

Installation, Operation, Maintenance Manual

Version 6.6

Document # LTRT-92224



Contents

1	Introduction	31
	Hardware Overview	33
2	Hardware Components	35
3	Front and Back Views	37
4	The Chassis	39
4.1	NEBS Compliancy	40
4.2	Midplane Keying.....	40
5	Power System.....	41
5.1	PEM/DC/8K Power Entry Module	41
5.2	PS/DC/8K Power Supply Module.....	42
5.2.1	DC Input Power	42
6	Cooling System	43
6.1	Air Flow.....	43
7	Alarm Indicators	45
8	TP-6310 Media Gateway Board	47
9	6310/RTM - Rear Transition Module.....	49
9.1	6310/RTM Redundant.....	51
10	TP-8410 Media Gateway Board	53
10.1	LED Array Display.....	55
11	8410/RTM Rear Transition Module.....	57
11.1	8410/RTM E1/T1 Trunk Connectors	58
11.2	8410/RTM Redundant.....	61
12	System Controller (SC) Board.....	63
12.1	SC Rev.1 board (Solaris OS)	64
12.1.1	SC Rev.1 Mini DIN 8 COM RS-232 Port.....	65
12.1.2	Status LEDs	65
12.2	SC Rev.2 Board (Linux OS)	66
12.2.1	SC Rev.2 RS-232 Serial Port	67
12.2.2	USB Ports	67
12.2.3	VGA Port.....	67
12.2.4	Status LEDs	68
12.3	SA/RTM Synchronization and Alarm Rear Transition Module	69
12.3.1	SA/RTM RS-232 Console Port	70
12.3.2	SA/RTM Terminal Block Connector	71
12.3.3	SA/RTM BITS (RJ48-c) Pin Signal Interface (Optional)	71
12.3.3.1	Built-In LED Interface.....	72

13 Ethernet Switch Board	73
13.1 ES/6600 ES (Ethernet Switch) Board	73
13.1.1 ES/6600 Board Panel	74
13.1.2 ES/6600 LEDs	75
13.1.3 ES/6600 Physical Slots to Ethernet Port Mapping	76
13.1.4 ES/6600/RTM Rear Transition Module	78
13.2 ES-2 ES (Ethernet Switch) Board	80
13.2.1 ES-2 Front Panel	81
13.2.2 ES-2 LEDs	82
13.2.3 ES-2 Physical Slots to Ethernet Port Mapping	83
13.2.4 ES-2 RTM Rear Transition Module	85
14 Board Assembly Order	87
Getting Started	89
15 Site Preparation	91
15.1 Equipment Requirements	91
15.2 Cables	92
15.2.1 E1/T1 Cables for TP-8410	93
15.3 Electrical Requirements	94
15.4 Environmental Requirements	95
15.5 Preparing the IP Network Connectivity	96
15.6 Allocating IP Addresses	97
15.7 Preparing the PSTN Network Connectivity	98
15.7.1 Preparing the STM-1/OC-3 PSTN Connections	98
15.7.2 Preparing the T3 PSTN Connections	98
15.7.3 Preparing the E1/T1 PSTN Connections	98
15.8 Installing the EMS Server and Client	98
16 Hardware Installation	99
16.1 Unpacking/Checking Contents	99
16.2 Mounting the Chassis on a Rack	100
16.3 Earthing the Chassis	102
16.4 Lightning Protection	103
16.5 Powering Up	103
16.5.1 Connecting the Mediant 8000 to the DC Power Supply	104
16.5.2 Initial Power On	107
17 The Command Line Interface (CLI)	109
17.1 Connecting to the CLI via an RS-232 Serial Console	109
17.2 Connecting to the CLI via the IP Internet Network	112
17.2.1 Connecting to the CLI via Secure Shell (SSH)	112
17.3 Command Line Interface Users	113
17.3.1 Logging into the Command Line Interface	115
17.3.2 Logging in as a Root User	115
17.3.2.1 Option 1	115
17.3.2.2 Option 2	115

18	Connecting to the IP Network	117
18.1	Preparing the External Layer Switches or Routers	117
18.2	Configuring the Basic IP Network Parameters of SC Boards	118
18.3	Connecting IP Network Cables	121
19	Connecting to the PSTN Network	123
19.1	Connecting STM-1/OC-3 PSTN Cables	123
19.1.1	SFP Modules.....	123
19.1.2	Fiber Optic Cables.....	124
19.2	Connecting the T3 PSTN Interfaces.....	125
19.3	Connecting E1/T1 PSTN Cables (TP-8410 Boards).....	125
20	Connecting to External Telco Alarm Equipment	127
21	Software Installation and Basic Configuration	129
21.1	Installing the Mediant 8000 Software.....	129
21.1.1	The Mediant 8000 Installation Package.....	130
21.1.2	Transferring the Mediant 8000 Installation Package to the SC Boards	131
21.1.3	Preparing for the Mediant 8000 Software Installation	133
21.1.4	Installing the Mediant 8000 Software on the SC Board to Operate as the Active board	134
21.1.5	Installing the Mediant 8000 Software on the SC Board to Operate as the Standby Board	140
21.2	Performing Basic Configuration of the Mediant 8000 Software	146
21.2.1	Performing Basic Configuration of the Mediant 8000 Software on the SC board to Operate as the Active Board	147
21.2.2	Performing Basic Configuration of the Mediant 8000 Software on the SC Board to Operate as the Standby Board.....	150
21.3	Starting Mediant 8000 Software	153
21.4	Configuring Connectivity with the EMS Server.....	154
22	Advanced Configuration.....	155
Configuring and Operating the Media Gateway (Part 1).....		157
23	Overview	159
23.1	Management Interfaces	159
23.2	AudioCodes Element Management System (EMS)	159
23.3	SNMP Management Interface	160
23.4	CLI Management Interface.....	160
23.5	Syslog Management Interface.....	160
23.6	Managed Objects, Administrative and Operational State	160
23.6.1	MO Tree Hierarchy.....	161
23.6.2	MO States	161
23.6.3	Lock/Unlock Actions	162
23.7	Managed Objects (MOs) in the EMS	162
23.8	Modifying the Media Gateway Configuration	165
23.9	Faults and Alarms Monitoring.....	167
23.9.1	Alarm Throttling	170

24	SNMP Management Interface	171
24.1	Configuring Connectivity between the Media Gateway and the EMS Server	171
24.2	Configuring Connectivity between the Media Gateway and Additional SNMP Managers.....	175
25	Syslog Management Interface.....	177
25.1	Configuring Connectivity between the Media Gateway and the Syslog Server	178
25.2	Securing the Syslog Management Interface	178
26	Connecting the Media Gateway to the IP Network	179
26.1	Establishing Connectivity with the EMS Server.....	180
26.2	Configuring Network Topology.....	183
26.2.1	Types of IP Network Traffic and Network Subnets.....	183
26.2.2	Use of OAM, Control and Media Subnets by Mediant 8000 Boards.....	185
26.2.3	Connecting Mediant 8000 to IP Network	185
26.2.4	Configuring IP Network Interfaces	186
26.2.5	Working with VLANs.....	188
26.2.5.1	Using Tagged VLANs for Subnet Separation	188
26.2.5.2	Configuring VLAN Tags	188
26.2.5.3	Configuring VLAN Tags for OAM Subnet	189
26.2.5.4	Configuring VLAN Tags for Media and Control Subnets.....	189
26.2.6	Media Link Aggregation.....	191
26.2.6.1	Benefits.....	191
26.2.6.2	Distribution Rules.....	191
26.2.6.3	Link Aggregation Control Protocol.....	193
26.2.6.4	Aggregated Link Failure Detection	193
26.2.6.5	Configuring Media Link Aggregation	194
26.3	Configuring IP Network Connectivity on SC Boards	196
26.3.1	Additional OAM Subnet Configuration	197
26.4	Configuring IP Network Connectivity on Media Gateway Boards	198
26.4.1	IP Subnets.....	198
26.4.1.1	Configuring IP Subnets.....	199
26.4.2	IP Network Profiles.....	200
26.4.2.1	Creating IP Network Profile	201
26.4.2.2	Attaching IP Network Profile to the Media Gateway Board	201
26.4.3	Configuring Media Gateway Board's IP Addresses	202
26.5	Additional Network Settings.....	203
26.5.1	Static Routes.....	203
26.5.1.1	Static Routes for SC Boards.....	203
26.5.1.2	Static Routes for Media Gateway (TP) Boards	204
26.5.2	Quality of Service	206
26.5.2.1	Ethernet Frame Priority Header	207
26.5.2.2	Differentiated Services (DiffServ)	208
26.5.3	Configuring IPv6.....	210
26.5.4	Configuring Media Realms	210
26.6	Additional Network Services and Settings.....	212
26.6.1	Activating New Network Interfaces Configuration	214
26.6.1.1	Offline Network Configuration of ES/6600.....	214
26.6.1.2	Offline Network Configuration of ES-2.....	215
26.6.1.3	Online Network Configuration.....	215
26.6.2	Activating Offline Network Configuration	216

26.7	Connecting the Mediant 8000 to the IP Network	217
26.7.1	Ethernet Ports Allocation on the ES/6600 Board	217
26.7.2	Ethernet Ports Allocation on ES-2-SINGLE boards	219
26.7.3	External Layer 3 Ethernet Switches or Routers	221
26.7.3.1	Configuring HSRP/VRRP Protocols on External Layer 3 Switches ..	222
26.7.3.2	Configuring the Mediant 8000 for the HSRP Protocol	222
27	Working with the SC Boards	223
27.1	Redundancy Mode	223
27.2	SC Boards in the EMS	224
27.3	SC Board Actions.....	225
27.4	SC Board Hardware Revisions.....	225
27.5	The Operating System on the SC Boards.....	226
27.6	Installing the Solaris OS on the SC Rev.1 Board	227
27.6.1	Verifying the Current Version of the Solaris OS on the SC Board.....	227
27.6.2	Installation Requirements	228
27.6.3	Preparing the 'Install Image' on the Install Server (EMS)	228
27.6.4	Installing the Solaris 9 OS on the SC Board	229
27.7	Installing the Linux OS on the SC Rev.2 Board	231
27.7.1	Verifying the Current Version of the Linux OS on the SC Board	231
27.7.2	Linux OS Installation Requirements.....	232
27.7.3	Re-installing the Linux OS via the Remote Network Connection.....	233
27.7.4	Re-installing the Linux OS via the RS-232 Serial Console	235
27.7.5	Installing the Linux OS from the USB Flash Drive via the RS-232 Serial Console.....	238
27.7.5.1	Preparing the USB Flash Drive	238
27.7.5.2	Installing from the USB Flash Drive.....	241
27.7.6	Installing the Linux OS from the USB CD/DVD Drive via the RS-232 Serial Console.....	244
28	Working with the Media Gateway Boards (TP-6310 and TP-8410)	245
28.1	Redundancy Model Overview.....	245
28.2	Media Gateway Boards in the EMS	246
28.3	Hardware and Application Types	247
28.4	Media Gateway Board Actions	247
28.5	The Redundancy Model	249
28.5.1	Configuring Redundant Media Gateway Board.....	249
28.5.2	Redundancy Modes	250
28.5.3	Desired Redundancy Mode	251
28.5.4	Actual Redundancy Mode	252
28.5.5	Activity Switchover	254
28.5.6	Multiple Redundancy Groups	255
28.5.7	Automatic Switchback	258

28.6	Updating License Key	259
29	Working with the ES Boards	261
29.1	ES Redundancy Mode	261
29.2	ES Boards in the EMS.....	261
29.3	ES Board Actions – ES/6600	262
29.4	ES Board Actions – ES-2	262
Configuring and Operating the Media Gateway (Part 2).....		263
30	Time and Date Configuration	265
30.1	Time Zone Settings	265
30.2	Using the EMS Server as the NTP Server.....	266
30.3	Using External NTP Servers	266
30.3.1	External NTP Servers Setup - Option 1	267
30.3.2	External NTP Servers Setup - Option 2	268
30.4	NTP Synchronization and Status	269
30.5	Internal NTP Implementation.....	270
30.6	Configuring NTP Servers.....	271
30.7	Viewing NTP Servers' Status.....	273
31	Configuring the MGCP/MEGACO Protocols	277
31.1	Media Gateway Controller	277
31.1.1	Media Gateway Controller in the EMS.....	277
31.2	MGCP Control Protocol	278
31.3	MEGACO Control Protocol.....	278
31.4	Media Gateway Controller Addressing.....	279
31.4.1	Via FQDN Name	279
31.4.2	Via IP Addresses.....	279
31.5	Endpoint Name Provisioning	280
31.5.1	Physical Terminations	280
31.5.2	Ephemeral Terminations (for MEGACO only)	281
31.5.2.1	Example 1	281
31.5.2.2	Example 2	281
31.5.2.3	Example 3	281
31.6	Domain Name Provisioning.....	282
31.7	MEGACO Virtual Gateways	282
31.8	Configuring MGCP/MEGACO Call Control Settings	283
31.8.1	Configuring MEGACO Virtual Gateways	283
31.8.2	Configuring Media Gateway Controller	285
31.8.3	Associating Media Gateway Controller with Media Gateway Boards	288
31.8.4	Configuring Additional MGCP/MEGACO Settings	289
32	V5.2 Access Gateway.....	293
32.1	Overview	293
32.1.1	Working with the V5.2 Access Gateway	294
32.1.1.1	V5.2 Interface Status and Maintenance Actions	294
32.1.1.2	V5.2 Link Status and Maintenance Actions	295
32.1.1.3	V5.2 User Ports Status	295

32.1.2	Configuring the V5.2 Access Gateway	296
32.1.2.1	Configuring Media Gateway board's PSTN parameters	296
32.1.2.2	Configuring Trunks for the V5.2 Access Gateway application	296
32.1.2.3	Configuring V5.2 Interfaces	297
32.1.2.4	Configuring V5.2 Links.....	298
32.1.2.5	Configuring V5.2 User Ports.....	299
32.1.2.6	Bringing V5.2 Interfaces "In Service".....	301
33	Configuring Security Settings.....	303
33.1	Security Configuration Guidelines	305
33.2	Secure Operation Mode.....	306
33.2.1	Enabling Secure Operation Mode.....	307
33.2.2	Disabling Secure Operation Mode.....	308
33.3	Secure Access to the SNMP Management Interface	308
33.4	Secure Access to the CLI Interface.....	309
33.4.1	SSH Protocol.....	309
33.4.2	SCP and SFTP Protocols	309
33.5	Disabled Remote Root Login	309
33.5.1	Enabling a Direct Remote Root Login.....	310
33.5.2	Disabling a Direct Remote Root Login.....	311
33.6	OS Hardening	311
33.7	OS Security Patches (on SC boards).....	312
33.7.1	Installing OS Security Patches from a Latest Installation Package	313
33.7.2	Installing the Latest OS Security Patches from the "OS Security Patch Bundle"	315
33.8	File System Integrity	316
33.8.1	Viewing the File System Integrity Status.....	316
33.8.2	Scheduling File System Integrity Check	318
33.8.3	Restoring File System Integrity.....	319
33.9	OS Auditing on SC Boards.....	320
33.9.1	Auditing Goal.....	320
33.9.2	Auditing Trail File.....	320
33.9.3	OS Auditing on the Mediant 8000 Media Gateway	321
33.9.3.1	Analyzing the Audit Trail File on the Solaris OS.....	321
33.9.3.2	Analyzing the Audit Trail File on the Linux OS	321
33.10	X.509 Public Key Infrastructure	325
33.10.1	Initial Configuration.....	326
33.10.2	Self-Signed Certificate.....	327
33.10.3	Generating a Certificate Signing Request (CSR).....	329
33.10.4	Adding Certificates to the Auxiliary Files Repository.....	331
33.10.5	Activating the new X.509 Certificates on the Media Gateway	331
33.10.6	Configuring an X.509 Certificate Expiration Date Reminder	336
33.10.7	Generating a New Private Key	337
33.10.8	Checking Certificate Revocation Status.....	338
33.11	IPSEC and IKE	339
33.11.1	For Management Interfaces (on SC boards).....	339
33.11.1.1	IKE Protocol.....	339
33.11.1.2	IPSEC Protocol.....	340
33.11.2	For Call Control and Signaling Interfaces (on TP boards).....	340
33.11.2.1	IKE Protocol.....	340
33.11.2.2	IPSEC Protocol.....	340

33.11.3 Configuring IPSEC/IKE for Management Interfaces (on SC boards).....	341
33.11.4 Configuring IPSEC/IKE for Call Control and Signaling Interfaces (on TP boards).....	346
33.12 SIP over SSL/TLS (SIPS).....	349
33.13 Media Security.....	350
33.13.1 Packet Cable Security	350
33.13.2 Secure RTP.....	350
33.14 Firewall Functionality on Media Gateway Boards.....	353
33.14.1 Firewall Rules.....	353
33.15 Network Services on the Mediant 8000	357
33.16 OpenBoot PROM on SC Rev.1 Boards	358
33.17 CLI Login Banner	360
33.18 Administering Command Line Interface (CLI) Users	361
33.18.1 CLI Users Database and Operation Modes	361
33.18.2 Administering the ROOT User	362
33.18.2.1 Changing the ROOT User Password	362
33.18.2.2 Recovering the ROOT User Password.....	364
33.18.3 Administering the EMS User	365
33.18.3.1 Changing the Password of the EMS User	365
33.18.4 Synchronizing the CLI Users Database with the EMS Server	367
33.18.4.1 Synchronization Modes	367
33.18.4.2 CLI User Synchronization with the EMS Server.....	368
33.18.5 Administering the Local CLI User Database	369
33.18.5.1 Creating a New CLI User.....	370
33.18.5.2 Deleting a CLI User	372
33.18.5.3 Changing Password of the CLI User	373
33.18.6 Centralized AAA Servers.....	375
33.18.6.1 Centralized TACACS+ Servers	375
33.18.6.2 Centralized RADIUS Servers.....	384
33.18.7 CLI Interface Access Control.....	389
33.18.8 Password-less Access to the CLI Interface.....	390
33.18.8.1 Generating a Private/Public Key Pair	390

33.19 Intrusion Detection Events	398
33.20 Configuration Freeze and Configuration Change Event	399
34 Performance Measurements	401
34.1 PM Profiles	401
34.2 Real-Time PMs	401
34.3 Historic PMs	401
34.4 PM Threshold Alarms	401
34.5 Performance Monitoring Profiles	402
34.6 Real-Time Performance Measurements	405
34.7 History Performance Measurements	409
34.8 Performance Measurement Threshold Alarms	412
35 Media Gateway Inventory	415
36 Media Gateway Boards' Configuration Backdoor	417
36.1 Supported Actions	420
36.2 Usage Tips	420
37 Using Auxiliary Files	421
37.1 Auxiliary Files Repository	422
37.2 Call Progress Tones (CPT) Files	422
37.2.1 Modifying the "Source" Call Progress Tones (CPT) File	423
37.2.1.1 The Call Progress Tones Section Format	423
37.2.1.2 The User-Defined Tones Section Format	425
37.2.1.3 Default Configuration	426
37.2.1.4 Editing the "Source" Call Progress Tones File	428
37.2.2 Converting the Call Progress Tones File to Binary Format	429
37.3 Pre-Recorded Tones (PRT) Files	430
37.3.1 Creating a Pre-Recorder Tones File	431
37.4 Voice Prompts Files	433
37.4.1 Creating a Voice Prompts File	433
37.5 CAS Files	437
37.5.1 CAS File Syntax	437
37.5.1.1 INIT Variables	438
37.5.1.2 Actions	438
37.5.1.3 Functions	438
37.5.1.4 States	438
37.5.1.5 Reserved Words	440
37.5.1.6 State's Line Structure	440
37.5.2 Converting CAS File to Binary Format	451
37.6 External Coders Files	453
37.6.1 Modifying the "Source" External Coders File	453
37.6.1.1 New Coders Introduced with the Table	454
37.6.1.2 Coders Support Level	454
37.6.2 Converting External Coders File to Binary Format	455

37.7	Dial Plan Prefix Tags for IP-to-Tel Routing.....	456
38	Configuring the PSTN Subsystem	459
38.1	Configuring Media Gateway Board's PSTN Settings.....	459
38.2	Configuring STM-1/OC-3 Interfaces	460
38.3	Configuring T3 Interfaces	463
38.3.1	Channelized T3	464
38.4	Configuring the E1/T1 Trunks	465
38.4.1	Status in the EMS.....	465
38.4.1.1	Supported Actions	466
38.4.1.2	Trunks Configuration	467
38.5	Viewing Trunk Channels Status	470
38.6	Configuring the SS7 Subsystem.....	472
38.6.1	SIGTRAN (or UAL).....	473
38.6.2	Supported SS7 Architectures	473
38.6.2.1	SS7 M2UA (SG Side) Architecture	474
38.6.2.2	SS7 MTP3/M3UA Architecture	474
38.6.2.3	SS7 M2TN Tunneling Architecture	475
38.6.3	Configuring the M2UA (SG Side) Application	476
38.6.3.1	M2UA (SG Side) Operational Status	482
38.6.3.2	Online Provisioning.....	482
38.6.3.3	Redundant Configuration.....	482
38.6.3.4	Advanced Configuration	483
38.6.4	Configuring the MTP3/M3UA Application	485
38.6.4.1	MTP3/M3UA Operational Status	498
38.6.4.2	Online Provisioning.....	498
38.6.4.3	Redundant Configuration.....	499
38.6.4.4	Advanced Configuration	503
38.6.4.5	STP Functionality (Alias Point Code)	503
38.6.5	Configuring the M2TN Application	504
38.6.5.1	Online Provisioning.....	506
38.6.5.2	Redundant Configuration.....	506
38.6.5.3	Advanced Configuration	506
38.7	Configuring the CAS/ISDN Subsystem.....	507
38.7.1	Configuring the CAS/ISDN Application	508
38.7.2	Configuring the IUA/DUA Application	513
38.7.3	Online Provisioning	515
38.7.4	ISDN Operational Status	515
38.7.5	Redundant Configuration.....	515
38.8	Configuring TDM Clock Synchronization.....	516
38.8.1	Stand Alone Board Clock Mode.....	516
38.8.1.1	Connecting the Media Gateway to the External Equipment.....	517
38.8.1.2	Configuring the Media Gateway Software	517
38.8.2	Timing Module BITS Sync Clock Mode	519
38.8.2.1	Connecting Media Gateway to the External Equipment.....	520
38.8.2.2	Configuring Media Gateway Software	520
38.8.3	Timing Module Line Sync Clock Mode.....	522
38.8.3.1	Connecting the Media Gateway to the External Equipment.....	523
38.8.3.2	Configuring Media Gateway Software	524

39	Configuring the Media Settings	527
39.1	DSP Templates	539
39.2	AMR Coder Policy	540
39.2.1	Configuring Pre-defined AMR Coder Rate Policy	541
Configuring and Operating the Media Gateway (Part 3)-SIP Subsystem		545
40	General SIP Configuration.....	547
40.1	The SIP Proxy.....	547
40.1.1	SIP Proxy Set.....	547
40.1.2	Redundancy Mechanisms	548
40.1.3	DNS Service Records (SRV)	548
40.1.4	SIP Proxy Sets	548
40.2	The SIP Registrar	558
40.3	SIP Protocol Settings.....	563
40.4	Configuring Coder Groups	608
40.5	Configuring Coders Table	609
40.6	IP Groups Table	611
40.6.1	Configuring the IP Group Table	611
40.7	Account Group.....	622
40.7.1	Configuring Account Group	622
40.8	SIP Routing DNS Table	625
40.8.1	Configuring the Internal DNS Table	625
40.9	SIP SRV to IP Table.....	626
40.9.1	Configuring the SIP SRV to IP Table	626
40.10	SRD Table	628
40.10.1	Configuring the SRD Table.....	629
40.11	SIP Interfaces Table	630
40.11.1	Configuring the SIP Interfaces Table	630
40.12	NAT Translation Table	632
40.12.1	Configuring the NAT Translation Table.....	632
40.13	Least Cost Routing (LCR) Table	633
40.13.1	Configuring the Routing Rule Groups Table	634
40.13.2	Configuring the Cost Group Table	635
40.13.3	Configuring the Time Band Table	636
40.14	SIP Message Policy Table	637
40.14.1	Configuring the SIP Message Policy Table.....	637
40.15	Routing Based on LDAP Active Directory Queries.....	639
40.15.1	Configuring LDAP Server Parameters	640
40.15.2	Querying the AD and Routing Priority.....	642
40.15.3	Configuring Query Attribute Key	644
40.15.4	Configuring AD-Based Routing Rules.....	645

41	PSTN Gateway and IP-to-IP Applications.....	649
41.1	PSTN Gateway Application	649
41.2	IP-to-IP Application	649
41.3	Trunk Groups Table	650
41.3.1	Configuring the Trunk Group Table	650
41.4	Trunk Group Settings Table	653
41.4.1	Configuring Trunk Group Settings Table	653
41.5	Manipulation Tables.....	658
41.5.1	Possible Uses for the Number Manipulation Tables	658
41.5.2	Manipulation on all Inbound/Outbound SIP INVITE	658
41.5.3	Configuring the Calling Name Manipulation Table for Tel to IP Routing.....	661
41.5.4	Configuring the Redirect Number Manipulation IP to Tel Routing	662
41.5.5	Configuring the Redirect Number Manipulation Tel to IP Routing	663
41.5.6	Operation Rules	665
41.5.7	Dialing Plan Notation.....	666
41.5.8	Numbering Plans and Type of Number.....	666
41.6	The Routing Tables.....	668
41.6.1	Telephone to IP/Outbound Routing Table.....	669
41.6.1.1	Telephone to IP/Outbound Routing Provisioning Rules	669
41.6.1.2	Possible Uses for Telephone to IP/Outbound Routing	669
41.6.1.3	Configuring Telephone to IP/Outbound Routing	671
41.6.2	IP to Telephone/Inbound Routing Table	675
41.6.2.1	IP to Telephone/Inbound Routing Provisioning Rules.....	675
41.6.2.2	Configuring IP to Telephone/Inbound Routing	676
41.6.3	Reasons for Alternative Routing	679
41.6.3.1	Alternative Routing Provisioning Rules	679
41.6.3.2	Configuring Alternate Routing	679
41.6.4	SIP to ISDN and ISDN to Release Cause Mapping	681
41.6.4.1	Configuring SIP / ISDN Cause Mapping.....	681
41.7	Profiles Tables	683
41.7.1	Tel Profile Table	684
41.7.2	IP Profile Table.....	689
42	Stand-Alone Survivability (SAS) Application.....	715
42.1	Overview	715
42.2	SAS Modes	715
42.2.1	The SAS Configuration.....	716
42.3	SAS Registration Manipulation	723
43	Session Border Controller (SBC) Application	725
43.1	Overview	725
43.2	VoIP Firewall.....	725
43.3	Topology Hiding.....	726
43.4	SIP Normalization.....	726
43.5	The SBC Configuration.....	727
43.6	SIP Network Definitions.....	737
43.6.1	Signaling Routing Domain (SRD)	737
43.6.2	SIP Interfaces.....	738
43.6.3	Media Realms	738

