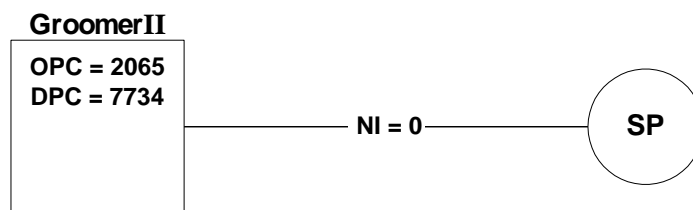


Figure 15-1 Single SS7 link option

The stack file would be

```

[SP]
  LocalPC=2065
  NI=0
  [ISUP]
    variant=ITU_UKISUP_2001
  [EndISUP]
  [MTP3]
    variant=ITU
    [DESTINATION]
      RemotePC = 7734
    [EndDESTINATION]
  [EndMTP3]
[EndSP]
  
```

Example 2

GroomerII uses two links (each with one or more trunks) to connect to a two different Signalling (Transfer) Points, using a different OPC's on each link. The system is configured as a signalling gateway.

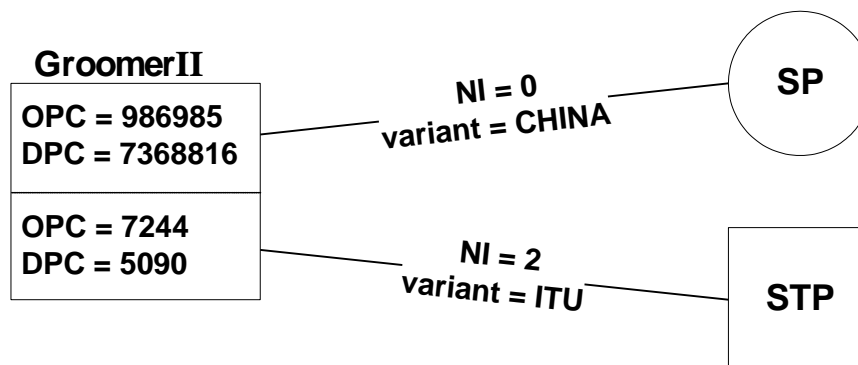


Figure 15-2 Two SS7 links option

The stack file would be

```
[SP]
  LocalPC=986985
  NI=0
  [ISUP]
    variant=CHINA
  [EndISUP]
  [MTP3]
    variant=CHINA
    [DESTINATION]
      RemotePC = 7368816
    [EndDESTINATION]
  [EndMTP3]
[EndSP]
[SP]
  LocalPC=7244
  NI=2
  [ISUP]
    variant=ITU
  [EndISUP]
  [MTP3]
    variant=ITU
    [DESTINATION]
      RemotePC = 5090
    [EndDESTINATION]
  [EndMTP3]
[EndSP]
```

Example 3

GroomerII uses a single link (one or more trunks) in a loopback configuration for testing purposes.

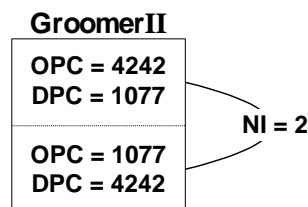


Figure 15-3 Single SS7 link looped back option

The stack file would be

```
[SP]
  LocalPC=4242
  NI=2
  [ISUP]
    variant=ANSI
  [EndISUP]
  [MTP3]
    variant=ANSI
    [DESTINATION]
      RemotePC = 1077
    [EndDESTINATION]
  [EndMTP3]
[EndSP]
[SP]
  LocalPC=1077
  NI=2
  [ISUP]
    variant=ANSI
  [EndISUP]
  [MTP3]
    variant=ANSI
    [DESTINATION]
```

```

RemotePC = 4242
[EndDESTINATION]
[EndMTP3]
[EndSP]

```

15.2 SS7 port firmware configuration

It is possible to configure non-provisioned SS7 ports that carry neither signalling links nor bearer channels. To create a non-provisioned port load the SS7 firmware (`ss7.pmx`) to the port with either no firmware switches (ITU-T, China and UK ISUP) or with only the `-cT1` switch (ANSI SS7) applied. These ports can subsequently be partly or fully provisioned by adding signalling links and/or bearer channels and reloading the firmware (see section 5.12).

NOTE

When configuring SS7 ports care must be taken to ensure that the bearer channels at each end of the trunk are identically configured, as mismatching configurations will prevent the circuit group reset (GRS) from completing. GroomerII cannot detect this condition, which may result in incorrect reporting by the GroomerII Traffic Monitor and/or attempts to place calls on bearer channels that are not in service.

15.3 Continuity checking

GroomerII supports inbound and outbound continuity checks when using the ITU-T and ANSI variants.

Both 2-wire and 4-wire continuity checks are supported. The type of continuity check to be used by each trunk must be selected in the Port Configuration window (see section 8.3.2). The default action is to use a 4-wire (Loopback) continuity check.

The tones used for continuity checking depend on the variant of SS7 being used by a circuit. The table below shows the tones used by GroomerII.

Variant and continuity check type	Outbound IAM or CCR	Inbound IAM or CCR
ITU-T/4-wire (Loopback)	Tone to send: 2000Hz Tone to detect: 2000Hz	Voice path loopback applied.
ITU-T/2-wire (Transponder)	Tone to send: 2000Hz Tone to detect: 1780Hz	Tone to detect: 2000Hz Tone to send: 1780Hz
ANSI/4-wire (Loopback)	Tone to send: 2010Hz Tone to detect: 2010Hz	Voice path loopback applied.
ANSI/2-wire (Transponder)	Tone to send: 2010Hz Tone to detect: 1780Hz	Tone to detect: 2010Hz Tone to send: 1780Hz

Inbound continuity checks

Inbound continuity checks, whether requested by an IAM or a CCR, are handled automatically without the need for additional configuration.

Outbound in-call continuity checks

GroomerII may be configured to perform outgoing continuity checks for all calls made on a route (see section 8.5.3), and to re-route the call should the continuity check fail (see section 8.5.7). If a call is routed to a circuit that fails an outgoing continuity

check, the circuit will be placed into the recheck state. GroomerII will automatically perform periodic continuity checks for circuits that are in the recheck state until a pass result is achieved or until the circuit is taken out of the recheck state for another reason. Whilst in the recheck state it will not be possible to route calls to the circuit. Circuits remain in the recheck state indefinitely until one of the following occurs:

- GroomerII performs a periodic continuity check that passes.
- The operator uses the Continuity Check dialog to perform a continuity check test call that passes.
- The circuit is reset.
- An incoming IAM is received.
- GroomerII is restarted or the SS7 firmware is reloaded.

Continuity check test calls

Outbound continuity check test calls (CCR) can be made on individual circuits using the Continuity Check dialog described in section 5.15.

16 CAMA telephony

CAMA is a pseudonym used to describe the MF and Enhanced MF signalling specified by the National Emergency Number Association (NENA) for use in an E911 environment. There are four distinct variants of CAMA, which are described in the following specifications:

NENA 03-502 (April 2003)	Trunking for Private Switch 9-1-1 Service
NENA 03-002 (January 2007)	Enhanced MF Signalling, E9-1-1 Tandem to PSAP

Each specification describes both single number (calling party number (ANI) only) and dual number (called party and calling party number (ANI)) signalling variants.

16.1 Configuration

16.1.1 Signalling firmware configuration

CAMA has been implemented as a variant of the Aculab T1 Robbed Bit protocol. Each CAMA port should be loaded with the `t1rb.pmx` firmware, and the appropriate configuration switch from the table below applied in addition to the mandatory switches (-s59,1 –s96,1 –s99,224). With the exception of the `-cMD` switch described in section 16.3, no other firmware switches should be applied.

Firmware switch	CAMA variant
-s60,1	CAMA 2003 single number (calling party number (ANI) only). Only single numbers can be signalled when this switch is applied.
-s60,2	CAMA 2003 dual number. Only dual numbers can be signalled when this switch is applied.
-s60,3	CAMA 2007 single number (calling party number (ANI) only). CAMA 2007 dual number. The signalling arrangements for CAMA 2007 differentiate between the single and dual number variants. This switch will allow both variants to be used on the same trunk simultaneously.

16.1.2 GroomerII application configuration

16.1.2.1 Port configuration

When an incoming call is received, the GroomerII application software collects the dialled digits using the ST/STP digits as an indication that dialling is complete. To ensure that the call is only routed on completion of dialling, the Call Routing controls on the Incoming page of the Port Configuration screen must always be configured as follows:

Minimum Digits – This must be set to zero.

Maximum Digits – This must be set to zero.

Inter-Digit Timeout – This must be set to zero.

Route on End of Send – This must be enabled.

The following diagram illustrates these settings.

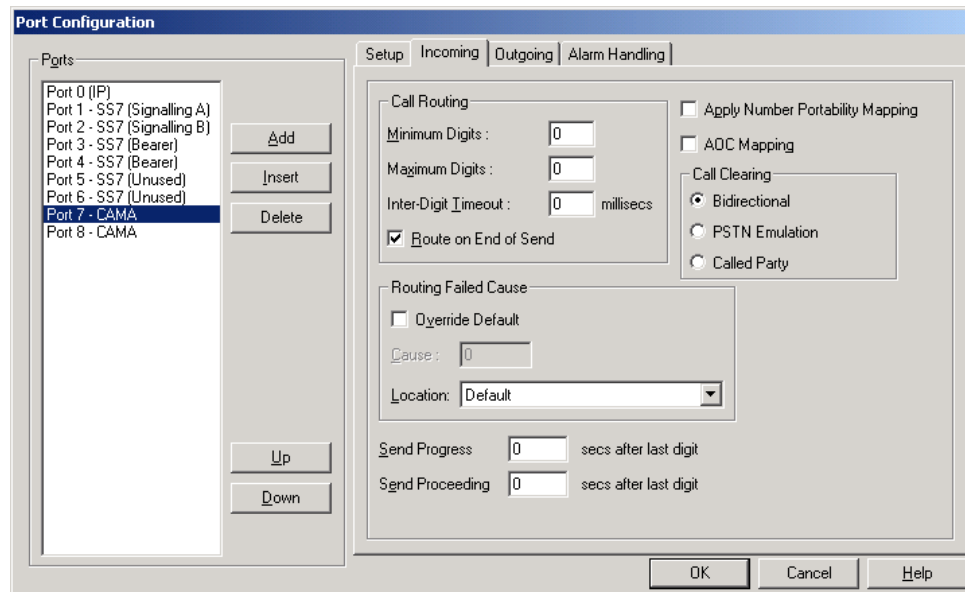


Figure 16-1 CAMA port configuration settings

16.1.2.2 Route configuration

When processing an incoming CAMA call, the KP and ST/STP digits will automatically be removed from the called and/or calling party numbers. Unlike some other Aculab CAS protocols, there is no need to accommodate these digits in the Dest Addr and Orig Addr masks in the routing table. The information digits (I or II) are not automatically removed from the dialled number, and must be removed using the routing table. See section 8.5.2 for an explanation of number translation.

When making an outgoing CAMA call, the KP and SP/STP digits will automatically be added to the called and/or calling party numbers. Unlike some other Aculab CAS protocols, there is no need to add these digits in the Dest Addr and Orig Addr masks in the routing table.

16.2 Interworking with CAMA

16.2.1 CAMA to SIP Interworking

All interworking from CAMA to SIP will be carried out in accordance with NENA 08-003 – Detailed Functional and Interface Specification for the NENA i3 Solution – Stage 3, where GroomerII will perform the role of a Legacy Network Gateway. The following behaviour is drawn to the attention of users.

When the incoming CAMA call does not present a called party number, the destination IP address alone will be used in the SIP Request-URI and To headers. If a called party number is required in the SIP INVITE, it should be inserted using the GroomerII routing table.

The incoming calling party number, after translation by the GroomerII routing table, will be presented in a P-Charge-Info header, with the From header containing only the IP address of the GroomerII host port.

16.2.2 SIP to CAMA Interworking

NENA 03-008 does not specify procedures for interworking from SIP to CAMA, and general GroomerII procedures for interworking from SIP to non-SS7 TDM calls will be applied. Specifically the called party number used in the outgoing CAMA call will be taken from either the `P-Asserted-Identity` or `From` header in the SIP INVITE (see section 8.5.2 for an explanation of which header will be used). Any `P-Charge-Info` header presented by the SIP INVITE will be ignored.

A call transfer request received from the CAMA side can be mapped to the SIP side as described in section 12.3.

16.2.3 Interworking between CAMA and TDM

All interworking between CAMA and other TDM protocols will be carried out using general GroomerII procedures.

When interworking from TDM to CAMA it should be noted that the Aculab implementation of CAMA supports en-bloc dialling only, overlapped dialling is not supported. All dialled digits from the incoming TDM call must be collected before the call is routed. See section 0 for an explanation of collecting dialled digits before routing a call.

16.3 Disabling incoming CAMA call clearing

In some situations it is desirable to prevent the calling party from clearing a call, and this can be achieved when interworking from CAMA to SIP.

This feature is available once the call has reached the connected state. When enabled and the calling party enters the on-hook condition, the outgoing SIP call leg is maintained and the idle pattern inserted onto the forward voice path. Should the calling party return to the off-hook condition, bidirectional speech between the two parties is restored. The feature can be invoked repeatedly on the same call, which will only be cleared when the outgoing SIP call leg signals a disconnect.

This feature requires the `-CMD` configuration switch to be applied when downloading the signalling firmware to a CAMA port, and the Called Party radio button in the Call Clearing group on the Incoming page of the Port Configuration screen to be selected.

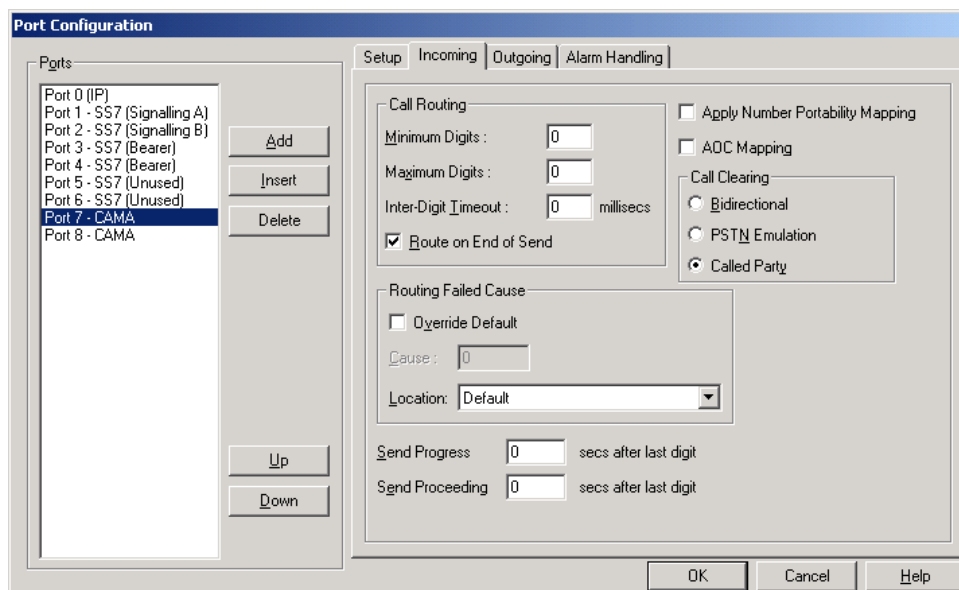


Figure 16-2 CAMA port configured for called party only call clearing

When a CAMA port is configured for called party clearing and the outgoing call leg is not a SIP call, bidirectional clearing will be applied and either party will be allowed to clear the call.

17 Interworking supplementary services

GroomerII supports interworking of a number of supplementary services between protocols. The following sections describe the ISDN and/or SIP support available for such services.

NOTE

This section describes those supplementary services where support has been implemented in only a limited number of protocols. Where a supplementary service is implemented by all supported protocols, it is documented more generally throughout this guide. Calling party number is an example of such a service.

17.1 Name identification supplementary services (CNIP/CONP)

The calling name identification presentation (CNIP) and connected name identification presentation (CONP) services can be interworked between Q.SIG and SIP.

17.1.1 Q.SIG

The CNIP and CONP services are implemented for the Q.SIG protocol as described in ECMA-164.

NOTE

The name identification supplementary service must be enabled by applying the `-cFNP` configuration switch when downloading the signalling firmware to a Q.SIG port.

17.1.2 SIP

CNIP/CONP information is transported in SIP using the `Remote-Party-ID` header. The `Remote-Party-ID` header is described in IETF Internet Draft `draft-ietf-sip-privacy-04`, and has the form:

```
Remote-Party-ID: "John Smith" <1234@192.168.1.100>;party=calling;
id-type=subscriber;privacy=name;screen=no
```

17.1.3 Q.SIG to Q.SIG interworking

Interworking CNIP/CONP information between two Q.SIG call legs is achieved by copying the calling/connected name component unmodified between the incoming and outgoing call legs.

17.1.4 Interworking between Q.SIG and SIP

The mapping of CNIP/CONP information between Q.SIG messages and SIP requests/responses is illustrated below.

SETUP + callingName	↔	INVITE Remote-Party-ID: party=calling
ALERTING + calledName	↔	180 Ringing Remote-Party-ID: party=called
CONNECT + connectedName	↔	200 Ok Remote-Party-ID: party=called
DISCONNECT + busyName	↔	3xx/4xx/5xx/6xx Remote-Party-ID: party=called

Mapping is only performed when an inbound CNIP/CONP component or `Remote-Party-ID` header of the correct type is received, otherwise the information is discarded.

The name information is mapped unmodified between the display parameter in the `Remote-Party-ID` header and the `NameData` field in the calling/connected name component.

When sending an outgoing `INVITE` the URI in the `Remote-Party-ID` header will be the same as that in the `Request-URI`. When sending a backward SIP request/response the URI will be the same as that received in the forward `From` header.

The `privacy` parameter in the `Remote-Party-ID` header will be set according to the following table when mapping from Q.SIG to SIP.

Q.SIG name presentation	privacy parameter
namePresentationRestrictedSimple namePresentationRestrictedExtended namePresentationRestrictedNull	privacy=name
namePresentationAllowedSimple namePresentationAllowedExtended	No privacy parameter included.

Name presentation will be set according to the following table when mapping from SIP to Q.SIG.

privacy parameter	Q.SIG name presentation
privacy=name privacy=full	namePresentationRestrictedSimple
All other values, or no privacy parameter.	namePresentationAllowedSimple

GroomerII does not process the `URI`, `id-type` and `screen` parameters in an incoming `Remote-Party-ID` header.

GroomerII will not include the `id-type` and `screen` parameters in an outgoing `Remote-Party-ID` header.

17.1.5 SIP to SIP interworking

A `Remote-Party-ID` header presented in an `INVITE` request/response will be passed unmodified between incoming and outgoing call legs.

17.2 User to user signalling (UUS)

GroomerII is able to map user-to-user service requests (UUS) and user-to-user information (UUI) between the ETS 300, SS7 and SIP protocols.

17.2.1 ETS 300

The user-to-user signalling service 1 (UUS1), described in ETS 300 286-1, is supported by the ETS 300 protocol as described in the sections below.