43.7 SIP Dialog Initiation Process.....	739
43.8 Determining Source and Destination URL	740
43.9 Source IP Group Classification.....	740
43.10 SBC Condition Table	744
43.11 SBC Routing.....	745
43.11.1 SBC IP to IP Routing Table	745
43.11.2 Configuring the SBC IP to IP Routing Table	747
43.11.3 Configuring SBC Alternative Route Reasons Table.....	753
43.12 SBC Inbound and Outbound Manipulation	754
43.12.1 SBC IP to IP Inbound Manipulation Table.....	755
43.12.2 SBC IP to IP Outbound Manipulation Table.....	758
43.13 SBC Message Manipulation	761
43.13.1 Configuring the SBC Message Manipulation Table.....	763
43.14 User Registration	765
43.14.1 Registration Request Processing	765
43.14.2 Registrations Database	766
43.14.3 Routing using Registrations Database.....	767
43.14.4 Registration Refreshes.....	767
43.15 SBC Admission Control.....	768
43.16 SBC Media Handling	770
43.16.1 Media Anchoring without Transcoding (Transparent)	771
43.16.2 Media Anchoring with Transcoding.....	772
43.16.3 Transcoding Modes.....	774
Maintenance.....	775
44 Media Gateway Software Backup/Restore Procedures	777
44.1 Backup Procedures	777
44.2 Backup Types.....	777
44.3 Creating the Media Gateway Software Backup.....	778
44.4 Restoring the Media Gateway Software from Backup.....	783
44.5 Automatic Backups.....	788
45 Hardware Replacement.....	791
45.1 Hardware Replacement Preliminaries	791
45.1.1 ESD Requirements.....	791
45.1.2 Slot Assignment	791
45.1.3 Empty Slots Cover Requirements.....	792
45.2 SC Board Replacement Procedure	793
45.2.1 Replacing the Failed SC Board	793
45.2.2 Installing the Operating System (OS) on the Replaced SC Board	794
45.2.3 Configuring IP Address on the Replaced SC Board.....	794
45.2.4 Installing the Software on the Replaced SC Board	795
45.3 Media Gateway Board Replacement Procedure.....	795
45.3.1 Replacing the Failed Media Gateway Board.....	795
45.3.2 Replacing the Media Gateway Board's RTM module.....	796
45.3.2.1 Connecting Cables to Media Gateway's RTM Module.....	797

45.4	Adding Media Gateway Boards to a Mediant 8000 System	797
45.4.1	Constraints for Adding Boards to the Mediant 8000 System	798
45.4.1.1	TP-6310 Boards	798
45.4.1.2	TP-8410 Boards	798
45.4.2	Troubleshooting the Newly installed Media Gateway Board	799
45.5	SA/RTM Replacement Procedure	800
45.6	Ethernet Switch Board Replacement Procedure	801
45.6.1	Replacing the Ethernet Switch Board	801
45.6.2	Replacing the Ethernet Switch RTM Module	802
45.6.3	Troubleshooting the ES/6600 Board Installation	803
45.7	Power Supply Modules Replacement	804
45.7.1	Replacing the Power Entry Module	806
45.8	Replacing the Fan Tray Modules	807
45.9	Replacing Air Filters	808
46	Online Software Upgrade	811
46.1	Overview	811
46.1.1	Hitless Upgrade Mode	812
46.1.2	Graceful Shutdown Mode	812
46.2	Pre-Upgrade Configuration Backup	813
46.3	Preparing for the Online Software Upgrade	813
46.3.1	Preparing the Media Gateway	813
46.3.2	Preparing the IP Network	814
46.3.3	Verifying that the Online Software Upgrade is Supported	814
46.3.4	Planning the Maintenance Time Period	814
46.3.5	Pre-installing OS Patches	817
46.3.6	EMS Verifications	817
46.3.6.1	Configuring the EMS and ROOT Passwords of the Mediant 8000 in the EMS	818
46.3.6.2	Adding the Media Gateway Software to the EMS Server	819
46.4	Performing the Online Software Upgrade	820
46.4.1	Starting the Online Software Upgrade Wizard	820
46.4.2	Welcome Questionnaire	821
46.4.3	Transferring the SC Software Package to the SC Boards	823
46.4.4	Upgrading the 2 nd SC Board	824
46.4.5	Upgrading the Media Gateway Boards	826
46.4.6	Upgrading the ES Boards	826
46.4.7	Upgrading the 1 st SC Board	826
46.4.8	Finish	826
46.5	After Completing the Online Software Upgrade	827
46.6	Rollback	828
46.7	Software Upgrade/Rollback Troubleshooting	828
46.7.1	Performing a Manual Rollback to the Previous Software Configuration	829
46.7.2	Recovery from a Network Failure or EMS Server/Client Crash	831
Diagnostics and Troubleshooting		833

47	Troubleshooting Strategy.....	835
48	Recovering the OAM VLAN Settings	843
49	Collecting Advanced Media Gateway Board Logs	845
49.1	Syslog Protocol.....	845
49.1.1	Configuring the Syslog Server	845
49.1.1.1	Displaying VoIP Board Log Files	846
49.1.2	SIP Board Syslog Level.....	846
49.2	Filtering Syslog Messages and Debug Recordings.....	848
49.2.1	Configuring Filter Rules	848
49.3	Media Gateway Board's Debug Recording Traces and Logging	850
49.3.1	Collecting Debug Recording Traces on the Standby SC board.....	851
49.4	Collecting Call Data Records (CDRs)	852
49.4.1	Collecting Call Data Records on SIP Boards	852
49.4.2	Collecting Call Data Records (CDRs) on MEGACO Boards	854
49.5	Collecting the Media Gateway Board's INI File	855
50	Accessing Advanced Status- Media Gateway Board via WEB.....	857
51	Collecting Traces from the Ethernet Switch Board's Mirror Port	859
51.1	Configuring ES Mirror Filters	859
51.1.1	ES/6600	859
51.1.2	ES-2.....	859
51.2	Configuring Mirroring on ES boards' Port	867
51.3	Configuring Mirror Destination	868
51.4	Starting Mirroring on ES Board.....	869
51.5	Stopping Mirroring on ES Board.....	869
52	Internal System Controller (SC) Software Logs.....	871
52.1	Log Areas	871
52.2	Customer's Log Area	871
52.2.1	AudioCodes Technical Support Log Areas	871
52.3	Log Files Storage.....	872
52.4	Viewing Log Files.....	873
52.5	Operating System Logs.....	874
52.6	Collecting the Report File.....	874
53	Information Needed when Contacting Technical Support.....	877
Appendices		879
A	Examples of IP Network Connectivity Configuration.....	881
A.1	Example 1: One Subnet, One Physical Interface, No VLAN Tags	881
A.2	Example 2: Three Subnets, VLAN Tags, One Physical Interface	885
B	Appendix - Configuring HSRP/VRRP.....	889
B.1	Overview	889
B.2	Configuring the Mediant 8000 Subnets	891
B.2.1	Subnet Configuration.....	891

B.2.2	VLAN Configuration.....	891
B.2.3	OAM Subnet Settings.....	891
B.2.4	Interface Separation Settings	891
B.2.5	VLAN Settings.....	891
B.2.6	Subnets and Network Profiles Settings.....	892
B.2.7	Media Gateway Board's IP Addresses	892
B.2.8	Gateway Parameters Provisioning	893
B.3	Configuring the User Environment (Cisco L3 switch)	893
B.3.1	IP Address.....	893
B.3.2	Link Aggregation	893
B.3.3	Cisco L3 Switch-HSRP.....	894
B.3.4	Example Configuration Output.....	895
B.3.5	"show running-config" of 3560_G3	899
B.4	HSRP/VRRP Quality Testing	899
B.4.1	Test Procedure.....	899
B.4.1.1	Initial State: 1 (default state).....	900
B.4.1.2	Initial State: 2	901
B.4.1.3	Initial State: 3	902
B.4.1.4	Initial State: 4	903
C	Appendix: Testing Installation and Basic Configuration	905
D	Appendix - List of Notification Traps.....	911
54	Index.....	913

List of Figures

Figure 1-1: Mediant 8000 Block Diagram.....	31
Figure 3-1: Mediant 8000 Front View	37
Figure 3-2: Mediant 8000 Back View	38
Figure 4-1: Midplane in Chassis.....	39
Figure 5-1: PEM/DC/8K Power Entry Module Panel.....	41
Figure 5-2: PS/DC/8K Power Supply Module.....	42
Figure 6-1: FM/8K Fan Tray Module	43
Figure 8-1: TP-6310 Board Front Panel	47
Figure 9-1: 6310 RTM Front Panel.....	50
Figure 9-2: 6310/RTM Redundant Front Panel	51
Figure 10-1: TP-8410 Board Front Panel	53
Figure 11-1: 8410 RTM Panel	57
Figure 11-2: 8410/RTM 100-Pin SCSI Connector.....	58
Figure 11-3: 8410/RTM 68-pin SCSI Connector	59
Figure 11-4: 8410/RTM Redundant Front Panel	61
Figure 12-1: SC Rev.1 Board Panel.....	64
Figure 12-2: SC Rev.1 Board Mini DIN 8 Serial Port Connector.....	65
Figure 12-3: SC Rev.2 Board Panel.....	66
Figure 12-4: SA/RTM Panel	69
Figure 12-5: RJ-48c Trunk Connectors	71
Figure 13-1: ES/6600 Board Panel	74
Figure 13-2: ES/6600/RTM Panel	78
Figure 13-3: ES-2 Board Panel	81
Figure 13-4: ES-2 RTM	85
Figure 16-1: Attaching the Chassis to the Rack.....	101
Figure 16-2: Chassis on the Rack - Front and Side Views	102
Figure 16-3: Connecting the Mediant 8000 to a DC Power Supply	104
Figure 16-4: Securing the PEM Plastic Cover Spacers (Hex).....	105
Figure 16-5: Secure the PEM Plastic Cover Screws.....	106
Figure 17-1: Using PuTTY for RS-232 Serial Connections.....	110
Figure 17-2: PuTTY RS-232 Serial Connection Settings	111
Figure 17-3: Using PuTTY for SSH connection.....	112
Figure 18-1: Connecting the IP Network for an Initial Installation	121
Figure 19-1: SFP Modules and Their Locks.....	124
Figure 19-2: T3 - Male Connector MOLEX PN: 73100-0255	125
Figure 20-1: Normal Logic External Alarm Equipment Connection.....	127
Figure 20-2: Inverse Logic External Alarm Equipment Connection	128
Figure 23-1: Sample MO Tree Hierarchy	161
Figure 23-2: Graphical EMS Status Screen	163
Figure 23-3: Textual EMS Status Screen.....	163
Figure 23-4: Navigation Pane and Info Panel in EMS.....	164
Figure 23-5: EMS Configuration Pane	166
Figure 23-6: Example Settings Screen-Trunk Settings	166
Figure 23-7: EMS Alarm Browser.....	167

Figure 23-8: MOs in the EMS Color-Coded according to their Severity.....	169
Figure 26-1: Network Subnets.....	184
Figure 26-2: An Example of “Two O & CM” Subnet Configuration.....	187
Figure 26-3: Ethernet Port Allocation	221
Figure 27-1: SC Boards in EMS	224
Figure 27-2: Format New Volume	239
Figure 27-3: ISO2USB.....	240
Figure 28-1: Media Gateway Boards in the EMS.....	246
Figure 28-2: Board Redundancy Status	253
Figure 29-1: ES Boards in the EMS	261
Figure 30-1: EMS Server Configured as NTP Server	266
Figure 30-2: External NTP Server Setup - Option 1.....	267
Figure 30-3: External NTP Server Configuration - Setup Option 2	268
Figure 30-4: Internal NTP Implementation	270
Figure 33-1: Security Features.....	304
Figure 33-2: Generating X.509 Files	328
Figure 33-3: Activating X.509 Certificates	335
Figure 33-4: IPSec Encryption	339
Figure 33-5: Synchronizing CLI Users Database with EMS Server.....	367
Figure 33-6: Local CLI Users Database on SC Boards	369
Figure 33-7: Working with Centralized TACACS+ Servers.....	377
Figure 33-8: Centralized User Authentication via RADIUS Protocol.....	385
Figure 33-9: PuTTY Key Generator	391
Figure 33-10: PuTTY Key Generator-Public Key	392
Figure 33-11: PuTTY Key Generator-Generate Action	392
Figure 33-12: PuTTY Client-SSH Authentication	394
Figure 33-13: PuTTY Configuration-Auto-login	395
Figure 33-14: PuTTY Configuration-Host Name	396
Figure 34-1: MG Background Monitoring	402
Figure 34-2: Do You Wish to Start Polling.....	403
Figure 34-3: Polling Started.....	403
Figure 34-4: Select Screen.....	405
Figure 34-5: Real-Time Performance Measurement Display Window	406
Figure 34-6: MG Monitoring Window.....	407
Figure 34-7: History PMs Select Screen	409
Figure 34-8: History Performance Measurements Display	410
Figure 34-9: History Performance Measurements Display-Results Screen.....	411
Figure 34-10: Threshold Alarms Parameters Screen.....	413
Figure 35-1: Mediant 8000 Inventory	415
Figure 37-1: Call Progress Tones Screen.....	429
Figure 37-2: Prerecorded Tones File(s) Screen with wav Files	432
Figure 37-3: File Data Dialog Box	432
Figure 37-4: Voice Prompts Screen	433
Figure 37-5: Select Files Window.....	434
Figure 37-6: Voice Prompts Window with wav Files	435
Figure 37-7: File Data Window.....	436

Figure 37-8: Call Associated Signaling (CAS) Screen	452
Figure 37-9: Coders Window.....	455
Figure 38-1: TP-6310 Board Status Screen	461
Figure 38-2: STM-1 PSTN Fiber Group Status Screen.....	461
Figure 38-3: OC-3 PSTN Fiber Group Status Screen	461
Figure 38-4: DS3 Status Screen	463
Figure 38-5: E1/T1 Trunks Status Screen.....	466
Figure 38-6: Trunk Channels Status Screen	470
Figure 38-7: OSI Reference Model and SS7 Protocol Stack	472
Figure 38-8: SS7 M2UA (SG side) Architecture.....	474
Figure 38-9: SS7 MTP3/M3UA Architecture	474
Figure 38-10: SS7 M2TN Tunneling Architecture	475
Figure 38-11: ISDN Relay via IUA.....	507
Figure 38-12: Stand-Alone Clock Synchronization Mode	517
Figure 38-13: Timing Module BITS Sync Clock Mode	519
Figure 38-14: Timing Module Line Sync Clock Mode	523
Figure 43-1: Example of SRD and SIP Interfaces Configuration for SBC Application.....	737
Figure 43-2: Example of an SBC application Call Flow	738
Figure 43-3: SBC Application SIP Dialog Initiation Process	739
Figure 43-4: SBC Application Classification Process.....	741
Figure 43-5: SBC Application IP to IP Routing Types	746
Figure 43-6: SBC Application Inbound and Outbound Manipulation	754
Figure 43-7: Example of SBC Application Manipulation	754
Figure 43-8: SBC Message Manipulation.....	762
Figure 43-9: Example of a SIP call with Media Anchoring without Transcoding.....	771
Figure 43-10: Example of SIP call with Media Anchoring with Transcoding	772
Figure 44-1: Backup Dialog screen	778
Figure 44-2: Backup files in the EMS	779
Figure 44-3: Gateway Restore Procedure.....	783
Figure 44-4: Select Backup File	784
Figure 45-1: Baffled Blank Panel for Front Slots.....	792
Figure 45-2: Blank Panel for Rear Slots.....	792
Figure 45-3: Red Ejector Buttons on a Board	793
Figure 45-4: Opening the Grill to Access the Power Supply Modules	804
Figure 45-5: Removing the PS from the Chassis.....	805
Figure 45-6: Power Supply Icon in EMS Status Screen.....	805
Figure 45-7: Power Supply Alarm in the Alarms Browser	805
Figure 45-8: Replacing the Fan Tray Unit	807
Figure 45-9: Replacing the Air Filter.....	808
Figure 46-1: MG Information dialog.....	818
Figure 46-2: File Manager Screen.....	820
Figure 46-3: Welcome Questionnaire.....	821
Figure 46-4: Start Upgrade Process.....	823
Figure 46-5: Upgrading the 2 nd SC Board	824
Figure 51-1: IP Packets	860
Figure 51-2: Ethernet Header.....	860

Figure 51-3: IP Header	860
Figure 51-4: TCP Header	861
Figure 51-5: UDP Header	861
Figure 51-6: ICMP Header	861
Figure 52-1: Viewing an 'SNMP Trap' Log	873
Figure A-1: Network Example 1: One Subnet, No VLANs	881
Figure A-2: Network Example 2 : Three Subnets, VLAN Tags, One Physical Interface.....	885
Figure B-1: HSRP/VRRP Configuration	890
Figure B-2: HSRP/VRPP Test State 1	900
Figure B-3: HSRP/VRPP Test State 2	901
Figure B-4: HSRP/VRPP Test State 3	902
Figure B-5: HSRP/VRPP Test State 4	903

List of Tables

Table 2-1: Mediant 8000 Hardware Component	35
Table 4-1: Version Chassis Dimension	40
Table 7-1: Alarm Indicator	45
Table 8-1: TP-6310 Board Status LED Indicators	48
Table 10-1: TP-8410 Board LEDs	54
Table 11-1: 8410/RTM 100-pin SCSI Connector	58
Table 11-2: 8410/RTM 68-pin SCSI Connector	60
Table 12-1: SC Rev.1 Board LED Indicators.....	65
Table 12-2: SC Rev.2 Board (Linux OS) RS-232 Connector Pinouts	67
Table 12-3: SC Rev.2 Board (Linux OS) LED Indicators	68
Table 12-4: SA-RTM LED Indicators	70
Table 12-5: SA/RTM RS-232 Console Port Connector	70
Table 12-6: SA/RTM Terminal Block Connector	71
Table 12-7: SA/RTM BITS Interface LEDs	72
Table 13-1: ES/6600 Board Status Led Indicators.....	75
Table 13-2: ES/6600 Physical Front Slots to Ethernet Port Mapping	76
Table 13-3:ES/6600/RTM Port Pin Outs	79
Table 13-4: ES-2 Board Status Led Indicators.....	82
Table 13-5: ES-2 Physical Front Slots to Ethernet Port Mapping	83
Table 13-6: ES-2 Physical Rear Slots to Ethernet Port Mapping.....	84
Table 13-7: ES-2/RTM Port Pin Outs	86
Table 13-8: ES-2 RS-232 Pin Layout	86
Table 14-1: Board Assembly Order	87
Table 15-1: Equipment Requirements.....	91
Table 15-2: Cabling Requirement	92
Table 15-3: Recommended E1/T1 Cable Parts for TP-8410 Board	93
Table 15-4: Electrical Requirement	94
Table 15-5: NEBS Requirement.....	95
Table 15-6: Allocating IP Addresses	97
Table 16-1: PEM LED.....	107
Table 17-1: RS-232 Serial Connection Properties	110
Table 17-2: Command Line Interface Users	114
Table 23-1: MO Attribute Provisioning Types.....	165
Table 23-2: EMS-Alarm Severity Color	168
Table 23-3: MO Severity Colors in the EMS	170
Table 25-1: SNMP to Syslog Severity Mapping	177
Table 26-1: Aggregated Link Failure Detection.....	193
Table 26-2: Media Link Aggregation Settings	194
Table 26-3: Subnet Properties	199
Table 26-4: SC Static Route Properties	204
Table 26-5: TP Static Route Properties.....	205
Table 26-6: Network Service Classes	206
Table 26-7: Media Gateway Quality Of Service Settings	208
Table 26-8: Network Profile Quality Of Service Settings.....	209

Table 26-9: Media Realm Settings	211
Table 26-10: Additional Media Gateway Board Network Settings	212
Table 26-11: Ethernet Ports Allocation on ES/6600 Boards	217
Table 26-12: Ethernet Ports Allocation on ES-2 Boards	219
Table 27-1: Linux OS Installation Requirements.....	232
Table 28-1: Redundancy Group Parameters	256
Table 28-2: Media Gateway board Redundancy Parameters	257
Table 28-3: Automatic Switchback Parameters	258
Table 30-1: NTP Server Configuration Parameters	271
Table 30-2: NTP Server Status Parameters.....	273
Table 31-1: Physical Termination Types	280
Table 31-2: Virtual Gateway Parameters	283
Table 31-3: Media Gateway Controller Parameters.....	285
Table 31-4: Media Gateway Controller Addressing Parameters.....	286
Table 31-5: Media Gateway Controller Endpoint Names Parameters	286
Table 31-6: MGC IP/FQDN Address Parameters	287
Table 31-7: Media Gateway Board's Call Control Parameters	289
Table 32-1: V5.2 Interface Properties	297
Table 32-2: V5.2 Link Properties.....	298
Table 33-1: Filesystem Integrity Status Parameters	317
Table 33-2: Filesystem Integrity Configuration Parameters of the Media Gateway.....	319
Table 33-3: Media Gateway Security Settings	332
Table 33-4: X.509 Files Status Parameters of the Media Gateway	333
Table 33-5: OCSP Server Settings	338
Table 33-6: SNMP Management Modes	341
Table 33-7: SC IPSEC Rule Parameters (SC Boards)	342
Table 33-8: SC IKE Proposal Parameters.....	345
Table 33-9: TP IPSEC Profile Parameters	346
Table 33-10: TP IPSEC Rules Parameters (TP Boards)	347
Table 33-11: TP IKE Proposal Parameters.....	348
Table 33-12: Media Gateway Board's Media Security (SRTP) Settings.....	351
Table 33-13: Firewall Rule Parameters.....	354
Table 33-14: Network Services	357
Table 33-15: Centralized AAA Server Settings	380
Table 33-16: AAA Server Settings	380
Table 33-17: TACACS+ Settings.....	381
Table 33-18: RADIUS Settings.....	387
Table 33-19: CLI Interface Access Control Parameters.....	389
Table 34-1: PM Threshold Alarm Settings	413
Table 36-1: Configuration-Backdoor Parameters.....	418
Table 37-1: Supported Auxiliary Files	421
Table 37-2: Default Call Progress Tones	426
Table 37-3: Pre-Recorded Tones (PRT) file Characteristics.....	430
Table 37-4: Example - ST_DIAL state in CAS File	438
Table 38-1: Media Gateway Board's PSTN Parameters.....	459
Table 38-2: PSTN Fiber Group Properties	462

Table 38-3: T3 Interface Properties.....	464
Table 38-4: Trunk Properties.....	468
Table 38-5: Trunk PSTN Alarm	471
Table 38-6: Trunk Channel Status	471
Table 38-7: SS7 Data Link Properties - Data Link General Info Tab	478
Table 38-8: SS7 Data Link Properties - Data Link MTP Tab	479
Table 38-9: UAL Group Properties.....	480
Table 38-10: UAL Interface Properties.....	481
Table 38-11: MTP2 Profile Properties	483
Table 38-12: MTP3 Group Properties	490
Table 38-13: SS7 Node Properties	491
Table 38-14: SS7 Linkset Properties.....	493
Table 38-15: SS7 Routeset Properties.....	494
Table 38-16: SS7 Linkset Link Properties	494
Table 38-17: SS7 Route Properties	495
Table 38-18: XE "M3UA Routing Context Properties" M3UA Routing Group Properties	495
Table 38-19: M3UA Routing Context Properties	495
Table 38-20: Media Gateway Board's MTP3/M3UA Properties.....	497
Table 38-21: SS7 Node Redundancy Properties	503
Table 38-22: Media Gateway board's CAS/ISDN Parameters.....	508
Table 38-23: E1/T1 Trunk's ISDN/DPNSS Parameters	509
Table 38-24: E1/T1 Trunk's CAS Parameters.....	512
Table 38-25: General Timing Module Settings Parameters	520
Table 38-26: TM External IF Settings Parameters.....	521
Table 38-27: TM Line Sync Settings Parameters.....	524
Table 39-1: Media Gateway Board's Voice Settings.....	527
Table 39-2: Media Gateway Board's RTP/RTCP Settings.....	532
Table 39-3: Media Gateway Board's Fax/Modem Settings.....	534
Table 39-4: Media Gateway Board's Caller ID Settings	535
Table 39-5: Media Gateway Board's Coder Settings	537
Table 39-6: Media Gateway Board's NFS Server Settings	537
Table 39-7: Media Gateway Board's No Op Settings.....	538
Table 39-8: Media Gateway Board's NFS Settings.....	538
Table 39-9: DSP Template Settings.....	539
Table 39-10: AMR Coder Profile Settings	542
Table 39-11: AMR Coder Policy Settings.....	542
Table 40-1: SIP Proxy Set Parameters	549
Table 40-2: SIP Proxy Set Settings.....	553
Table 40-3: SIP Proxy Server Settings.....	558
Table 40-4: SIP Registration and Authentication Settings	558
Table 40-5: SIP General Settings.....	563
Table 40-6: SIP Protocol Settings	566
Table 40-7: SIP Routing Settings	578
Table 40-8: SIP Supplementary Services Settings	582
Table 40-9: SIP PSTN Settings.....	587
Table 40-10: SIP Media Settings.....	601

Table 40-11: SIP Media Server Settings	604
Table 40-12: SIP Radius Settings	606
Table 40-13: SIP Emergency Gateway Setting.....	606
Table 40-14: Coder Parameters.....	610
Table 40-15: IP Group Parameters	612
Table 40-16: Account Group Parameters.....	622
Table 40-17: SIP Routing DNS Settings Parameters.....	625
Table 40-18: SIP SRV to IP Table Parameters.....	627
Table 40-19: SRD Parameters	629
Table 40-20: SIP Interface Parameters.....	630
Table 40-21: NAT Translation Parameters.....	632
Table 40-22: SIP Message Policy Parameter	638
Table 40-23: LDAP Server Parameters.....	640
Table 40-24: Parameters for Configuring Query Attribute Key	642
Table 40-25: Query Attribute Key.....	644
Table 40-26: Destination Username Prefixes.....	645
Table 40-27: Destination Username Prefixes.....	646
Table 40-28: AD-Based Tel-to-IP Routing Rule Configuration Examples.....	647
Table 40-29: AD-Based SBC IP-to-IP Routing Rule Configuration Examples.....	647
Table 41-1: SIP IP-to-IP Parameters.....	649
Table 41-2: Trunk Group Parameters	651
Table 41-3: SIP Trunk Group Settings Parameters	653
Table 41-4: GW Inbound/Outbound Manipulation Set ID Parameter.....	659
Table 41-5: Calling Name Manipulation Table for IP to Tel Table Parameter	660
Table 41-6: Calling Name Manipulation Table for Tel to IP Table Parameter	661
Table 41-7: Redirect Number Manipulation IP to Tel Table Parameter	662
Table 41-8: Redirect Number Manipulation Tel to IP Table Parameter	664
Table 41-9: NPI/TON Values for ISDN ETSI.....	666
Table 41-10: SIP Routing Table	668
Table 41-11: Telephone to IP / Outbound Routing Table "Matching Rules".....	672
Table 41-12: Telephone to IP / Outbound Routing Table "Destination Rules"	673
Table 41-13: IP to Telephone / Inbound Routing Table "Matching Rules"	677
Table 41-14: IP to Telephone / Inbound Routing Table "Destination Rules"	677
Table 41-15: Alternative Routing Parameters	680
Table 41-16: SIP to ISDN Cause Mapping Parameters.....	682
Table 41-17: ISDN to SIP Cause Mapping Parameters.....	683
Table 41-18: Tel Profile Parameters	684
Table 41-19: IP Profiles Parameters	690
Table 43-1: SIP SBC Parameters	727
Table 43-2: SBC Classification Parameters "Matching Rules".....	742
Table 43-3: SBC Classification Parameters "Operation Rules"	743
Table 43-4: SBC Condition Parameter	744
Table 43-5: SBC IP to IP Routing Table "Matching Rules".....	747
Table 43-6: SBC IP to IP Routing Table "Destination Rules".....	749
Table 43-7: SBC Alternative Route Reasons Parameters	753
Table 43-8: SIP Manipulations Examples	755

Table 43-9: SBC IP to IP Inbound Manipulation Table "Matching Rules"	756
Table 43-10: SBC IP to IP Inbound Manipulation Table "Operation Rules"	757
Table 43-11: SBC IP to IP Outbound Manipulation Table "Matching Rules"	758
Table 43-12: SBC IP to IP Outbound Manipulation Table "Operation Rules"	760
Table 43-13: SIP SBC Message Manipulation Table	763
Table 43-14: SBC Admission Control Settings	768
Table 44-1: Automatic Backup Parameters	788
Table 46-1: New Features of Version 6.6 Software that must be Manually Activated after Upgrading from an Earlier Version	827
Table 47-1: Troubleshooting Faults in the Media Gateway	835
Table 49-1: SIP Logging Filter Properties	849
Table 49-2: CDR Report Level	853
Table 51-1: ES/6600 and ES-2 Mirror Filter Properties	862
Table 51-2: Additional ES/6600 Mirror Filter Properties	864
Table C-1: Test Procedures	905

This page is left blank intentionally.

Notice

This manual describes the installation, operation and maintenance of the Mediant 8000.

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document and other documents can be viewed by registered customers at: www.audiocodes.com/downloads

© 2014 AudioCodes Ltd. All rights reserved.

This document is subject to change without notice.

Date Published: 30/10/2014

Trademarks

AudioCodes, AC, AudioCoded, Ardito, CTI2, CTI², CTI Squared, HD VoIP, HD VoIP Sounds Better, InTouch, IPmedia, Mediant, MediaPack, NetCoder, Netrake, Nuera, Open Solutions Network, OSN, Stretto, TrunkPack, VMAS, VoicePacketizer, VoIPerfect, VoIPerfectHD, What's Inside Matters, Your Gateway To VoIP and 3GX are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

Customer Support

Customer technical support and service are generally provided by AudioCodes' Distributors, Partners, and Resellers from whom the product was purchased. For technical support for products purchased directly from AudioCodes, or for customers subscribed to AudioCodes Customer Technical Support (ACTS), contact support@audiocodes.com.

WEE EU Directive

Pursuant to the WEEE EU Directive, electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

Abbreviations and Terminology

Each abbreviation, unless widely used, is spelled out in full when first used. Only industry-standard terms are used throughout this manual. VoP boards are referred to as Media Gateway boards or SIP boards.

Related Documentation

The documentation package contains the following publications available on the AudioCodes Web site.

- **Mediant 8000 Product Description** - contains the description of the product features, components, standard control protocols and management protocols (*Document # LTRT-907xx*).
- **Mediant 8000 Installation, Operation & Maintenance Manual** - Provides steps and information for preparing the area where the equipment is to be set-up, supplies instructions on the physical and electrical installation of a chassis and includes operation instructions and maintenance guidelines/troubleshooting procedures. It is intended for skilled installers, system level technicians and system managers (*Document # LTRT-925xx*).
- **Programmer's User's Manual** - The Programmer's User's Manual is written for System Integrators and Software Developers who need to quickly and easily develop an efficient Network solution, with the Mediant 8000 Media Gateway. (*Document # LTRT-914xx*).
- **CLI Reference Guide** - Provides a predefined set of commands with a choice of options that comprehensively cover the maintenance tasks required on the media gateway (*Document # LTRT-892xx*).
- **EMS User's Manual** - The EMS (Element Management System) is an application that is used to configure and monitor all gateway elements from a remote location. Through the EMS, the system operator can also configure the Mediant 8000 to send EMS and Gateway alarms to different destinations using various filtering rules. The manual is intended for System level operators who are to use the EMS. The EMS can also be connected to an NMS (*Document # LTRT-963xx*).
- **Mediant 5000 and Mediant 8000 Alarm and Performance Monitoring Guide** - *Document # LTRT-237xxx*
- **Mediant 5000/8000 Media Gateway Release Notes** - *Document # LTRT-909xx*
- **EMS Release Notes** - *Document # LTRT-912xx*

Open Source Software

The Mediant 8000 product may contain open source software that may be governed by and distributed under open source licenses, including, but not limited to, the terms of the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), BSD and other licenses.

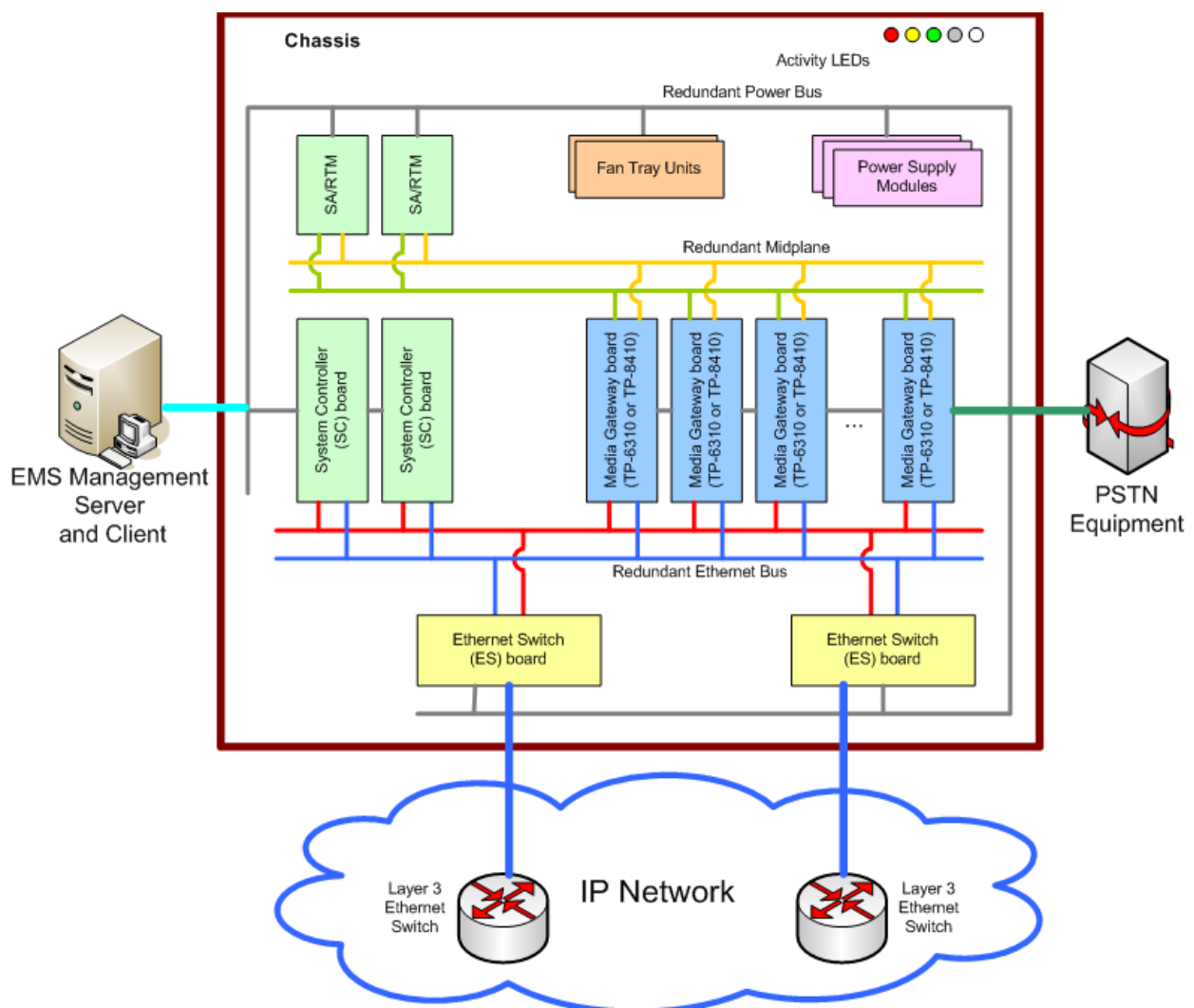
To receive the relevant source code, refer to <http://www.audiocodes.com/open-source>.

1 Introduction

The gateway is a high channel density, Large sized version of the AudioCodes series of market-ready, standards-compliant, VoIP, wireless, cables and wireline media gateway systems. The Mediant 8000 incorporates AudioCodes' leading Voice over Packet technology to enable Network Equipment Providers (NEP) and System Integrators rapid time-to-market and reliable cost-effective deployment of next-generation networks.

The Mediant 8000 is a robust, scalable and modular solution, designed for the carrier environment, matching the density requirements for Large deployments, while meeting Network Service Providers' demands for high available and reliable new voice infrastructure networks. For maximum reliability, the Mediant 8000 features protection switching and full redundancy of all common equipment.

Figure 1-1: Mediant 8000 Block Diagram



This page is intentionally left blank.

Part I

Hardware Overview

This part describes the hardware overview of the Mediant 8000 chassis.

2 Hardware Components

The Mediant 8000 is a modular system that consists of the following major hardware components:

Table 2-1: Mediant 8000 Hardware Component

Component	Module Name	Quantity
Chassis	–	1
System Controller board	SC	2
Synchronization and Alarm Rear Transition Module	SA/RTM	2
Ethernet Switch board	ES-2, ES/6600	2
Ethernet Switch boards' Rear Transition Module	ES-2 RTM, ES/6600/RTM	2
Media Gateway boards	The following boards may be used: TP-6310,, TP-8410,	Up to 9
Media Gateway boards' Rear Transition Modules	Each Media Gateway board must be equipped with appropriate RTM. Special RTMs must be used for the redundant boards.	Up to 9
Power Supply Modules	PS/DC/8K (8K DC Power Supply Modules).	Up to 3
Power Entry Modules	PEM/DC/8K (8K DC Power Entry Modules)	2
Fan Tray Modules	FM/8K Fan Tray Module	2
Air Filter	AF/8K Air Filter	1

The Mediant 8000 is offered with the following hardware configurations:

- Mediant 8000 + TP-6310 boards - Redundant configuration
- Mediant 8000 + TP-8410 boards - Redundant configuration

This page is intentionally left blank.

3 Front and Back Views



Note: Depending on the ordered configuration, the actual views of your Mediant 8000 may differ from the figures below. For example, you may have different type or number of Media Gateway boards installed.

Figure 3-1: Mediant 8000 Front View



Figure 3-2: Mediant 8000 Back View



4 The Chassis

The Mediant 8000 chassis has a 12U form factor and features 19 slots, occupied by System Controller boards, Ethernet Switch boards, Media Gateway boards and corresponding Rear Transition Modules.

The boards are inserted from the front and the back and engage the mid-plane on either side inside the chassis.

Board slots are numbered from one to nineteen on the top of the card cage in the front of the chassis and on the bottom of the card cage in the back, for identifying board placement. The mid-plane contains slot keys to match the appropriate board; there are separate slot keys for the ES, SC and TP boards. This prevents insertion of a board in an incorrect slot.

The Mediant 8000 chassis is divided into three basic sections:

- The upper section holds the Fan Tray units and Alarm LEDs
- The middle section is the card cage with 21 slots which holds the SC, ES and TP boards
- The lower section houses two PEMs, three power supply modules and the air filter

Figure 4-1: Midplane in Chassis

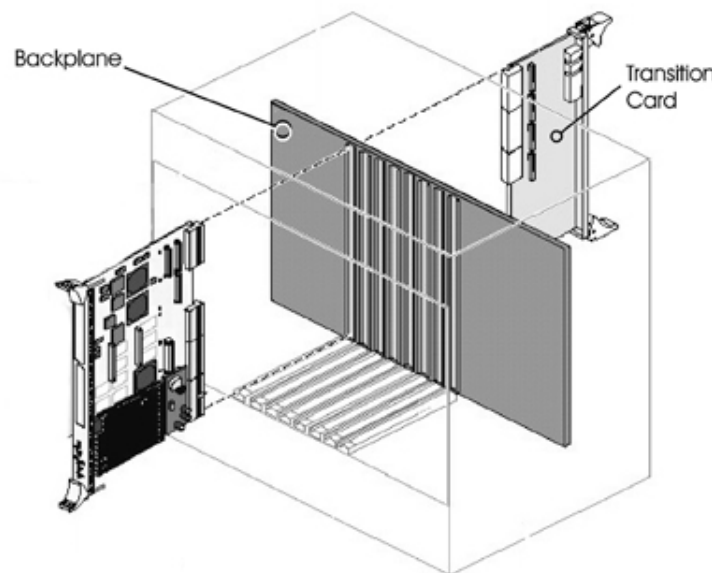


Table 4-1: Version Chassis Dimension

Dimension	Value
Width	48.3 cm (19 inches)
Height	53.34 cm (21 inches)
Depth	48.3 cm (19 inch)
Weight (Fully loaded)	45 kg (99.2 lb)

4.1 NEBS Compliance

The Mediant 8000 chassis complies with NEBS Level 3 requirements.

The unit is compatible with Common Bonding Network (CBN) and Isolated Bonding Network (IBN) installations.

The Equipment is compatible with DC-C and DC-I networks.

4.2 Midplane Keying

Each chassis slot is equipped with a key on the midplane to match the appropriate board type to prevent inserting an incorrect board type into the slot.



Note: While the slot keys on the midplane are designed to prevent the insertion of a board in an incorrect location, do NOT force a board into a slot to avoid damaging either the board or the midplane.

5 Power System

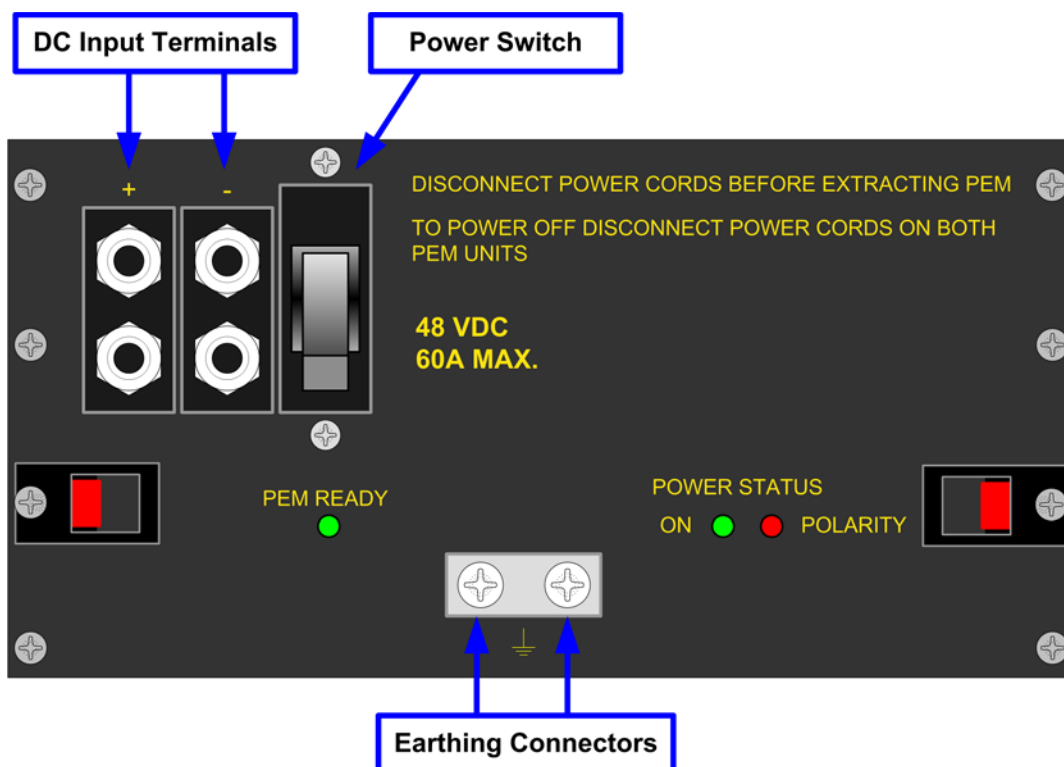
The DC Power System powers the Mediant 8000 from the DC power sources. It consists of the following hardware components:

- PEM/DC/8K Power Entry Module
- PS/DC/8K Power Supply Module

5.1 PEM/DC/8K Power Entry Module

PEM/DC/8K Power Entry Modules are used for connecting the Mediant 8000 chassis to the DC power sources. Two PEM/DC/8K modules are installed in the back of the chassis and enable chassis connection to two independent DC power sources. Such a connection provides chassis power high-availability in the event of DC power source failure. Each of the DC input terminals is reverse current protected.

Figure 5-1: PEM/DC/8K Power Entry Module Panel



5.2 PS/DC/8K Power Supply Module

PS/DC/8K Power Supply modules convert DC input voltage (that may be between -40 and -60 VDC) into DC used for local power inside the chassis. Three PS/DC/8K Power Supply modules are installed in the front of the chassis – below the board slots. PS/DC/8K Power Supply modules are hot-swappable.

Figure 5-2: PS/DC/8K Power Supply Module



5.2.1 DC Input Power

DC power sources must meet the following requirements:

- -48V SELV direct current power source
- Power input between -40.5 and -57 VDC
- Maximum allowable voltage should not exceed -60 VDC
- Provide sufficient capacity for the average power consumption of Mediant 8000 chassis (see 'Electrical Requirements' on page 93)
- Ensure that power supply complies with the safety requirements of CAN/CSA-C22.2 No. 60950-00 and UL 60950, and EN 60950

6 Cooling System

The Mediant 8000 components are cooled by Fan Tray Modules, FM/8K, located in front of the chassis, above the board slots. The FM/8K Fan Tray Module draws air in through a perforated grill at the front bottom of the chassis.

The incoming air passes through a removable filter (located under the front of the card cage and covered by a perforated grill), whose honeycombed design prevents RF interference.

The second FM/8K Fan Tray Module provides redundant protection should one develop a fault.

Figure 6-1: FM/8K Fan Tray Module



6.1 Air Flow

Clean air is drawn in by the fans and passes through the entire set of plug-in front and rear boards residing in the slots, cooling each one. The air exits the Mediant 8000 via perforated vents in the chassis.

Blank panels are used to cover all unoccupied slots (as per the customer's configuration) on both sides of the chassis. The front blank baffled panels are specially constructed to allow optimal air flow within the chassis.

This page is intentionally left blank.

7 Alarm Indicators

Chassis Alarm Indicators are located in the front of the Mediant 8000 chassis above the FM/8K Fan Tray Module's protective cover. They are used to indicate failure conditions on hardware components – e.g. malfunction of the Fan Tray Module or lack of the power input in a Power Supply.

Information provided via the Chassis Alarm Indicators are very brief and high-level. Use the EMS management interface for obtaining detailed information about the status of each hardware module.

Table 7-1: Alarm Indicator

LED	Description	Color Code	Remarks
SYSTEM	Not in use		
CRITICAL	Indicates critical alarm on one of the hardware modules	Green	Normal Critical alarm is cleared
		Red	Critical alarm is set
MAJOR	Indicates major alarm on one of the hardware modules	Green	Normal Major alarm is cleared
		Orange	Major alarm is set
MINOR	Indicates minor alarm on one of the hardware modules	Green	Normal Minor alarm is cleared
		Orange	Minor alarm is set
SHELF	Not in use		

This page is intentionally left blank.

8 TP-6310 Media Gateway Board

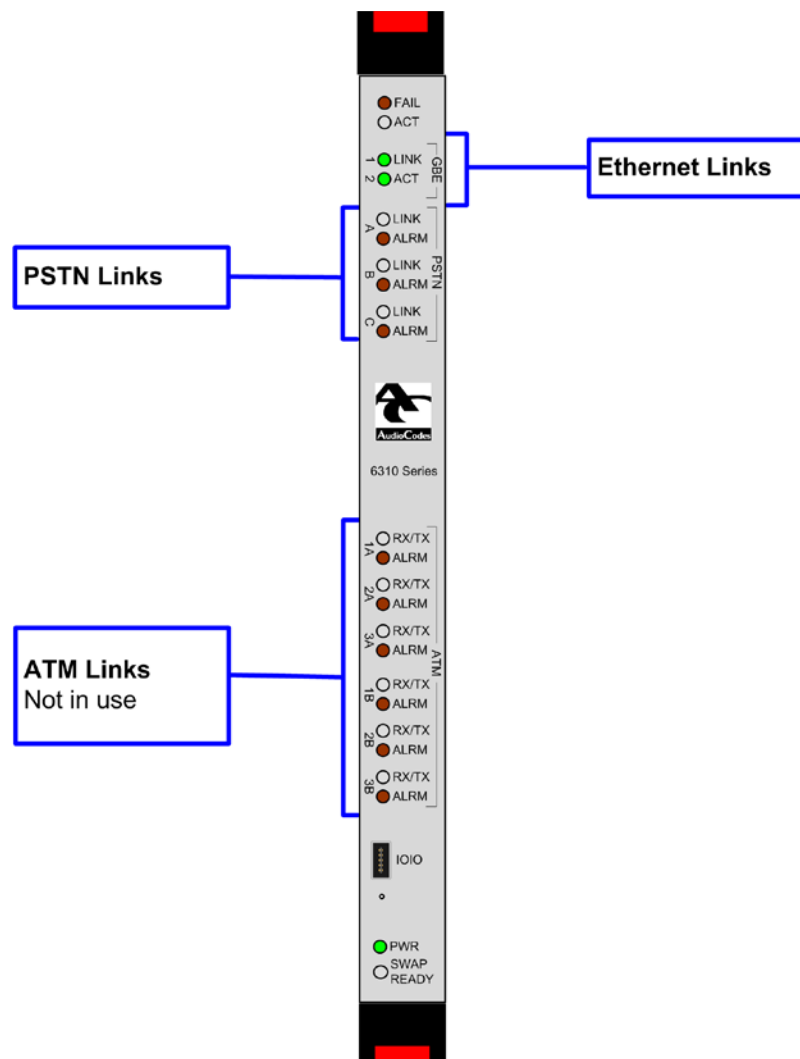
The TP-6310 board is a high-density, hot-swappable resource board with a capacity of up to 2016 DS0 channels, supporting all necessary functions for voice, data and fax streaming over IP networks. It provides the following PSTN interfaces:

- 1+1 STM-1/OC-3 interfaces (APS protected)
- 3 T3 (DS-3) interfaces (6 connectors – 3 RX and 3 TX)

TP-6310 Media Gateway boards feature N+1 redundant protection which ensures that when specific TP-6310 board fails, all traffic and signaling processed by it is recovered on a designated “redundant” TP-6310 board. Redundant TP-6310 board must be equipped with a special Redundant RTM that has no PSTN interfaces on it.

The TP-6310 Media Gateway boards should be inserted into the designated slots. For more information, see 'Board Assembly Order' on page 87.

Figure 8-1: TP-6310 Board Front Panel





Note: There is an unmarked pinhole on the front panel of the TP-6310 board. This pinhole should never be used when the TP-6310 is inserted into the Mediant 8000 chassis.

The TP-6310 Media Gateway board has LED indicators on its front panel that are used to indicate status of the board and of its PSTN interfaces. The Indication provided via these LEDs is very brief and high-level. Use the EMS management interface for obtaining detailed information about the status of the board and each of its component.

Table 8-1: TP-6310 Board Status LED Indicators

Group	LED #	LED Label	Color	Description
		ACT	---	Not in use
PSTN (for STM-1/OC3 configuration)	A,B	Link	Off	No link
			Green	Working link OK
			Yellow	Protection link OK
		Alrm	Off	Normal operation
			Red	Alarm detected on the link
	C	Link	---	Not in use
		Alrm	---	Not in use
PSTN (for T3 configuration)	A,B,C	Link	Off	No Link
			Green	T3 Synchronized
			Yellow	Remote Alarm (RAI) detected on link
		Alrm	Off	Normal operation
			Red	Near End Alarm (LOS, LFA or AIS) detected on link
		PWR	Off	Board Power is down
			Green	Normal Operation
		SWAP READY	Off	Normal Operation
			Blue	Board is ready to be extracted from the chassis (latch is open)

9 6310/RTM - Rear Transition Module

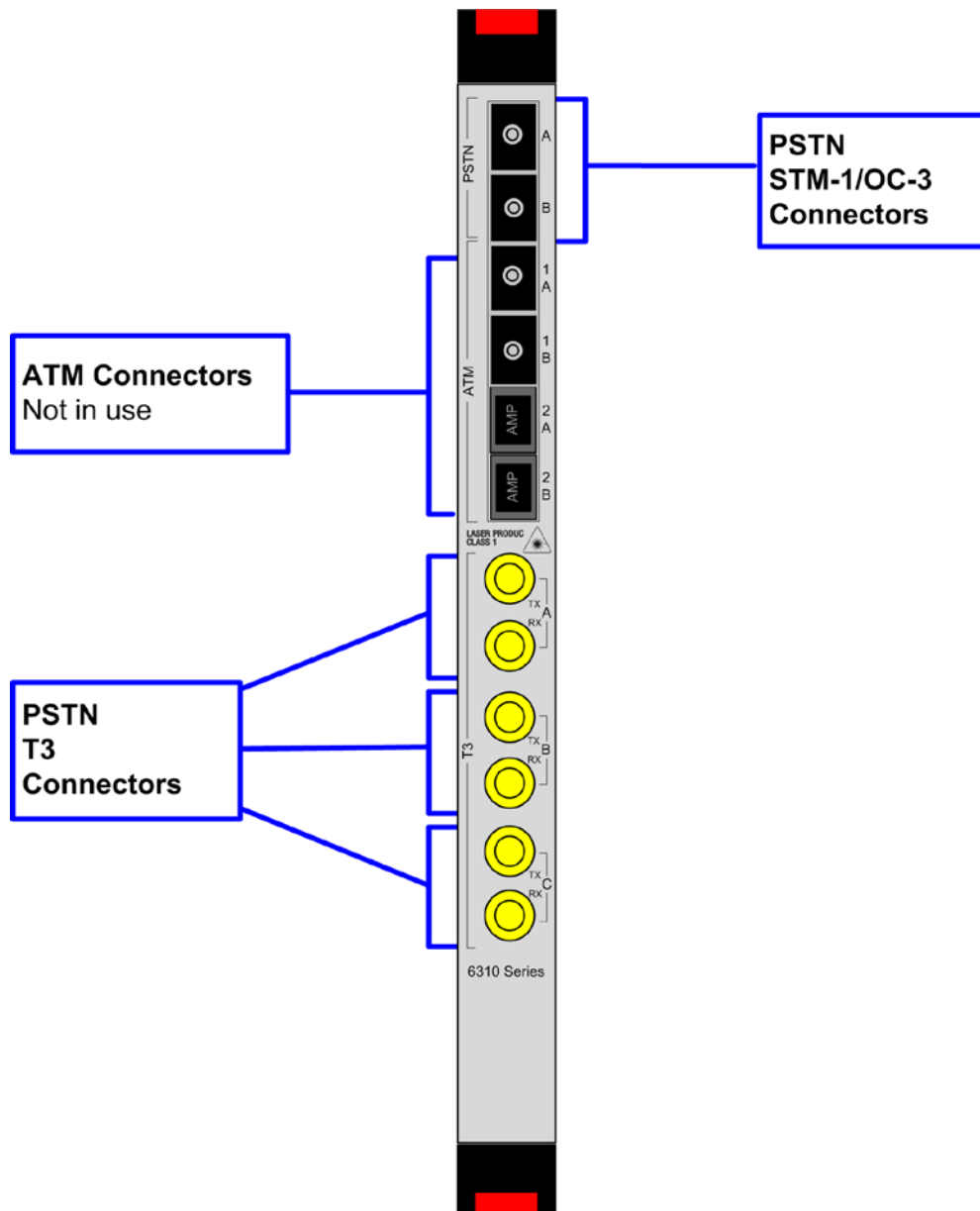
The 6310/RTM Rear Transition Module is a hot-swappable rear module that provides PSTN connectivity for TP-6310 Media Gateway board. It is installed in the rear side of the chassis behind the corresponding TP-6310 board and features the following interfaces:

- STM-1/OC-3 PSTN
- T3 (DS-3) PSTN

Each STM-1/OC-3 connection uses a 155 Mbps optical SFP (Small Form-factor Pluggable) module with hot-insertion capabilities.