NOTE

The UUS supplementary service must be enabled by applying both the `-cFU` and `-cDAUUS` configuration switches when downloading the signalling firmware to an ETS 300 port.

If an incoming ETS 300 call requests UUS2 and/or UUS3 activation and either request is for required activation then the incoming call will be disconnected with clearing cause #50 (Requested facility not subscribed), otherwise the first appropriate backward message will carry a rejection response and the call will be allowed to proceed.

NOTE

Some legacy ETS 300 equipment imposes a limit of 35 octets on the length of a User-user information element. By default GroomerII supports the current 131 octet standard. Applying the `-s8,1` switch when downloading the ETS 300 signalling firmware will truncate all outgoing User-user information elements to 35 octets. No truncation is carried out on incoming User-user information elements.

NOTE

Incoming ETS 300 calls that have requested explicit UUS1 activation cannot be re-routed. Call re-routing is described in section 8.5.7.

17.2.2 SS7

The user-to-user signalling service 1 (UUS1), described in Q.737.1, is supported by the SS7 protocol as described in the sections below.

NOTE

GroomerII does not support the user-to-user signalling service when using the ANSI variants of SS7.

If an incoming SS7 call requests UUS2 and/or UUS3 activation and either request is for required activation then the incoming call will be disconnected with clearing cause #50 (Requested facility not subscribed), otherwise the first appropriate backward message will carry a rejection response and the call will be allowed to proceed.

NOTE

Incoming SS7 calls that have requested explicit UUS1 activation cannot be re-routed. Call re-routing is described in section 8.5.7.

17.2.3 SIP

GroomerII supports the transfer of user-to-user information in the setup and disconnect phases of a SIP call. This is implemented using the `User-to-User` header described in IETF Internet Draft draft-ietf-cuss-sip-uu-09. An example of the `User-to-User` header is:

```
User-to-User: 001234ABCD;encoding=hex;purpose=foo;content=bar
```

Including the `User-to-User` header as a parameter in a redirection URI is not supported.

17.2.4 ETS 300 to ETS 300 interworking

The UUIE is mapped unmodified between the incoming and outgoing call legs with the following rules applied.

If the incoming SETUP contains a UUIE then this will be mapped unmodified to the outgoing call leg, otherwise a UUIE with an empty User Information parameter will be inserted into the outgoing call leg to invoke an implicit UUS1 service.

The mapping of UUI between PROGRESS messages is supported. However, if an explicit UUS request has been made and a UUIE is received in a backward PROGRESS message ahead of the explicit UUS response, then that UUIE will be discarded.

17.2.5 SS7 to SS7 interworking

The User-to-user information parameter is mapped unmodified between the incoming and outgoing call legs.

17.2.6 Interworking between ETS 300 and SS7

Interworking between SS7 and ETS 300 is based upon the procedures described in ITU-T Recommendation Q.699.

17.2.7 Interworking between ETS 300 and SIP

Interworking between ETS 300 and SIP is based upon the procedures described in ETSI TS 183 036.

The mapping of UUI between ETS 300 messages and SIP requests/responses during call setup is illustrated below.

SETUP	↔	INVITE
PROGRESS	↔	183 Session Progress
ALERTING	↔	180 Ringing
CONNECT	↔	200 Ok
DISCONNECT	↔	3xx/4xx/5xx/6xx

The mapping of UUI between ETS 300 messages and SIP requests/responses during normal call clearing initiated by the ETS 300 side is illustrated below.

DISCONNECT	→	BYE
RELEASE	←	200 Ok

The mapping of UUI between ETS 300 messages and SIP requests/responses during normal call clearing initiated by the SIP side is illustrated below.

DISCONNECT	←	BYE
RELEASE	→	200 Ok

Mapping of UUI to and from RELEASE COMPLETE messages is not supported.

The following table describes how GroomerII uses the parameters in the User-to-User header.

Parameter	Application
UII data	This is a concatenation of the protocol discriminator and UII data, in hexadecimal form. The first two digits are the protocol discriminator and the remaining digits are the UII data.
encoding	When present in an inbound header this parameter must be in the form <code>encoding=hex</code> , otherwise the header will be discarded. If the parameter is not present in an inbound header <code>encoding=hex</code> will be assumed. This parameter will always be included in outbound headers in the form <code>encoding=hex</code> .
purpose	When present in an inbound header this parameter is discarded. It will not be included in an outbound header.
content	When present in an inbound header this parameter is discarded. This parameter may optionally be included in outbound headers, see section 8.6.7 for details.

When interworking from ETS 300 to SIP, and the incoming call leg requests explicit UUS1 activation, GroomerII will automatically send an accepted response in the first appropriate backward message.

17.2.8 Interworking between SS7 and SIP

There are no formal procedures specified for interworking the UUS service between SS7 and SIP. The procedures adopted are similar to those applied when interworking between ETS 300 and SIP.

The mapping of UII between SS7 messages and SIP requests/responses during call setup is illustrated below.

IAM	↔	INVITE
ACM/PRG ¹	↔	183 Session Progress
ACM/PRG ²	↔	180 Ringing
ANM/CON	↔	200 Ok
REL	↔	3xx/4xx/5xx/6xx

¹ When there is no subscriber free/alerting indication.

² When subscriber free/alerting is indicated.

The mapping of UII between SS7 messages and SIP requests/responses during normal call clearing is illustrated below.

REL	↔	BYE
-----	---	-----

Mapping of UII to and from a 200 Ok at this stage is not supported.

The table in section 17.2.7 describes how GroomerII uses the parameters in the User-to-User header.

When interworking from SS7 to SIP, and the incoming call leg requests UUS1 activation, GroomerII will automatically send an accepted response in the first appropriate backward message.

When interworking between SS7 and SIP with Functional Number mapping enabled:

- If the incoming IAM includes a User-to-user information parameter containing a Functional Number, both `Aculab-Functional-Number` and `User-to-User` headers will be included in the outgoing `INVITE`.
- If the incoming `INVITE` contains both `Aculab-Functional-Number` and `User-to-User` headers, the `Aculab-Functional-Number` header will be mapped into the User-to-user information parameter in the outgoing IAM and the `User-to-User` header discarded.

See section 14.6 for a description of Functional Numbers.

17.2.9 SIP to SIP interworking

A `User-to-User` header presented in `INVITE` requests and responses, or `BYE` requests and responses will be passed unmodified between incoming and outgoing call legs.

17.3 Multi level precedence and pre-emption (MLPP)

GroomerII is able to map MLPP service requests between the ETS 300, Q.SIG and SIP protocols. MLPP service requests are mapped transparently, and neither management nor enforcement of is performed.

17.3.1 ETS 300 and Q.SIG

The MLPP supplementary service for ETS 300 and Q.SIG is based upon ITU-T Recommendation Q.955.

The Look-ahead For Busy (LFB) query described in Q.955 is not supported, and such queries are discarded.

17.3.2 SIP

MLPP service requests are mapped in SIP calls using the `Resource-Priority` header described in IETF RFC 4412. An example of the `Resource-Priority` header is:

```
Resource-Priority: q735.4
```

The single parameter is composed of a namespace and priority value in the form `namespace.priority`. In the above example `q735` is the namespace and `4` is the priority.

GroomerII will only process a `Resource-Priority` header presented in an `INVITE`. If a `Resource-Priority` header is presented in any other request, or any request response, it will be discarded.

GroomerII will only insert a `Resource-Priority` header into an outbound `INVITE`.

The `resource-priority` option tag is not supported.

17.3.3 ETS 300/Q.SIG to ETS 300/Q.SIG interworking

The MLPP request will be mapped unmodified between the incoming and outgoing `SETUP` messages, with the exception that the MLPP Service Domain for the outgoing call leg may be modified as described in section 8.5.3.

The MLPP request response will be mapped unmodified between the `ALERTING` message received from the outgoing call leg and the `ALERTING` message sent to the incoming call leg.

NOTE

Calls requesting MLPP that bypass the ringing stage (for example by moving directly to the connected stage) will be allowed to proceed, although the requested MLPP support is unlikely to be enforced.

If the outgoing call is disconnected with a clearing cause other than #8 before the ringing stage has been reached, the clearing cause along with any MLPP request response in the DISCONNECT and RELEASE messages will be mapped unmodified to the incoming call leg.

If either call leg receives a DISCONNECT message with clearing cause #8 (Preemption) then:

- If the MLPPCallpreemption component in the inbound DISCONNECT message is set to circuitReservedForReuse, the timeslot carrying that call will be reserved for 12 seconds to receive the incoming preempting call.
- A DISCONNECT message will be sent to the opposite call leg using clearing cause #8, with the MLPPCallpreemption component set to circuitNotReservedForReuse.
- The MLPP information in the subsequent RELEASE message will be mapped unmodified between the two call legs.

NOTE

The incoming pre-empting call will be treated as a new call and routed in the normal fashion.

17.3.4 ETS 300/Q.SIG to SIP interworking

When interworking from ETS 300/Q.SIG to SIP, a `Resource-Priority` header with a `q735` namespace will be included in the outgoing `INVITE`, with the priority determined by the Q.955 precedence level in the MLPP request. The following table illustrates the mapping between the precedence levels defined in Q.955 and the priority values in the `q735` namespace defined in RFC 4412.

Q.955 precedence	RFC 4412 priority
flashOverride (0)	q735.0
flash (1)	q735.1
immediate (2)	q735.2
priority (3)	q735.3
routine (4)	q735.4

When the SIP call reaches the ringing stage, an `ALERTING` message will be sent to the incoming call leg with an MLPP request response of `successCalledUserMLPPSubscriber`.

If the SIP call leg is cleared before the ringing stage is reached and the response includes a `Reason` header specifying a Q.850 cause of #8 (Preemption) or #46 (Precedence call blocked), a DISCONNECT message will be sent to the incoming call using that Q.850 clearing cause and an MLPP request response as shown in the table below.

Q.850 cause	MLPP request response
8	failureCaseB
46	failureCaseA

If the SIP call leg is cleared after the ringing stage is reached, and the `INVITE` response or `BYE` includes a `Reason` header specifying a Q.850 cause of #8, a `DISCONNECT` message will be sent to the incoming call with clearing cause #8 and an MLPP request response of `circuitNotReservedForReuse`.

When the incoming call leg is cleared at any stage with clearing cause #8 a `Reason` header will be included in the `CANCEL/BYE` specifying Q.850 cause #8, and if the `MLPPCallpreemption` component in the `DISCONNECT` message is set to `circuitReservedForReuse` the timeslot will be reserved for 12 seconds to receive the preempting call.

NOTE

The incoming pre-empting call will be treated as a new call and routed in the normal fashion.

In all other circumstances standard call clearing will be used.

17.3.5 SIP to ETS 300/Q.SIG interworking

The `Resource-Priority` header presented by the SIP `INVITE` must contain a `q735` namespace, otherwise the header will be discarded and MLPP will not be requested.

The outgoing call will be made with an `MLPPCallRequest` component initialized as follows:

- The MLPP service domain will be set according to the GroomerII routing table (see section 8.5.3).
- The precedence level will be set using the table in section 17.3.4 above.

If the outgoing call leg is disconnected with clearing cause #46 (Precedence call blocked), the `INVITE` response sent to the incoming SIP call will include a `Reason` header specifying Q.850 cause #46.

If the outgoing call leg is disconnected with clearing cause #8 (Preemption) the `INVITE` response/`BYE` sent to the incoming SIP call will include a `Reason` header specifying Q.850 cause #8, and if the `MLPPCallpreemption` component in the `DISCONNECT` message is set to `circuitReservedForReuse` the timeslot will be reserved for 12 seconds to receive the preempting call.

NOTE

The incoming pre-empting call will be treated as a new call and routed in the normal fashion.

When the SIP call leg is cleared and the `CANCEL/BYE` includes a `Reason` header specifying Q.850 cause #8, a `DISCONNECT` will be sent to the outgoing call leg with clearing cause #8 and an `MLPPCallpreemption` component set to `circuitNotReservedForReuse`.

In all other circumstances standard call clearing will be used.

17.3.6 SIP to SIP interworking

A `Resource-Priority` header presented in an `INVITE` request will be passed unmodified between incoming and outgoing call legs.

17.3.7 Interworking to protocols without MLPP support

If an incoming ETS 300/Q.SIG call containing an MLPP request is routed to a protocol that does not have MLPP support, GroomerII will return a request response of `successCalledUserNotMLPPSubscriber` in the ALERTING message, and the call will be allowed to proceed.

SIP has no mechanism to indicate that a called user is not an MLPP subscriber. If an incoming SIP INVITE containing a `Resource-Priority` header is routed to a protocol that does not have MLPP support, then the `Resource-Priority` header will be discarded and the call will be allowed to proceed.

17.3.8 Call diversion and re-routing

If an incoming MLPP call is re-routed or diverted and the new outgoing call is made using a protocol with MLPP support, an MLPP request will be included in the new outgoing call.

If the re-routing/diversion takes place before the ringing stage has been reached, then all MLPP responses will be mapped to the incoming call in the appropriate manner. However, if the call re-routing/diversion takes place after the ringing stage has been reached (i.e. an MLPP response has already been sent to the incoming call leg), the call will proceed on the basis of the MLPP response already sent to the incoming call leg.

17.3.9 Call recovery

When an outgoing SIP call is recovered and the original INVITE included a `Resource-Priority` header, an identical `Resource-Priority` header will be included in the recovery call leg.

17.4 Additional calling party number

Additional calling party number is supported by, and interworked between, the SS7 and Q.931 protocols.

Q.931 protocols present an additional calling party number by including two Calling Party Number information elements in the SETUP message. The first Calling Party Number information element is interpreted as the calling party number, with the second interpreted as the additional calling party number.

NOTE

The ETS 300 protocol allows the calling party number and additional calling party number to be reversed in the SETUP message by applying the `-s7,1` firmware download switch.

GroomerII supports additional calling party number interworking between SIP and SS7/ETS 300, as described in the specifications listed in section 14.8.

17.5 Connected party number (COLP/COLR)

GroomerII supports connected party number interworking between the Q.931, SS7 and SIP protocols. The connected party information presented by the outgoing call at the connected stage is passed through to the incoming call.

17.5.1 Q.931

GroomerII supports connected party number when using the ETS 300, Q.SIG and AT&T protocols. The connected party number is presented using a Connected number parameter in the CONNECT message as described in ITU-T Recommendation Q.951.

17.5.2 SS7

GroomerII supports connected party number when using the ITU-T, China and UK ISUP variants. The connected party number is presented using a Connected number parameter in the ANM/CON message as described in the protocol specification for the variant in use.

17.5.3 SIP

Connected party number presentation (COLP)

GroomerII uses a `P-Asserted-Identity` header in the 200 OK response to present the connected party number. The `P-Asserted-Identity` header is described in IETF RFC 3325, and has the form:

```
P-Asserted-Identity: "Bob" <sip:+441908273800@192.168.16.100>
```

In the above example +441908273800 will be used as the connected party number.

Connected party number restriction (COLR)

The 200 OK may use a `Privacy` header to indicate connected party number presentation. The `Privacy` header is described in IETF RFC 3323 and has the form:

```
Privacy: id;header;user
```

17.5.4 TDM interworking

Interworking of connected party number between TDM calls is based upon standard procedures.

17.5.5 TDM to SIP interworking

The following table describes how a Q.931 Connected number parameter will be formed from the inbound `P-Asserted-Identity` and `Privacy` headers.

Q.931 parameter	Setting
Type of number	If the connected number digits are preceded by a + then this will be set to international number otherwise it will be set to national number.
Numbering plan identification	ISDN/Telephony numbering plan (CCITT Rec. E.164/E.163).
Presentation indicator	If a <code>Privacy</code> header containing any of the tags <code>id</code> , <code>header</code> or <code>user</code> is received this will be set to presentation restricted otherwise it will be set to presentation allowed.
Screening indicator	This will be set to the value configured in the Q.931/ISUP page of the Routing Configuration screen (see section 8.5.3). If <code>Transparent</code> is selected network provided will be used.
Number digits	The connected number digits are transferred unmodified, with the exception of a leading +, which will be discarded.

The following table describes how an SS7 Connected number parameter will be formed from the inbound P-Asserted-Identity and Privacy headers.

SS7 parameter	Setting
Nature of address indicator	If the connected number digits are preceded by a + then this will be set to international number otherwise it will be set to national (significant) number.
Numbering plan indicator	ISDN (Telephony) numbering plan (ITU-T recommendation E.164).
Address presentation restricted indicator	If a Privacy header containing any of the tags id, header or user is received this will be set to presentation restricted otherwise it will be set to presentation allowed.
Screening indicator	This will be set to the value configured in the Q.931/ISUP page of the Routing Configuration screen (see section 8.5.3). If Transparent is selected network provided will be used.
Address signal	The connected number digits are transferred unmodified, with the exception of a leading +, which will be discarded.

A connected subaddress may be included in the P-Asserted-Identity header, and this will be mapped as described in section 14.7.

17.5.6 SIP to TDM interworking

The information in the inbound Connected number parameter will be used to present a P-Asserted-Identity header in the following form:

P-Asserted-Identity: <sip:01908273800@192.168.1.100>

The Number digits/Address signal will be copied unmodified into the URI user part. If the Type of number/Nature of address indicator is set to international number then the user part will be prefixed with a +.

The URI host part will contain the IP address of the GroomerII host port.

If the Presentation indicator/Address presentation restricted indicator is set to a value other than presentation allowed, then a Privacy header will be added to the 200 OK as shown in the following table.

TDM protocol	Privacy header
ETS 300	Privacy: id;header;user
All others	Privacy: id

If a connected subaddress is presented by the TDM call leg, this will be mapped into the P-Asserted-Identity header as described in section 14.7.

17.5.7 SIP interworking

When interworking between SIP calls, any P-Asserted-Identity and Privacy headers presented in the 200 OK response from the outgoing call leg will be passed through unmodified to the incoming call leg.

18 TTY/RTT mapping

When interworking between TDM and SIP calls, GroomerII can be configured to convert Baudot tones generated by a TTY device to and from a real time text (RTT) stream.

The frequencies and codes used by Baudot tones are described in ANSI TIA/EIA-825 (2000). The RTT stream is described in IETF RFC 4103.

18.1 Configuring a TTY system

In order to perform TTY/RTT mapping GroomerII must be converted from a standard system to a TTY system. The system is configured for TTY operation by loading the alternative layout file `TTY_GroomerII.lyt`. This layout file must be loaded to all TiNG DSPs in the system, mixing standard and TTY operation is not supported. Loading layout files is described in section 4.9.

GroomerII will detect the `TTY_GroomerII.lyt` file and automatically run in TTY mode. If your system is configured for TTY operation, the message `SYSTEM CONFIGURED FOR TTY/RTT MAPPING` will be printed in the Maintenance Messages panel of the GroomerII Kernel window at startup.

18.2 Operating limits

The `TTY_GroomerII.lyt` file loads alternative and additional firmwares required for TTY operation. These firmwares consume extra DSP resources and so place a number of limitations on system operation. Where necessary, GroomerII will override system configuration to enforce these limitations.