Each T3 (DS-3) PSTN connection uses an unshielded mini-SMB female connector, MOLEX PN: 73396-0010. On the cable side, the male connector, MOLEX PN: 73100-0255 or the equivalent should be used.

Figure 9-1: 6310 RTM Front Panel



Note: The unused SFP receptacles must be covered with dust covers.

9.1 6310/RTM Redundant

The TP-6310 board that is configured as a redundant board must be accompanied by a proper Redundant RTM module. The latter has no connectors on it and is used for routing PSTN links from the failed TP-6310 board to the redundant board.

Figure 9-2: 6310/RTM Redundant Front Panel



Note: Do not mistake the 6310/RTM Redundant with a blank panel that is used for covering empty slots.

This page is intentionally left blank.

10 TP-8410 Media Gateway Board

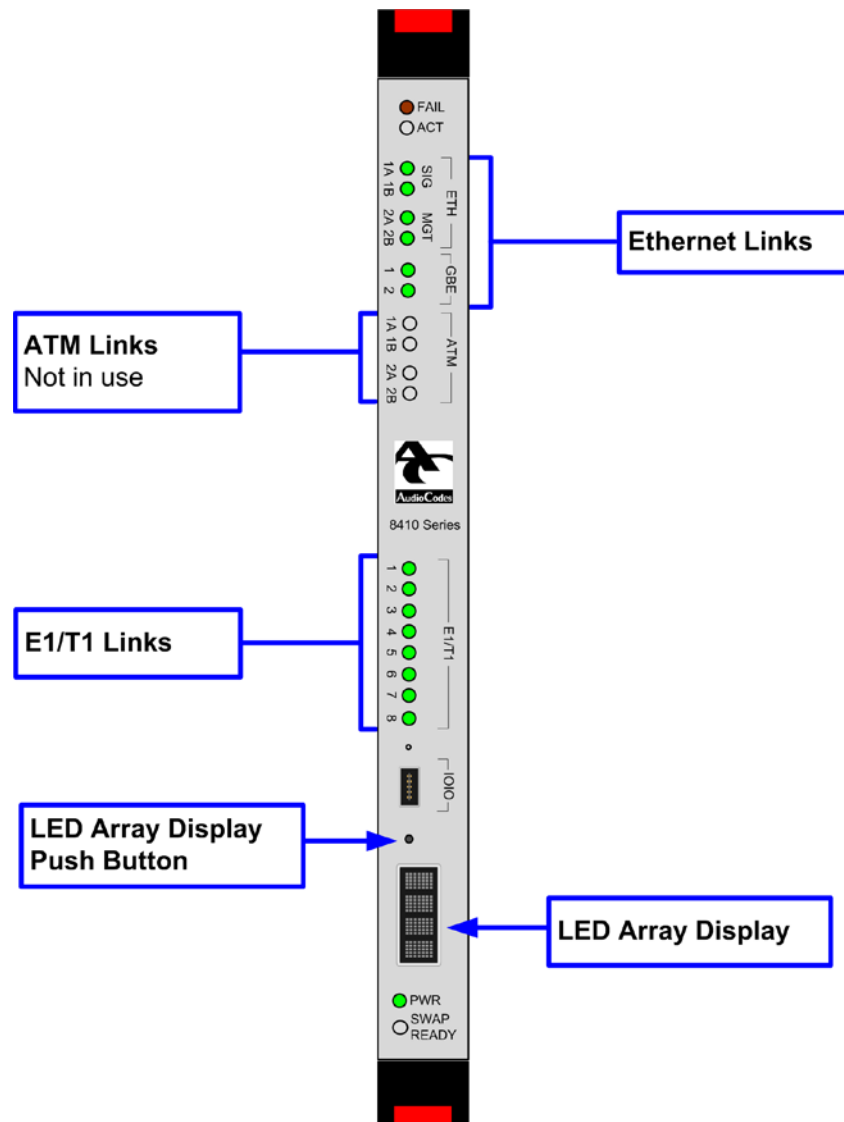
The TP-8410 board is a high-density, hot-swappable resource board with a capacity of up to 2016 VoP channels, supporting all necessary functions for voice, data and fax streaming over IP networks. It provides the following PSTN interfaces:

- 42 E1 interfaces with up to 31 channels per trunk (1302 DS0 channels)
- 42 T1 interfaces with up to 24 channels per trunk (1008 DS0 channels)

TP-8410 Media Gateway boards feature N+1 redundant protection which ensures that when specific TP-8410 board fails, all traffic and signaling processed by it is recovered on a designated “redundant” TP-8410 board. The Redundant TP-8410 board must be equipped with a special Redundant RTM that has no PSTN interfaces on it.

TP-8410 Media Gateway boards should be inserted into the designated slots. See 'Board Assembly Order' on page 87 for the details.

Figure 10-1: TP-8410 Board Front Panel





Note: There is an unmarked pinhole on the front panel of the TP-8410 board. This pinhole should never be used when the TP-8410 board is inserted into the Mediant 8000 chassis.

The TP-8410 Media Gateway board has LED indicators on its front panel that are used to indicate the status of the board and its PSTN interfaces. The indication provided via these LEDs is very brief and high-level. Use the EMS management interface for obtaining detailed information about the status of the board and each of its components.

Table 10-1: TP-8410 Board LEDs

LED Label	Description	Color
ACT	Not in use	--
E1/T1(1-8)	E1/T1 is synchronized	Green
	Alarm (LOS, LFA or AIS) is detected on E1/T1 trunk	Red
	No E1/T1 trunk	Off
GBE (1,2)	Media Network interface 1Gb Ethernet link operates normally (LED may blink when data is transmitted)	Green
	Media Network interface 1Gb Ethernet link is disconnected	Off
ETH (1A, 1B)	Control Network interface 10/100Mb Ethernet link operates normally (LED may blink when data is transmitted)	Green
	Control Network interface 10/100Mb Ethernet link is disconnected.	Off
ETH (2A, 2B)	OAM Network interface 10/100Mb Ethernet link operates normally (LED may blink when data is transmitted)	Green
	OAM Network interface 10/100Mb Ethernet link is disconnected	Off
PWR	Normal Operation	Green

LED Label	Description	Color
	Board Power is down	Off
SWAP READY	Normal Operation	Off
	Board is ready to be extracted from the chassis (latch is open)	Blue

10.1 LED Array Display

The LED Array display indicates the trunk numbers currently represented by the TP-8410 board's PSTN LEDs (labeled E1/T1). The status of the E1/T1 trunks is indicated by the eight E1/T1 LEDs in groups of eight trunks. Each time you press the LED Array Display button (located to the left of the LED display) the status of the next eight consecutive trunks is indicated by the E1/T1 LEDs. For example, when you first press the LED Array Push button, the first group of trunks indicated by the LEDs is 1-8. The next time you press the LED Array Push button, the next group of trunks indicated by the LEDs is 9-16. You can continue this process until reaching trunk 42.

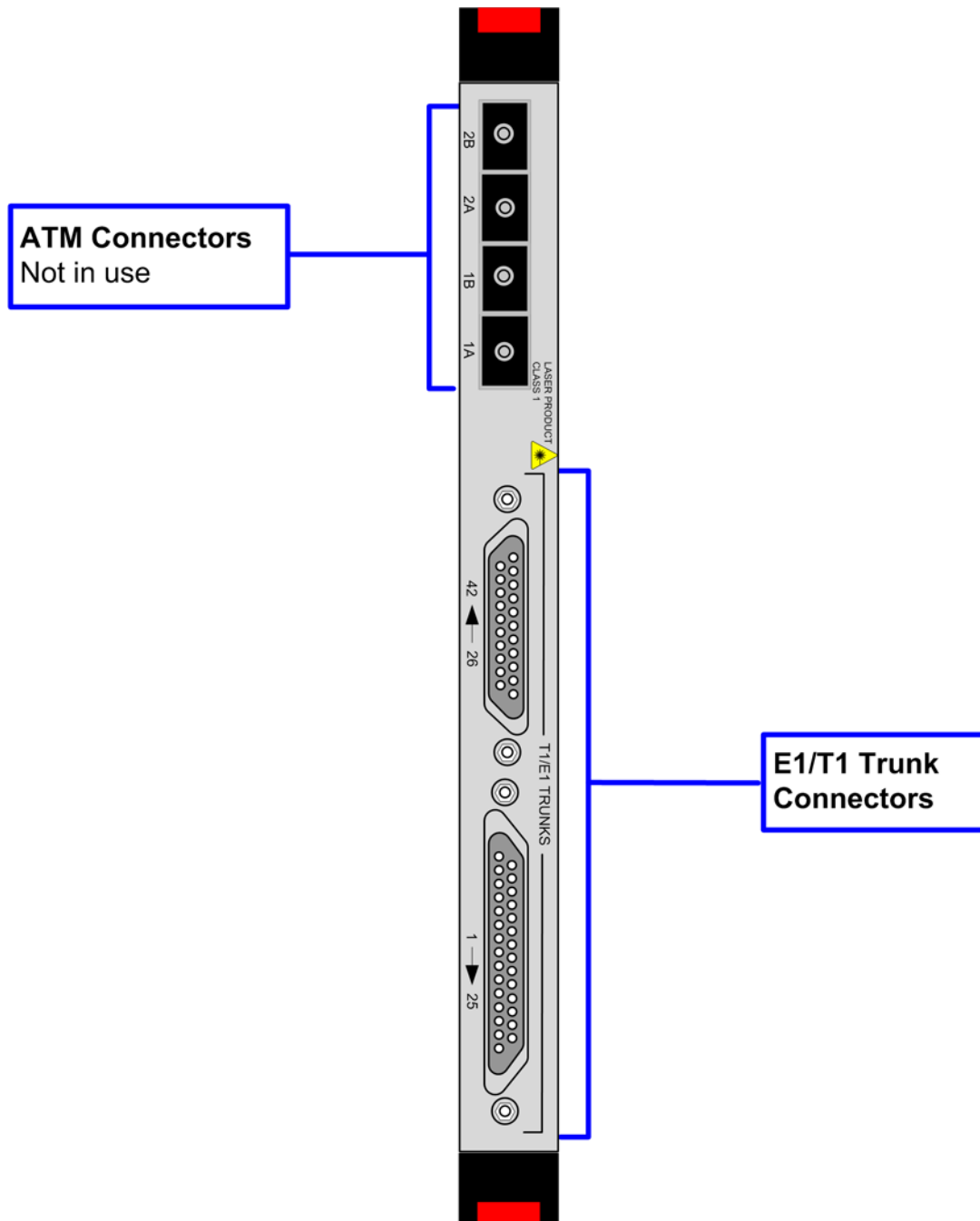
The LED Array display also displays the TP-8410 board's MAC address. Press the LED Array Display button until the last group of trunks is displayed, and then press again to display the MAC address. (When the MAC address is displayed, the E1/T1 LEDs turn off.) The next press of the button displays the first trunk group.

This page is intentionally left blank.

11 8410/RTM Rear Transition Module

The 8410/RTM Rear Transition Module is a hot-swappable rear module that provides PSTN connectivity for the TP-8410 Media Gateway board. It is installed in the rear side of the chassis behind the corresponding TP-8410 board and features two SCSI connectors (100-Pin and 68-Pin) that are used for connecting up to 42 DS1 (E1/T1) trunks.

Figure 11-1: 8410 RTM Panel





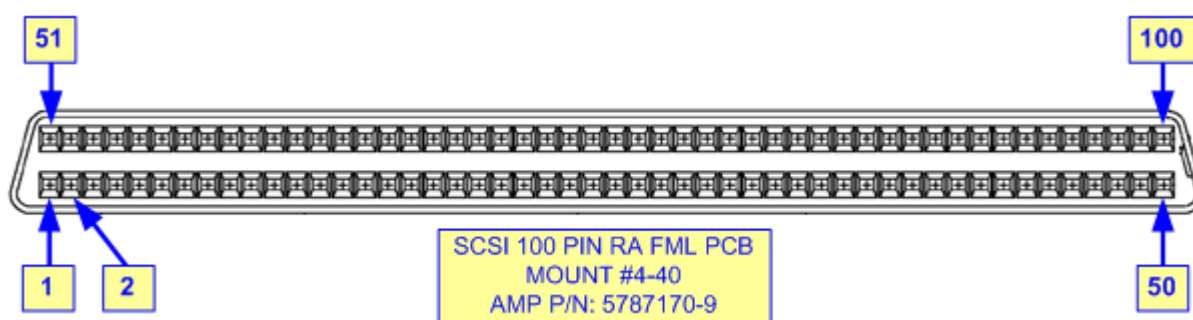
Note: The unused SFP receptacles are covered with dust covers.

11.1 8410/RTM E1/T1 Trunk Connectors

The 8410/RTM provides two SCSI connectors that are used for connecting up to 42 E1/T1 trunks:

- 100-pin female connector-used for connecting trunks 1-25
- 68-Pin female connector-used for connecting trunks 26-42

Figure 11-2: 8410/RTM 100-Pin SCSI Connector



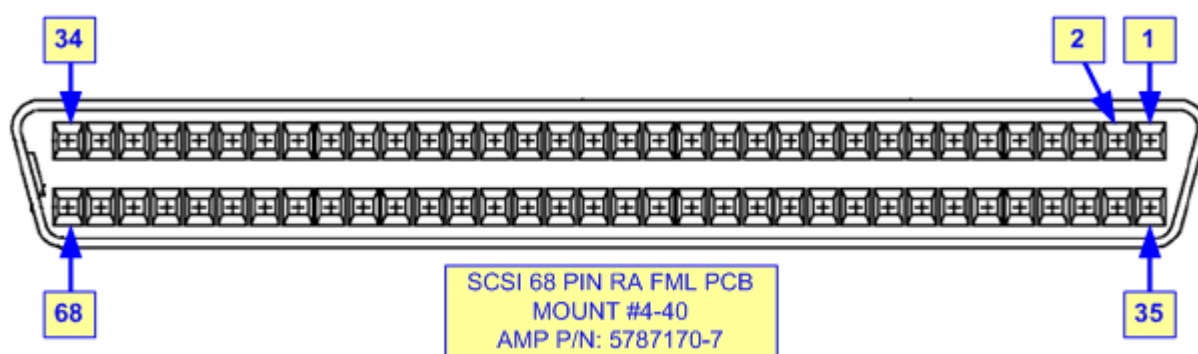
The 100-pin female SCSI connector is shown in the figure above must mate with a male connector that is wired according to the connector pinouts in the following table.

Table 11-1: 8410/RTM 100-pin SCSI Connector

E1/T1 Number (1 to 25) RTM-8410	Tx Pins (Tip/Ring)	Rx Pins (Tip/Ring)
1	2/1	52/51
2	4/3	54/53
3	6/5	56/55
4	8/7	58/57
5	10/9	60/59
6	12/11	62/61
7	14/13	64/63
8	16/15	66/65
9	18/17	68/67
10	20/19	70/69
11	22/21	72/71

E1/T1 Number (1 to 25) RTM-8410	Tx Pins (Tip/Ring)	Rx Pins (Tip/Ring)
12	24/23	74/73
13	26/25	76/75
14	28/27	78/77
15	30/29	80/79
16	32/31	82/81
17	34/33	84/83
18	36/35	86/85
19	38/37	88/87
20	40/39	90/89
21	42/41	92/91
22	44/43	94/93
23	46/45	96/95
24	48/47	98/97
25	50/49	100/99

Figure 11-3: 8410/RTM 68-pin SCSI Connector



The 68-pin female SCSI connector is shown in the figure above and must mate with a male connector that is wired according to the connector pinouts in the following table.

Table 11-2: 8410/RTM 68-pin SCSI Connector

E1/T1 Number (26 to 42) RTM-8410	Tx Pins (Tip/Ring)	Rx Pins (Tip/Ring)
26	2/1	36/35
27	4/3	38/37
28	6/5	40/39
29	8/7	42/41
30	10/9	44/43
31	12/11	46/45
32	14/13	48/47
33	16/15	50/49
34	18/17	52/51
35	20/19	54/53
36	22/21	56/55
37	24/23	58/57
38	26/25	60/59
39	28/27	62/61
40	30/29	64/63
41	32/31	66/65
42	34/33	68/67

11.2 8410/RTM Redundant

The TP-8410 board that is configured as a redundant board must be accompanied by a proper Redundant RTM module. The latter has no port connections and is used for routing PSTN E1/T1 trunks from the failed TP-8410 board to the redundant board.

Figure 11-4: 8410/RTM Redundant Front Panel



Note: Do not mistake the 8410/RTM Redundant with a blank panel that is used for covering empty slots.

This page is intentionally left blank.

12 System Controller (SC) Board

The SC (System Controller) board is a hot-swappable Single Board Computer (SBC). It provides management interface to the Mediant 8000 and is responsible for system configuration, status monitoring and high-availability operation.

Two SC boards are provided for high-availability and are installed in slots 1 and 2 (color coded *red*).

The following hardware revisions of the SC Boards are available:

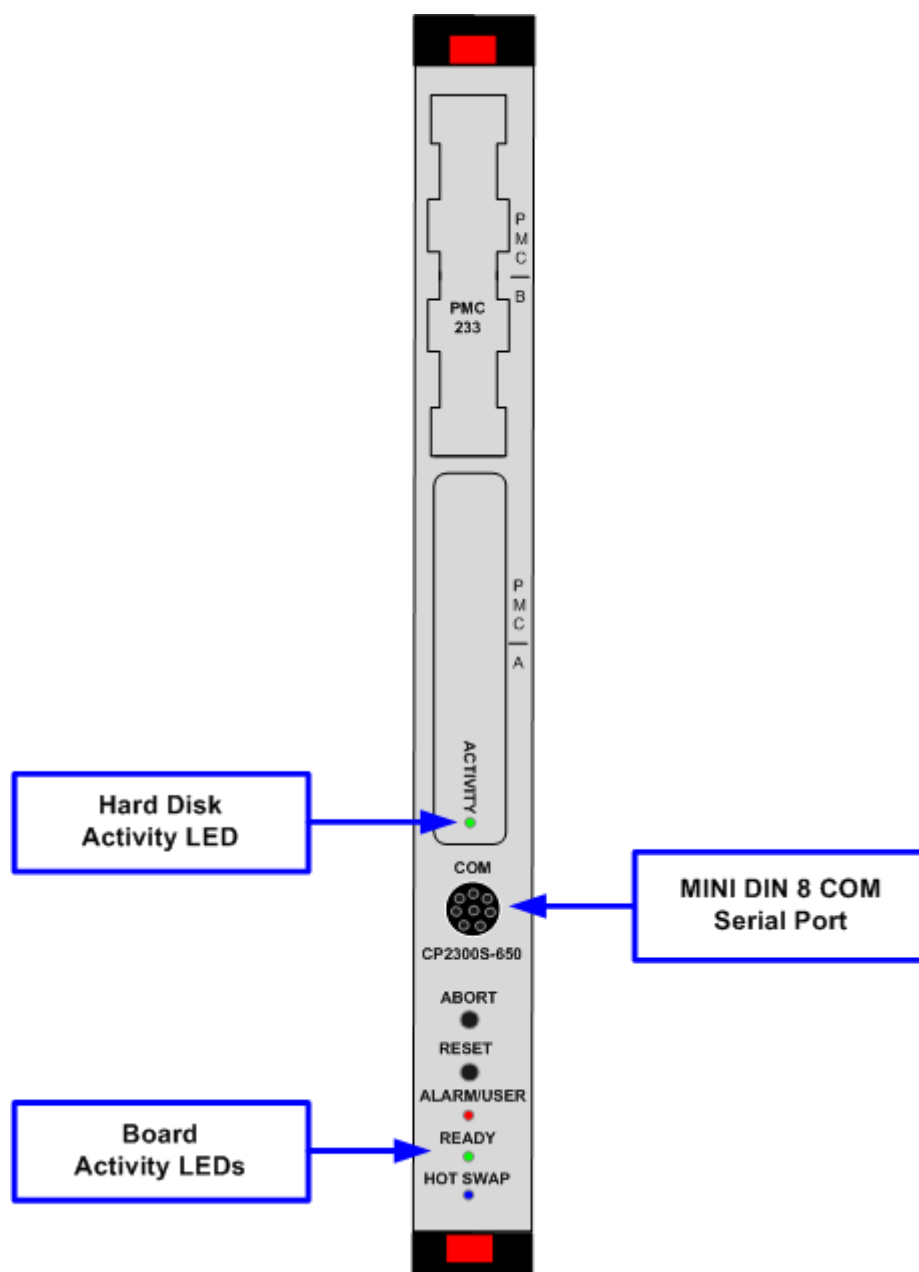
- SC Rev.1 – first-generation SC board based on SUN CP2300 SBC, runs SUN Solaris OS
- SC Rev.2 – second-generation SC board, uses Intel CPU and runs Linux OS

SC Rev.2 boards are supported starting from version 5.8 of the Mediant 8000 software. Note however that you may not install SC boards of different hardware revisions in the same chassis and you should use the software installation disk that matches the revision of SC boards installed in your Mediant 8000 chassis (see 'Installing the Mediant 8000 Software' on page [129](#) for details).

12.1 SC Rev.1 board (Solaris OS)

The SC Rev.1 board is based on the SUN CP2300 SBC and runs the SUN Solaris 9 OS.

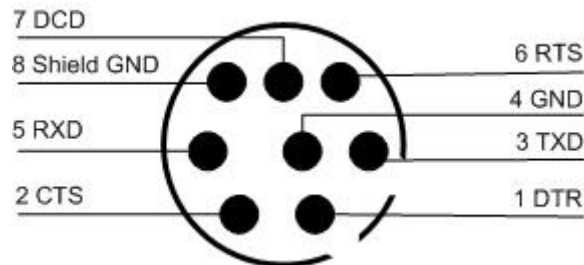
Figure 12-1: SC Rev.1 Board Panel



12.1.1 SC Rev.1 Mini DIN 8 COM RS-232 Port

The SC Rev.1 board provides Mini DIN 8 COM RS-232 serial port connector on its front panel that may be used for accessing board's Command Line Interface (CLI). Alternatively RS-232 serial port connector on the SA/RTM module may be used for accessing the SC boards' CLI.

Figure 12-2: SC Rev.1 Board Mini DIN 8 Serial Port Connector



12.1.2 Status LEDs

The SC Rev.1 board has LED indicators on its front panel that are used to indicate the status of the board.

Table 12-1: SC Rev.1 Board LED Indicators

LED	Description	Color
Activity	Located on the hard disk PMC module. Blinks during normal operation when SC software accesses the hard disk.	Green
ALARM/USER	Normal operation	Green
	Alarm is detected	Yellow
READY	Normal operation	Green
	Board is not ready for operation	Off
HOT SWAP	Normal operation	Off
	Board is ready for extraction from the chassis (latches are open).	Blue

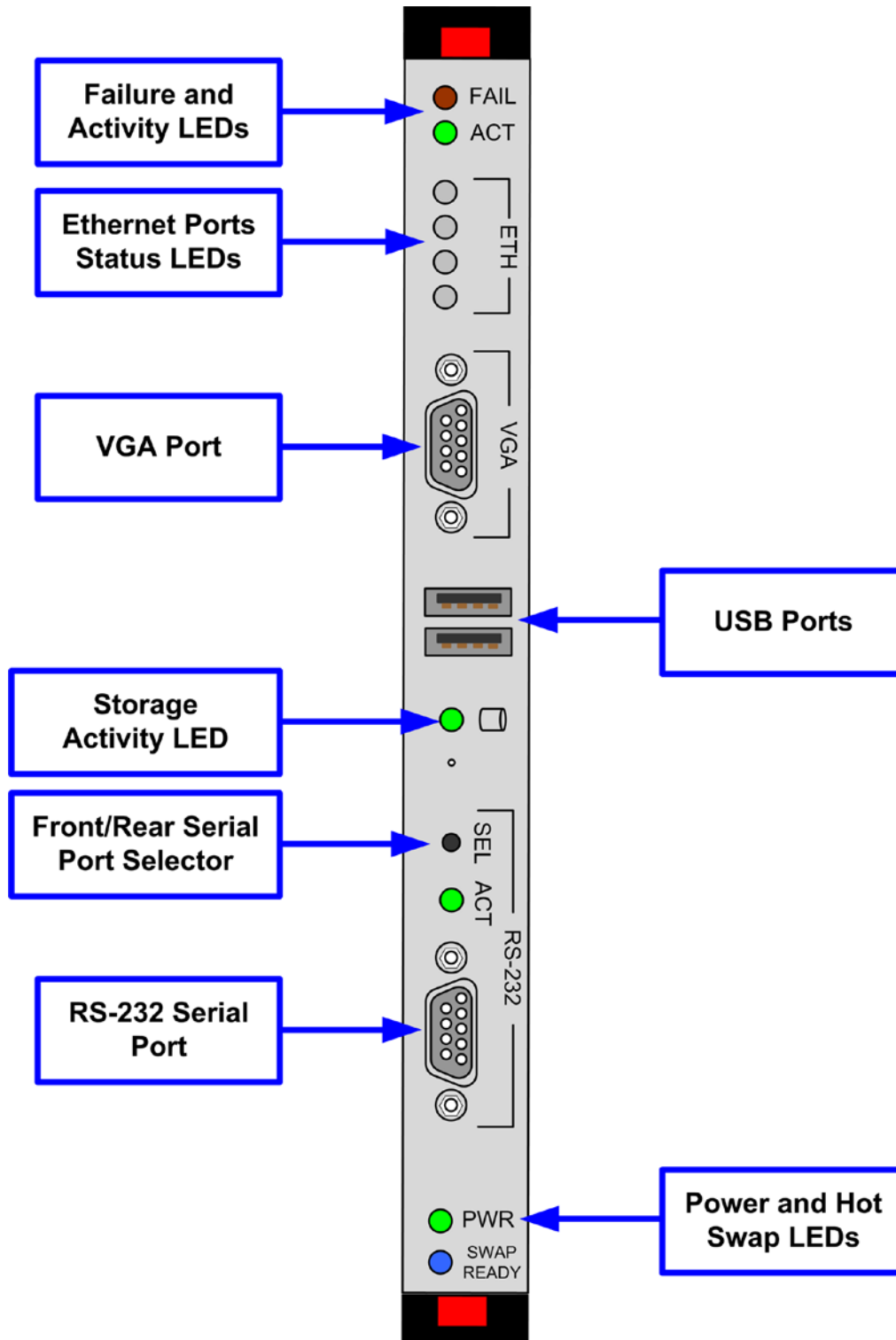


Note: There are two recessed push buttons on the front panel of the SC board, marked ABORT and RESET. These buttons should never be used when the SC board is inserted into the Mediant 8000 chassis.

12.2 SC Rev.2 Board (Linux OS)

SC Rev.2 is a next-generation SC board that uses an Intel CPU and runs on the Linux OS.

Figure 12-3: SC Rev.2 Board Panel



12.2.1 SC Rev.2 RS-232 Serial Port

The SC Rev.2 board provides an RS-232 serial console port that may be used for connecting to its Command Line Interface (CLI). The port is provided as a 9-pin female D-type connector (P2). The corresponding cable is a straight through cable with a 9-pin male D-type connector (P1). The table below describes the connector pinouts.

Table 12-2: SC Rev.2 Board (Linux OS) RS-232 Connector Pinouts

P2 Pin #	Signal Name	P2 Pin #
2	RX-(Receive Data) (to CPU)	3
3	TX (Transmit Data) (from CPU)	2
5	GND (Ground)	5

Alternatively an RS-232 console port on the corresponding SA/RTM board (located in the rear of the chassis, behind the SC board) may be used instead. At any time, only one serial console port is active (either on the SC board or on the SA/RTM board). To switch between these serial console ports, use the Front/Rear serial port selector button (labeled **SEL**). The Serial Port activity LED (labeled **ACT**) indicates the serial console port that is currently in use.

12.2.2 USB Ports

The SC Rev.2 board provides two USB ports that may be used for connecting standard USB storage devices (e.g. USB Flash Drive or USB CD-ROM) and USB peripherals (e.g. keyboard or mouse) to the SC board. Use of these ports should be limited to the software installation (as described in 'Installing Mediant 8000 Software' on page [129](#)) and debugging only.

12.2.3 VGA Port

The SC Rev.2 board provides a VGA port that may be used for connecting an external monitor to the SC board. Use of the VGA port is not imperative for normal SC board operation and should be used for debugging purposes only.

12.2.4 Status LEDs

The SC Rev.2 board has LED indicators on its front panel that are used to indicate the status of the board.

Table 12-3: SC Rev.2 Board (Linux OS) LED Indicators

Label	Function	Color
FAIL	Normal operation	Off
	Board failure	Red
ACT	Currently not in use	Off
ETH	Ethernet link status. Only the first two LEDs are in use.	
	Normal operation (1Gbps mode)	Green
	Normal operation (100 Mbps mode)	Orange
	Link disconnected	Off
Storage Activity	Blinks during normal operation when the SC software accesses the storage device (SSD).	Green
RS-232 ACT	Front serial console port is in use	Green
	Rear serial console port (on SA/RTM board) is in use	Off
PWR	Power is received (normal operation)	Green
	Power is not supplied to the board	Off
SWAP READY	Normal operation	Off
	Board is ready for extraction from the chassis (latches are open).	Blue

12.3 SA/RTM Synchronization and Alarm Rear Transition Module

The SA/RTM Synchronization and Alarm Rear Transition Module is a hot-swappable rear module that is used to complement the SC board. It provides chassis management functionality, utilized by the SC board management software, such as control over the fan trays, monitoring of the chassis voltages etc.

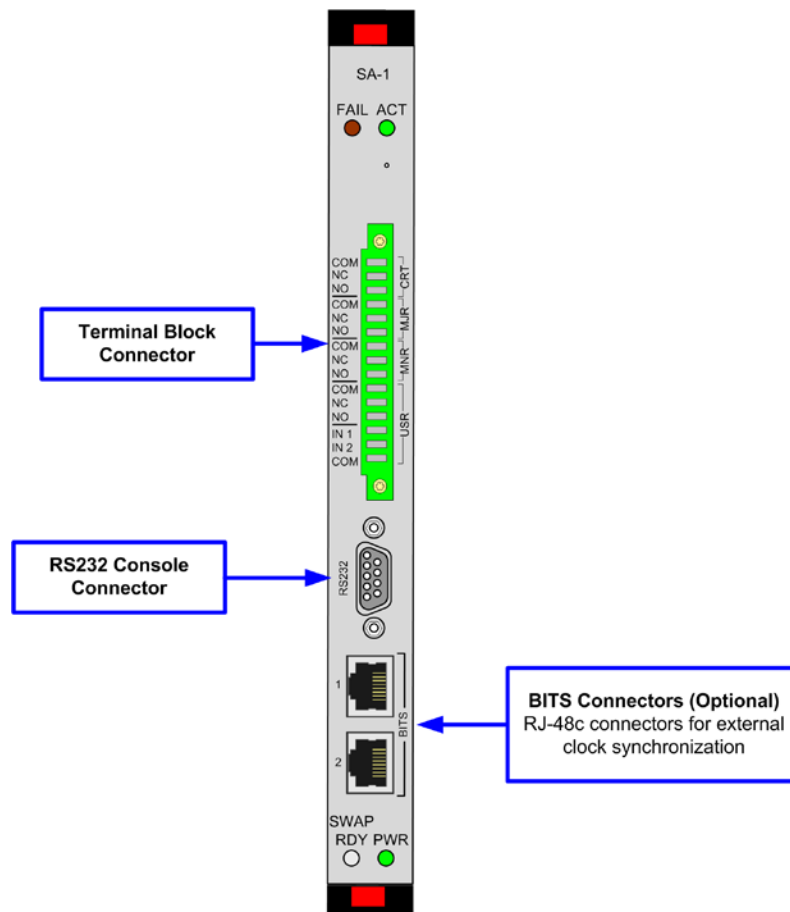
The SA/RTM board may be optionally equipped with a Timing Module that is used to provide clock synchronization on the Media Gateway PSTN interfaces.



Note: To order the SA/RTM board with a resident Timing Module (SA-1/RTM board), refer to the AudioCodes price list.

Two SA/RTM boards are provided for high-availability and installed in the chassis' rear slots 1 and 2, behind the corresponding SC boards.

Figure 12-4: SA/RTM Panel



The SA/RTM board has LED indicators on its front panel that are used to indicate the status of the board.

Table 12-4: SA-RTM LED Indicators

Label	Function	Color
FAIL	Normal operation	Off
	Board failure	Red
ACT	Active board	Green
	Standby board	Yellow
PWR	Normal operation	Green
	Power is not supplied to the board	Off
HOT SWAP	Normal operation	Off
	Board is ready for extraction from the chassis (latches are open).	Blue

12.3.1 SA/RTM RS-232 Console Port

The SA/RTM board provides RS-232 console port that may be used for connecting to the corresponding SC board's Command Line Interface (CLI).

SA/RTM board's RS-232 console port is a 9-pin female D-type connector (P2). The corresponding cable is a straight through cable with a 9-pin male D-type connector (P1).

Table 12-5: SA/RTM RS-232 Console Port Connector

P1 Pin #	Signal Name	P2 Pin #
2	RX (Receive Data)	3
3	TX (Transmit Data)	2
5	GND (Ground)	5

12.3.2 SA/RTM Terminal Block Connector

The SA/RTM board provides a Terminal Block Connector that may be used for connecting the Telco alarm equipment. Three dry contacts – COM (Common), NO (Normally Open) and NC (Normally Closed) – are provided for each alarm.

Table 12-6: SA/RTM Terminal Block Connector

Alarm Type	Description	Connector Types	Number of Connectors
CRT	Critical	COM, NC, NO	3
MJR	Major	COM, NC, NO	3
MNR	Minor	COM, NC, NO	3
USR	User Defined	COM (x2)*, NC, NO, *IN 1, *IN 2	6

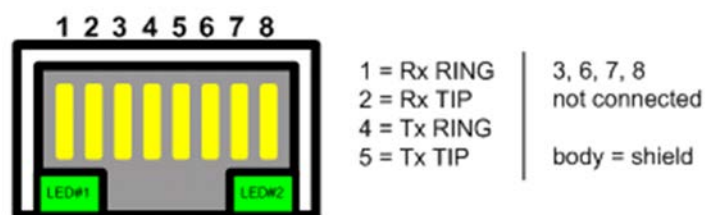
*One COM connector and IN 1 and IN 2 connectors are for future use.

To mute the Telco alarm relay devices attached to the SA/RTM Terminal Block, use the ACO Alarm push button located below the Chassis Alarm Indicators LEDs.

12.3.3 SA/RTM BITS (RJ48-c) Pin Signal Interface (Optional)

The SA/RTM board with a resident Timing Module provides two BITS (RJ48-c) Interfaces for connecting to the external Building Integrated Timing Supply (BITS) equipment. The following table describes the signal interface of the connector.

Figure 12-5: RJ-48c Trunk Connectors



12.3.3.1 Built-In LED Interface

Each SA/RTM BITS Interface has LEDs that indicate its status.

Table 12-7: SA/RTM BITS Interface LEDs

Label	Color	Function
LED#1	Off	No Signal
	Green	BITS signal – synchronized
LED#2		Not in use

13 Ethernet Switch Board

The Ethernet Switch board is a hot-swappable Compact PCI board that provides full wire-speed Layer2 Gigabit Ethernet switch functionality. It is used for connecting the Mediant 8000 to the external IP network, as well as interconnecting the Media Gateway and the SC boards.

Two ES boards are provided for high-availability and are installed in slots 9 and 19.

The following hardware revisions of the ES Boards are available:

- ES/6600 – first-generation ES board
- ES-2 – second-generation ES board

ES-2 boards are supported, starting from Version 6.2 of the Mediant 8000 software.



Note: You may not install ES boards of different hardware revisions on the same chassis.

13.1 ES/6600 ES (Ethernet Switch) Board

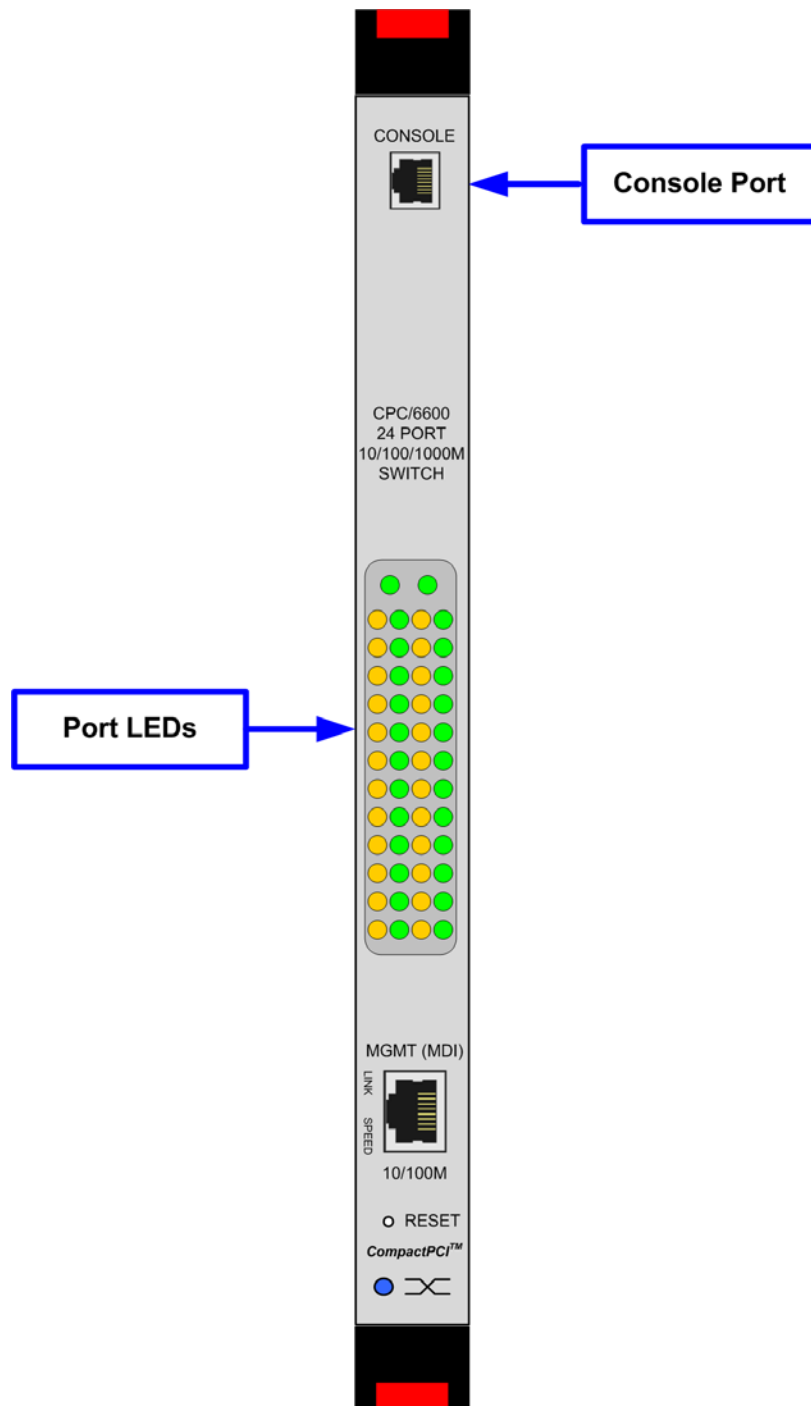
The ES/6600 is a hot-swappable Compact PCI board that provides full wire-speed Layer2 Gigabit Ethernet switch functionality. It is used for connecting the Mediant 8000 to the external IP network as well as interconnecting the Media Gateway and the SC boards.

The ES/6600 has 24 10/100/1000Mbps Ethernet Ports. Eleven of these ports are connected to the Mediant 8000 that correspond to SC and Media Gateway boards). Six of these ports are connected to the ES/6600/RTM module and may be used for connecting the Mediant 8000 to the external IP network. The remainder of the ports are currently not in use. See Section 'ES/6600 Physical Slots to Ethernet Port Mapping' on page 76 for additional details.

13.1.1 ES/6600 Board Panel

The figure below illustrates the ES/6600 board panel.

Figure 13-1: ES/6600 Board Panel



13.1.2 ES/6600 LEDs

The ES/6600 Ethernet Switch board has LED indicators on its front panel that are used to indicate the status of the board and its Ethernet Ports.

Table 13-1: ES/6600 Board Status Led Indicators

LED	Description	Color Code	Remarks
SYSTEM	Indicates board operation status	Green	Normal operation
		Yellow	Board is rebooting
		Off	Power is not available
FAULT	Indicates the fault condition on the board	Off	Normal state
		Red	Fault condition is detected
Port Activity	Indicates the activity status for each of the 24 available Ethernet Ports. See ES/6600 Physical Slots to Ethernet Port Mapping below to determine where the specific Ethernet Port is connected.	Green	Port is connected
		Off	Port is disconnected
		Flashing Green	Activity on port (transmit or receive)
Port Speed	Indicates speed for each of the 24 available Ethernet Ports.	Yellow	Port operates at 1000 Mbps speed
		Off	Port operates at 10 or 100 Mbps speed
HOT SWAP	Indicates board readiness for extraction from the chassis	Off	Normal state
		Blue	Board is ready for extraction (latches are open)

13.1.3 ES/6600 Physical Slots to Ethernet Port Mapping

Use the following table to determine which Mediant 8000 physical slot is connected to the specific Ethernet Switch Port.

Table 13-2: ES/6600 Physical Front Slots to Ethernet Port Mapping

Chassis Slot Number	Slot 9 Ethernet Switch Port	Slot 19 Ethernet Switch Port	Dedicated to Board Type
1	13	13	SC
2	14	14	SC
3	-	-	N/A
4	15	15	Redundant TP-8410
5	-	-	N/A
6	-	-	N/A
7	16	16	TP-6310 or TP-8410
8	17	17	TP-6310
9	-	11,12	Ethernet Switch
10	-	-	N/A
11	18	18	TP-6310 or TP-8410
12	19	19	TP-6310 or TP-8410
13	20	20	TP-6310 or TP-8410
14	21	21	TP-6310 or TP-8410
15	22	22	TP-6310 or TP-8410
16	23	23	TP-6310
17	24	24	Redundant TP-6310
18	-	-	N/A
19	11,12	-	Ethernet Switch
-	18	18	Uplink When Interface Separation is enabled, used for O&M or Control traffic (depending on the separation mode).
-	19	19	Uplink When Interface Separation is enabled, used for Control traffic

Chassis Slot Number	Slot 9 Ethernet Switch Port	Slot 19 Ethernet Switch Port	Dedicated to Board Type
-	20	20	Uplink When Interface Separation is disabled, used as the only uplink for the Mediant 8000. When Interface Separation is enabled, used for Media traffic. May be aggregated with ports 21 and 22 for additional capacity.
-	21	21	Uplink When Interface Separation is enabled, used for Media traffic. Aggregated with ports 20 and 22.
-	22	22	Uplink When Interface Separation is enabled, used for Media traffic. Aggregated with ports 20 and 21.
-	23	23	Uplink Used as a Mirror Port for maintenance purposed.

13.1.4 ES/6600/RTM Rear Transition Module

The ES/6600/RTM Rear Transition Module is inserted in the rear Mediant 8000 chassis slots behind the corresponding ES/6600 Ethernet Switch Boards. It provides 10/100/1000Base-T ports that are used for connecting the Mediant 8000 chassis to the external Ethernet equipment.

The ES/6600/RTM also contains an RS-232 console port, which is used for configuration or debugging.

Figure 13-2: ES/6600/RTM Panel

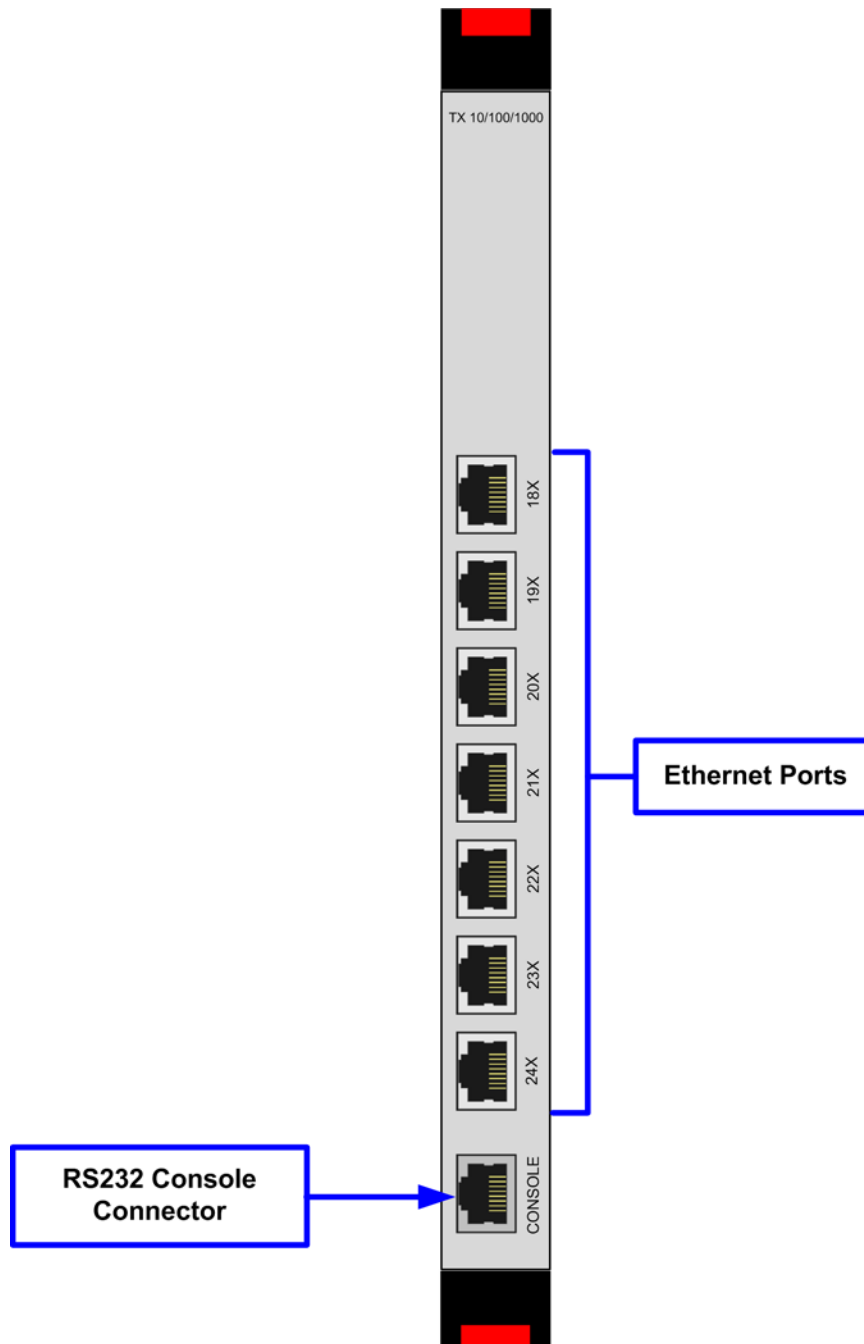


Table 13-3:ES/6600/RTM Port Pin Outs

Pin Number	Signal Name
1	TRDB+
2	TRDB+
3	TRDA+
4	TRDD+
5	TRDD-
6	TRDA-
7	TRDC+
8	TRDC-

13.2 ES-2 ES (Ethernet Switch) Board

The ES-2 is a hot-swappable Compact PCI board that provides full wire-speed Layer2 Gigabit Ethernet switch functionality. It is used for connecting the Mediant 8000 to the external IP network as well as interconnecting the Media Gateway and the SC boards.

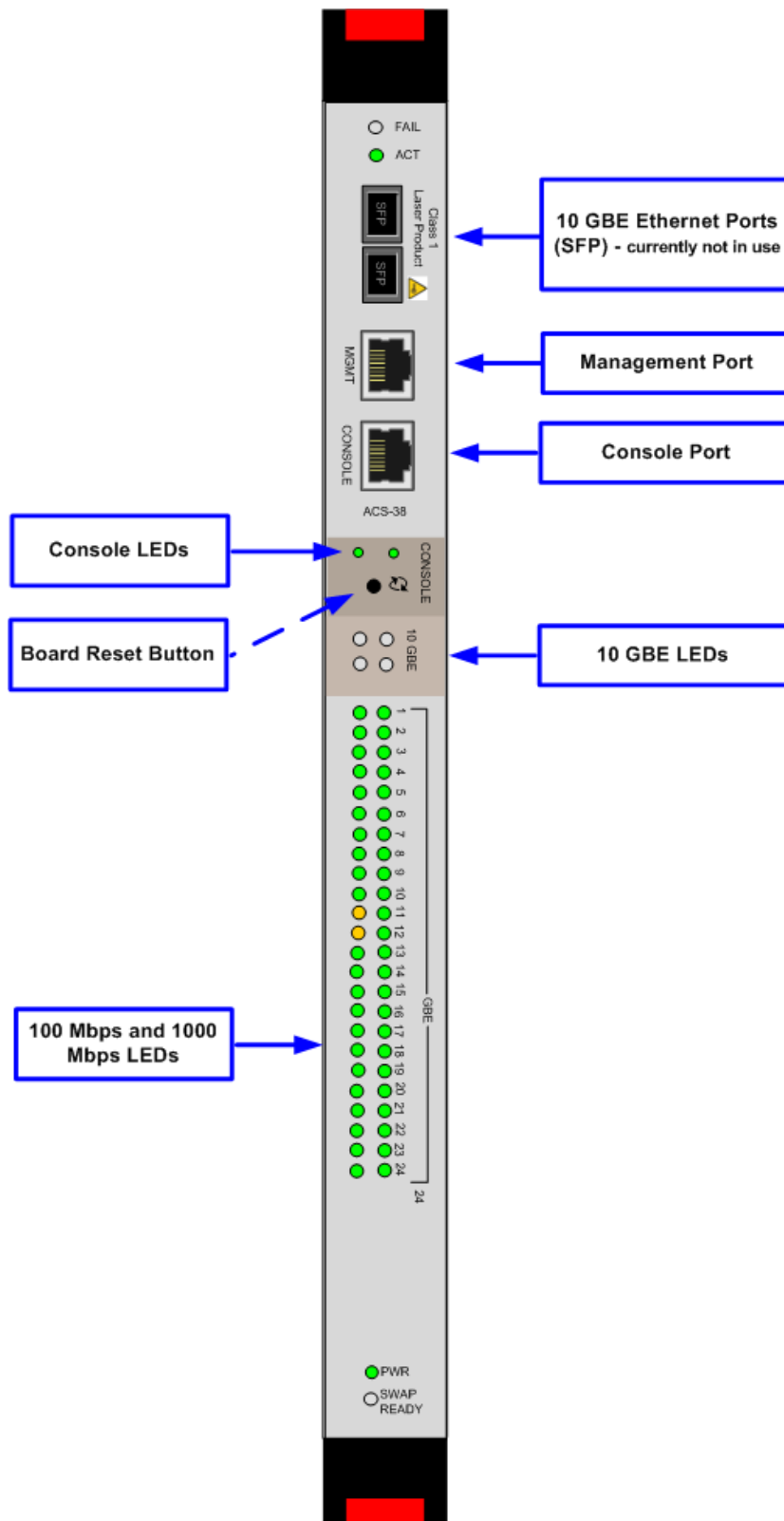
The ES-2 board has 24 10/100/1000Mbps ethernet ports; 14 of these ports are connected to the Mediant 8000 midplane slots (that correspond to SC, Media Gateway boards and F-LINK); 10 of these ports are connected to the ES-2/RTM module and may be used for connecting the Mediant 8000 to the external IP network (ports 8 and 9 are not in use). Refer to 'ES-2 Physical Slots to Ethernet Port Mapping' below for additional details.

The ES-2/RTM also contains an RS-232 console port, which is used for configuration or debugging.

13.2.1 ES-2 Front Panel

The figure below illustrates the ES-2 board panel.

Figure 13-3: ES-2 Board Panel



13.2.2 ES-2 LEDs

The ES-2 Ethernet Switch board has LED indicators on its front panel that indicate the status of the board and its Ethernet Ports.

Table 13-4: ES-2 Board Status Led Indicators

LED	Description	Color Code	Remarks
ACT		Off	Currently not in use
FAIL	Indicates the fault condition on the board	Off	Normal state
		Red	Fault condition is detected
Port Activity	Indicates the activity status for each of the 24 available Ethernet Ports. See Section 'ES-2 Physical Slots to Ethernet Port Mapping' below to determine where the specific Ethernet Port is connected.	Green	Port is connected
		Off	Port is disconnected
		Flashing Green	Activity on port (transmit or receive)
Port Speed	Indicates speed for each of the 24 available Ethernet Ports.	Yellow	Port operates at 1000 Mbps speed
		Off	Port operates at 10 or 100 Mbps speed
PWR	Power status	Off	Power is not supplied to the board
		Green	Power is received (normal operation)
HOT SWAP	Indicates board readiness for extraction from the chassis	Off	Normal state
		Blue	Board is ready for extraction (latches are open)

13.2.3 ES-2 Physical Slots to Ethernet Port Mapping

Use the following table to determine which Mediant 8000 physical slot is connected to the specific ethernet switch port.

Table 13-5: ES-2 Physical Front Slots to Ethernet Port Mapping

Chassis Slot Number	Slot 9 Ethernet Switch Port	Slot 19 Ethernet Switch Port	Dedicated to Board Type
1	13	13	SC
2	14	14	SC
3	-	-	N/A
4	15	15	Redundant TP-8410
5	-	-	N/A
6	-	-	N/A
7	16	16	TP-6310 or TP-8410
8	17	17	TP-6310
9	-	11,12	Ethernet Switch
10	-	-	N/A
11	18	18	TP-6310 or TP-8410
12	19	19	TP-6310 or TP-8410
13	20	20	TP-6310 or TP-8410
14	21	21	TP-6310 or TP-8410
15	22	22	TP-6310 or TP-8410
16	23	23	TP-6310
17	24	24	Redundant TP-6310
18	-	-	N/A
19	11,12	-	Ethernet Switch

Use the following table to determine which Mediant 8000 physical rear slot is connected to the specific ethernet switch port according to the specific interface type.

Table 13-6: ES-2 Physical Rear Slots to Ethernet Port Mapping

Interface Separation	1	2	3	4	5	6	7	8	9	10
ONE_O_C_M	OCM	OCM	OCM							Mirror
TWO_O_CAND_M	OC		M	M	M					Mirror
TWO_OAND_C_M	O		CM	CM	CM					Mirror
THREE_OAND_CAND_M	O	C	M	M	M					Mirror
TWO_O_LAN_AND_WAN	OLAN	OLAN			WAN					Mirror
THREE_OAND_LAN_AND_WAN	O	LAN	LAN		WAN					Mirror

13.2.4 ES-2 RTM Rear Transition Module

The ES-2/RTM (Rear Transition Module) is inserted in the rear Mediant 8000 chassis slots behind the corresponding ES-2 Ethernet Switch boards. It provides 10/100/1000Base-T ports that are used for connecting the Mediant 8000 chassis to the external Ethernet equipment.