NOTE

For clarity it is recommended that you reconfigure your system when switching to TTY operation, rather than rely on GroomerII to override your configuration settings.

18.2.1 Call capacity

The TTY functionality in GroomerII is designed for use in T1 environments, and so each Prosody X card is limited to handling 192 (eight trunk) or 96 (four trunk) SIP calls, rather than the 240/120 available on a standard system.

Any surplus TDM channels (for example where one or more trunks on the card is configured with an E1 protocol) remain available for TDM interworking.

NOTE

Although the TTY functionality is designed for use in T1 environments, GroomerII is able to detect Baudot tones on both E1 and T1 trunks.

18.2.2 Audio codec selection

Only the use of G.711 audio codecs is supported.

GroomerII will remove all codecs other than G.711 from the codec list selected by the route prior to making a media offer. If the codec list does not contain the G.711 codec, then G.711 with voice activity detection disabled will be offered.

Only the G.711 codec will be selected from an offer made by the remote endpoint. If the remote endpoint does not include a G.711 codec in its media offer then the offer will be declined.

18.2.3 Secure SIP

Secure SIP telephony (TLS and SRTP) is not available on TTY systems. Access to the TLS Certificates dialog will not be available, and any TLS certificate that may have been configured prior to switching to TTY operation will not be loaded.

GroomerII will not use TLS signalling nor will it make media offers requesting secure RTP.

Offers from remote endpoints requesting secure SIP will be declined.

18.3 RTT stream negotiation

When making a media offer, GroomerII can be configured to request an RTT stream in one of two ways:

- Always include an RTT stream in the media offer.
- Request an RTT stream only when Baudot tones have been detected on the TDM side. If media negotiation has already been completed prior to this a SIP reINVITE will be used.

RTT stream negotiation is configured using the System Configuration window in the GroomerII Configuration Editor (see section 8.6.7).

GroomerII will always accept a media offer from the remote endpoint requesting an RTT stream.

18.4 T.140 redundancy

The RTT stream can be configured to use up to ten levels of T.140 redundancy. The redundancy level is configured using the System Configuration window in the GroomerII Configuration Editor (see section 8.6.7).

18.5 Voice and hearing carry over

GroomerII supports voice carry over (VCO) and hearing carry over (HCO):

- Any Baudot tones detected on the inbound TDM audio path are removed and transported across the outbound RTT stream. All other inbound audio is passed unmodified across the outbound RTP stream.
- All text characters received on the inbound RTT stream are converted to Baudot tones and played on the outbound TDM audio path. All audio received on the inbound RTP stream is passed unmodified across the outbound TDM audio path.

18.6 SIP call retry

If an outgoing SIP call that offered an RTT stream is retried, then an identical RTT stream will be offered in the retry call.

18.7 SIP call recovery

If an outgoing SIP call has negotiated an RTT stream prior to call recovery being invoked, then an identical RTT stream will be offered in the recovery call.

19 Advanced fault finding and maintenance

19.1 GroomerII not starting

Normally the GroomerII Kernel will start-up and any errors will be shown on the message dialog.

NOTE

GroomerII will only be started once Microsoft Windows has been fully started and logged on.

19.2 Kernel errors.

19.2.1 Dongle not present

Check that the dongle is connected to the system parallel port or USB port, as appropriate, and that the device driver is installed.

19.2.2 Invalid activation key

Should the GroomerII fail to validate its Activation Key, you will be prompted to enter a valid key.

If the software you are using is the version pre-installed when your GroomerII was delivered, then the activation key will be found on the CD case that accompanied the system.

If the software you are using is an upgrade provided to you on CD-ROM, then the activation key will be found on the CD case.

If the software you are using is an upgrade received by email, the email will have included the activation key.

If you have lost your Activation Key, contact Aculab Support, quoting the serial number of your GroomerII chassis (G5xxx), and they will be able to tell you what the activation key is. They will not give out activation keys for any version of software other than the one you are authorised to use.

19.2.3 Problem with GRSCHE.DAT

Problem with `GRSCHE.DAT` this file defines the configuration to be loaded on boot-up, a common problem is a missing carriage return at the end of the last statement.

19.2.4 CFG FAILED TO LOAD

Check that the `CFG` file stated in `GRSCHE.DAT` is valid for this system by loading it into the Configuration Editor Check the Ports, Clocks and Routing have been configured correctly.

19.3 Status errors

19.3.1 Openin failed

`Openin Failed` can be due to configuration problems:

- Firmware download problems, can be checked by going to the diagnose page on the status screen and checking for a valid firmware signature.
- Too many Ports defined in the Configuration file. There should only be one Port defined per port installed in the system.

19.3.2 Card clock stopped (TDM ports only)

`Card Clock Stopped`, seen on the alarms page, indicates a card fault. A reboot may clear the problem.

19.3.3 NO SIGNAL DETECTED (TDM ports only)

`No Signal Detected` seen on the Alarms page indicates a cable fault or a failure of the far end equipment. A loop back on that port can be used to prove the card, status `No Alarms` proves the cabling is OK.

19.3.4 DISCONNECTED (IP ports only)

`Disconnected` on an IP port indicates a cable fault or a failure of the Ethernet switch to which the port is connected. If both IP ports on a Prosody X card show `Disconnected`, the card will be unable to send or receive calls. When both the IP ports on a Prosody X card are cabled and working correctly, the status should read `Active` and `Connected`.

19.3.5 REMOTE ALARM INDICATION (TDM ports only)

`Remote Alarm Indication` seen on the alarms page indicates that the connected equipment is sending an alarm towards GroomerII because it is not seeing a signal from GroomerII or is receiving a major alarm from GroomerII. The alarm may be present while the equipment is initialising and should disappear when the switch has settled.

19.3.6 ALARM INDICATION SIGNAL (TDM ports only)

`Alarm Indication Signal` is the highest level of alarm possible, the connected equipment should be restarted and the configuration checked.

19.4 Microsoft Windows error messages.

Please note down all information, before taking any action such as re-booting the machine.

19.5 Obtaining protocol trace from GroomerII (TDM ports only)

The GroomerII Status can display the raw protocol transmitted and received on an ISDN port. From this trace file, all information about a call is displayed allowing the source of a problem to be quickly traced.

On the Events page of the Status screen, select Filters, then the Protocol page. Select the Ports to be monitored and destination of the trace e.g. Window and Disk. The Disk log files are written to the `GroomerII\Trace` directory.

19.6 Using CDRs to monitor system performance

If GroomerII is running under a very high load, the protocol trace may be missing from the trace files. The best way to monitor system performance is to log the CDR information to a file; this can show where calls are routing and if they are failing. Select the CDR type from the Kernel program to find the information you require.

19.7 Monitoring a single call through the Groomer

Using Call Control, Routing and Protocol trace watch the progress of a call through the system.

The example below shows a successful call through the system without protocol trace enabled.

NOTE

Depending on protocol and system configuration the trace may look slightly different. See Appendix E: for a detailed description of trace file contents.

```
12:09:59 P:08 C:01 ID:0000000241 Incoming Call (0x5040802), opened ts 1
12:09:59 P:08 C:01 ID:0000000241 Called Num : 0123
12:09:59 P:08 C:01 ID:0000000241 Calling Num : 3210
12:09:59 P:08 C:01 ID:0000000241 Routing "Route 8 - SIP" P:01 C:--
12:09:59 P:08 C:01 ID:0000000241 Opened outgoing (0x05260802) on P:01
(SIP) channel 00 to <sip:6001@192.168.1.2;transport=tcp>
12:09:59 P:01 C:00 ID:0000000241 SIP:Outgoing call from channel 00 on
st:48, ts:00
12:09:59 P:08 C:01 ID:0000000241 Send progress
12:10:03 P:01 C:00 ID:0000000241 SIP:Outgoing Connected
12:10:03 P:08 C:01 ID:0000000241 Incoming Call Accepted
12:10:03 P:08 C:01 ID:0000000241 Incoming Connected
12:10:08 P:01 C:00 ID:0000000241 SIP:Outgoing Call Gone Idle
12:10:08 P:08 C:01 ID:0000000241 Incoming Call Disconnected
12:10:08 P:08 C:01 ID:0000000302 Openin from previous call ID:0000000241
12:10:08 P:08 C:01 ID:0000000302 waiting for incoming
```

19.8 Common set-up problems

19.8.1 System clock

The most common set-up problem concerns the configuration of the system clock, this is the source of the clock within the system. This should be set to clock from a network source. If a long distance CAS trunk is connected, you may have to clock from the CAS link to stop calls being dropped.

19.8.2 Dedicated timeslots

Some CAS switches and even some PRI ISDN (US local lines) have dedicated incoming and outgoing time slots, this should be considered when constructing the configuration file.

19.9 Aculab technical support

Aculab offer technical support to customers with a valid technical support agreement. Should you not have a technical support agreement, please contact your Aculab account manager.

NOTE

Aculab can only support a GroomerII purchased directly from Aculab. In all other cases please contact your supplier.

To assist Aculab in resolving your problem as quickly as possible, the following information should accompany any problem report.

- The GroomerII serial number (G5XXX) of the system experiencing the problem.
- A full description of the problem you are experiencing.
- A backup of the system produced using the GroomerII Backup and Restore utility - section 11.1 refers.
- A copy of the `kernel.log` file from the `C:\Program Files (x86)\Aculab\GroomerII` folder.
- A trace file produced by the GroomerII Status Monitor showing both a good and bad call, with the following event filters enabled on both incoming and outgoing ports. See section 6.2 for a description of trace logging.
 - Call Control
 - Routing
 - Switching
 - RTP/RTT
 - Protocol

If you can arrange internet access to the system via the pre-installed pcAnywhere software or remote management module, this will allow our support engineers to interrogate GroomerII remotely.

Contact details

Aculab

Lakeside

Bramley Road

Mount Farm

Milton Keynes

MK1 1PT

UK

Tel +44 (0)1908 273805

Fax +44 (0)1908 273801

email support@aculab.com

Appendix A: SNMP facility

Simple network management protocol (SNMP) is used for the exchange of management information between host systems on IP networks.

The GroomerII SNMP agent is implemented as a sub-agent of the host SNMP agent. The following host SNMP agents can be used:

- The Microsoft SNMP Agent, which supports SNMP versions 1 and 2C. This is the default agent and is installed on all GroomerII systems.
- New systems and upgraded legacy systems also have the NuDesign SNMPv3 Agent installed, which supports SNMP versions 1, 2C and 3.

The SNMP agent must be configured to enable traps to be sent to the correct destination and to allow requests to be processed. For more details on the configuration of the SNMP service consult the appropriate vendor documentation.

The `Aculab-GroomerII.mib` MIB file contains the complete specification of the Aculab SNMP traps and objects.

Refer to section 5.4, SNMP reporting, for information on enabling and configuring the Aculab SNMP sub-agent.

A.1 Enabling the NuDesign SNMPv3 agent

NOTE

The NuDesign SNMPv3 Agent requires GroomerII application software V10.32.2 or later to be installed.

When shipped GroomerII systems are configured to use the Microsoft SNMP Agent. If your system also has the NuDesign SNMPv3 Agent installed, you may switch to this by following the steps below:

- Close all GroomerII applications.
- Open a Command Prompt window and navigate to `C:\Program Files (x86)\Aculab\GroomerII`.
- In the Command Prompt window execute the command `grSNMPService -remove`.
- From the Control Panel select Administrative Tools followed by Services to open the Microsoft Windows service manager, and locate the SNMP Service entry. Stop this service and re-configure it for manual start.
- In the Microsoft Windows service manager locate the NuDesign SNMPv3 Master Agent Service entry and re-configure it for automatic start. Now start the service and close the Microsoft Windows service manager.
- Return to the Command Prompt window and execute the command `grSNMPService -install`, then close the Command Prompt window.
- Power cycle the system to restart the GroomerII applications.

A.2 SNMP Alarms

The following application specific traps are supported. As well as containing objects specific to its purpose, each trap also contains the following common objects:

- groomerTimestamp, time when the trap was raised:
 - Format: YYYY-MM-DD-hh:mm:ss
 - Example: 2016-05-02-07:06:57
- groomerTrapSeverity, one of:
 - Information (0)
 - Warning (1)
 - Error (2)
 - Cleared (3)
- groomerTrapInformation:
 - Textual description of the trap.
 - Example: "Received L1 Alarm is now (No Alarm) on Port 1 (Port 1 mobile network)"

The conditions by which groomerTrapSeverity is set are detailed for each trap.

groomerRunningTrap

Issued at GroomerII start-up, and thereafter whenever the operational state of GroomerII changes. To prevent spurious alarms being raised, the service will not issue an initial 'stopped' trap until three minutes after system start-up.

groomerTrapSeverity:

- Information, if the operational state is running.
 - Note: In the unusual case that SNMP reporting is disabled but the SNMP Agent is configured, a trap at this severity level will be generated at start-up.
- Error, if the operational state is stopped.

groomerSNMPReportingTrap

At start-up the service reports whether SNMP is enabled. If during operation the SNMP reporting state changes, the new state will be reported.

groomerTrapSeverity:

- Information.

Note: If SNMP reporting is disabled, it will not be possible to get the running state of GroomerII, the response will be reported as `unknown`.

groomerWindowsProcessStateTrap

A configuration facility is provided that allows a list of Windows processes to be built. The minimum and maximum instances for each process can be configured. GroomerII will periodically check the number of instances running for each process. A trap is issued if the number of instances is outside the configured range. If the number of instances returns to being within the configured range then a trap will be issued. When the system returns to the all processes running normally state then an additional 'all processes running' trap will be issued.

groomerTrapSeverity:

- Information, if all processes are running normally (or none are being monitored).
- Error, if the number of instances of a particular process is outside the configured range.
- Cleared, if the number of instances is now within the range.

groomerInternalProcessStateTrap

GroomerII periodically checks that its internal processes and threads are running. If any are stopped, a trap will be issued. If a process/thread restarts after stopping then a trap will be issued. When the system returns to the all processes running state then an additional 'all processes running' trap will be issued.

groomerTrapSeverity:

- Information, if all internal processes and threads are running (or, during startup or shutdown, if any internal process or thread is not running).
- Cleared, if an internal process or thread has started.
- Error, if any internal process or thread has stopped.

groomerTDMRxL1AlarmTrap

Issued once for each port at start-up, and whenever the link state (more strictly, the received alarm state) changes. This trap can be suppressed on a port-by-port basis.

groomerTrapSeverity:

- Cleared, if no alarm is present.
- Error, if alarm is present.

groomerTDMRxCASMultiframeAlarmTrap

Only CAS ports will produce this trap. It is issued once for each port at start-up, and whenever the multiframe alarm state changes. This trap can be suppressed on a port-by-port basis.

groomerTrapSeverity:

- Cleared, if no alarm is present.
- Error, if alarm is present.

groomerTDMClockSlipsTrap

Only TDM ports issue this trap. The slip threshold as an average of slips per second over the previous minute is configurable. This trap can be suppressed on a port-by-port basis.

groomerTrapSeverity:

- Cleared, if TDM clock slips are below the threshold.
- Error, otherwise.

groomerTDMTxL1AlarmTrap

Issued once for each TDM port at start-up, and whenever the transmitted alarm state changes.

groomerTrapSeverity:

- Cleared, if no alarm is present.
- Error, if alarm is present.

groomerTDMLayer2Trap

On TDM Ports, with the exception of CAS and SS7, this trap is issued once for each port at start-up, and whenever the layer 2 state changes. The trap can be suppressed on a port-by-port basis.

groomerTrapSeverity:

- Cleared, if layer 2 is up.
- Error, if layer 2 is down.

groomerPortIPStatusTrap

This trap is issued once for each Prosody X card IP port at start-up, and whenever the state of the port changes.

groomerTrapSeverity:

- Cleared, if both IP ports are connected.
- Warning, if only one IP port is connected.
- Error, if neither IP port is connected.

groomerPortOperationalStatusTrap

Issued once for each TDM port at start-up, and whenever the state of the port changes.

groomerTrapSeverity:

- Information, if the port is running.
- Error, otherwise.

groomerConfigLoadTrap

Issued every time a Groomer configuration file is loaded, including at start-up. Reload information is retrieved using the system status object.

groomerTrapSeverity:

- Information, if the configuration file loaded successfully.
- Error, otherwise.

groomerFirmwareReloadTrap

An information trap issued whenever a port is reloaded. No status is reported, a failure of the operation will be obtained through other SNMP objects.

groomerTrapSeverity:

- Warning.

groomerPortBlockingStateChangeTrap

Issued for each port at start-up, and whenever the port blocking state changes.

groomerTrapSeverity:

- Information.

groomerCallRoutingFailedTrap

Issued whenever GroomerII cannot route an incoming call. This trap can be suppressed on a port-by-port basis.

groomerTrapSeverity:

- Information

groomerCallState2Trap

Indicates a fault whenever a call has remained in one of its non idle states for longer than the configured time interval.

groomerTrapSeverity:

- Error, if a call has remained in one of its non idle states for too long.
- Cleared, otherwise.

groomer33VoltStateTrap

This alarm is issued at system startup to report the current state of the system 3.3V supply. Thereafter it will be raised whenever the system 3.3V supply moves outside of, or returns to the acceptable range (3.14V to 3.46V).

groomerTrapSeverity:

- Cleared, the supply is within range.
- Warning, otherwise.

NOTE

Not all chassis models support 3.3V supply monitoring.

groomer5VoltStateTrap

This alarm is issued at system startup to report the current state of the system 5V supply. Thereafter it will be raised whenever the system 5V supply moves outside of, or returns to the acceptable range (4.75V to 5.25V).

groomerTrapSeverity:

- Cleared, the supply is within range.
- Warning, otherwise.

NOTE

Not all chassis models support 5V supply monitoring.

groomer12VoltStateTrap

This alarm is issued at system startup to report the current state of the system 12V supply. Thereafter it will be raised whenever the system 12V supply moves outside of, or returns to the acceptable range (11.4V to 12.6V).

groomerTrapSeverity:

- Cleared, the supply is within range.

- Warning, otherwise.

NOTE

Not all chassis models support 12V supply monitoring.

groomerChassisTemperatureTrap

This alarm is issued at system startup to report the current state of the internal chassis temperature. Thereafter it will be raised whenever the internal chassis temperature exceeds the recommended maximum for the chassis, or returns to normal. If a system has multiple temperature sensors separate alarms are used for each.

groomerTrapSeverity:

- Cleared, the temperature is below the recommended maximum.
- Warning, otherwise.

NOTE

Not all chassis models support internal temperature monitoring.

groomerSystemFanTrap

System fans are monitored in one of two ways. Some chassis use simple state detection (rotating or stopped), whilst others report the actual speed of rotation. In the latter case GroomerII will raise alarms should the speed of a fan fall to a level where it is reasonable to assume that the fan is about to fail.

This alarm is issued at system startup to report the current state of the system fans. Thereafter it will be raised whenever a fan moves between the working and failed states. If a system has multiple fans fitted separate alarms are used for each.

groomerTrapSeverity:

- Cleared, if the fan is running or running normally.
- Warning, if the fan is stopped or running too slowly.