Figure 13-4: ES-2 RTM

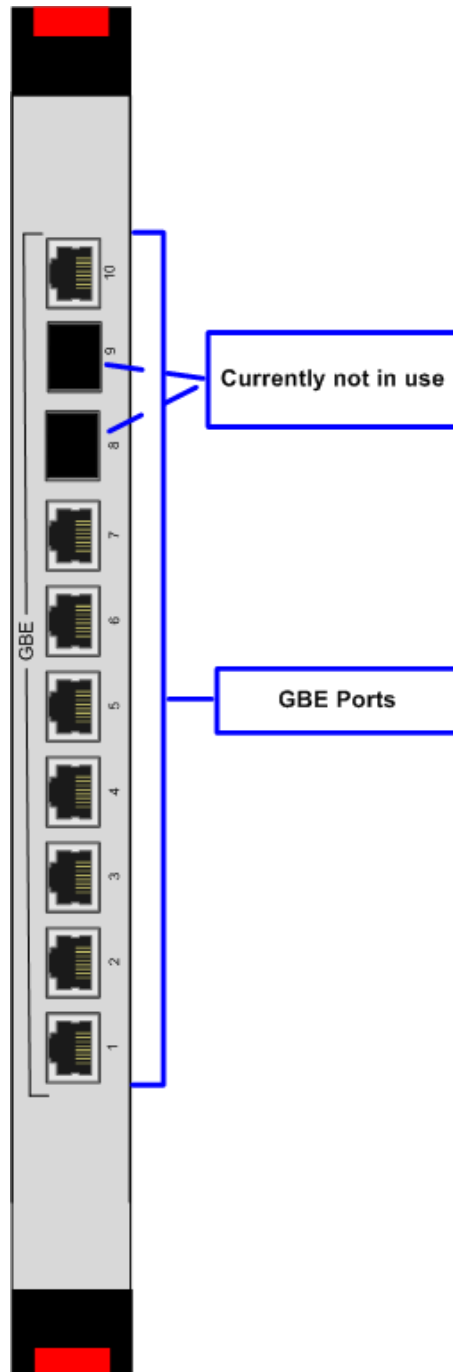


Table 13-7: ES-2/RTM Port Pin Outs

Pin Number	Signal Name
1	TRDB+
2	TRDB-
3	TRDA+
4	TRDD+
5	TRDD-
6	TRDA-
7	TRDC+
8	TRDC-

The following table shows the ES-2 RS-232 Terminal PIN layout.

Table 13-8: ES-2 RS-232 Pin Layout

Pin Number	Signal Name
1	8
2	6
3	2
4	5
5	5
6	3
7	4
8	7

14 Board Assembly Order

For a system configuration with less than the full complement of Media Gateway boards, the board assembly should follow the tables below.



Note : The Redundant Media Gateway board must be accompanied with a redundant RTM module.

Table 14-1: Board Assembly Order

Slot #	Front Board	Rear Board
Slot 1	SC	SA/RTM
Slot 2	SC	SA/RTM
Slot 3	Blank Panel	Blank Panel
Slot 4	TP-8410 Redundant board	8410/RTM/Redundant
Slot 5	Blank Panel	Blank Panel
Slot 6	Blank Panel	Blank Panel
Slot 7	TP-6310 #8 or TP-8410 #6	6310/RTM or 8410/RTM
Slot 8	TP-6310 #7	6310/RTM
Slot 9	ES/6600 or ES-2	ES/6600/RTM or ES-2/RTM
Slot 10	Blank Panel	Blank Panel
Slot 11	TP-6310 #6 or TP-8410 #5	6310/RTM or 8410/RTM
Slot 12	TP-6310 #5 or TP-8410 #4	6310/RTM or 8410/RTM
Slot 13	TP-6310 #4 or TP-8410 #3	6310/RTM or 8410/RTM
Slot 14	TP-6310 #3 or TP-8410 #2	6310/RTM or 8410/RTM
Slot 15	TP-6310 #2 or TP-8410 #1	6310/RTM or 8410/RTM
Slot 16	TP-6310 #1	6310/RTM
Slot 17	TP-6310 Redundant board	6310/RTM/Redundant
Slot 18	Blank Panel	Blank Panel
Slot 19	ES/6600 or ES-2	ES/6600/RTM or ES-2/RTM



Caution

For continuous compliance with EMS standards, unoccupied slots should be covered with either blank covers with air baffles or blank covers.

This page is intentionally left blank.

Part II

Getting Started

This part describes how to prepare your site and perform basic connectivity and configuration of the Mediant 8000.

Take the following steps to install the new Mediant 8000 in your operational environment (lab or deployment site):

- Prepare your site for the Mediant 8000 installation. For more information, see Section 'Site Preparation' on page [91](#).
- Install the Mediant 8000 hardware (mount chassis on a rack and power it up). For more information, see Section 'Hardware Installation' on page [98](#) and 'Powering Up' on page [103](#).
- Connect to the Mediant 8000 Command Line Interface. For more information, see Section 'Command Line Interface' on page [107](#).
- Connect the Mediant 8000 to the IP network. For more information, see Section 'Connecting to IP Network' on page [116](#).
- Connect the Mediant 8000 to the PSTN network. For more information, see Section 'Connecting to the PSTN Network' on page [122](#).
- Install the Mediant 8000 software and perform basic configuration. Establish connectivity with the Element Management System (EMS) for advanced configuration and the Media Gateway maintenance. For more information, see Section 'Software Installation and Configuration' on page [128](#).

Via EMS, complete configuration of the Mediant 8000 and load to service all its components (including Media Gateway boards). For more information, see Section 'Advanced Configuration' on page [154](#).

15 Site Preparation

Take the following steps to prepare your site for Mediant 8000 installation:

- Prepare all needed equipment and cables
- Verify that your site satisfies the Mediant 8000 electrical and environmental requirements
- Prepare IP connectivity on site and allocate IP addresses to be assigned to the Mediant 8000 components
- Prepare PSTN connectivity on site
- Install EMS server and client

15.1 Equipment Requirements

The following equipment must be available on site for the proper installation of the Mediant 8000.

Table 15-1: Equipment Requirements

Item	Requirement
Telco Rack	The Mediant 8000 chassis must be installed in a 19 inch Telco Rack. Space requirements, as per GR-63-CORE, are: ■ Maintenance access: 762 mm (2' 6") ■ Wiring access: 610 mm (2')
Screws and washers	Appropriate for installing the Mediant 8000 chassis in a rack.
Wrist strap and banana plug or alligator clip	For electrostatic discharge (ESD) connection, while installing the Mediant 8000.
Earthing lugs and screws	Appropriate for Mediant 8000 earthing.
Two Ethernet Switches	Two Layer 2 or Layer 3 Ethernet Switches are required for connecting the Mediant 8000 to the IP network. See 'Connecting to the IP Network' on page 116 for additional details.
EMS Server and Client	AudioCodes EMS (Element Management System) is required for the configuration and management of the Mediant 8000.
RS-232 Terminal Console	A PC with RS-232 COM port or a dedicated RS-232 Terminal Console is required for initial Mediant 8000 software configuration.

15.2 Cables

The following cables are required for proper Mediant 8000 installation.



Note : Some of the cables described in this section are not supplied with the system and should be provided by the customer.

Table 15-2: Cabling Requirement

Item	Requirement
Power Cables	8 AWG or lower DC power cables are needed to power the Mediant 8000.
Earthing Cables	4 AWG or better copper cables are required for earthing Mediant 8000. Earthing cable length must not exceed 3 feet (1 meter).
RS-232 Cables	RS-232 cables are used for connecting to the RS-232 Console Terminal on SC boards and starting up Media Gateway software. Mediant 8000 is supplied with a standard RS-232 cable. However ensure that your Terminal Console (or PC) has a matching RS-232 port.
Ethernet Cables	CAT 5 Gigabit Ethernet copper cables are required for connecting the Mediant 8000 to the IP network. At least two CAT 5 cables are required - one for each Ethernet Switch board. More cables are needed if interface separation is implemented .
PSTN Cables	Depending on the supplied configuration, one of the following cables are required for connecting Mediant 8000 to the PSTN equipment: STM-1/OC-3 cables (for TP-6310): Twin fiber optic cables with Dual-LC optical connectors are used for connecting each STM-1/OC-3 interface on TP-6310 board with PSTN equipment. These cables should be as specified in GR-253-CORE. Length is determined by the customer. Small Factor Optical transceivers (SFP) modules are supplied with Mediant 8000. T3 cables (for TP-6310 boards): T3 cables are used for connecting each T3 interface on the TP-6310 board with PSTN equipment. T3 cables must use an unshielded mini-SMB female connector MOLEX PN: 73396-0010 (or equivalent) on one side; and male connector MOLEX PN: 73100-0255 (or equivalent) on the other side.

Item	Requirement
	E1/T1 cables (for TP-8410 boards): E1/T1 cables are used for connecting each E1/T1 trunk interface on the TP-8410 board with the PSTN equipment. Shielded cables are required for NEBS GR-1088-CORE compliance. For a detailed specification of E1/T1 cables see 'Connecting the E1/T1 PSTN Cables (TP-8410 Boards)' on page 58.

15.2.1 E1/T1 Cables for TP-8410

If you use the Mediant 8000 with TP-8410 boards, provide two cables for connecting E1/T1 trunks to each TP-8410 board – one with the 100-pin SCSI connector and another with the 68-pin SCSI connector.



Note : E1/T1 cables are not supplied with the system and should be provided by customer.

The cables should match the following requirements:

- **Cable:** 26 AWG (100 to 120 Ohm) cable.
- **Connector:** see 'TP-8410/RTM E1/T1 Trunk Connectors' on page 58

Table 15-3: Recommended E1/T1 Cable Parts for TP-8410 Board

Part	Description	No. of Pins	Part #	Supplier
Male Connector	1.27 mm Cable Plug	68	R-ZI-013068	All Best Electronics Co Ltd.
		100	R-ZI-013100	
Cable Hood or Shroud	0.050 Series Backshell	68	R-ZC-013068-S3	
		100	R-ZC-013100-S	

15.3 Electrical Requirements

The site must satisfy the following electrical requirements for the proper Mediant 8000 installation.

Table 15-4: Electrical Requirement

Item	Requirement
Power Feeding	In order to maintain the full HA capabilities of the system, a centralized DC power system must be used as specified in UL60950-1, CAN/CSA-C22.2 NO 60950-1-03 Annex NAB.
Outlets	DC outlets are required for connecting the Mediant 8000. For more information, see 'Power System' on page 41.
Circuit breaker	To meet the system power HA scheme, the system should not be current limited to less than 60A. If a circuit breaker is used, it must be 60A or higher rated.
Power consumption	A fully occupied Mediant 8000 chassis in a TP-6310 (8+1) DC power configuration has the following average power consumption: - TP-6310 1494 watts at 48 VDC A fully occupied Mediant 8000 chassis in a TP-8410 (5+1) DC power configuration has the following average power consumption: - TP-8410 1200 watts at 48 VDC

15.4 Environmental Requirements

The site must satisfy the following environment requirements:

The Mediant 8000 complies with the requirements of GR-63-CORE Issue 1 for network switching systems (NEBS) standard . The system operation is guaranteed under the following conditions.

Table 15-5: NEBS Requirement

Item	Requirement	GR-63 Reference
Temperature Range for Operation	0° C to +40° C / 32° F to 104°F	4.1.2
Thermal Shock	-40° C to +25° C / -158° F to 77° F within 5 minutes	4.1.1.1 4.1.1.2
Normal Range Humidity	5 to 90%	4.1.2
Nominal Relative Humidity	70% (wet bulb)	4.1.2
Altitude	-60 to 3048 m (10,000 ft)	4.1.3
Fire Resistance		4.2.3
Drop Test, Packaged	Drop height: 600 mm	4.3.1 (10-25 kg, one person carrying)
Drop Test, Unpackaged	Drop height: 75 mm	4.3.2 (10-25 kg, one person carrying)
Earthquake	Zone 4	4.4.1
Office Vibration	5-100-5 Hz/0.1g, 0.1 oct/minute; 3 axes	4.4.3
Transportation Vibration	5-100 Hz, 0.1 oct/min; 100-500 Hz, 0.25 oct/min	4.4.4
Airborne Contaminants		4.5
Rack Requirements	Telco 19-Inch	
	Space	As per GR-63-CORE Maintenance access 762 mm (2' 6") Wiring access 610 mm (2')

15.5 Preparing the IP Network Connectivity

The Mediant 8000 must be connected to the IP network for proper operation.

The Mediant 8000 may operate in different IP network topologies, including networks with multiple VLANs and subnets. For more information, see Section 'Connecting the Media Gateway to the IP Network' on page [178](#) and 'Appendix : Examples of IP Network Connectivity Configuration' on page [877](#).

Verify the configuration of the IP network available on the site and ensure the following:

- Two fully-redundant Layer 3 Ethernet Switches or Routers are available (to be connected to the two ES boards).
- 1GB Ethernet interfaces are used
- Switches are interconnected by at least 1Gb Ethernet interface (when interface separation is configured and media traffic is aggregated, 3Gb interconnection may be required).

15.6 Allocating IP Addresses

Consult with the Network Administrator and allocate the proper IP addresses for all Mediant 8000 components according to the table 'Allocating IP Addresses' below. Ensure that you know the Subnet Mask and Default Gateway for each subnet that will be connected to the Mediant 8000.

Table 15-6: Allocating IP Addresses

Address	Amount	Description
IP Addresses for SC boards	2	Each SC board must be assigned with a unique IP address, that is used for connecting to it's Command Line Interface (CLI) and performing maintenance tasks.
Global IP Address for SC boards	1	A Global SC address is assigned to the Active SC board and used by EMS (or any other management server) for connecting to the Mediant 8000 management interface. The same Global SC address is used to connect to the second SC board when activity switchover is performed.
IP Addresses for Media Gateway boards	According to the number of Media Gateway boards.	Each Media Gateway board must be assigned with a unique IP address that is used for communication with external VoP equipment (other Media Gateways, Call Agents, Proxy Servers etc). Depending on the network configuration, separate IP addresses may be assigned for Management (OAM), Call Control and Media subnets. For more information, see Section 'Connecting the Media Gateway to the IP Network' on page 178 .

15.7 Preparing the PSTN Network Connectivity

Prepare the PSTN Network connections that will be used for connecting the Mediant 8000 Gateway to the other PSTN equipment. The PSTN network connection type depends on the type of the Media Gateway boards installed in the Mediant 8000 Gateway:

- TP-6310 STM-1/OC-3 fiber links or T3 trunks
- TP-8410-E1/T1 trunks

15.7.1 Preparing the STM-1/OC-3 PSTN Connections

For STM-1/OC-3 PSTN connections, perform the following checks:

1. Check that the STM-1/OC3 interface bit-rate is 155Mbps.
2. Verify that the provided link is behind the Add-Drop Multiplexer (ADM). The STM-1/OC-3 interfaces on Mediant 8000 are designed to support point-to-point topology only. They cannot be part of the SONET/SDH ring.
3. Verify that provided STM-1/OC-3 links have the following multiplexing hierarchy:
 - VC12 for SDH
 - VT1.5 for SONET
4. Investigate APS (Automatic Protection Switching) capabilities of the connected STM-1/OC-3 PSTN equipment.
5. Investigate the clock synchronization plan of the site.

15.7.2 Preparing the T3 PSTN Connections

For T3 PSTN connections, perform the following checks:

1. Verify the framing method of the provided T3 trunks.
2. Investigate the clock synchronization plan of the site.

15.7.3 Preparing the E1/T1 PSTN Connections

For E1/T1 connections, perform the following checks:

1. Verify the framing method of provided E1/T1 trunks.
2. Investigate the clock synchronization plan of the site.

15.8 Installing the EMS Server and Client

AudioCodes Element Management System (EMS) is used for performing configuration and management tasks on the Mediant 8000. The EMS consists of two components – the EMS server and the EMS client – that must be installed on the site prior to installing the Mediant 8000 system.

See the “EMS Installation and Operation Manual” for detailed instructions.

16 Hardware Installation

Take the following steps to install the Mediant 8000 hardware on the site:

- Unpack the Mediant 8000 package and verify its content
- Mount the Mediant 8000 chassis on a rack
- Earth the Mediant 8000 (connect earthing contacts to the ground)
- Connect the Mediant 8000 to power sources and power it up

16.1 Unpacking/Checking Contents

The Mediant 8000 (configured and populated as per the customer's order) is shipped in a heavy-duty wooden crate. Two technicians are required to lift the chassis from its wooden crate.



Note : Detailed instructions for unpacking the chassis are provided in the document "UnPacking Instructions" which is attached to the side of the chassis's wooden crate along with the Packaging List.

16.2 Mounting the Chassis on a Rack

The Mediant 8000 is provided with mounting flanges on either side of the front of the chassis, appropriate for standard 19-inch racks.



Rack Mount Safety Instructions (UL)

Note: When mounting the chassis on a rack, be sure to implement the following Safety instructions:

- **Elevated Operating Ambient** - If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (Tma) specified by the manufacturer.
- **Maintain Air Flow** - Installation of the equipment in a rack should be such that the amount of air flow required for safe operation on the equipment is not compromised.
- **Mechanical Loading** - Mounting of the equipment in the rack should be such that a hazardous condition is not caused due to uneven mechanical loading.
- **Circuit Overloading** - Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.
- **Reliable Earthing** - Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g., use of power strips.)

➤ To mount the chassis on a 19-inch rack:

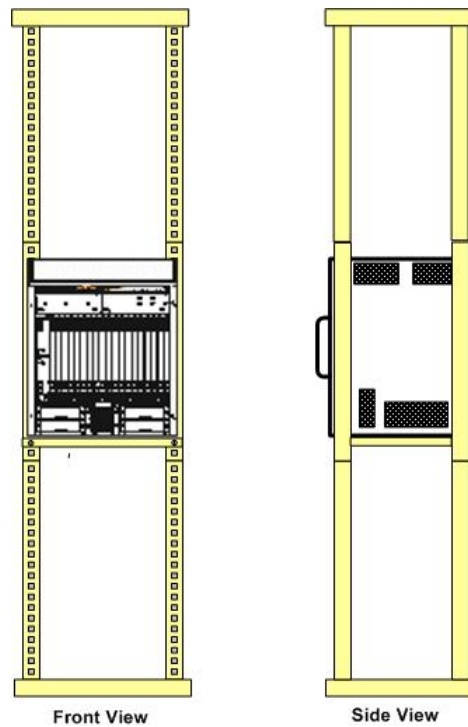
1. Grasp the handles on either side of the chassis as well as on the base of the chassis (this requires two people, one on each side of the carton, grasping the handle and base on that side). Lift it and fit it onto the rack.

2. While the two people are holding the chassis in place; a third person fastens the chassis to the rack rails using eight screws (not provided), four on each side of the chassis or as appropriate for your rack type. See the figure below.

Figure 16-1: Attaching the Chassis to the Rack



Figure 16-2: Chassis on the Rack - Front and Side Views



16.3 Earthing the Chassis

The Mediant 8000 chassis must be earthed to a stable local earth reference. Both of the chassis earth terminals (located on PEM modules) should be connected through a separate earth wire (4 AWG or better) to the rack's earthing. The earth connection's resistance must not be greater than 0.1 ohm.

Earthing lugs and screws are supplied with the chassis.

➤ To earth the chassis:

- Locate two pairs of the earthing connectors on the PEM modules on the rear of the chassis.
- To each pair of the earthing connectors (on each PEM), connect a two-hole crimp terminal tongue (supplied with the Mediant 8000) attached to earthing wire using 4 AWG copper wire. An example of an appropriate lug is a Molex heavy duty terminal connector #19221-0169.



Earthing: The Mediant 8000 chassis must be earthed to a stable local earth reference.

16.4 Lightning Protection

In addition to correct earthing, sufficient lightning protection must be included at the site in order to prevent damage to the equipment. Damage to the equipment can result either from a direct strike of lightning or from propagated high voltage surges.

In order to avoid damage caused by lightning surges, installation of equipment should be compatible with Class 3 classification as defined by EN61000-4-5 Annex B, which specifies that the surge level may not exceed 2kV.

16.5 Powering Up

After mounting the chassis and connecting it to the earth, the Mediant 8000 is ready to power up.



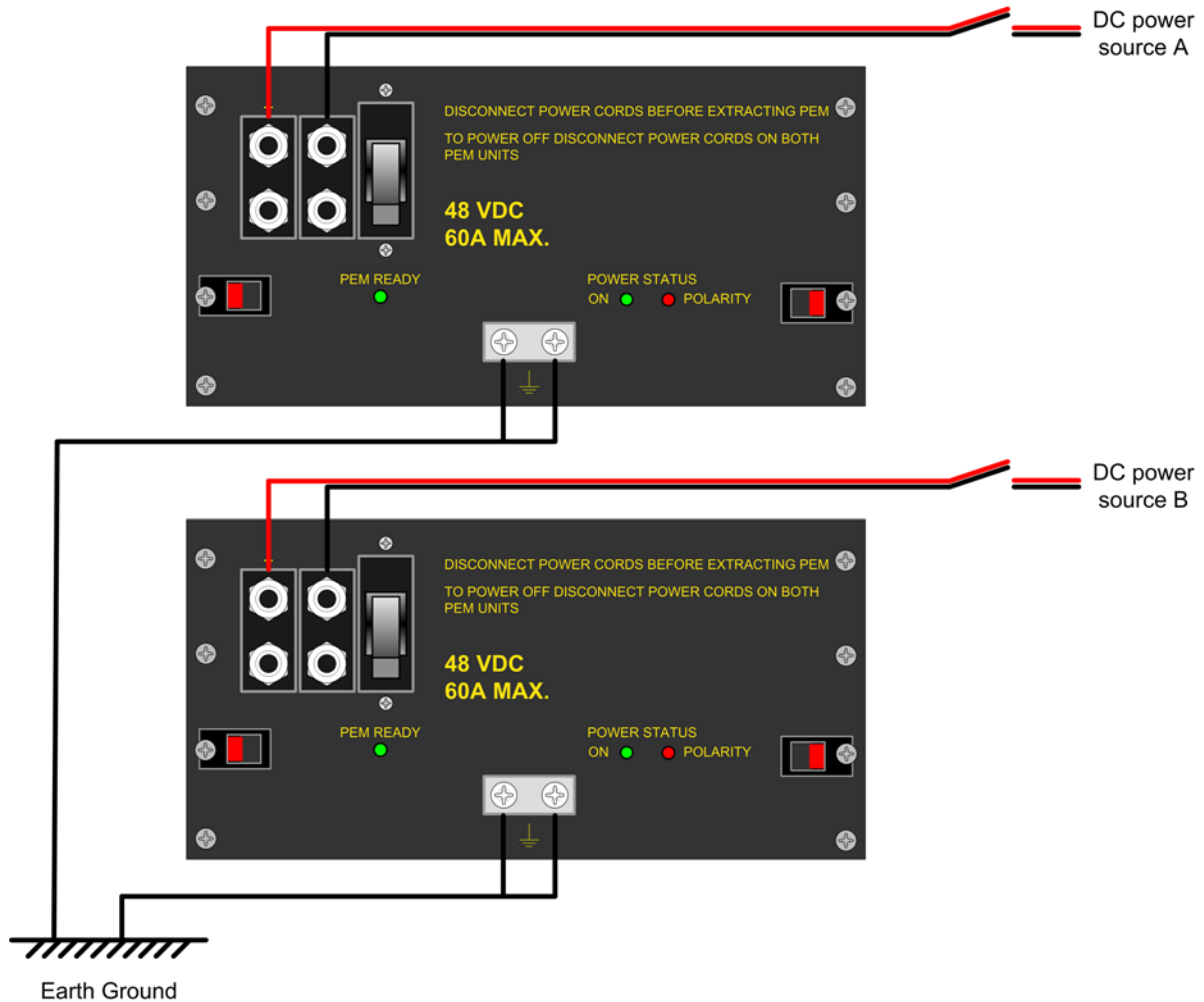
Note: Prior to connecting the Mediant 8000 to the power supply, verify the following:

- The Chassis is properly earthed (ensure that the earthing lugs are present and connections on both ends of the cable are tight).
- All front and rear slots are occupied (either by board or by an appropriate blank panel).

16.5.1 Connecting the Mediant 8000 to the DC Power Supply

Two PEM/DC/8K units reside at the bottom-rear of the chassis (see the figure above) and provide redundant power input terminal blocks for DC. Each terminal block must be connected to a separate power source to guarantee redundancy of the power main supply.

Figure 16-3: Connecting the Mediant 8000 to a DC Power Supply



Note: Ensure that the power connections are according to the indicated polarity.

➤ **To connect the DC power to the terminals:**

1. Verify that the circuit breakers for the DC power are set to the off (O) position.
2. Remove the clear protective covers from the terminal blocks.
3. Use two insulated crimp terminal tongues for ¼" stud size for making the connections to the terminal block (supplied with the Mediant 8000). Prepare the two connections using 8 AWG stranded wiring (for more information, see) and mount them in place paying attention to the polarity.
4. Secure the PEM plastic cover spacers (Hex) as illustrated in the figure below.

Figure 16-4: Securing the PEM Plastic Cover Spacers (Hex)



5. Align the holes of the PEM protective plastic cover with the secured Hex spacers and fasten the screws as illustrated in the figure below.

Figure 16-5: Secure the PEM Plastic Cover Screws



Note: The plastic covers, spacers and screws are required to fasten the plastic covers are provided in the Mediant 8000 Accessory kit.

16.5.2 Initial Power On

➤ To power on, take this step:

- Turn on the DC power input by energizing both circuit breakers (set to I). (One is enough to power-up the chassis).

Table 16-1: PEM LED

	Functional Unit	Indicator	Indicator Status	Description
PEM	PEM Ready		Green	The PEM is correctly receiving power from the backplane
	Power Status	In	Green	Indicates correct connection polarity to the PEM.
		Polarity	Red	Normally OFF Is lit if the connection wires are reversed causing incorrect connection polarity.

This page is intentionally left blank.

17 The Command Line Interface (CLI)

The Mediant 8000 Command Line Interface is used for the following tasks:

- Software installation and basic configuration
- Software backup and restore
- Advanced Mediant 8000 configuration and maintenance (refer to the 'CLI User Manual' LTRT-892XX for more information)

The Command Line Interface (CLI) is provided by each SC board. You may connect to the CLI using one of the following methods:

- Connect to the RS-232 serial console of the SC board
- Connect to the SC board via the IP network (using SSH or Telnet protocols)

For most configuration and maintenance tasks, you should connect to the CLI interface on the Active SC board. However, for installation and basic configuration of the Mediant 8000 you will have to establish connection with the CLI interface on both SC boards.

17.1 Connecting to the CLI via an RS-232 Serial Console

Connection to the CLI via RS-232 serial console is typically needed when IP connectivity with the Mediant 8000 is not available (e.g. during initial installation).

A regular PC with a serial COM port and terminal client software may be used to connect to the CLI via RS-232. For example, the following software clients may be used:

- HyperTerminal (available in default Windows install under Accessories -> Communications programs menu folder)
- PuTTY (<http://www.putty.nl>)
- TeraTerm Pro v4.x (<http://sourceforge.jp/projects/ttssh2>)

Starting from v5.8, the PuTTY application is provided on the "Mediant 5000/Mediant 8000 System Software Installation" CD included in the accessory kit accompanying the Mediant 8000 (in **Utilities\PuTTY** folder).