NOTE

Not all chassis models support system fan monitoring.

groomerHBCDeviceTemperatureTrap

This alarm is issued at system startup to report the current temperature of an HBC (Host Board Computer) device. Thereafter it will be raised whenever the temperature exceeds the recommended maximum for the device, or returns to normal. If a system has multiple HBC devices separate alarms are used for each.

groomerTrapSeverity:

- Cleared, if the temperature is within range.
- Warning, otherwise.

NOTE

Some HBC devices report PECI temperatures. Under normal circumstances

these are negative values that indicate how far below the throttling temperature the device is working.

NOTE

Not all chassis models support HBC device monitoring, and not all HBC devices report a temperature status.

groomerHBCDeviceFanTrap

This alarm is issued at system startup to report the current state of the cooling fan on an HBC (Host Board Computer) device. Thereafter it will be raised whenever the fan speed falls to a level where it is reasonable to assume that the fan is about to fail, or when the fan returns to normal working speed. If a system has multiple HBC devices separate alarms are used for each.

groomerTrapSeverity:

- Cleared, if the fan is running normally.
- Warning, if the fan is stopped or running too slowly.

NOTE

Not all chassis models support HBC device monitoring, and not all HBC devices report a fan status.

groomerPSUStatusTrap

Power supply units are monitored in one of two ways. Some chassis use simple state detection (working or failed), whilst others report the actual voltage output by the PSU. In the latter case GroomerII will raise alarms should the output of a PSU move outside an acceptable range.

This alarm is issued at system startup to report the current state of the PSUs. Thereafter it will be raised whenever a PSU moves between the working and failed states. If a system has multiple PSUs fitted separate alarms are used for each.

groomerTrapSeverity:

- Cleared, a PSU is working or its voltage has returned to a value within the recommended range.
- Warning, a PSU is not working or its voltage is at a value outside the recommended range.

NOTE

Not all chassis models support PSU monitoring.

groomerCPUUsageTrap

Warns when the CPU load constantly exceeds a configured threshold. To overcome the effects of applications such as PC Anywhere, which run at a low priority but tend to use up all excess CPU capacity, a list of processes to exclude is included in the

configuration. The trap is issued when the CPU load exceeds the upper threshold, and when it returns below the lower threshold.

groomerTrapSeverity:

- Cleared, if the CPU load is now below the lower threshold.
- Error, if the CPU load is now above the upper threshold.

groomerMemoryUsageTrap

Raised to warn when system memory usage has risen above a configured upper threshold, and when it falls below the lower threshold.

groomerTrapSeverity:

- Cleared, if the memory usage is now below the lower threshold.
- Error, if the memory usage is now above the upper threshold.

groomerAvailableDiskSpaceTrap

Raised to warn when the available disk space has fallen below a configurable threshold, and when the condition clears.

groomerTrapSeverity:

- Cleared, if the available disk space is now above the threshold.
- Error, if the available disk space is now below the threshold.

groomerClockSourceUpdatedTrap

Raised at start-up, and whenever the clock source used by the H.100 bus changes.

groomerTrapSeverity:

- Information.

groomerCardStatusTrap

Issued once at start-up for each card in the system. For E1/T1 Digital Access Cards the trap is issued when the Kernel application reaches the system started state. For Prosody X cards, the trap is issued once the card is detected. The system waits for three minutes after startup to detect a Prosody X card before issuing a not found alarm. If a card that was not detected at start-up is subsequently found, a further trap is issued.

groomerTrapSeverity:

- Cleared, if the card has been detected.
- Error, if the card has not been found.

groomerCardModuleStatusTrap

This alarm is raised to report the operational state of the DSP modules on a Prosody X card. The alarm is raised when the Prosody X card is detected to notify the initial state of the module, and thereafter whenever the state of the module changes. Separate alarms are used for each module on the card.

groomerTrapSeverity:

- Cleared, if the module has started running.
- Error, otherwise, for example if the module has stopped running.

groomerSystemInitialisedTrap

This trap is for information, and is raised at start-up when GroomerII initialisation is completed and the system is ready to pass calls.

groomerTrapSeverity:

- Information

groomerReceivedRTPStoppedTrap

Raised when the RTP traffic from a remote endpoint stops unexpectedly. If this alarm has been issued to warn of an RTP fault it will be issued again to clear the fault when either RTP traffic is detected once more, or the associated call is cleared.

groomerTrapSeverity:

- Error, the RTP traffic has stopped unexpectedly.
- Cleared, otherwise.

groomerSS7SignallingLinkStateTrap

This alarm will be raised at system startup for each SS7 signalling link in the system, and thereafter whenever the signalling link state changes between available (able to pass traffic) and unavailable (unable to pass traffic).

groomerTrapSeverity:

- Information, if an SS7 signalling link has been removed by a configuration change.
- Cleared, if an SS7 signalling link has become available.
- Error, if an SS7 signalling link has become unavailable.

groomerContinuityCheckStateTrap

This alarm will be raised when an SS7 bearer channel fails an in-call continuity check. The alarm is cleared when the bearer channel next passes a continuity check, receives an incoming call or is reset. Note that GroomerII does not persist continuity check status across shutdown.

groomerTrapSeverity:

- Warning, if an SS7 bearer channel has failed a continuity check.
- Cleared, if an SS7 bearer channel has now passed a continuity check.

A.3 SNMP Requests

The following elements from the Aculab-GroomerII MIB allow GroomerII information to be presented as tables:

groomerPortTable

This table collects alarm information, counters and the current status for a GroomerII port.

groomerCallStateTable

This table contains details of the current state for each TDM timeslot in the system. It will show the state of the incoming call, and any outgoing port and timeslot associated with this call. This is a legacy report designed for use on system fitted with E1/T1 cards. Systems fitted with Prosody X cards will respond to this request, but will only return details of the TDM ports in the system.

groomerCallTable2

This table contains details of the current state of each call in the system. This table should be used in all new designs.

groomerCardTable

This table contains details of each Prosody X card that GroomerII expects to be fitted in the system, including the status of the DSP modules on the card.

groomerProcessStatusTable

This table lists the state of any internal threads the GroomerII has started.

groomerSystemProcessTable

This table lists the state of system processes being monitored by the GroomerII.

groomerPSUTable

This table lists the current state of each power supply unit in the system.

NOTE

Not all chassis models support PSU monitoring.

groomerVoltageTable

This table lists the current state of the chassis power rails.

NOTE

Not all chassis models support power rail monitoring.

groomerChassisTemperatureTable

This table lists the current state of each chassis temperature sensor.

NOTE

Not all chassis models support chassis temperature monitoring.

groomerSystemFanTable

This table lists the current state of each system fan.

NOTE

Not all chassis models support system fan monitoring.

groomerHBCDeviceTable

This table lists the current state of each HBC (Host Board Computer) device in the system.

NOTE

Not all chassis models support HBC device monitoring.

groomerCLEITable

Retrieves the Common Language Equipment Identification (CLEI) codes of the GroomerII chassis and all installed cards.

NOTE

Not all chassis have a CLEI code.

groomerSS7SignallingLinkStatusTable

This table lists the current state of all SS7 signalling links in the system.

groomerContinuityCheckStatusTable

This table lists the current continuity check status of all SS7 bearer channels in the system.

Requesting the following elements from the Aculab-GroomerII MIB using a 'walk' allows other, non-table based, information to be presented:

groomerServiceStatus

This collects information on the status of the GroomerII restricted to the version, whether the GroomerII is running and whether SNMP reporting is currently enabled.

groomerKernelStatus

This collects information on the current configuration of the GroomerII (if running).

groomerSystemResources

This collects information on memory usage, CPU usage and free disk space on the GroomerII system.

Appendix B: Call data records specifications

The Call data record and their layouts are generated by the Kernel and reported by the Status program. CDRs may be logged to any combination of screen, disk or RS232 port. Some fields are padded with spaces which are represented by '-'. Spaces used as delimiters are represented as such.

To select the CDR to use, see section 5.8 of this manual.

Definitions for some parameters are pre-defined, for example:

Parameter	Description
Answered	Y or N to indicate if a call was answered
Result	Y, I, E, X, H, R, O, U, N, M, or L
Call type	V or F, all non fax calls will be displayed as voice

The definitions of values used by Result or call type are as follows:

Value	Description
V	Not fax
F	Fax
Y	Call was successful or normal disconnect
I	Incomplete dialling timeout
E	Busy
X	No answer
H	Hang up before answer
R	Routing failed
O	Failed to get outgoing channel
U	Number unobtainable
N	Non-specific failure
M	Maximum ringing timeout expired
L	Disconnected due to layer 1 alarm

B.1 Fixed format type CDRs

All record lengths quoted are data lengths only, and do not include a terminal null.

B.1.1 CDR type A structure

This is a comma de-limited CDR with the following parameters:

Parameter	Fixed Length
Incoming port number	2
Incoming timeslot	2
Outgoing port number	2
Outgoing timeslot	2
Call start date	8
Call start time	8
Incoming destination address	18
Incoming originating address	18
Call duration	8#

in exceptional circumstances this value may be exceeded, for example, if the call duration exceeds 99Hrs 59 minutes and 59 seconds.

- DA & OA can normally be up to 31 digits, however in this CDR they are limited to 18 digits
- The maximum length of this CDR is 76 characters

Example:

01,10,00,01,11:12:01,22:36:57,0123456789-----,9876543210-----,00:00:05

A duration of 00:00:00 is an indication that the call may not have been answered.

B.1.2 CDR type B structure

This is a comma de-limited CDR with the following parameters displayed in quotation marks:

Parameter	Fixed Length
Billing reference – unique for each end to end call	6
Static text 000001	6
Incoming port number	2
Incoming timeslot	2
Call start date	8
Call start time	8
Incoming destination address	16
Call duration	8#
Total charged units	6
Total charged units/100 in the format xxxx.xx	6

in exceptional circumstances this value may be exceeded, for example, if the call duration exceeds 99Hrs 59 minutes and 59 seconds.

- OA can normally be up to 31digits, however in this CDR it is limited to 16 digits
- The maximum length of this CDR is 97 characters

Example:

```
"000000","000001","01","06","11:12:01","22:38:45","0123456789-----
","00:00:05","000000","000.00"
```

B.1.3 CDR type C structure

This is a non de-limited CDR with the following parameters displayed in fixed length fields:

Parameter	Fixed Length
Billing reference	6
Incoming port number	2
Incoming timeslot	2
Incoming Originating address	6
Padding - spaces	12
Outgoing port number	2
Outgoing timeslot	2
Call start date	6
Call start time	6
Call end time	6
Incoming destination address	16
Call duration	6#
Total charged units	6
Answered	1
Padding - spaces	11

in exceptional circumstances this value may be exceeded, for example, if the call duration exceeds 99Hrs 59 minutes and 59 seconds.

- OA is limited to 6 digits; DA is limited to 16 digits.
- The maximum length of this CDR is 90 characters

Example:

```
0000000106987654-----00011112012240032240110123456789-----000005--
0.00Y-----
```


B.1.4 CDR type D structure

NOTE

CDR Type D is retained within GroomerII for backwards compatibility only and must not be used.

This is a non de-limited CDR with the following parameters displayed in fixed length fields:

Parameter	Fixed Length
Incoming timeslot	2
Call state – ringing (R), connected (A) or idle (I)	1
Incoming originating address	20
Incoming destination address	20

- This CDR type consists of three records, each with identical formats, generated at the ringing (R), connected (A), and idle (I) states.
- OA and DA are limited to 20 digits.
- The maximum length of this CDR is 43 characters.

Examples:

```
01R3210-----0123-----
01A3210-----0123-----
01I3210-----0123-----
```

B.1.5 CDR type E structure

This is a comma de-limited CDR with the following parameters:

Parameter	Fixed Length
Incoming group number	4
Incoming port number	2
Incoming timeslot	2
Outgoing group number	4
Outgoing port number	2
Outgoing timeslot	2
Call start date	8
Call start time	8
Incoming destination address	16
Outgoing destination address	16
Incoming originating address	16
Outgoing originating address	16
Call duration	8#
Answered	1
Total charged units	6

in exceptional circumstances this value may be exceeded, for example, if the call duration exceeds 99Hrs 59 minutes and 59 seconds.

- OA and DA are limited to 16 digits
- The maximum length of this CDR is 125 characters

Example:

```
0000,01,21,0000,00,01,11:12:01,22:42:25,0123456789-----,0123456789-----
,9876543210-----,9876543210-----,00:00:05,Y,000000
```

B.1.6 CDR type F structure

This is a space de-limited CDR with the following parameters:

Parameter	Min Length	Max Length	Fixed Length
Static Text (I)			1
Call start date (yymmdd)			6
Call end time (hhmmss)			6
Incoming port name	1	29	
Outgoing port name	0	29	
Incoming destination address			22
Call duration			6
Zeros			4
Padding – extra spaces			4
Zeros			3
Padding – extra spaces			3
Zeros			2

- DA is limited to 22 digits
- The maximum length of this CDR is 126 characters

Example:

```
I 011211 224539 ETS_NET 1 ETS_USR 0 0123456789----- 000005 0000-----
000----- 00
```

B.1.7 CDR type G structure

This is a non de-limited CDR with the following parameters displayed in fixed length fields:

Parameter	Min Length	Max Length	Fixed Length
Groomer ID	0	29	
Billing reference			6
Incoming port number			2
Static text - spaces			12
Incoming timeslot			2
Incoming Originating address			6
Outgoing Originating address			6
Static Text - spaces			12
Outgoing port			2
Outgoing timeslot			2
Call start date (ddmmyy)			6
Call start time (hhmmss)			6
Call end time (hhmmss)			6
Incoming destination address			16
Outgoing destination address			16
Call duration			6#
Total charged units			6
Call Type - V/F			1
Result - Y/I/E/X/H/R/O/U/N			1

in exceptional circumstances this value may be exceeded, for example, if the call duration exceeds 99Hrs 59 minutes and 59 seconds.

- OA is limited to 6 digits; DA is limited to 16 digits
- The maximum length of this CDR is 119 characters

Example:

```
GRM_ID0000000122987654-----987654-----
00011112012246422246500123456789-----0123456789-----000005  0.00VY
```

B.1.8 CDR type H structure

This is a comma de-limited CDR with the following parameters displayed in quotation marks:

Parameter	Fixed Length
Incoming port number:timeslot (xx:xx)	5
Outgoing port number:timeslot (xx:xx)	5
Call start date	8
Call start time	8
Incoming destination address	25
Incoming originating address	25
Outgoing destination address	25
Outgoing originating address	25
Call end time	8
Call duration	8#
Call Type - V/F	1
Result - Y/I/E/X/H/R/O/U/N	1

in exceptional circumstances this value may be exceeded, for example, if the call duration exceeds 99Hrs 59 minutes and 59 seconds.

- DA & OA are limited to 25 digits
- The maximum length of this CDR is 176 characters

Example:

```
"01:30","00:01","11:12:01","22:47:58","0123456789-----
", "9876543210-----", "0123456789-----", "9876543210-----
-----", "22:48:06", "00:00:05", "VY"
```

NOTE

Call type and Result are reported as a single delimited value i.e. "VY" and not "V","Y"

B.1.9 CDR type I structure

This is a comma de-limited CDR with the following parameters:

Parameter	Fixed Length
Incoming port number	2
Incoming timeslot	2
Outgoing port number	2
Outgoing timeslot	2
Call start date	8
Call start time	8
Outgoing destination address	18
Outgoing originating address	18
Call duration	8#

in exceptional circumstances this value may be exceeded, for example, if the call duration exceeds 99Hrs 59 minutes and 59 seconds.

- DA & OA are limited to 18 digits
- The maximum length of this CDR is 76 characters

Example:

01,24,00,01,11:12:01,22:49:18,0123456789-----,9876543210-----,00:00:05

B.1.10 CDR type J structure

This is a comma de-limited CDR with the following parameters displayed in quotation marks:

Parameter	Fixed Length
Incoming port number:timeslot (xx:xx)	5
Outgoing port number:timeslot (xx:xx)	5
Call start date (dd:mm:yy)	10
Call start time	8
Incoming destination address	25
Incoming originating address	25
Outgoing destination address	25
Outgoing originating address	25
End time	8
Call duration	8#
Call Type - V/F	1
Result - Y/I/E/X/H/R/O/U/N	1

in exceptional circumstances this value may be exceeded, for example, if the call duration exceeds 99Hrs 59 minutes and 59 seconds.

- DA & OA are limited to 25 digits
- The maximum length of this CDR is 178 characters

Example:

```
"01:01","00:01","14:01:2001","22:50:35","0123456789-----
", "9876543210-----", "0123456789-----", "9876543210-----
-----", "22:50:43", "00:00:05", "VY"
```

NOTE

Call type and Result are reported as a single delimited value i.e. "VY" and not "V","Y"

B.1.11 CDR type K structure

This is a non de-limited CDR with the following parameters displayed in fixed length fields:

Parameter	Fixed Length
Billing reference	6
Incoming port number	2
Incoming timeslot	2
Incoming Originating address	6
Static text – 12 spaces	12
Outgoing port	2
Outgoing timeslot	2
Call start date (ddmmyyyy)	6
Call answer time (hhmmss)	6
Call end time (hhmmss)	6
Incoming destination address	16
Call duration (hhmmss)	6#
Total charged units	6
Answered	1

in exceptional circumstances this value may be exceeded, for example, if the call duration exceeds 99Hrs 59 minutes and 59 seconds.

- OA is limited to 6 digits; DA is limited to 16 digits
- The maximum length of this CDR is 79 characters

Example:

```
00000002011428-----03012505991443051443091720-----
000003000000N
```

Should a call not be answered, answer time will indicate the time that the call came in.

B.1.12 CDR type L structure:

This is a comma de-limited CDR with the following parameters displayed in quotation marks:

Parameter	Fixed Length
Incoming port number:timeslot (xx:xx)	5
Outgoing port number:timeslot (xx:xx)	5
Call start date (dd:mm:yyyy)	10
Call start time	8
Incoming destination address	25
Incoming originating address	25
Outgoing destination address	25
Outgoing originating address	25
End time	8
Call duration	8#
Bearer Type	7
Result	1
Raw cause	3
Generic cause	3

in exceptional circumstances this value may be exceeded, for example, if the call duration exceeds 99Hrs 59 minutes and 59 seconds.

- OA and DA are limited to 25 digits
- The maximum length of this CDR is 199 characters

Example:

```
"02:01","03:01","14:01:2001","14:44:29","1720-----","1428-----
-----","1720-----","1428-----
","14:44:32","00:00:00","Speech ","N","000","000"
```

B.1.13 CDR type M structure

This is a comma de-limited CDR with the following parameters:

Parameter	Min Length	Max Length	Fixed Length
Incoming port number			2
Incoming port timeslot			2
Outgoing port number or null			2
Outgoing port timeslot or null			2
Call start date (dd/mm/yyyy)			10
Call start time			8
Incoming originating address	0	31	
Incoming destination address	0	31	
Call end time			8
Call duration			8#
Bearer Type	3	7	
Result			1
Raw cause			3
Generic cause			3

in exceptional circumstances this value may be exceeded, for example, if the call duration exceeds 99Hrs 59 minutes and 59 seconds.