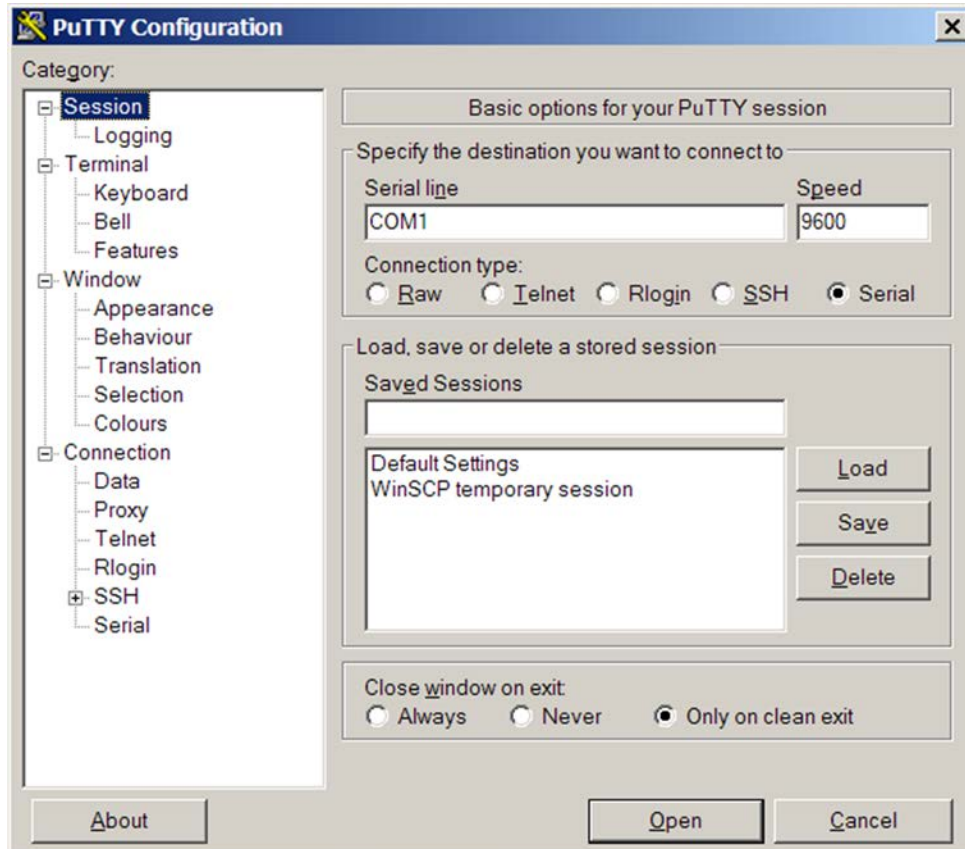
You may also use a dedicated RS-232 Console Terminal (or Terminal Server) to complete this task.

The Console Terminal must be connected to either the SC board's RS-232 serial port or the RS-232 serial port on the SA/RTM. See the 'SC Rev.2 Board (Linux OS)' on page 66 and 'Synchronization and Alarm Rear Transition Module' on page 69 for a detailed description of these connectors.

➤ **To connect to the CLI via an RS-232 serial console:**

1. Connect the PC or RS-232 Console Terminal via the appropriate RS-232 cable to either the SC's RS-232 serial port or the serial port on the SA/RTM.
2. If you are using a PC, run the terminal client software and choose the serial port where the RS-232 cable is connected.

Figure 17-1: Using PuTTY for RS-232 Serial Connections

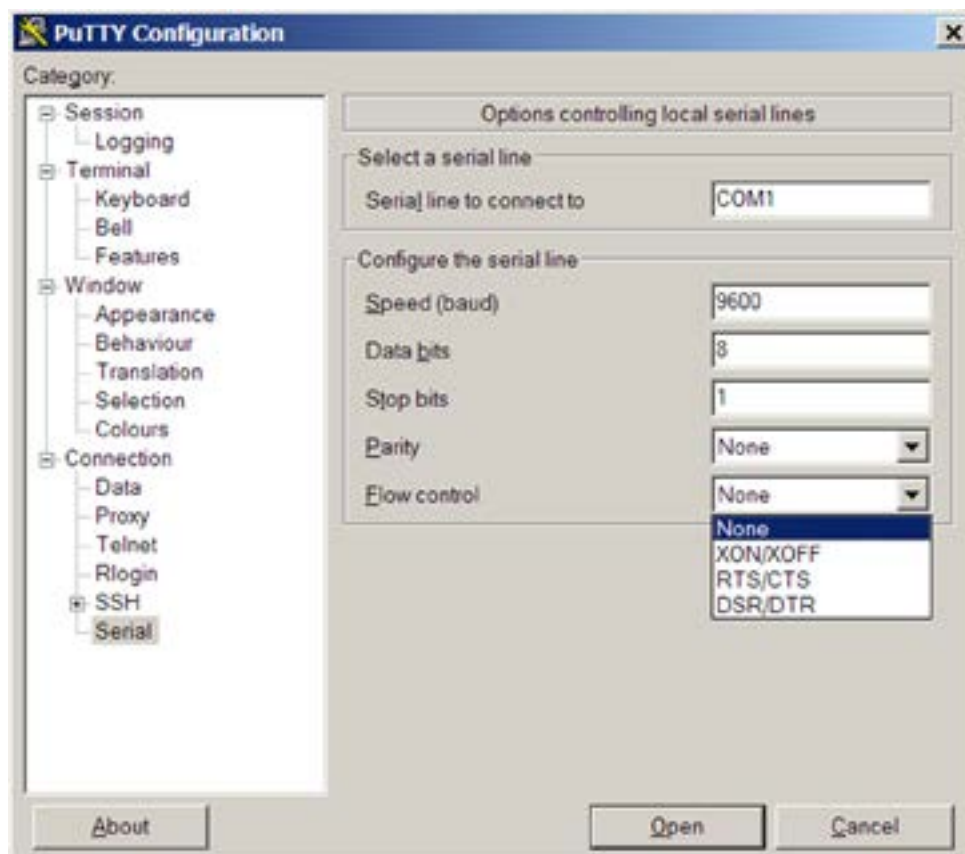


3. Configure the serial connection properties as follows:

Table 17-1: RS-232 Serial Connection Properties

Property	Value
Bits per second	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	None

Figure 17-2: PuTTY RS-232 Serial Connection Settings



17.2 Connecting to the CLI via the IP Internet Network

When IP connectivity with the Mediant 8000 is available, use Secure Shell (SSH) or Telnet client to connect to the Mediant 8000 CLI interface.

If you wish to connect to the CLI interface on the Active SC board, establish connection with the Global IP address on the SC board (this floating IP address is automatically assigned to the Active SC board and is moved to another SC board when activity switchover is performed). If you wish to connect to the CLI interface on a specific SC board, use the corresponding SC board's private IP address.

17.2.1 Connecting to the CLI via Secure Shell (SSH)

The SSH software is not available on Windows-based PC by default. Install the standards-compliant SSHv2 client to connect to the SC board's CLI interface via SSH protocol, for example:

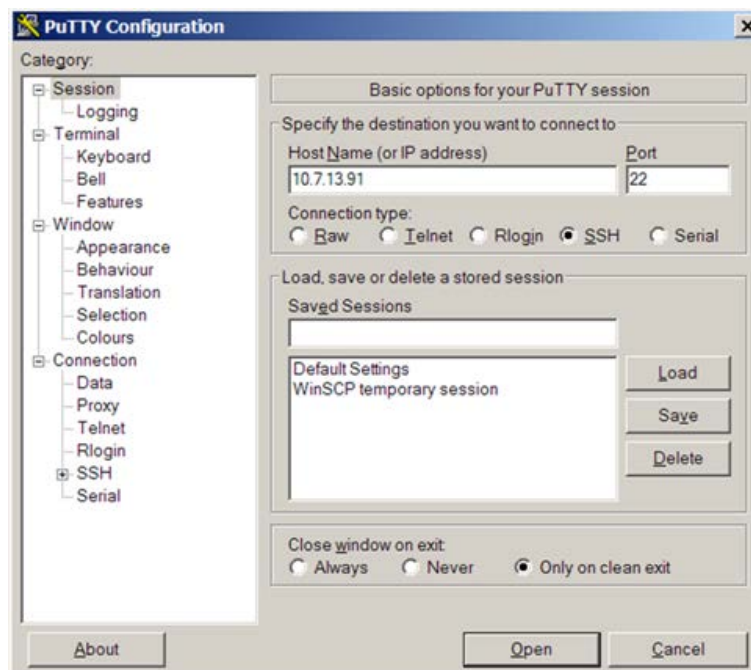
- PuTTY (<http://www.putty.nl>)
- TeraTerm Pro v4.x (<http://sourceforge.jp/projects/ttssh2>)

Starting from v5.8, the PuTTY application is provided on the "Mediant 5000/Mediant 8000 System Software Installation" CD included in the accessory kit accompanying the Mediant 8000 (in **Utilities\PuTTY** folder).

➤ To connect to the CLI via SSH protocol using PuTTY:

1. Start PuTTY. The PuTTY Configuration dialog appears.

Figure 17-3: Using PuTTY for SSH connection



2. In the **Host Name** (or **IP address**) field, type the IP address of the specific SC board.
3. In the **Protocol** field choose **SSH**.
4. Click the **Open** button. An SSH session is opened.

17.3 Command Line Interface Users

Each SC board typically has several CLI users defined on it. These users may be categorized into the following types (groups):

- **Root** – **root** is a super-user that has unrestricted permissions on the SC board and should be used for installation, restore from backup and user management tasks only; there is only one **root** user available on the CLI interface; the **root** user may not be deleted; however, its password may be modified.
- **CLI administrators** – this group of users should be used for performing regular Mediant 8000 maintenance and configuration tasks; the **root** user may add new users to this group or remove existing ones.
- **CLI monitors** – this group of users should be used for performing status and fault monitoring tasks only; configuration tasks are not allowed for users belonging to the CLI monitor group; the **root** user may add new users to this group or remove existing ones.
- **EMS user** – **ems** is a reserved username used by EMS to perform maintenance tasks on Mediant 8000 (e.g. Online Software Upgrade); the **ems** user has permissions identical to the CLI administrators group.



Note: In the following discussion, the term “regular CLI users” is used to refer to any user belonging to the “CLI administrators” or “CLI monitors” group.

By default, the following CLI users are available:

Table 17-2: Command Line Interface Users

Command Line Interface Users	Default Password	Type	Description
root	root	Superuser	root user is a superuser who has unrestricted permissions on the SC board. Use it to perform OS configuration tasks and Mediant 8000 software installation. Note: Some commands, available to root user, may cause serious damage to the SC board's software, therefore use this user only where appropriate and with a great caution.
acladmin	pass_1234	CLI administrator	acladmin is a default CLI user created during the Mediant 8000 installation. Use it to perform most maintenance and configuration tasks. Note, however, that the acladmin is a regular CLI administrator user and therefore may be deleted and other CLI users may be created instead of it. Refer to 'Administering Command Line Interface Users' on page 361
ems	N/A	EMS User	The ems user is used by the Element Management System (EMS) to perform maintenance tasks on the Mediant 8000 (e.g. to perform Online Software Upgrade). It has permissions equivalent to the CLI administrator user. It is strongly recommended not to remove the ems user from the SC board's CLI, otherwise some maintenance tasks that are performed via EMS may be unavailable.

Additional CLI users may exist on the SC board as a result of CLI users' administration and/or synchronization with EMS users. Refer to 'Administering Command Line Interface Users' on page [361](#) for more information.

**Notes:**

- On SC boards with v5.6 or earlier software version pre-installed, the following default CLI user was created instead of acladmin user:
 - Username: **cli**
 - Default password: **cli_12345**
- The above table shows default passwords of CLI users as defined on SC boards on a new Mediant 8000. For security reasons it is strongly recommended to modify passwords for all CLI users (including **root** and **ems** users) prior to field deployment.

17.3.1 Logging into the Command Line Interface

Regular CLI users (except **root** user) may connect to the Command Line Interface by any of the methods described in 'Connecting to the CLI via RS-232 Serial Console' on page 109 and 'Connecting to the CLI via IP Network' on page 111 and provide their username and password when prompted for it.

Note, however, that the following advanced security features may affect the CLI user's ability to log in:

- CLI Interface Access Control – see Section 'CLI Interface Access Control' on page 389 for details.
- Password-less Access to CLI Interface – see Section 'Password-less access to the CLI Interface' on page 390 for details.

17.3.2 Logging in as a Root User

For security reasons, **root** user is not allowed to directly login over a remote network connection. Instead, you can use one of the following options to login as a **root** user to the CLI interface on the SC board:

17.3.2.1 Option 1

Connect to the CLI via an RS-232 serial console (see 'Connecting to the CLI via RS-232 Serial Console' on page 109) and provide **root** username and corresponding password when explicitly asked for it.

17.3.2.2 Option 2

Connect to the CLI via the IP Network ('Connecting to the CLI via IP Network' on page 111). Login as a regular CLI user (e.g. **acladmin** user) and then use **su** (substitute user) command to switch to the **root** user, as follows:

- At the prompt, type **su - root**
- Provide **root** password, when prompted for it.

```
client238::~~# su - root  
Password: *****
```



Note: Do not omit the "dash" from the **su - root** command, otherwise **root** user environment will be improperly set up.

18 Connecting to the IP Network

After powering up the Mediant 8000, you need to connect the Media Gateway to the IP network. Take the following steps to complete this task:

- Prepare two external fully-redundant Layer 3 switches or routers
- Configure Basic IP Network Parameters of SC boards (SC boards are used for performing chassis management and configuration tasks)
- Connect IP network cables

18.1 Preparing the External Layer Switches or Routers

The Mediant 8000 must be connected to two external Layer 3 Switches or Routers that are configured for fully redundant operation via the use of HSRP (Hot Standby Router Protocol) or VRRP (Virtual Router Redundancy Protocol) protocols. See 'Connecting the Mediant 8000 to the IP Network' on page 217 for details.



Note: In a temporary lab environment, it is possible to connect uplinks of both ES boards to the same external Layer 3 Switch or Router. However such a configuration does not provide a redundant IP network connection for the Mediant 8000 and therefore should not be used for live deployments.

For an initial installation of the Mediant 8000 in a customer environment, an IP subnet that doesn't use VLAN tagging is required. This subnet will be used as an OAM subnet during the initial installation and/or basic software configuration. The Mediant 8000, the EMS server and client machines should be connected to this subnet during the initial installation and/or configuration. When the installation and/or configuration has completed and connectivity between the Mediant 8000 and the EMS is properly established, more complex IP network configurations may be provisioned on the Mediant 8000. See 'Connecting the Media Gateway to the IP Network' on page 178 for more details.

If the Mediant 8000 is installed on a site that lacks a proper IP subnet without VLAN tagging, proceed with the rest of this chapter and then perform installation and/or basic configuration, using the RS-232 serial console to connect to the CLI interface. As soon as the Mediant 8000 software is up and running, use the procedures described in 'Recovering the OAM VLAN Settings' on page 842 to configure the VLAN tag for the OAM subnet on the Mediant 8000.

18.2 Configuring the Basic IP Network Parameters of SC Boards

Basic IP Network Parameters must be configured on the SC boards prior to connecting the Mediant 8000 to the external IP network. This configuration allows the basic connectivity between the SC boards and external management equipment (e.g. EMS server).



Note: Failure to perform Basic IP Network Configuration prior to connecting the Mediant 8000 chassis to the external network may result in a disruption of service on other equipment connected to the same IP network, due to possible IP address collision with default/previous configuration of SC boards.



Note: All IP addresses and hostnames in the following examples are for demonstration purposes only and must be designated by the customer according to the network settings.

➤ To configure SC boards' Basic IP Network parameters:

1. Connect to the 1st SC board's CLI interface via RS-232 serial console. For more information, see Section 'Connecting to the CLI via an RS-232 Serial Console' on page 109.
2. Login as user **root** and provide a corresponding password. For more information, see Section 'Logging into the SC CLI as a Root User'.
3. Stop SC software by running the **tools sc dn** command; confirm the operation by typing **y** and pressing **Enter**.

```
client238::~~# tools sc dn
STOP SC SOFTWARE
```

```
Stop SC software? ([y]/n) : y
```

```
>>> Stop watchdog process...
>>> Wait for application to stop...
```

4. At the prompt, type **install** and press **Enter**.
5. Choose option 1.

```

client238::~~# install
Found uncompressed Media Gateway installation package...
Verify installation package integrity...

SC Software Installation & Basic Configuration

1 - Change network configuration.
2 - Install the software.
3 - Change basic configuration.
4 - Copy basic configuration from Active SC.
5 - Uninstall the software.
0 - Quit.
Choose (0-5) : 1

**                                     **
** This option will change IP parameters of      **
** current SC board.                             **
**                                     **

```



Note: On SC boards with v5.6 or earlier software version installed, the **install** command may produce the following error:

usage: install [options] file [dir1 ...]

In this case, type the command **/install.pl** instead.

6. The current network configuration is displayed; type **y** and press **Enter** to change the current network configuration.

```

Current Network Configuration
Hostname      : client33
IP Address    : 10.6.8.33
Subnet Mask   : 255.255.0.0
Default Gateway : 10.6.0.1

Do you wish to change it? (y/n)           [n]: y

```

7. Enter the unique hostname you designate for the SC board. Press **Enter**.

```
Hostname                               [client33]: SC1
```

8. Enter the unique IP address for the SC board and press **Enter**. The provisioned address is an "private IP address" of the SC board that may be used for connecting to it even when the Media Gateway software is not running.

```
IP address                             [10.6.8.33]: 10.7.13.91
```

9. Enter the subnet mask for the SC board and press **Enter**.

```
Subnet Mask                           [255.255.0.0]: 255.255.0.0
```

10. Enter the IP address for the *Default Gateway* and press **Enter**.

```
Default Gateway                       [10.6.0.1]: 10.7.0.1
```

11. To apply the new configuration, type **y** and press **Enter**.

```
According to IP and mask, network is 10.7.0.0.
Start configuring (y/n) ?              [y]: y
>>> Updated /etc/hosts ...
>>> Updated /etc/nodename ...
>>> Updated /etc/defaultrouter ...
>>> Updated /etc/hostname.dmfe0 ...
>>> Updated /etc/netmasks ...
>>> Updated hostname ...

Done
```

12. The SC board must be rebooted to activate the new configuration. To reboot the SC board, type **y** and press **Enter**.

```
SC board must be rebooted to activate the new
network configuration.
```

```
Reboot now? (y/n)                     [y]: y
```

13. If the Media Gateway software is installed on the SC board, you will receive the following additional warning prior to reboot:

```
After reboot completes, re-login to the SC board
(using new network settings), run "install" command
and choose options 3 or 4 to re-configure the Media Gateway software to
match the new network settings.
```

Perform the procedure as described in the above message – i.e. re-login to the SC board after the reboot, run **install** command and choose option **3** or **4** (on SC1 and SC2 correspondingly) to re-configure the Media Gateway software. Failure to complete this procedure will prevent the Media Gateway software from running.



Note: The above procedure ensures that the Media Gateway software configuration fully matches the IP network configuration and must be performed even after a “minor” change to the basic network configuration (e.g. change of SC board’s hostname).

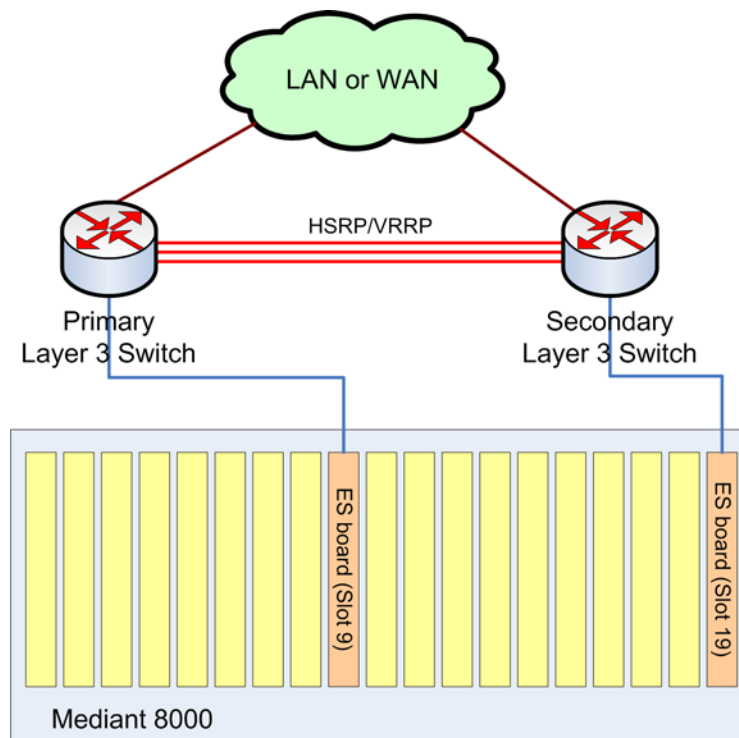
14. Repeat steps 1-13 on the 2nd SC board. Ensure to configure a different hostname and IP address on each SC board.

18.3 Connecting IP Network Cables

IP Network connectors are located on the ES RTM modules in the rear of the Mediant 8000 chassis. See 'ES/6600/RTM Rear Transition Module' on page 78 and 'ES/ACS-38-SINGLE ES (Ethernet Switch) Board' on page 80 for a detailed connectors description.

The Mediant 8000 software by default uses a “single subnet without VLAN tagging” configuration. Therefore two external redundant Layer 3 switches or routers should be connected to port 20 on both the ES RTM modules. Use CAT 5 or better 1Gb Ethernet cables for this connection. Ensure that the CAT 5 cables that you use are threaded according to customers' exterior cable management guides.

Figure 18-1: Connecting the IP Network for an Initial Installation



After you complete the Mediant 8000 software installation and/or basic configuration, see 'Connecting the Media Gateway to the IP Network' on page [178](#) for detailed instructions on how to perform the advanced IP network configuration (e.g. define interface separation and/or VLAN tagging). As part of this advanced configuration, you may be required to re-connect Ethernet cables from the external Layer 3 switchers or routers to different ES board ports. See 'Ethernet ports allocation on ES boards' on page [217](#) for details.

19 Connecting to the PSTN Network

The Mediant 8000 features the following interfaces for connecting to the PSTN network:

- STM-1/OC-3 – provided by TP-6310 boards
- T3 – provided by the TP-6310 boards
- E1/T1-provided by the TP-8410 board

Choose the appropriate interfaces and connect them to the PSTN network as described below. Make sure to perform redundant connection if applicable.



Caution Laser

Mediant 8000 (specifically TP-6310 boards) contain a Class 1 LED/Laser emitting device, as defined by 21CFR 1040 and IEC825.

Do NOT stare directly into the beam as this can damage your eyesight.

19.1 Connecting STM-1/OC-3 PSTN Cables

The following parts are needed to connect the STM-1/OC-3 PSTN cables to the TP-6310 boards on the Mediant 8000:

- 155 Mbps SFP modules (supplied with Mediant 8000)
- Twin single-mode fiber optic cables with Dual-LC plug (must be provided by the customer)

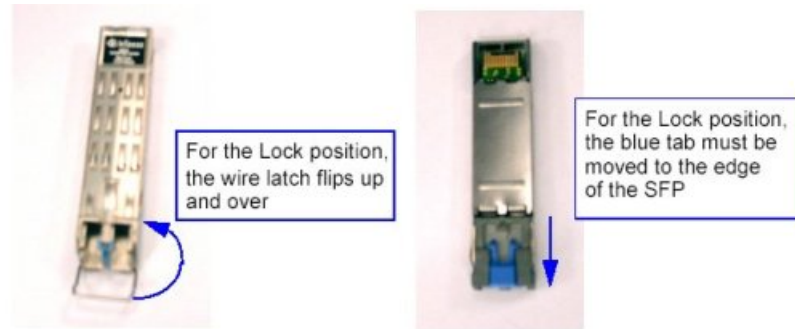
19.1.1 SFP Modules

The SFP modules contain a locking mechanism that ensures that the module can not be inadvertently pulled out of the port socket. There are several types of SFP modules, two of which are displayed in the figure below.



Note: The SFP modules, supplied with the Mediant 8000, are already inserted into the 6310/RTM module. If you remove SFP module from the RTM, be sure to set the SFP module to the Lock position BEFORE inserting it back.

Figure 19-1: SFP Modules and Their Locks



19.1.2 Fiber Optic Cables

Twin single-mode fiber optic cables with Dual-LC plug must be connected to the PSTN transceivers 1A and 1B on the 6310/RTM module in the rear of the chassis. For PSTN interface redundancy, it is recommended to connect two STM-1/OC-3 links to each 6310/RTM module.

Care in Handling Fiber Optic Cabling

When handling the fiber optic cables, be sure to note the following:

- Excessive bending of the Fiber Optic Cable can cause distortion and signal losses
- Ensure you abide by the minimum bending radius recommended by the Fiber Optic Cable supplier
- Maximum Fiber Optic Cable length for multi-mode fiber is 2 km
- Maximum Fiber Optic Cable length for single-mode fiber is 22 km



19.2 Connecting the T3 PSTN Interfaces

T3/DS-3 PSTN cables are connected to the 6310/RTM module in the rear of the chassis. Three T3/DS-3 interfaces are provided on each 6310/RTM module.

Use a proper cable with MOLEX PN: 73100-0255 or the equivalent mini-SMB male connector.

Figure 19-2: T3 - Male Connector MOLEX PN: 73100-0255



19.3 Connecting E1/T1 PSTN Cables (TP-8410 Boards)

E1/T1 PSTN cables are connected to the 8410/RTM module in the rear of the chassis. Two SCSI interfaces are provided on each 6310/RTM module for connecting up to 42 E1/T1 trunks.

Use proper cables for connecting E1/T1 trunks. For more information, refer to Cables on page [92](#).

This page is intentionally left blank.

20 Connecting to External Telco Alarm Equipment

The Mediant 8000 may be connected to the external Telco alarm equipment via a Terminal Block Connector provided on the SA/RTM module.

The alarm outputs are rated for 2A at 30V. A maximum gauge of 20 AWG for standard copper wire may be used.