- The maximum length of this CDR is 131 characters

Example:

```
02,04,01,13,20/02/2003,16:31:27,01908273800,01908273806,16:38:12,00:06:45,Speech,Y,000,000
```


Appendix C: Licensed codecs – legal notice

As of 1st January 2017, G.729 and its annexes are royalty free, meaning that fees for using it are no longer payable. If you require further clarification or additional information on this matter, please contact your Account Manager or email <mailto:sales@aculab.com>

Appendix D: TDM signalling firmware configuration options

This section describes signalling firmware configuration options that are additional to those listed in the firmware release notes, and the protocols with which each may be used.

D.1 -cA/B and X/Y bits configuration (DPNSS only)

Default setting: A/X

This option allows the dpnss A/B X/Y bits to be configured for layers 2 and 3 to enable DPNSS to DPNSS configuration

```
-cAX
-cAY
-cBX
-cBY
```

Incorrect setting of the A/B bits will result in an inactive DPNSS layer 2.

D.2 -cBBY Backbusy control (CAS only)

Instructs the CAS driver (and signalling system) to use 'backbusy':

```
-cBBY          configure all timeslots all ports
-cBBY, xxxxxxxx configure all timeslots indicated in the mask xxxxxxxx
```

The mask is an 8 digit hexadecimal representation of a 32bit value where each bit indicates the busy mode. A bit set to 1 will enable backbusy. A bit reset to 0 will disable backbusy. Bit 0 of the 32bit value controls timeslot 0 and bit 31 controls timeslot 31, for example:

```
1110 0110 0000 0010 0000 0000 0100 0000 will enable backbusy on timeslots:
31, 30, 29, 26, 25, 17, 6 and would be represented by the value:
E6020040 and would therefore be configured by: -cBBY, E6020040
```

NOTE

On E1 systems timeslots 0 and 16 are reserved and will be ignored.

D.3 -cCA connect acknowledgement (ETS300 only)

Some equipment require a `CONNECT_ACKNOWLEDGE` from the user end of the protocol after receipt of a `CONNECT` message. This configuration switch provides for this behaviour.

D.4 -cCICnnnn circuit identification codes (ISUP only)

```
-cCICnnnn
-cCICnnnn, aaaaaaaaaa
-cCICnnnn, aaaaaaaaaa, bbbbbbbb
```

Where *nnnn* is a decimal number of 1 to 4 digits that will be the CIC assigned to the first bearer timeslot, with subsequent CICs allocated sequentially (including any timeslot used for signalling, although this CIC will never be used). The OPC and DPC assigned to the ISUP circuits will be the most recent values preceding the `-cSLC` parameter itself.

If specified, *aaaaaaaa* is a CIC MAP, which allows the user to define which timeslots have CICs assigned to them. It is specified as a 32bit number expressed in hexadecimal, where bit zero corresponds to timeslot zero etc. If not specified, a value of `fffffffe` is assumed.

If specified, *bbbbbbbb* is a Circuit MAP, which allows the user to define which timeslots have may be used for ISUP call control. It is specified as a 32bit number expressed in hexadecimal, where bit zero corresponds to timeslot zero etc. If not specified, a value of *fffffffe* is assumed Any timeslots which are in use for signalling are automatically excluded from ISUP call setup, regardless of whether this is explicitly shown in the circuit map.

If *-cCICnnnn* is not specified, ISUP will not be available for call setup on the timeslots of that port.

D.5 -cCn number of CLI digits (CAS only)

It is necessary for the device driver and signalling system firmware to know the number CLI digits supported by the trunk. The driver configuration switch available for this purpose is *-cCn*, where n is a one or two digit decimal value of the number of digits required.

The *-cCn* option specifies the number of CLI digits expected by the system, for example, *-cC4* instructs the driver/signalling system to expect 4 CLI digits

It is important that this initial configuration is correct or unexpected behaviour may result.

D.6 -cDn number of DDI digits (CAS only)

It is necessary for the device driver and signalling system firmware to know the number of DDI digits supported by the trunk. The driver configuration switch available for this purpose is *-cDn*, where n is a one or two digit decimal value of the number of digits required.

The *-cDn* option specifies the number of DDI digits expected by the signalling system, for example, *-cD3* instructs the driver/signalling system to expect 3 DDI digits

It is important that this initial configuration is correct or unexpected behaviour may result.

D.7 -cDPCnnnnn signalling point code (ISUP only)

-cDPCnnnnn

Where *nnnnn* is a decimal number equating to the signalling pointcode of the adjacent network component to which the link connects. The network component may be a Signalling Transfer Point, or, if using fully associated signalling, a Signalling End Point. *nnnnn* must coincide with the pointcode of an STP (*AdjacentPC*), or of an SP (*RemotePC*) in the stack configuration file as described in the SS7 installation and administration guide.

This parameter may be repeated to specify that signalling link(s) and ISUP bearer timeslots have different DPC values. See *-cSLC* and *-cCIC*.

D.8 -cEn Call Charging Switch (ETS300 only)

This switch allows the application to send or receive call charging information depending on the country or exchange being used at the time. For further information on the *call_put_charge()* and *call_get_charge()* functions it is advisable to consult the 'Receiving Call Charge Information' and 'Sending Call Charge Information' sections in the Call Control Driver API Guide. The value transmitted will be one of two categories of charging for EuroISDN.

1. **UNITS** - One method is to transmit the value as **UNITS**. When charging uses the **UNITS** format a value representing the number of units accrued up to that point during the call will be transmitted. This value is initially one and is incremented by one each time the `call_put_charge()` function is used. The driver does not require any parameters in the call to `call_put_charge()` by the application.
2. **CURRENCY** - The second method is **CURRENCY**. When this type of information is used by the protocol the transmitted value is the accumulated cost of the call up to that point. This information is passed to the driver in the "charge" field of `put_charge_xparms`. The format of this string is an ASCII representation of the numeric value. Example : To send the value of 100 the three ASCII characters necessary to encode 100 as a string would be used. Printing this string to the screen should show '100' (without quotes).

Codes For Different Countries (n)

n=1 Switzerland/**CURRENCY** Charging will use Facility information elements based on ETS300 182. A charging string in `put_charge_xparms()` is required.

n=2 Germany/**UNITS** Charging will use Facility information elements based on ETS300 182. The charging string in `put_charge_xparms()` is ignored.

n=3 Holland/**UNITS** Charging will use Display information elements based on a country Specific specification. The charging string in `put_charge_xparms()` should be left blank.

n=4 Switzerland/**CURRENCY** Charging will use Display information elements based on a country Specific specification. A charging string in `put_charge_xparms()` is required.

n=5 Austria/**CURRENCY** Charging will use Facility information elements based on ETS300 182. A charging string in `put_charge_xparms()` is required.

n=6 Norway/**CURRENCY** Charging will use Facility information elements based on ETS300 182. A charging string in `put_charge_xparms()` is required.

n=7 Sweden/**CURRENCY** Charging will use Facility information elements based on ETS300 182. A charging string in `put_charge_xparms()` is required.

n=99 Disable Charging

D.9 -cEX Primary Rate Call Charging (ETS300 only)

This configuration switch is for use with ETS300 Advice of Charging where there may well be some national/network dependent differences in the way the charging information is presented.

X is a one or two digit decimal country code:

- 0 is the default
- 1 for Switzerland (type I)
- 2 for Germany
- 3 for Holland
- 4 for Switzerland (type II old style)
- 5 for Austria
- 6 for Norway
- 7 for Sweden

99 for disable charging

Consult the release notes supplied with the latest revision of firmware for further details.

D.10 -cFD Diversion (QSIG, ETS300, AT&T T1, and NI-2)

This configuration switch activates the diversion feature in the driver.

If the switch for this service is not set, any attempt to use this service through the API will fail.

Example:

If Diversion and Facility features are required for QSIG on port zero then the switches can be supplied as follows using `fwdspldr`.

```
Fwdspldr 12345 0 qsig_sup.upr -cFF -cFD
```

D.11 -cFF facility (QSIG, ETS300, and NI2)

This configuration switch activates the facility feature in the driver.

If the switch for this service is not set, any attempt to use this service through the API will fail.

Example:

If Diversion and Facility features are required for QSIG on port zero then the switches can be supplied as follows using `fwdspldr`.

```
Fwdspldr 12345 0 qsig_sup.upr -cFF -cFD
```

D.12 -cFP MLPP activation (ETS300 only)

Activates Multi-Level Precedence and Pre-emption (MLPP Q.955) in the firmware and driver.

D.13 -cFR Raw Data (ETS300 and QSIG)

Activates firmware to use Raw Data information. See the Call Control Driver API guide.

D.14 -cFU user to user (QSIG and ETS300)

This configuration switch activates the user-to-user feature in the driver.

User to User : `-cFU`

User to User : `-cFUN` (no negotiation)

If the switch for this service is not set, any attempt to use this service through the API will fail.

D.15 -cIMP75

Sets line impedance to 75 ohms (default is 120 ohms).

D.16 -cME

If an outbound DASS/DPNSS call is made with the sending complete flag set, then an ISRMC is used, otherwise an ISRMI will be sent. If the `-cMC` switch is applied an ISRMC will be used for all outbound calls, regardless of whether the sending complete flag is set.

D.17 -cNA1 release link trunk (NI-2 only)

Enables RLT (release link trunk) call transfer with NI-1 signalling. Without the switch NI-2 signalling is used for call transfers.

D.18 -cNCRC disable CRC4 (ISUP only)

This instructs the firmware not to use CRC4 framing at L1.

D.19 -cNE network end configuration (DASS, ETS300, AT&T, and NI2)

Default setting: `User end`

Network end configuration, sets up the device driver for network end working

`-cNE` configure port for network end

This switch applies to signalling systems with the exception of `CAS`, `DPNSS`, `QSIG` and `ISUP`.

NOTE

For correct network end operation, you will require the network end firmware for that signalling system.

D.20 -cOPCnnnnn[,i] (ISUP only)

Where `nnnnn` is a decimal number equating to the signalling pointcode, and optional instance, of your application. This must coincide with the pointcode (`LocalPC`) of an SS7 signalling point in the stack configuration file, as described in the SS7 installation and administration guide.

D.21 -cQM/S-A/B master/slave priority (QSIG only)

This configuration switch enables the QSIG Master and Slave bits, M for master and S for slave, and also the 'priority if call clash' bits A/B. Valid options are:

`-cQSB`

`-cQMA`

`-cQSA`

`-cQMB`

One end must be set to be master and the other end must be set to be slave. Incorrect setting of these bits will result in an inactive QSIG layer 2. The default configuration for QSIG is `-cQSB`.

D.22 -cRn Default clearing cause (all versions)

Default setting: `BUSY`

This option allows the default clearing cause to be configured, where `n` is a one or two digit hexadecimal value of the required clearing cause and must be a correct value supported by the signalling system.

`-cR3E` configure 'Call Rejected' on all ports

`-cR3En0` configure 'Call Rejected' on port 0 only

`-cR3En1` configure 'Call Rejected' on port 1 only

`-cR3En2` configure 'Call Rejected' on port 2 only

`-cR3En3` configure 'Call Rejected' on port 3 only

The above example shows the `CALL_REJECTED` cause for 1TR6.

D.23 -cSLCnn signalling link code (ISUP only)

Where *nn* is a decimal number equating to the MTP3 Signalling Link Code for the signalling link. The signalling link is created when the -cSLCnn parameter is processed, the parameters for the link must appear in this option. If -cSLCnn is specified more than once, multiple signalling links will be created. The OPC and DPC assigned to the signalling link will be the most recent values preceding the -cSLC parameter itself.

D.24 -cSO disable service message (AT&T and NI2)

This configuration switch disables the transmission of the 'service message' by the protocol stack. The service message brings the timeslot into service and may cause problems with some manufacturers equipment.

D.25 -cSP stop call proceeding (ETS300 only)

-cSP switch stops a CALL_PROCEEDING message from being sent automatically after a SETUP message has been received. It is useful if extra information is required to be included in the message by the use of the call_proceeding function.

- cSP configure for all ports

D.26 -cSU stop setup acknowledge (ETS300 only)

Stops a SETUP_ACKNOWLEDGE message from being sent automatically after a SETUP message has been received. It is useful if extra information is required to be included in the message by the use of the call_setup_ack function.

D.27 -cSW configuration (ETS300 only)

This configuration switch modifies the driver for use in Sweden where a call_proceeding message is required instead of a setup_acknowledge message.

D.28 -cTS[I]nn (ISUP only)

Where *nn* is a decimal number equating to the timeslot that will be used for the signalling link on the E1 line connected to the network port. For E1 cards that support the function, if *i* is specified, then the signalling link will face inwards (that is towards the switch matrix and H.110 bus), it can then be switched out on a different E1 using the Aculab switch API.

D.29 -cSPEEDnnk (ISUP only)

Where *nn* is a multiple of 8 less than, or equal to, 64. This sets the speed of the MTP2 signalling links. If specified once it will apply to all signalling links on the trunk, otherwise the last setting prior to the -cSLC parameter is used.

If not specified the default is 64k unless -cAMI is specified.

D.30 -cDAUUS (ETS 300 only)

The call driver will automatically respond to UU service requests by either accepting them (if the -cFU switch is set) or refusing them (if the -cFU switch is omitted). The automatic UU service response occurs when the application fails to supply the call driver with a UU service response before the ringing/connected state is reached. This switch will disable the automatic response.

Appendix E: Interpreting GroomerII trace file

GroomerII event reports are too extensive in number and dynamic in content for an exhaustive reference to be produced. This purpose of this section is purely to illustrate the types of event report that can be expected and give an insight into their meaning.

With the exception of a CDR, all trace entries begin with a timestamp, port and channel number, and call ID, for example 16:26:48 P:02 C:001 ID:0002141615.

The timestamp is the time at which the record was generated.

The port and channel numbers are those being used by the call that generated the report. If the call is an IP telephony call the channel number is an arbitrary value assigned by GroomerII for reporting purposes only.

The call ID is a unique identifier assigned to each incoming call by GroomerII. The call ID is used to identify all events generated by a particular incoming call and its corresponding outgoing call leg.

E.1 Alarms

The alarms filter reports changes in transmitted alarms on a TDM port, section 8.6.5 refers.

```
10:07:32 P:04 C:--- ID:----- GENERATING AIS ON PORT : 04 FROM NOS ON
PORT : 05
10:23:11 P:04 C:--- ID:----- CLEARED AIS ON PORT : 04 FROM NOS ON PORT :
05
```

The report is generated by the port transmitting the alarm. It shows whether the alarm is being generated or cleared, which alarm is being generated, for example AIS ON PORT : 04, and the reason it is being generated, for example NOS ON PORT : 05.

E.2 Layer 1

The layer 1 filter reports the received alarm state of a telephony port at two second intervals.

```
12:14:02 P:04 C:--- ID:----- LAYER 1 ESTABLISHED
12:14:02 P:05 C:--- ID:----- NO SIGNAL DETECTED
12:14:02 P:05 C:--- ID:----- LOSS OF SYNCHRONISATION
12:14:02 P:05 C:--- ID:----- SLIPS : 02720
```

Where multiple alarms are present on a port, each is reported separately.

E.3 Data Link

The data link filter reports the layer 2 status of a TDM port at two second intervals.

```
16:26:48 P:02 C:--- ID:----- LAYER 2 ESTABLISHED - 0XFFFFFFFE
16:26:48 P:03 C:--- ID:----- LAYER 2 DOWN
```

The hexadecimal bitmask indicates which bearer timeslots on the port are available for calls.

SS7 CIC blocking operations are also reported using the layer 2 filter.

```
16:30:50 P:22 C:--- ID:----- MAINTENANCE BLOCKING USING 0X000000FE FROM
0X000000FE
16:30:50 P:22 C:--- ID:----- MAINTENANCE UNBLOCKING USING 0XFFFFFFF0
FROM 0X000000FE
```

The first bitmask shows which channels were blocked/unblocked. The second bitmask shows the settings from which this bitmask was derived (these are the settings in the Port Blocking dialog, section 5.11.1 and 5.11.2 refers).

In all of the above bitmasks, bit 0 represents channel 0 and bit 31 represents channel 31.

E.4 Call Control

Call control trace will report the significant events between setup and completion of an end-to-end call. The examples shown below are produced by a Euro ISDN to SIP call.

NOTE

Call control events will not always appear in the strict order shown below, and may be interleaved with events from other calls or filters.

NOTE

Events from IP telephony ports are prefixed with `SIP:`.

NOTE

When tracing an end-to-end call, logging must be enabled on the ports carrying both the incoming and outgoing leg of the call.

The first events to appear show that an incoming call has been detected on port 2 channel 1, and report it's called and calling party numbers. An incoming SIP call will also report the SIP URI from which these numbers were parsed. The hexadecimal number and `OPENED TS 1` have no meaning outside Aculab.

```
16:26:48 P:02 C:001 ID:0002141615 INCOMING CALL (0X3b7002), OPENED TS 1
16:26:48 P:02 C:001 ID:0002141615 CALLED NUM : 234501
16:26:48 P:02 C:001 ID:0002141615 CALLING NUM : 543201
```

The incoming call will generate an event to report that an outgoing call has been made. It shows the port and channel (TDM calls only) on which the call has been placed, along with the called number/network address. The hexadecimal number has no meaning outside Aculab.

```
16:26:48 P:02 C:001 ID:0002141615 OPENED OUTGOING (0X00239802) ON P:00 (SIP)
TO <SIP:234501@192.168.16.248>
```

The outgoing call leg will generate events to show that the call has been established, and that alerting has been received from the called party. The `ST:` and `TS:` values are present only on IP telephony calls and have no meaning outside Aculab.

```
16:26:48 P:00 C:000 ID:0002141615 SIP:OUTGOING CALL ON ST:64, TS:00
16:26:48 P:00 C:000 ID:0002141615 SIP:OUTGOING RINGING
```

This event is generated by the incoming call and shows that alerting has been mapped through and the calling party is now waiting for the called party to answer.

```
16:26:48 P:02 C:001 ID:0002141615 WAIT FOR ACCEPT
```

Only IP telephony calls will generate this event, which reports the codec selected for the RTP stream along with the RTP endpoint addresses.

```
16:26:50 P:00 C:000 ID:0002141615 ESTABLISHED G.711 RTP CONNECTION (LOCAL
192.168.16.229:16642 REMOTE 192.168.16.248:3084)
```

The outgoing call leg generates this event to show that the calling party has answered and the call leg between GroomerII and the called party is now fully connected.

```
16:26:50 P:00 C:000 ID:0002141615 SIP:OUTGOING CONNECTED
```

These events show that GroomerII has answered the incoming call, which has now become fully connected.

```
16:26:50 P:02 C:001 ID:0002141615 INCOMING CALL ACCEPTED
16:26:50 P:02 C:001 ID:0002141615 INCOMING CONNECTED
```

These events are generated by the outgoing call to show the called party has disconnected the call, and the RTP resources have therefore been relinquished.

```
16:27:00 P:00 C:000 ID:0002141615 DISCONNECTING G.711 RTP CONNECTION (LOCAL
192.168.16.229:16642 REMOTE 192.168.16.248:3084)
16:27:00 P:00 C:000 ID:0002141615 SIP:OUTGOING CALL GONE IDLE
16:27:00 P:00 C:000 ID:0002141615 SIP:RTP_RELEASE(OUT)
```

These events show that GroomerII has disconnected the incoming leg of the call in response to the called party hangup.

```
16:27:00 P:02 C:001 ID:0002141615 INCOMING CALL DISCONNECTED
16:27:00 P:02 C:001 ID:0002141615 INCOMING CALL HAS GONE IDLE
```

These two events appear at the end of each call to show that GroomerII has prepared the incoming channel to receive a new call.

```
16:27:00 P:02 C:001 ID:0002141645 OPENIN FROM PREVIOUS CALL ID:0002141615
16:27:00 P:02 C:001 ID:0002141645 WAITING FOR INCOMING
```

E.5 Routing

The following is an example of routing trace.

```
16:26:48 P:02 C:001 ID:0002141615 ROUTING "ROUTE TDM - SIP" P:00 C:--
```

The report is generated by the incoming leg of the call and identifies the route against which it was matched, along with the port and channel selected for the outgoing call leg. No channel is specified when an IP telephony port is selected for the outgoing call.

E.6 Switching

The following is a typical example of switching trace.

```
16:26:48 P:02 C:001 ID:0002141615 ON CARD BI ITOO : SW:00 IST:33 ITS:01
OST:64 OTS:00
16:27:00 P:02 C:001 ID:0002141615 SWITCH DISABLE : SW:00 OST:33 OTS:01
```

Switching trace identifies the point at which voice paths switching takes place, and also the resources used on the Aculab telephony card. This latter information has no meaning outside of Aculab.

E.7 RTP/RTT

Events of this type will only be seen when at least one leg of the call is an IP telephony call. They report the various stages of resource allocation and configuration for the RTP and RTT streams. The following are examples of such events.

```
16:26:48 P:00 C:000 ID:0002141615 RTP (OUT) ALLOCATED
16:26:48 P:00 C:000 ID:0002141615 RTT (OUT) ALLOCATED
16:26:49 P:00 C:000 ID:0002141615 RTP (OUT) ECHO CANCELLATION DISABLED
16:26:50 P:00 C:000 ID:0002141615 ESTABLISHED G.711 RTP CONNECTION (LOCAL
192.168.16.229:16642 REMOTE 192.168.16.248:3084)
16:26:50 P:00 C:000 ID:0002141615 ESTABLISHED RTT CONNECTION (LOCAL
192.168.16.229:16412 REMOTE 192.168.16.248:16422)
16:27:00 P:00 C:000 ID:0002141615 DISCONNECTING G.711 RTP CONNECTION (LOCAL
192.168.16.229:16642 REMOTE 192.168.16.248:3084)
```

E.8 Protocol

Protocol trace contains the raw protocol messages sent and received by GroomerII in hexadecimal form. The following is an example of protocol trace.

```
16:26:49 P:02 C:-- RX: 02 01 00 00 08 02 00 2F 05 A1 04 03 80 90 A3
                        18 03 A9 83 81 6C 08 00 80 32 33 34 35 30 31
                        70 07 80 32 33 34 35 30 31
16:26:49 P:02 C:-- TX: 00 01 00 02 08 02 80 2F 02 18 03 A9 83 81
```

Protocol trace is identified only by the port from which it was retrieved. The channel number is usually encoded in the trace itself. Messages received from the remote end are identified by `RX:`, whilst messages transmitted by GroomerII are identified with `TX:`.

The format of protocol trace is specific to the protocol in use, and its interpretation is outside the scope of this document.

Appendix F: SIP custom headers

F.1 SS7 to SIP mapping headers

This section describes the SIP custom headers that are provided to allow SS7 parameters to be presented in a SIP `INVITE`.

Aculab-SS7-Calling-Party-Category

When this header is presented in the `INVITE` of an incoming SIP call:

- If the outgoing call leg is ANSI SS7 the content will be used to populate the Calling Party's Category parameter in the outgoing Initial Address Message, subject to the rules of the route being used.
- If the outgoing call leg is SIP then a copy of this header will be presented unmodified in the outgoing `INVITE`.

This header will be included in the `INVITE` presented by an outgoing SIP call if the incoming call is:

- An ANSI SS7 call. The content of the Calling party's category parameter from the incoming Initial Address Message will be used to populate the header.
- A SIP call that has presented an `Aculab-SS7-Calling-Party-Category` header in the incoming `INVITE`. The incoming header will be copied unmodified into the outgoing call.

The following is an example of the header, along with a description of its parameters.

`Aculab-SS7-Calling-Party-Category: Category=224`

Field	Description
Category	This is the Calling party's category parameter defined in ANSI T1.113-1995, para 3.8. The value is expressed in decimal form.

Aculab-SS7-Carrier-Identification

When this header is presented in the `INVITE` of an incoming SIP call:

- If the outgoing call leg is ANSI SS7 the content will be used to populate a Carrier identification parameter in the outgoing Initial Address Message.
- If the outgoing call leg is SIP then a copy of this header will be presented unmodified in the outgoing `INVITE`.

This header will be included in the `INVITE` presented by an outgoing SIP call if the incoming call is:

- An ANSI SS7 call that contains a Carrier identification parameter in the incoming Initial Address Message. The contents of this parameter will be used to populate the header.
- A SIP call that has presented an `Aculab-SS7-Carrier-Identification` header in the incoming `INVITE`. The incoming header will be copied unmodified into the outgoing call.

The following is an example of the header, along with a description of its parameters.

`Aculab-SS7-Carrier-Identification: ID=2;Plan=1;Digits=e34`

Field	Description						
ID	This is the Type of network identification subfield from the Carrier identification parameter defined in ANSI T1.113-1995, para 3.8A. The value is expressed in decimal form.						
Plan	This is the Network identification plan subfield from the Carrier identification parameter defined in ANSI T1.113-1995, para 3.8A. The value is expressed in decimal form.						
Digits	<p>This is a hexadecimal representation of the Digits subfield from the Carrier identification parameter defined in ANSI T1.113-1995, para 3.8A. The correlation between the digits in the above example and their positions in Figure 9A/T1.113.3 of the specification is:</p> <table> <tr> <td>e</td><td>Digit 1</td></tr> <tr> <td>3</td><td>Digit 2</td></tr> <tr> <td>4</td><td>Digit 3</td></tr> </table>	e	Digit 1	3	Digit 2	4	Digit 3
e	Digit 1						
3	Digit 2						
4	Digit 3						

Aculab-SS7-Carrier-Selection-Information

When this header is presented in the `INVITE` of an incoming SIP call:

- If the outgoing call leg is ANSI SS7 the content will be used to populate a Carrier selection information parameter in the outgoing Initial Address Message.
- If the outgoing call leg is SIP then a copy of this header will be presented unmodified in the outgoing `INVITE`.

This header will be included in the `INVITE` presented by an outgoing SIP call if the incoming call is:

- An ANSI SS7 call that contains a Carrier selection information parameter in the incoming Initial Address Message. The contents of this parameter will be used to populate the header.
- A SIP call that has presented an `Aculab-SS7-Carrier-Selection-Information` header in the incoming `INVITE`. The incoming header will be copied unmodified into the outgoing call.

The following is an example of the header, along with a description of its parameters

`Aculab-SS7-Carrier-Selection-Information: Sel=2`

Field	Description
Sel	This is the Carrier selection information parameter defined in ANSI T1.113-1995, para 3.8B. The value is expressed in decimal form.

Aculab-SS7-Charge-Number

When this header is presented in the `INVITE` of an incoming SIP call:

- If the outgoing call leg is ANSI SS7 the content will be used to populate a Charge number parameter in the outgoing Initial Address Message.
- If the outgoing call leg is SIP then a copy of this header will be presented unmodified in the outgoing `INVITE`.

This header will be included in the `INVITE` presented by an outgoing SIP call if the incoming call is:

- An ANSI SS7 call that contains a Charge number parameter in the incoming Initial Address Message. The contents of this parameter will be used to populate the header.
- A SIP call that has presented an `Aculab-SS7-Charge-Number` header in the incoming `INVITE`. The incoming header will be copied unmodified into the outgoing call.

The following is an example of the header, along with a description of its parameters.

`Aculab-SS7-Charge-Number: NOA=3;Plan=1;Digits=1234bc7`

Field	Description														
NOA	This is the Nature of address indicator subfield from the Charge number parameter defined in ANSI T1.113-1995, para 3.10. The value is expressed in decimal form.														
Plan	This is the Numbering plan indicator subfield from the Charge number parameter defined in ANSI T1.113-1995, para 3.10. The value is expressed in decimal form.														
Digits	<p>This is a hexadecimal representation of the Address signal subfield from the Charge number parameter defined in ANSI T1.113-1995, para 3.10. The correlation between the digits in the above example and their positions in Figure 10B/T1.113.3 of the specification is:</p> <table> <tr><td>1</td><td>1st Address signal</td></tr> <tr><td>2</td><td>2nd Address signal</td></tr> <tr><td>3</td><td>3rd Address signal</td></tr> <tr><td>4</td><td>4th Address signal</td></tr> <tr><td>b</td><td>5th Address signal</td></tr> <tr><td>c</td><td>6th Address signal</td></tr> <tr><td>7</td><td>7th Address signal</td></tr> </table>	1	1 st Address signal	2	2 nd Address signal	3	3 rd Address signal	4	4 th Address signal	b	5 th Address signal	c	6 th Address signal	7	7 th Address signal
1	1 st Address signal														
2	2 nd Address signal														
3	3 rd Address signal														
4	4 th Address signal														
b	5 th Address signal														
c	6 th Address signal														
7	7 th Address signal														

Aculab-SS7-Jurisdiction-Information

When this header is presented in the `INVITE` of an incoming SIP call:

- If the outgoing call leg is ANSI SS7 the content will be used to populate a Jurisdiction information parameter in the outgoing Initial Address Message.
- If the outgoing call leg is SIP then a copy of this header will be presented unmodified in the outgoing `INVITE`.

This header will be included in the `INVITE` presented by an outgoing SIP call if the incoming call is:

- An ANSI SS7 call that contains a Jurisdiction information parameter in the incoming Initial Address Message. The contents of this parameter will be used to populate the header.
- A SIP call that has presented an `Aculab-SS7-Jurisdiction-Information` header in the incoming `INVITE`. The incoming header will be copied unmodified into the outgoing call.

The following is an example of the header, along with a description of its parameters.

`Aculab-SS7-Jurisdiction-Information: Address=2075d4`

Field	Description
Address	This is a hexadecimal representation of the Address signal subfield from the Jurisdiction information parameter defined in ANSI T1.113-1995, para 3.23A. The correlation between the digits in the above example and their positions in Figure 21A/T1.113.3 of the specification is: <div> <div>2</div> <div>1st Address signal</div> </div> <div> <div>0</div> <div>2nd Address signal</div> </div> <div> <div>7</div> <div>3rd Address signal</div> </div> <div> <div>5</div> <div>4th Address signal</div> </div> <div> <div>d</div> <div>5th Address signal</div> </div> <div> <div>4</div> <div>6th Address signal</div> </div>

Aculab-SS7-Originating-Line-Information

When this header is presented in the `INVITE` of an incoming SIP call:

- If the outgoing call leg is ANSI SS7 the content will be used to populate an Originating line information parameter in the outgoing Initial Address Message.
- If the outgoing call leg is SIP then a copy of this header will be presented unmodified in the outgoing `INVITE`.

This header will be included in the `INVITE` presented by an outgoing SIP call if the incoming call is:

- An ANSI SS7 call that contains an Originating line information parameter in the incoming Initial Address Message. The contents of this parameter will be used to populate the header.
- A SIP call that has presented an `Aculab-SS7-Originating-Line-Information` header in the incoming `INVITE`. The incoming header will be copied unmodified into the outgoing call.

The following is an example of the header, along with a description of its parameters.

`Aculab-SS7-Originating-Line-Information: II=34`

Field	Description
II	This is the Originating line information parameter defined in ANSI T1.113-1995, para 3.26A. The value is expressed in decimal form.

Aculab-SS7-Transit-Network-Selection

When this header is presented in the `INVITE` of an incoming SIP call:

- If the outgoing call leg is ANSI SS7 the content will be used to populate a Transit network selection parameter in the outgoing Initial Address Message.
- If the outgoing call leg is SIP then a copy of this header will be presented unmodified in the outgoing `INVITE`.

This header will be included in the `INVITE` presented by an outgoing SIP call if the incoming call is:

- An ANSI SS7 call that contains a Transit network selection parameter in the incoming Initial Address Message. The contents of this parameter will be used to populate the header.

- A SIP call that has presented an `Aculab-SS7-Transit-Network-Selection` header in the incoming `INVITE`. The incoming header will be copied unmodified into the outgoing call.

The following is an example of the header, along with a description of its parameters.

`Aculab-SS7-Transit-Network-Selection: ID=2;Plan=2;Digits=56f8;Circuit=0`

Field	Description								
ID	This is the Type of network identification subfield from the Transit network selection parameter defined in ANSI T1.113-1995, para 3.31C. The value is expressed in decimal form.								
Plan	This is the Network identification plan subfield from the Transit network selection parameter defined in ANSI T1.113-1995, para 3.31C. The value is expressed in decimal form.								
Digits	<p>This is a hexadecimal representation of the Digits subfield from the Transit network selection parameter defined in ANSI T1.113-1995, para 3.31C. The correlation between the digits in the above example and their positions in Figure 27D/T1.113.3 of the specification is:</p> <table> <tr> <td>5</td><td>Digit 1</td></tr> <tr> <td>6</td><td>Digit 2</td></tr> <tr> <td>f</td><td>Digit 3</td></tr> <tr> <td>8</td><td>Digit 4</td></tr> </table>	5	Digit 1	6	Digit 2	f	Digit 3	8	Digit 4
5	Digit 1								
6	Digit 2								
f	Digit 3								
8	Digit 4								
Circuit	This is the Circuit code subfield from the Transit network selection parameter defined in ANSI T1.113-1995, para 3.31C. The value is expressed in decimal form.								

F.2 SIP call recovery headers

This section describes the SIP custom headers that are provided to support SIP call recovery. Section 14.3 describes SIP call recovery.

Aculab-Call-Recovery

This header is presented in the `INVITE` of an outgoing SIP call when that call is a recovery call. The purpose of this header is to allow a remote system to identify a recovery call, and the failed call that it is replacing.

This header has a single parameter, which is the `SIP Call-ID:` header presented by the failed SIP call that is being replaced. At present the maximum length of this field is 51 characters.

The following is an example of the header.

`Aculab-Call-Recovery: 09b3c801-00000000-49b69f65-00001698@192.168.16.247`

F.3 Advice of charge headers

This section describes the SIP custom headers that are provided to allow advice of charge information to be passed to and from a SIP call.

Aculab-Charge

This header is presented in an `INFO` message when the end-to-end call is in the connected state. An `INFO` message can only contain one `Aculab-Charge` header. Where multiple headers are presented the behaviour is undefined.

When interworking from Finnish ISUP to SIP, if the incoming Finnish ISUP port has AOC Mapping enabled then any Aculab-Charge header presented by the outgoing call will be mapped into Finish ISUP Metering pulse message and forwarded to the incoming side.

When interworking from SIP to Finnish ISUP, if the incoming SIP port has AOC Mapping enabled then a Metering pulse message presented by the outgoing call will be mapped into an Aculab-Charge header and forwarded to the SIP side.

The following is an example of the header.

```
Aculab-Charge: Type=sfs-meter;Pulses=15;Tariff=1a
```

Field	Description
Type	This is a string that indicates how the header will be decoded, and must always be set to <code>sfs-meter</code> .
Pulses	This is the decimal representation of the value retrieved from, or to be used in, the Number of metering pulses parameter defined in SFS 5779:1996, para 3.62 and SFS 5869:2001 para 3.101. Valid values for pulses are 1 to 15 inclusive. The behaviour for values outside of this range is undefined.
Tariff	This is a hexadecimal representation of the data retrieved from, or to be used in the Tariff Type parameter defined in SFS 5779:1996, para 3.63 and SFS 5869:2001 para 3.100. This is an optional field, and if not specified a value of 0 (tariff type not indicated) will be used.

F.4 Call information headers

This section describes the SIP custom headers that are provided to allow fault finding information to be presented to remote systems.

Aculab-Call-Information

When making an outgoing call GroomerII will present this header in the SIP `INVITE`.

When receiving an incoming call GroomerII will present this header in each of the following backward messages:

```
183 Session Progress
180 Ringing
200 OK
BYE
```

The following is an example of the header.

```
Aculab-Call-Information: Call-ID=0000001234;Trunk=05;Channel=015
```

Field	Description
Call-ID	This is the <code>ID</code> : against which the call will be recorded in the GroomerII call control trace.
Trunk	<p>When the header is presented by an outgoing SIP call, this is the number of the GroomerII trunk carrying the incoming call leg.</p> <p>When the header is returned to an incoming SIP call, this is the number of the GroomerII trunk selected to carry the outgoing call leg.</p> <p>When the header is presented in a <code>BYE</code> returned to the incoming call leg this will contain the value <code>-1</code> if the call was rejected before a trunk was selected for the outgoing leg (for example the call could not be routed).</p>
Channel	<p>When the header is presented by an outgoing SIP call, this is the number of the channel within the above trunk carrying the incoming call leg.</p> <p>When the header is returned to an incoming SIP call, this is the number of the channel within the above trunk selected to carry the outgoing call leg.</p> <p>When the header is presented in a <code>BYE</code> returned to the incoming call leg this will contain the value <code>-1</code> if the call was rejected before a trunk and/or channel for the outgoing leg was selected (for example the call could not be routed).</p>

F.5 Call control and interworking headers

This section describes the SIP custom headers that are provided to allow miscellaneous call control parameters to be passed between SIP endpoints.

Aculab-Functional-Number

This header is used to pass a Functional Number parameter between GroomerII and a remote endpoint. See section 14.6 for an explanation of Functional Number mapping.

GroomerII will present the header in an outgoing SIP `INVITE`, and will process the header when received in an incoming SIP `INVITE`. The header is not supported in any other SIP message.

The following is an example of the header:

```
Aculab-Functional-Number: 01908273800
```

The Functional Number may be between 1 and 31 characters in length, and may include any combination of the hexadecimal digits `0` to `E`.

Appendix G: Adding and Replacing Prosody X cards

G.1 Adding a Prosody X card

This section explains how to add a Prosody X expansion card into your GroomerII system. Expansion cards may be fitted into all 2U models. 1U systems cannot be fitted with additional cards.

Up to four cards may be fitted into a GroomerII 2U (R720/R730) system, whilst GroomerII 2U (CG2100) systems may be fitted with a maximum of three. If you wish to add additional cards into your system, in the first instance contact your Aculab account manager.

To fit your new card, carry out the following steps:

1. Close down the system and fit the additional card into the chassis as described in the installation guide for your chassis. See section 1.1 to identify the installation guide for your chassis.
2. Power on the system and wait for Microsoft Windows to start (the GroomerII applications will also be started). When the system has started the card will be detected and the Installing device driver software balloon will appear. Wait for this to be replaced by the Intel(R) 82574L Gigabit Network Connection #n and then close down the GroomerII applications.

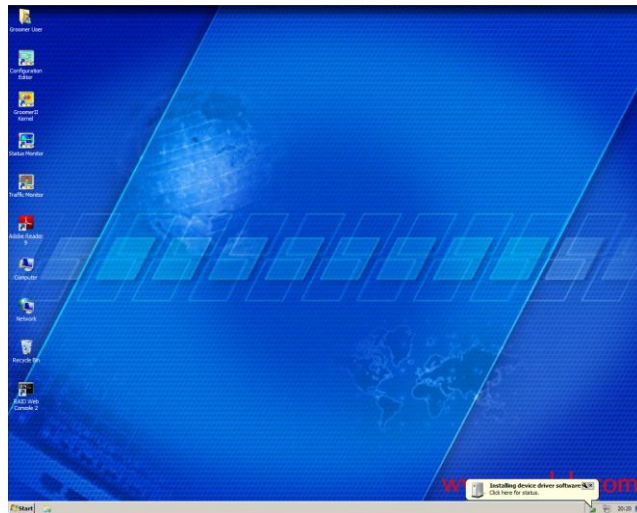


Figure G-1 Microsoft Windows Installing device driver software balloon

3. Open the Microsoft Windows Network Connections window and:
 - Configure the Prosody X NIC address and metric as described in section 3.1.2.
 - Update the network connection order as described in section 3.3.
4. Start the Aculab Configuration Tool (ACT) and configure the new card:
 - Navigate to the Prosody X page and:
 - Configure the Prosody X network settings as described in section 4.8. Ensure that Boot Card is checked before clicking Apply, and wait for the card to reach the In Service state.
 - Use the Flash Card button to apply any updates available for the new card as described in section 4.7. Wait for the card to reach the In Service state.

- Navigate to the Card List page and configure the card name and TDM protocols as described in section 4.4.
 - Navigate to the Clocking Settings page (see section 4.5), and ensure that:
 - The first and last cards in the system are configured to terminate the H.100 bus,
 - All other settings for the new card are configured to the correct default values.
 - Navigate to the TiNG Settings screen and configure each DSP module to load the layout file as described in section 4.9.
 - Return to the Card List screen and verify that the new card is at the end of the list.
 - Click the Apply Settings button and verify that the card is loaded without errors, then close the ACT.
5. Start the GroomerII Configuration Editor, and modify each of your configuration files in turn:
 - Add the new ports as described in section 8.3.
 - Create additional groups for the new ports and/or add them to existing groups as described in section 8.4.
 - Add any new routes required to accommodate the ports on the new card, as described in section 8.5.
 - If any of the ports on the new card are to be used as a clock source, then add them to the Clock Fallback List as described in section 8.6.1.
 - Create any alarm mappings required for the new ports as described in section 8.6.5.
 6. Close the Configuration Editor and power cycle GroomerII.
 7. When GroomerII has restarted the message `NO PORT BLOCKING RECORD - PORT UNBLOCKED` will appear in the Maintenance Messages window for each of the ports on the new card.

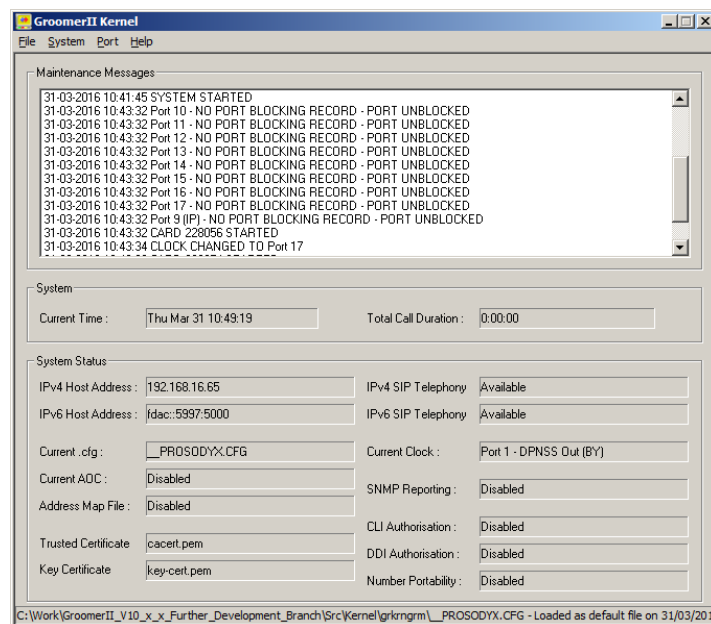


Figure G-2 GroomerII Kernel window showing port blocking message

This message warns that no port blocking record exists for the new port, and the default setting of unblocked has been applied. To create a port blocking record for the new ports, and so prevent the message from being displayed each time GroomerII is started, open the Port Blocking dialog (use the Port – Blocking... menu option) and then close the dialog with the OK button.

8. GroomerII is now ready to pass calls on the new card.

G.2 Replacing a Prosody X card

This section explains how to replace a failed Prosody X card in a GroomerII chassis. Replacement cards may be fitted into 1U carrier grade, 2U carrier grade and 6U chassis. Non-carrier grade 1U systems are not field serviceable, and these chassis must be returned to Aculab for a replacement card to be fitted.

To fit your new card, carry out the following steps:

1. Stop all calls and close down all GroomerII applications.
2. Start the Aculab Configuration Tool (ACT), then:
 - Navigate to the Prosody X page, select the card to be replaced and use the Remove button to delete the card.
 - Click the Save Settings button, followed by Cancel Changes to close the ACT.
3. Power off the system and follow the instructions in the installation guide for your chassis to remove the failed card and fit the replacement. See section 1.1 to identify the installation guide for your chassis.
4. Power on the system and wait for the GroomerII applications to start, then close down these applications.
5. Open the Microsoft Windows Network Connections window then:
 - Select the adapter that is being replaced (this can be identified by the serial number) and open its properties window, then open the Internet Protocol (TCP/IP) properties window for the adapter.
 - Use the OK button to exit both windows without making any changes. This will update the adapter name to show the serial number of the new card.
 - Close the Network Connections window.
6. Start the Aculab Configuration Tool (ACT) and configure the new card:
 - Navigate to the Prosody X page and:
 - Configure the Prosody X network settings as described in section 4.8. Ensure that Boot Card is checked before clicking Apply, and wait for the card to reach the In Service state.
 - Use the Flash Card button to apply any updates available for the new card as described in section 4.7. Wait for the card to reach the In Service state.
 - Navigate to the Card List page and configure the card name and TDM protocols as described in section 4.4.
 - If the card being replaced is the first or last card in the system, navigate to the Clocking Settings page (see section 4.5), and configure the new card to terminate the H.100 bus.
 - Navigate to the TiNG Settings screen and configure each DSP module to load the layout file as described in section 4.9.
 - Return to the Card List screen and use the Card Up and Card Down buttons to move the new card to the correct position in the list.

- Click the Apply Settings button and verify that the card is loaded without errors, then close the ACT.
7. Power cycle GroomerII, and your replacement card will be ready to pass calls.

NOTE

The new card will inherit the port blocking settings of the card it has replaced. If the ports on the original card were blocked to prevent calls from being routed to the faulty card, they must be unblocked before the new card will be able to pass calls.

Appendix H: Host NIC adapter teaming

Host NIC teaming allows multiple host NIC ports to be grouped in a redundant configuration, with each presenting the same IP address to the network. Host NIC teaming is supported on all GroomerII 2U carrier grade chassis (Models 82xx, 100xx and 101xx). These chassis are installed with NIC drivers that support teaming, although it is not enabled by default.

Host NIC teaming is not supported on GroomerII 1U systems (Model 71xx).

H.1 Types of teaming

The Intel PROSet software allows five types of teaming to be configured:

Adapter Fault Tolerance (AFT) – This type of teaming protects against adapter, cable or switch port failure. All host adapters can be included in an AFT team, with a minimum of two being required, and all of the adapters in the team must be connected to the same switch. Primary and secondary adapters may be configured if required.

Switch Fault Tolerance (SFT) – This type of teaming protects against adapter, cable, switch port or switch failure. Only two host adapters can be included in an SFT team, and each must be connected to a separate switch. Primary and secondary adapters may be configured if required. When using SFT each adapter must be connected to a switch, the use of hubs is not supported.

NOTE

If the switches used in a Switch Fault Tolerance configuration are cross-connected, the Spanning Tree Protocol must be supported.

Adaptive Load Balancing – GroomerII does not support this type of teaming.

Static Link Aggregation – GroomerII does not support this type of teaming.

IEEE 802.3ad Dynamic Link Aggregation – GroomerII does not support this type of teaming.

It is the responsibility of the customer to identify and implement any network configuration that may be required to support host NIC teaming.

H.2 Teaming configuration

This section explains how to configure teaming on GroomerII. Note that additional or alternative adapters may be present on some models.

From the Windows desktop use the Computer icon to open the System window and select Device Manager to open the Device Manager Window. Select the first host adapter, open it's properties window and select the Teaming tab.

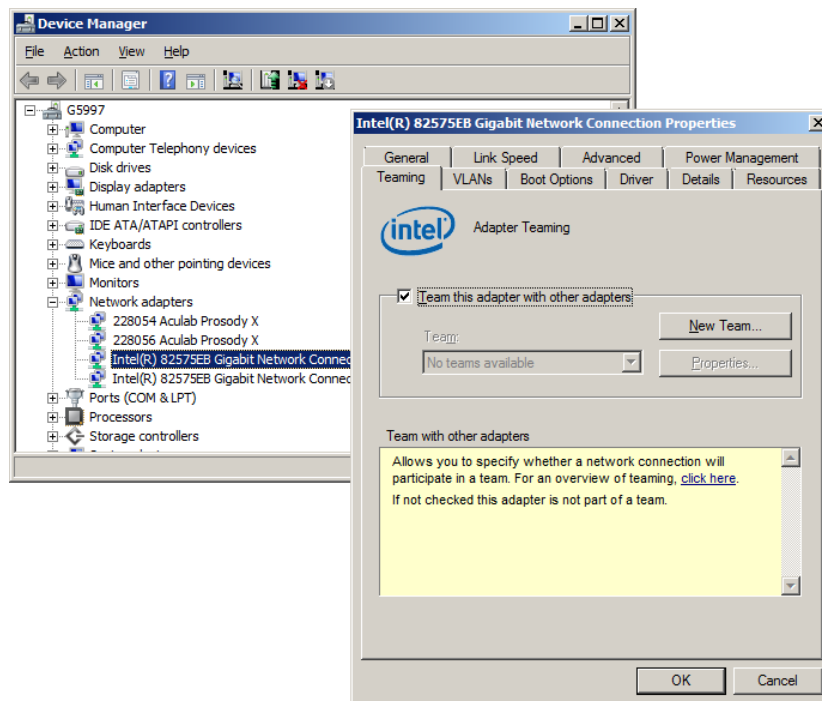


Figure H-1 Device Manager and host adapter properties window

Tick the Team this adapter with other adapters checkbox and click the New Team... button to start the New Team Wizard.

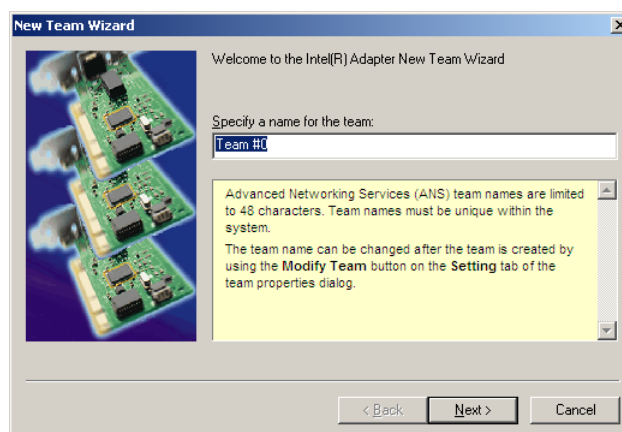


Figure H-2 New Team Wizard – Specify team name

Enter the team name and proceed to the next screen.

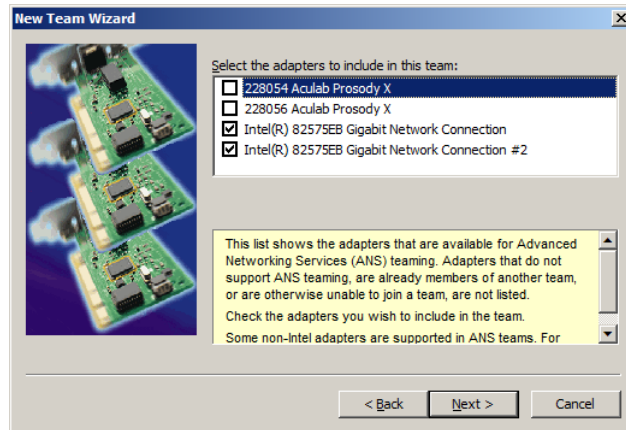


Figure H-3 New Team Wizard – Select adapters

Select the host NIC adapters to be included in the team and proceed to the next screen.

NOTE

Aculab Prosody X cards must not be included in a team.

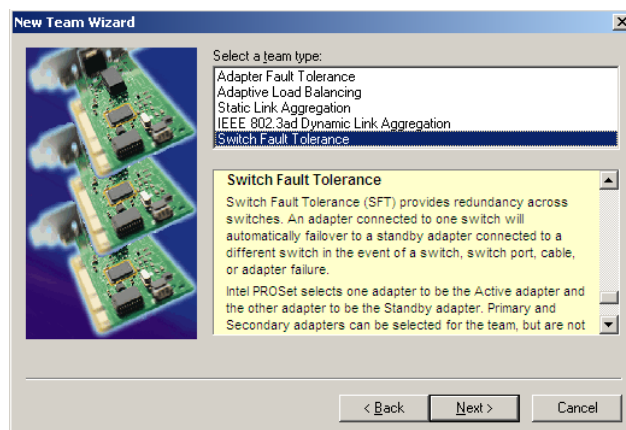


Figure H-4 New Team Wizard – Select team type

Select the type of team to be configured. This should be either Adapter Fault Tolerance or Switch Fault Tolerance. Proceed to the next screen.

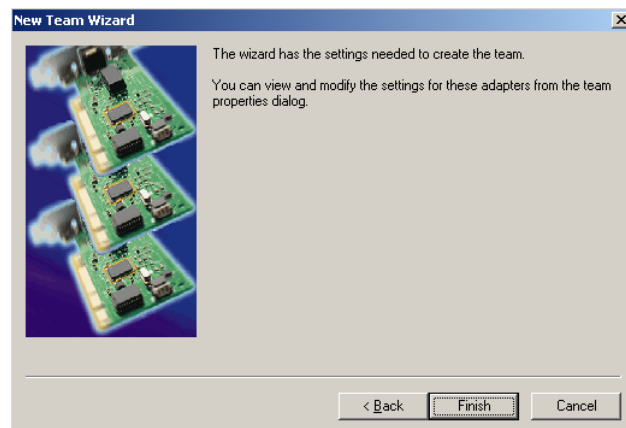


Figure H-5 New Team Wizard - Finish

Click the Finish button. The team will be created and added to the Device Manager window, and the team properties dialog opened. Close all windows and dialog boxes and then open the Network Connections window.

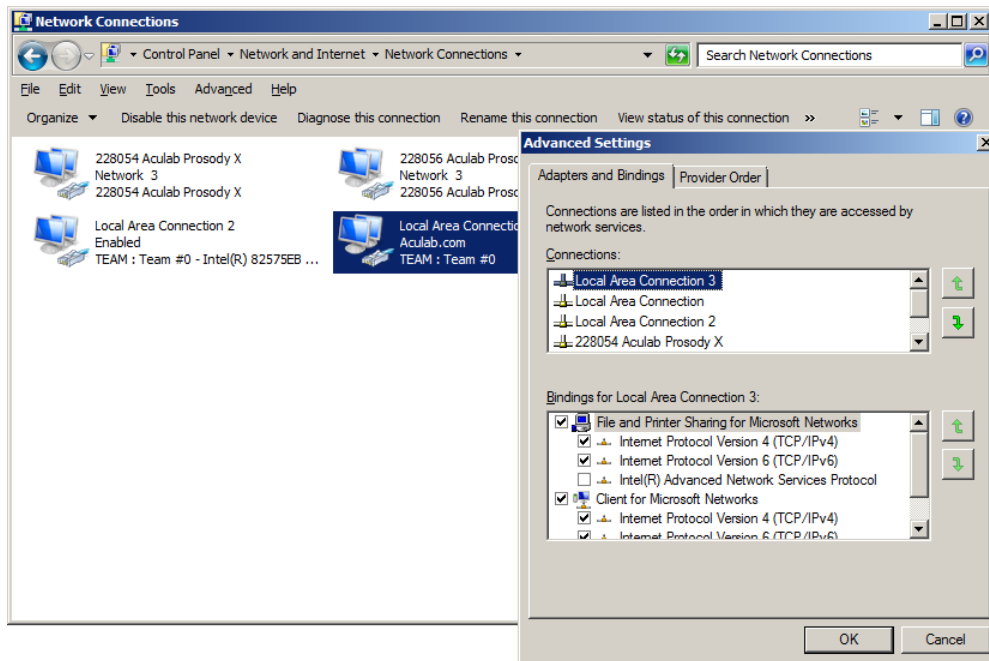


Figure H-6 Network Connections window

The team will appear as an additional Local Area Connection, and must now be configured as described in section 3. In the Connections pane of the Advanced Settings dialog (described in section 3.3), place the network connections in the following order

- The host NIC team
- The team member adapters
- Any non-teamed host adapters
- The Prosody X cards in their installed order

Any other connections present should follow the above.

H.3 Primary and secondary adapter configuration

By default the Intel PROSet software will automatically manage the selection of primary and secondary adapters. Should you prefer to nominate the order in which adapters will be selected, use the following procedure

- Open the Device Manager and select the team
- Open the team properties dialog, select the Settings tab and click the Modify Team... button to open the team dialog

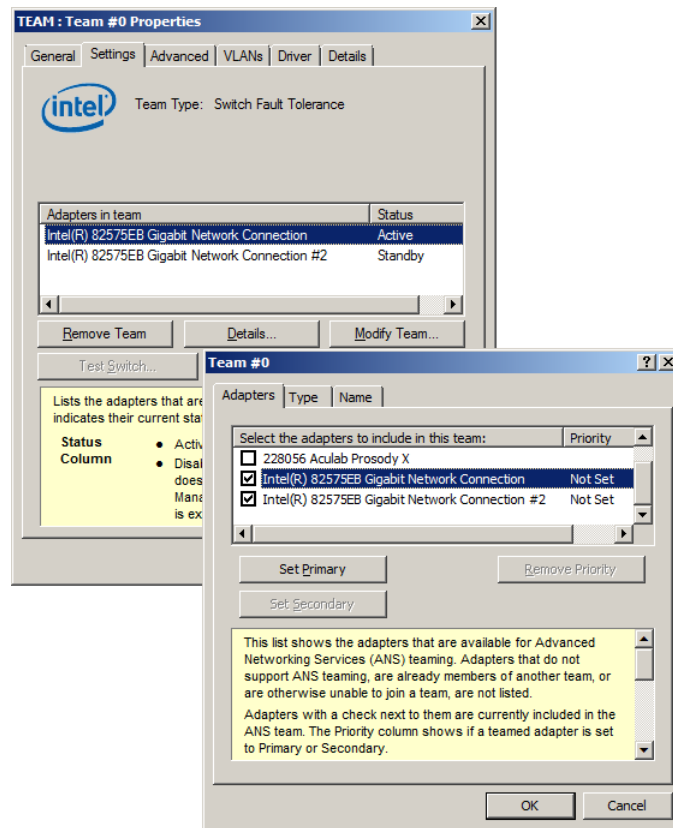


Figure H-7 Setting adapter priority

Use the Set Primary, Set Secondary and Remove Priority buttons to set the adapter priorities.

NOTE

If the team contains more than two adapters, you will only be able to assign primary and secondary adapters. All other adapters in the team are given tertiary status, and the driver will determine the order in which they are used.

Appendix I: Configuring SIP signalling QoS on Microsoft Windows 7 and Microsoft Windows Server 2008

This section describes how to apply QoS marking to SIP signalling traffic generated by GroomerII when running the Microsoft Windows 7 Professional or Microsoft Windows Server 2008 R2 operating system. When using the Microsoft Windows XP Professional or Microsoft Windows Server 2003 operating systems, QoS marking of SIP signalling traffic should be applied using the GroomerII Configuration Editor (refer to section 8.6.7).

QoS marking is applied by creating one or more policies using the Local Group Policy Editor. The instructions below show how to create a simple policy that will apply a single QoS setting to all SIP signalling traffic generated by GroomerII.

NOTE

Should you wish to do any of the following, you will need to create multiple policies:

- Apply different QoS settings to individual source and/or destination IP addresses,
- Apply different QoS settings dependent upon the type of transport,
- Apply different QoS settings to individual source and/or destination ports.

Start the Local Group Policy Editor by using Run... to execute `gpedit.msc`.

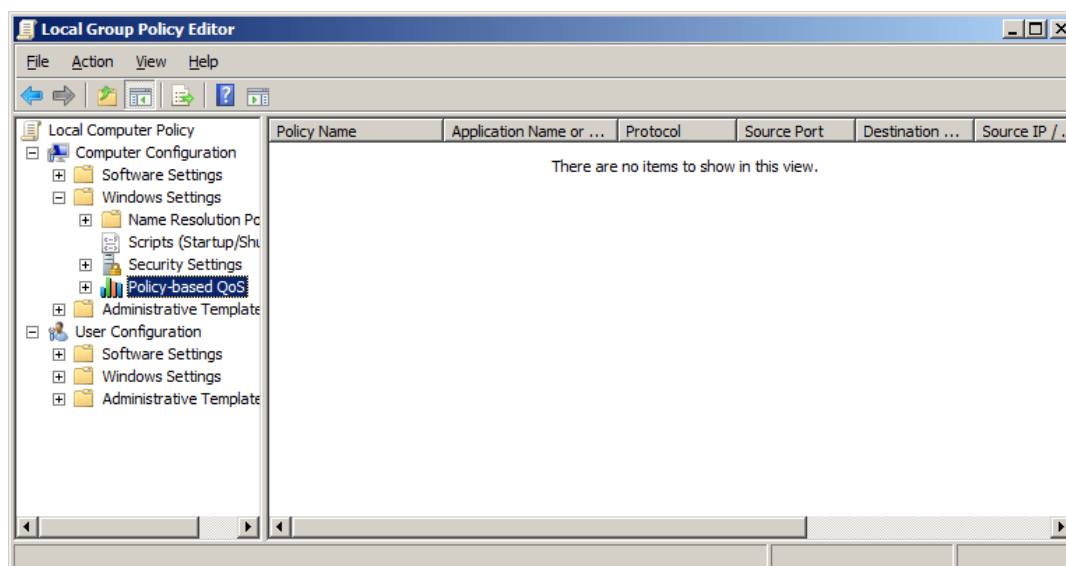


Figure I-1 Local Group Policy Editor

Right click on Computer Configuration – Windows Settings – Policy-based QoS and select Create new policy... to open the Create a QoS policy window.

Figure I-2 Policy-based QoS – Create a QoS policy window

Enter a suitable name, for example *SIP Signalling Traffic*, into the Policy name field.

Tick Specify DSCP Value and set the required value using the spin control. This setting will be applied to all SIP signalling traffic using this policy.

The following values correspond to the named constants specified in IETF RFC 4595.

DSCP name	DSCP value
AF11	10
AF12	12
AF13	14
AF21	18
AF22	20
AF23	22
AF31	26
AF32	28
AF33	30
AF41	34

DSCP name	DSCP value
AF42	36
AF43	38
CS0	0
CS1	8
CS2	16
CS3	24
CS4	32
CS5	40
CS6	48
EF	46

Leave the Specify Outbound Throttle Rate checkbox clear, and click the Next > button to proceed to the This QoS policy applies to: window.

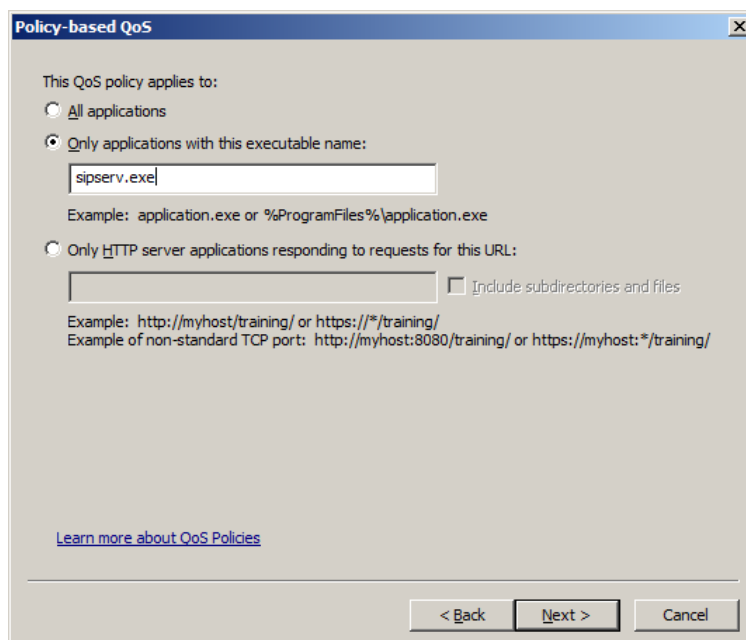


Figure I-3 Policy-based QoS – This QoS policy applies to window

Select the Only applications with this executable name radio button and type *sipserv.exe* into the edit field.

Click the Next > button to proceed to the Specify the source and destination IP addresses window.

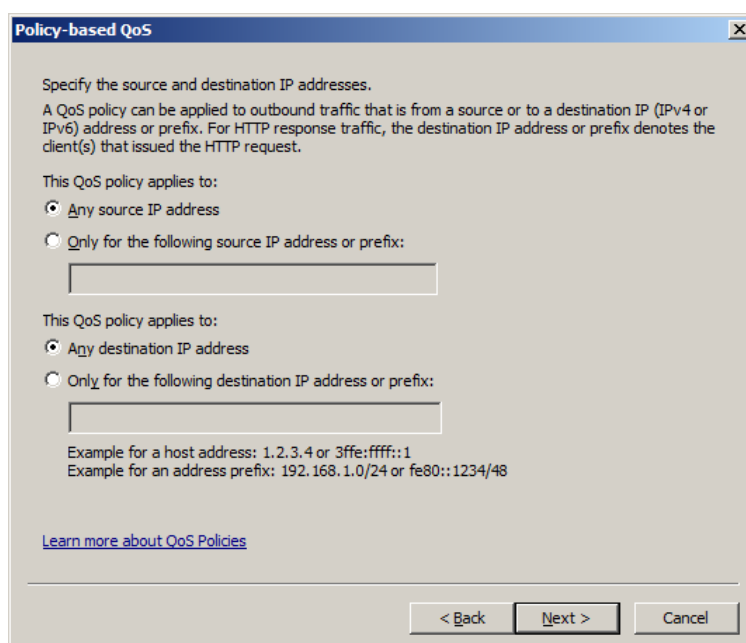
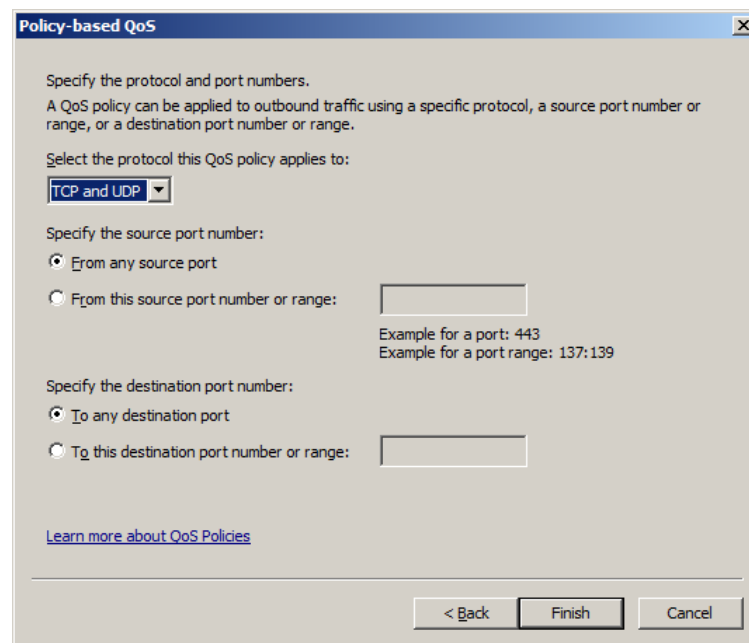


Figure I-4 Policy-based QoS – Specify the source and destination IP addresses window

Select the Any source IP address radio button. This will apply QoS marking to SIP signalling traffic, regardless of whether it is sent from the SIP signalling (host) port, or a Prosody X card during failover.

Select the Any destination address radio button. This will apply QoS marking to SIP signalling traffic sent to any destination address.

Click the Next > button to proceed to the Specify the protocol and port numbers window.



Policy-based QoS

Specify the protocol and port numbers.
A QoS policy can be applied to outbound traffic using a specific protocol, a source port number or range, or a destination port number or range.

Select the protocol this QoS policy applies to:

Specify the source port number:
☒ From any source port
☐ From this source port number or range:
Example for a port: 443
Example for a port range: 137:139

Specify the destination port number:
☒ To any destination port
☐ To this destination port number or range:

[Learn more about QoS Policies](#)

< Back Finish Cancel

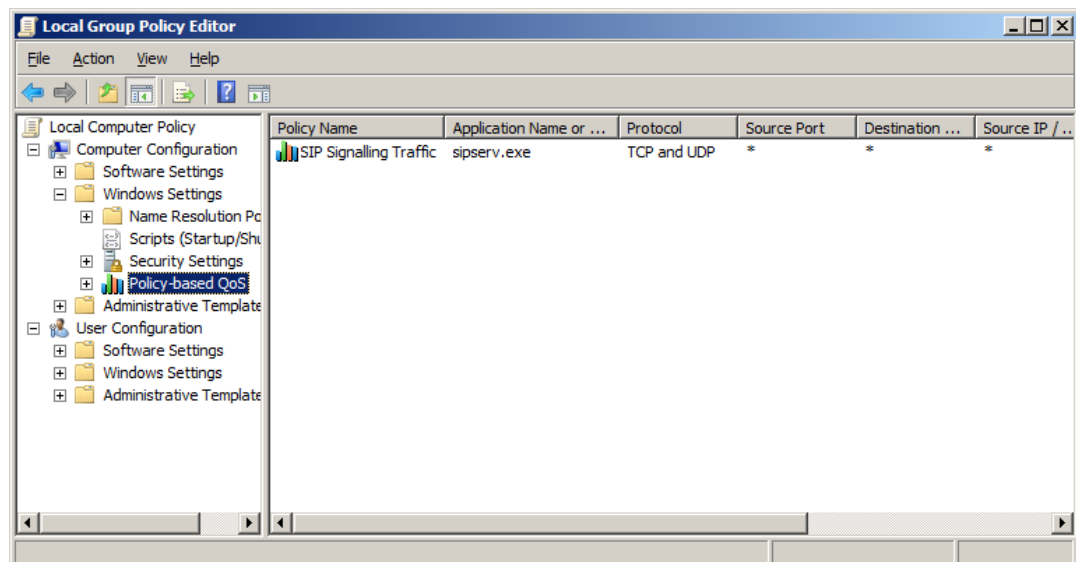
Figure I-5 Setting adapter priority

Set the Select the protocol this QoS applies to dropdown to TCP and UDP. This will apply QoS marking to both TCP and UDP traffic.

Select the From any source port radio button. This will apply QoS marking to SIP signalling traffic sent from any port.

Select the To any destination port radio button. This will apply QoS marking to SIP signalling traffic directed to any destination port.

Click the Finish button save the policy and return to the Local Group Policy Editor window.



Local Group Policy Editor

File Action View Help

Local Computer Policy

- Computer Configuration
 - Software Settings
 - Windows Settings
 - Name Resolution Policies
 - Scripts (Startup/Shutdown)
 - Security Settings
 - Policy-based QoS**
 - Administrative Template
- User Configuration
 - Software Settings
 - Windows Settings
 - Administrative Template

Policy Name	Application Name or ...	Protocol	Source Port	Destination ...	Source IP / ..
SIP Signalling Traffic	sipserv.exe	TCP and UDP	*	*	*

Figure I-6 Local Group Policy Editor

Appendix J: The sipserv.cfg file

The `sipserv.cfg` file is a configuration file that allows the default behaviour of the Aculab SIP service to be modified.

In general the GroomerII application software relies upon the default behaviour of the SIP service in order to operate correctly, and modifying this behaviour may have unpredictable results such as call failure or a system crash. Section J.1 describes the `sipserv.cfg` parameters that are available for use with GroomerII, whilst section J.2 lists those that must not be used. If the parameter you wish to use is not listed in either section contact Aculab Technical Support for advice.

The `sipserv.cfg` file does not form part of the standard installation, and is generated by executing `sipserv -g` at the command line. The file is located at `C:\Program Files (x86)\Aculab\v6\cfg`.

The GroomerII Backup and Restore utility will backup and restore the `sipserv.cfg` file if present.

NOTE

GroomerII must be power cycled before any changes to `sipserv.cfg` will take effect.

J.1 Supported parameters

The following parameters may be used with GroomerII. These parameters have been tested to ensure they have no impact upon GroomerII operation, and their use will be maintained in future versions.

Allow headers

A number of `Allow` headers are automatically added by the SIP service (currently `INVITE`, `ACK`, `BYE`, `CANCEL`, `OPTIONS`, `NOTIFY`, `REFER`, `PRACK`, `INFO`, `UPDATE`, and `MESSAGE`). Automatic production of these headers can be disabled with the `AllowUseSupplied` parameter:

```
AllowUseSupplied = 1
```

When `AllowUseSupplied` is set to 1, each `Allow` parameter present in the file will be used to generate an `Allow:` header. For example

```
AllowUseSupplied = 1
Allow = INVITE
Allow = ACK
Allow = BYE, CANCEL, OPTIONS
```

would produce an `INVITE` containing the headers

```
Allow: INVITE
Allow: ACK
Allow: BYE, CANCEL, OPTIONS
```

Setting `AllowUseSupplied = 1` in a file that contains no `Allow` parameters will produce SIP messages that contain no `Allow:` headers.

Any `Allow` parameters present in the file will be ignored when `AllowUseSupplied` is set to zero.

Supported headers

A number of `Supported` headers are automatically added by the SIP service (currently `replaces` and `100rel`). Automatic production of these headers can be disabled with the `SupportedUseSupplied` parameter:

```
SupportedUseSupplied = 1
```

NOTE

The GroomerII application will add additional `Supported` headers dependent upon the functionality in use (for example, `Supported: histinfo`). The inclusion of such parameters is not controlled by the `SupportedUseSupplied` parameter, and so it is not possible to remove them.

When `SupportedUseSupplied` is set to 1, each `Supported` parameter present in the file will be used to generate a `Supported:` header. For example

```
SupportedUseSupplied = 1
Supported = replaces
Supported = 100rel, mytag
```

would produce an `INVITE` containing the headers

```
Supported: replaces
Supported: 100rel, mytag
```

Setting `SupportedUseSupplied = 1` in a file that contains no `Supported` parameters will produce SIP messages that contain no `Supported:` headers.

Any `Supported` parameters present in the file will be ignored when `SupportedUseSupplied` is set to zero.

Raw cause on timeout

When an outgoing SIP call is made to an unresponsive endpoint the call is cleared after a timeout, and the SIP service sends a default response of zero to the GroomerII application. An alternative SIP response can be configured using the `RawCauseOnTimeout` parameter, for example:

```
RawCauseOnTimeout = 486
```

This cause will be returned by all calls that are cleared due to a timeout, and will be mapped through to the incoming call leg.

J.2 Unsupported parameters

GroomerII does not support use of the following parameters, which must always remain at their default settings.

Parameter	Default setting
<code>OneLineHeaders</code>	<code>OneLineHeaders = 0</code>

Appendix K: GroomerII chassis identification

The GroomerII Chassis ID application is available on the GroomerII 1U (AC2460) chassis only. Its purpose is to allow the system identification LED to be illuminated when accessing the chassis remotely. Refer to the GroomerII 1U chassis (AC2460) installation guide (MAN1028) for system information.



Use the GroomerII Chassis ID icon on the desktop to open the GroomerII Chassis ID dialog.

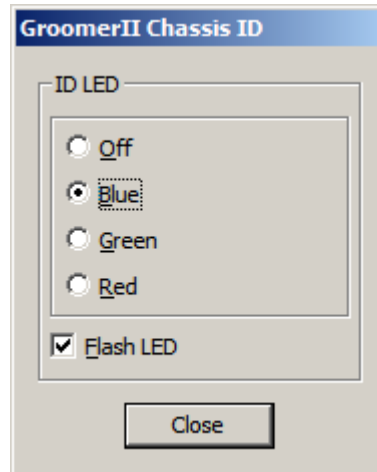


Figure K-1 GroomerII Chassis ID dialog

The dialog controls will be initialized to show the current state of the chassis identification LED when the dialog is opened.

The Blue, Green and Red radio buttons are used to illuminate the LED in the selected colour. Select the Off radio button to extinguish the LED.

Tick the Flash LED checkbox to set the LED into continuous blinking mode at a rate of one second on, one second off. Unticking the checkbox returns the LED to solid illumination.

Use the Close button to close the dialog. The LED will continue to be illuminated in the selected colour and mode once the dialog has been closed.

NOTE

The LED settings are not maintained across system shutdown. When the system is powered on the system identification LED is always initialised to off.