➤ **To connect the contact relays to Telco alarm equipment:**

1. Open the screws that connect the terminal block to the PCB's connector.
2. Unplug the terminal block.
3. Connect the relays of both SA/RTMs to the Telco alarm equipment either using normal logic or inverse logic:
 - If the equipment has NO (Normally Open) and COM terminals, use normal logic scheme
 - If the equipment has NC (Normally Closed) and COM terminals, use inverse logic scheme

Figure 20-1: Normal Logic External Alarm Equipment Connection

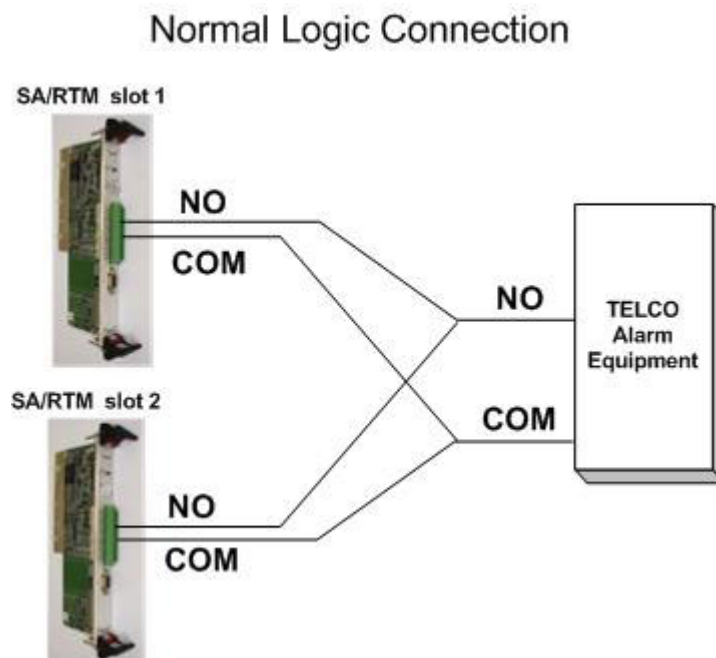
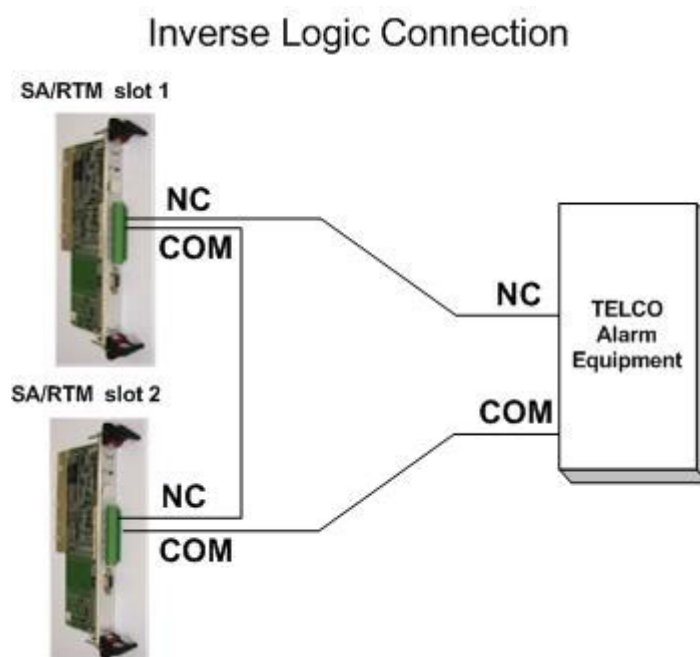


Figure 20-2: Inverse Logic External Alarm Equipment Connection



4. Plug-in the terminal block into the PCB connector.

21 Software Installation and Basic Configuration

This section describes how to install, configure and start up the Mediant 8000 software. To do this, complete the following tasks:

- Install the Mediant 8000 software (this step is typically omitted, because the Mediant 8000 comes with a pre-installed software).
- Perform the basic configuration of the software (the basic configuration is a minimal configuration required for the software to start).
- Start the Mediant 8000 software.
- Configure connectivity with the EMS server.
- Complete configuration of the Mediant 8000 (this additional configuration is typically performed via the EMS and is eventually completed when all Mediant 8000 components, including the Media Gateway boards, are in service).

21.1 Installing the Mediant 8000 Software

The Mediant 8000 software is installed on the SC boards located in Slots 1 and 2. The SC boards are responsible for managing all the Mediant 8000 components – including the Media Gateway and the Ethernet Switch boards – and distributing the proper software and configuration files to them.

The Mediant 8000 is typically supplied with the proper software pre-installed on it. Therefore most customers only need to perform the basic configuration of the Mediant 8000 software and do not need to install it. Nevertheless, sometimes the software version pre-installed on the Mediant 8000 does not match the version required by the customer. In this case, the proper version of the Mediant 8000 software should be installed as described in this chapter.

➤ **To verify the current Mediant 8000 software version installed on the SC board:**

1. Connect to the SC board's CLI interface. For more information, see Section 'The Command Line Interface (CLI)' on page 107.
2. Login as a regular CLI user (e.g. **acladmin**) and provide the corresponding password. For more information, see Section 'Logging into the Command Line Interface' on page 115.
3. At the prompt, type **version** and press **Enter**.

```
client238::~~# version
6.6.15
```

4. Repeat the above procedure on both SC boards. If the software version on both SC boards is correct, proceed to the next chapter 'Performing Basic Configuration of the Mediant 8000 Software' on page 146. Otherwise, install the proper Mediant 8000 software versions as described in this chapter.

21.1.1 The Mediant 8000 Installation Package

The Mediant 8000 software installation package is provided on the “Mediant 5000/Mediant 8000 System Software Installation” CD included in the accessory kit accompanying the Mediant 8000.

The package consists of a single file with a name comprised of the following elements:

- **tg_** prefix
- specific Mediant 8000 software version number
- name of the operating system, that this package is built for (“solaris” or “linux” – for SC boards SC Rev.1 and SC Rev.2 correspondingly)

.install suffix For example:

- **tg_6.6.16_solaris.install** – v6.6.16 installation package for SC Rev.1 boards
- **tg_6.6.32_linux.install** – v6.6.32 installation package for SC Rev.2 boards

The “Mediant 5000/Mediant 8000 System Software Installation” CD also contains additional documentation and software utilities.

The Mediant 8000 software must be installed on both SC boards, located in Slots 1 and 2 correspondingly. The Software installation consists of the following steps:

- Transferring the Mediant 8000 installation package to both SC boards
- Installing the Mediant 8000 software on the SC board to operate as the Active board (in Slot 1)
- Installing the Mediant 8000 software on the SC board to operate as the Standby board (in Slot 2).



Note: Both SC boards installed in the Mediant 8000 chassis must be of the same hardware revision – SC Rev.1 or SC Rev.2 and use the same OS (Solaris or Linux correspondingly). Do not mix SC boards of different hardware revisions in the same chassis. Ensure that you use the correct version of the Mediant 8000 software installation package.

21.1.2 Transferring the Mediant 8000 Installation Package to the SC Boards

Prior to installing the Mediant 8000 software, you must transfer the Mediant 8000 installation file (e.g. **tg_6.6.16_linux.install**) to both SC boards.



Note: When performing the Mediant 8000 software installation or Online Software Upgrade, ensure that you use the correct version of the installation package that matches the hardware revision of the SC boards installed in your chassis.

This may be done via one of the following file transfer protocols:

- SFTP
- SCP
- FTP



Note: File transfer via FTP protocol is allowed only when the Mediant 8000 is configured for non-secure operation mode (see 'Secure Operation Mode' on page 274 for details). However, even when using non-secure mode, it is strongly recommended to use SFTP/SCP protocols instead (due to weak security features of FTP protocol that expose username and passwords in clear-text).

You can use any standard-compliant SFTP/SCP/FTP client software to transfer the Installation Package to SC boards. For example, on Windows-based PC, you may use the following clients:

- PSFTP (<http://www.putty.nl>) – command-line SFTP client
- WinSCP (<http://winscp.net>) – GUI client that supports all available file transfer protocols
- FileZilla (<http://filezilla-project.org>) – GUI client that supports FTP and SFTP protocols

Starting from v5.8, the PSFTP application is provided on the “Mediant 5000/Mediant 8000 System Software Installation” CD included in the accessory kit accompanying the Mediant 8000 (in Utilities\PuTTY folder).

➤ To transfer the installation package to the SC board:

1. Open the SFTP/SCP/FTP client and connect to the private SC IP address.
2. Login as a regular CLI user (e.g. acladmin) and provide the corresponding password when prompted.
3. Transfer the installation package to the SC board. The package will be transferred to the home directory of the logged in CLI user.

Transferring the Installation Package to the SC board via the Command-line SFTP Client

```
Microsoft Windows XP [Version 5.1.2600]
© Copyright 1985-2001 Microsoft Corp.

C:\> psftp acladmin@10.7.13.91
Using username "acladmin"

+-----+
| WARNING: To protect systems from unauthorized use and to ensure
| that the system is functioning properly,
| activities on this system are monitored and recorded and
| subject to audit. Use of this system is expressed consent
| to such monitoring and recording. Any unauthorized access
| or use of this system is prohibited and could be subject
| to criminal and civil penalties.
+-----+

Password: *****
Remote working directory is /data/acladmin
psftp> lcd \Install
New local directory is c:\Install
psftp> put tg_6.6.16_linux.install
local:tg_6.6.16_Linux.install =>
remote:/data/acladmin/tg_6.6.16_linux.install

psftp> bye
```



Note: If you transfer the Installation Package via the FTP protocol, ensure to choose "binary file transfer mode" (command bin in a console FTP client).

21.1.3 Preparing for the Mediant 8000 Software Installation

The Mediant 8000 software must be installed on both SC boards, located in Slots 1 and 2 correspondingly.



Note: Installation of the new Mediant 8000 software version completely erases all the existing Media Gateway configuration (including all IP network configuration, definitions of the Media Gateway boards and the signaling protocols configuration). If you wish to preserve the current Media Gateway configuration, use the Online Software Upgrade feature instead (see the 'Online Software Upgrade' on page [811](#) for more details).

Prior to installing the new software version, ensure that the SC software is stopped on both SC boards by using the following procedure:

➤ **To stop the Mediant 8000 software:**

1. Connect to the 1st SC board's CLI interface. For more information, see Section 'Command Line Interface' on page [107](#).
2. Login as a regular CLI user (e.g. **acladmin**) and provide the corresponding password. For more information, see Section 'Logging into Command Line Interface' on page [115](#).
3. Type **tools sc dn** command to stop the SC software.
4. At the prompt, type **y** and press **Enter**.

```
client238::~~# tools sc dn
STOP SC SOFTWARE
```

```
Stop SC software? ([y]/n) : y
```

```
>>> Stop watchdog process...
>>> Wait for application to stop...
```

5. Repeat steps 1-4 on the 2nd SC board.

After stopping the software on both SC boards, perform installation of the Mediant 8000 software in the following order:

- Install software on the SC board in Slot 1 as described in 'Installing Mediant 8000 Software on the SC Board to Operate as the Active Board' on page [134](#).
- Install software on the SC board in Slot 2 as described in 'Installing Mediant 8000 Software on the SC Board to Operate as the Standby board' on page [140](#).

If you install the SC software on a failed SC board (while another SC board continues to operate normally) refer to procedures described in 'Installing the Mediant 8000 Software on the SC Board to Operate as the Standby Board' on page [140](#).

21.1.4 Installing the Mediant 8000 Software on the SC Board to Operate as the Active board

The following installation instructions are relevant only if you are installing the new version of the Mediant 8000 software on both SC boards and should be performed on the SC board residing in Slot 1.

If you install the Mediant 8000 software on the replacement SC board, while another SC board continues to operate normally, use the procedures described in 'Installing Mediant 8000 Software on the SC Board to Operate as the Standby board' on page 140.

➤ To install the Mediant 8000 software on the SC board to operate as the Active SC board:

1. Connect to the CLI interface on the SC board to operate as the Active board. For more information, see Section 'Command Line Interface' on page 107.
2. Login as **root** user. For more information, see Section 'Logging in as a Root User' on page 115.
3. At the prompt, type **install ~acladmin/tg_6.6.16_linux.install** and press **Enter**. Replace **acladmin** with the name of the CLI user, that you used while transferring the Mediant 8000 package to the SC board. Replace **tg_6.6.16_linux.install** with the actual name of the Mediant 8000 installation package.

```
client241::~~# install ~acladmin/tg_6.6.16_linux.install
```

```
Core Network Media Gateway
```

```
Version : 6.6.16
```

```
WARNING: installation of the new software version will erase
the current Media Gateway configuration.
To upgrade the Media Gateway software to the new version and to retain
the current configuration, run the Online Software Upgrade.
```



Note: On SC boards with version 5.6 or earlier software version installed, the install command may produce the following error:

```
usage: install [options] file [dir1 ...]
```

In this case, use the following commands to start the Mediant 8000 software installation:

```
chmod u+x ~acladmin/tg_6.6.16_linux.install
```

```
~acladmin/tg_6.6.16_linux.install
```

4. When you are prompted if you wish to start the installation, type **y** and press **Enter**. The software installation begins.

```
Start installation? (y/n) : y
Extract /sc_software.tar installation archive... done
Extract /sc_install.pl installation script... done
```

```
Install SC Software
```

```
>>> save snmp.conf in /tmp/snmp.conf.prev ...
>>> save SNMP++ stack configuration in /tmp/snmp.prev ...
(This sequence is abbreviated)
```

5. After the installation successfully completes the extraction of all software binary components, you will be prompted to perform the basic configuration of the SC software.

```
Software is successfully extracted.
```

```
SC board must be configured to complete the installation.
```

```
Choose one of the following configuration options:
```

- a) "configure now" - you will be prompted to perform a new SC configuration
- b) "copy configuration" - an existing SC configuration will be copied from another SC board

```
If you install the Media Gateway software on a failed SC board, choose the "copy configuration" option to copy an existing configuration from another SC board (currently up and running).
```

```
If you install the Media Gateway software on both SC boards, do the following:
```

- a) for the SC board in slot 1, choose the "configure now" option
- b) for the SC board in slot 2, choose the "copy configuration" option

```
How do you want to configure this SC board? (1=configure now/2=copy configuration) [1]: 1
```

6. Since you are installing software on the SC board to operate as the Active board, type **1** and press **Enter** to select "configure now" option.

System Configuration

Keyboard shortcuts:

ENTER - leave the default parameter value as is
 \ - return to the previous parameter
 Ctrl-C - abort the configuration script

7. At the **Global SC IP Address** prompt, type the IP address to be assigned to the Active SC board and used to connect to the Media Gateway's management interface (e.g., from EMS server).

Global SC IP Address [0.0.0.0]: **10.7.13.90**

8. At the **1st SC IP Address** prompt, enter the internal IP address of the SC board in Slot 1.

1st SC IP Address [0.0.0.0]: **10.7.13.91**

9. At the **2nd SC IP Address** prompt, enter the internal IP address of the SC board in Slot 2.

2nd SC IP Address [0.0.0.0]: **10.7.13.92**



Note: Parameters **1st SC IP Address** and **2nd SC IP Address** are used to identify SC boards in Slot 1 and 2 correspondingly and not to change their existing network configuration. Software installation will fail if these parameters do not match the IP addresses currently configured on both SC boards. If you wish to change the private IP address of an SC board, see 'Configuring the Basic IP Network Parameters of SC Boards' on page [117](#)

10. At the **Time Zone** prompt, enter the local time zone where the Media Gateway resides.

The time zone may be specified as an offset from the **Greenwich Mean Time (GMT)** (e.g. **GMT-2** or **GMT+3**) or as a name of a geographical area where the Media Gateway resides (e.g. **Europe/Paris** or **America/Denver**). In the latter case, Daylight Saving Time will be activated if the specific time zone supports it.

Time Zone [GMT]: **Europe/Paris**

The name of the time zone uses standard **UNIX tz/zoneinfo** format. Geographical Locations are identified by continent or ocean and then by the name of the location, which is typically the largest city within the region. For example, **America/New_York** represents most of the US eastern time zone and **America/Phoenix** represents most of Arizona, which uses mountain time without daylight saving time (DST).

For major US and European cities, short time zone name (without continent name) is supported as well – e.g. **Paris instead of Europe/Paris**.

See the 'TimeZone Converter' '<http://www.timezoneconverter.com>' for a complete list of valid time zone names, their DST settings and current time in each time zone. Alternatively, use the following commands on the SC board to view a complete list of supported time zone names:

```
cd /usr/share/lib/zoneinfo
```

```
find . -type f,l -print | grep -v src | cut -b 25-
```

11. At the **Enable Security** prompt, type **1** to enable the Mediant 8000 software to operate in Secure Mode or accept the **0** to leave the Mediant 8000 software in its default mode. For more information, see Section 'Secure Operation Mode' on page 306.

```
Enable Security (0-no, 1-yes) [0]: 0
```



Note: If your system uses the SC Rev.2 boards (with the Linux OS), the "Enable Security" prompt does not appear as the software always operate in a Secure Mode. See 'Secure Operation Mode' on page 306 for details.

12. At the **SC Root Password** prompt, enter the new password for the **root** user or press **Enter** to leave it unchanged. Re-enter the new password when prompted. Use the following rules when specifying a new **root** password:
 - The password must have at least 8 characters.
 - The password must contain at least two alphabetic characters and at least one numeric or special character. In this case, "alphabetic" refers to all upper or lower case letters.
 - The password must differ from the user's login name (**root**) and any reverse or circular shift of that login name.

```
SC Root Password [leave unchanged]: *****
```



Note: For security purposes, it is strongly recommended to change **root** password from its default value. Make a note of the new password you create and keep this record in a secure location for future reference.

13. At the **Product Type** prompt, type the number that corresponds to the system that you are installing and press **Enter**.

```
Product Type (0-Mediant 8000, 2-Mediant 5000, 6-IPmedia 5000, 7-IPmedia 8000) [2]: 0
```

14. After all basic configuration parameters are prompted, a summary of the settings is displayed.

Configuration Summary:	
Global SC IP Address	: 10.7.13.90
1 st SC IP Address	: 10.7.13.91
2 nd SC IP Address	: 10.7.13.92
Time Zone	: Europe/Paris
Enable Security	: 0 (no)
SC Root Password	: *****
Product Type	: 0 (Mediant 8000)

15. You are prompted to start configuring. To commence the configuration, type **y** and press **Enter**.

```
Start configuring ([y]/n) [n]: y
>>> Configure INET services ...
>>> Update /etc/inet/inetd.conf file ...
>>> Restore file /etc/inet/inetd.conf from the backup ...
>>> Update /etc/inet/services file ...
(This sequence is abbreviated)
```

16. After the installation successfully completes the SC software configuration, it will determine whether OS Patches need to be installed on the specific SC board. OS patches installation ensures that the latest operating system's security and stability fixes are applied. It also ensures that the Mediant 8000 software operates in the same well-defined software environment that was used during the software verification and validation process.

When prompted to start the OS patches installation, type **y** and press **Enter**.

```
>>> Install OS patches ...
```

SC software contains new OS patches that must be installed.

Installation of OS patches may take considerable time.
However without these OS patches, SC software may not function properly and/or SC security may be compromised.

```
Install OS patches? (y/n) [y]: y
Applying 112785-65 (1 of 25) ... done
Applying 112837-16 (2 of 25) ...
```

(This sequence is abbreviated)



Note: Installation of the OS patches on the SC Rev.1 board (using the Solaris OS) may take a considerable amount of time – up to 1.5 hours. The exact amount of time depends on which previous Mediant 8000 software version was installed on the specific SC board.

Installation of OS patches on the SC Rev.2 board (using the Linux OS) is considerably shorter and typically takes only a few minutes.

17. After the installation successfully completes, you will be prompted to reboot the SC board.

```
SC board must be rebooted to complete the installation.
```

After the reboot, do the following:

- 1) connect to the Active SC board (via Global IP address)
- 2) run "tools ems" script to configure connectivity between Media Gateway and EMS server
- 3) if VLAN must be configured on the OAM interface, run "tools vlan" script

IMPORTANT: If you install the Media Gateway software on both SC boards, do not reboot the SC board in slot 1 until the installation of the SC board in slot 2 is completed.

```
REBOOT now (y/n)                [y]: y
Are you sure (y/n)              [y]: y
```

If you install the software on both SC boards, do not reboot the SC board to operate as the Active board (that you are currently installing) until you complete the installation of the other SC board (to operate as the Standby board). When both SC boards are ready to be rebooted, reboot them simultaneously by typing **y** and pressing **Enter** on the respective SC board's CLI interfaces.

18. The SC board reboots. It typically takes 2 minutes to complete the reboot. The Media Gateway software starts automatically after the SC board completes the reboot process.
19. After the SC board completes the reboot, re-connect to its CLI interface and login as the regular CLI user that you used to transfer the installation package (e.g. **acladmin**). Type the **rm tg_6.6.16_linux.install** command to remove the Mediant 8000 installation package from the SC board. Replace **tg_6.6.16_linux.install** with the actual Mediant 8000 software package name.

```
client238::~~# rm tg_6.6.16_linux.install
```

21.1.5 Installing the Mediant 8000 Software on the SC Board to Operate as the Standby Board

The following installation instructions apply in one of the following cases:

- If you install the new version of the Mediant 8000 software on both SC boards (follow these instructions for SC board that resides in Slot 2).
- If you install the Mediant 8000 software on the replacement SC board, while another SC board continues to operate normally.

➤ To install the Mediant 8000 software on the SC board to operate as the Standby SC board:

1. Connect to the CLI interface on the SC board that is to operate as the Standby board. For more information, see Section 'Command Line Interface' on page 107.
2. Login as user **root**. For more information, see Section 'Logging in as a Root User' on page 115.
3. At the prompt, type **install ~acladmin/tg_6.6.16_linux.install** and press **Enter**. Replace **acladmin** with the name of the CLI user that you used while transferring the Mediant 8000 package to the SC board. Replace **tg_6.6.16_linux.install** with the name of the Mediant 8000 installation package.

```
client241::~~# install ~acladmin/tg_6.6.16_linux.install
```

```
Core Network Media Gateway
```

```
Version : 6.6.16
```

```
WARNING: installation of the new software version will erase
the current Media Gateway configuration.
To upgrade the Media Gateway software to the new version and to retain
the current configuration, run the Online Software Upgrade.
```



Note: On SC boards with v5.6 or earlier software version installed, the install command may produce the following error:

```
usage: install [options] file [dir1 ...]
```

In this case, use the following commands to start the Mediant 8000 software installation:

```
chmod u+x ~acladmin/tg_6.6.16.install
~acladmin/tg_6.6.16_linux.install
```

4. When you are prompted to start the installation, type **y** and press **Enter**. The software installation begins.


```
Start installation? (y/n) : y
Extract /sc_software.tar installation archive... done
Extract /sc_install.pl installation script... done
```

```
Install SC Software
```

```
>>> save snmp.conf in /tmp/snmp.conf.prev ...
>>> save SNMP++ stack configuration in /tmp/snmp.prev ...
(This sequence is abbreviated)
```

5. After the installation successfully completes extraction of all the software binary components, you are prompted to perform the basic configuration of the SC software.

```
Software is successfully extracted.
```

```
SC board must be configured to complete the installation.
```

```
Choose one of the following configuration options:
```

- a) "configure now" - you will be prompted to perform a new SC configuration
- b) "copy configuration" - an existing SC configuration will be copied from another SC board

```
If you install the Media Gateway software on a failed SC board, choose the "copy configuration" option to copy an existing configuration from another SC board (currently up and running).
```

```
If you install the Media Gateway software on both SC boards, do the following:
```

- a) for the SC board in slot 1, choose the "configure now" option
- b) for the SC board in slot 2, choose the "copy configuration" option

```
How do you want to configure this SC board? (1=configure now/2=copy configuration) [1]: 2
```

6. Since you are installing software on the SC board to operate as the Standby board, type **2** and press **Enter** to select "copy configuration" option.



Note: If you make a mistake and choose option 1 “configure now” for SC board to operate as the Standby board, do one of the following:

- Abort installation via Ctrl-C and re-start it from the beginning (this is the preferred option)
- Continue installation as described in 'Installing Mediant 8000 Software on the SC Board to Operate as the Active Board' on page 134 and provide exactly the same values that are currently configured on the Active SC board. This option is more prone to user syntax errors (due to possible mismatches in parameter values), however so long as the configuration information of the two SC boards fully match, it will produce a fully functional software configuration on both Active and Standby SC boards.

7. You will be prompted to enter the IP address of the Active SC board (or the board to operate as the Active board, if you install software on both SC boards). Enter the corresponding IP address and press **Enter**.

```
Active SC IP Address           [10.7.13.91]: 10.7.13.91
Verify that Active SC 10.7.13.91 responds to ping...
10.7.13.91 is alive
```

```
Configuration will be copied from Active SC 10.7.13.91 via SSH.
```

8. At the **CLI user name** prompt, enter the name of a regular CLI user on the Active SC board (e.g. **acladmin**). See 'Command Line Interface Users' on page 113 for more details.

```
Please provide CLI user credentials:
CLI user name [acladmin]: acladmin
```

9. At the **CLI user password** prompt, enter the password of the specific CLI user on the Active SC board (e.g. **pass_12345**).

```
CLI user password: *****
```

10. At the **ROOT user password** prompt, enter the password of **root** user on the Active SC board (e.g. **root**).

```
ROOT user password: *****
```



Note: If you changed **root** password as part of Active SC software installation, ensure that you enter the new **root** password at this prompt.

11. The configuration is copied from the Active SC board and a summary of the settings is displayed:

Configuration Summary:	
Global SC IP Address	: 10.7.13.90
1 st SC IP Address	: 10.7.13.91
2 nd SC IP Address	: 10.7.13.92
Time Zone	: Europe/Paris
Enable Security	: 0 (no)
SC Root Password	: *****
Product Type	: 0 (Mediant 8000)



Note: If you install the Mediant 8000 software on both SC boards, it is possible that copying the configuration from the Active to the Standby SC boards may fail despite the fact that correct credentials for **CLI** and **root** users are provided. If you experience this scenario, reboot the Active SC board at this point (by answering y to the **REBOOT now?** prompt on its CLI interface), wait for 2 minutes until the Active SC board completes the reboot and re-try copying the configuration.

12. You are prompted to start configuring. To commence the configuration, type **y** and press **Enter**.

```
Start configuring ([y]/n) [n]: y
>>> Configure INET services ...
>>> Update /etc/inet/inetd.conf file ...
>>> Restore file /etc/inet/inetd.conf from the backup ...
>>> Update /etc/inet/services file ...
(This sequence is abbreviated)
```

13. After installation successfully completes the SC software configuration, it determines whether OS Patches need to be installed on the specific SC board. OS patches installation ensures that the latest operating system's security and stability fixes are applied. It also ensures that the Mediant 8000 software operates in the same well-defined software environment that was used during the software verification and validation process.
- When prompted to start OS patches installation, type **y** and press **Enter**.

```
>>> Install OS patches ...
```

```
SC software contains new OS patches that must be installed.
```

```
Installation of OS patches may take considerable time.  
However without these OS patches SC software may not function  
properly and/or SC security may be compromised.
```

```
Install OS patches? (y/n)      [y]: y  
Applying 112785-65 (1 of 25) ... done  
Applying 112837-16 (2 of 25) ...
```

```
(This sequence is abbreviated)
```



Note: Installation of the OS patches may take a considerable amount of time – up to 1.5 hours. The exact amount of time depends on which previous Mediant 8000 software version was installed on the specific SC board.

Installation of OS patches on the SC Rev.2 board (using the Linux OS) is considerably shorter and typically takes only a few minutes.

14. After the installation successfully completes, you will be prompted to reboot the SC board.

```
SC board must be rebooted to complete the installation.
```

```
After the reboot, do the following:  
1) connect to the Active SC board (via Global IP address)  
2) run "tools ems" script to configure connectivity  
between Media Gateway and EMS server  
3) if VLAN must be configured on the OAM interface,  
run "tools vlan" script
```

```
REBOOT now (y/n)                [y]: y  
Are you sure (y/n)              [y]: y
```

If you are installing the Mediant 8000 software on both SC boards, prior to this installation (on the Standby SC board), you have waited for the SC board to operate as the Active board to complete the reboot process. Reboot both SC boards simultaneously by typing **y** and pressing **Enter** on the respective SC board's CLI interfaces.

15. The SC board reboots. It typically takes 2 minutes to complete the reboot process. The Media Gateway software starts automatically after the SC board completes the reboot.

16. After the SC board completes the reboot, re-connect to its CLI interface and login as a regular CLI user that you used to transfer the installation package (e.g. **acladmin**). Type the **rm tg_6.6.16_linux.install** command to remove the Mediant 8000 installation package from the SC board. Replace **tg_6.6.16_linux.install** with the actual Mediant 8000 software package name.

```
client241::~~# rm tg_Version 6.6.16_linux.install
```

21.2 Performing Basic Configuration of the Mediant 8000 Software



Note: If you performed Mediant 8000 software installation as described in 'Installing Mediant 8000 Software' on page [129](#), skip this chapter and proceed directly to the chapter 'Starting Mediant 8000 Software' on page [153](#).

The basic configuration of the Mediant 8000 software re-defines some high-level configuration parameters (e.g. Global IP Address) and ensures that the Mediant 8000 software's configuration fully matches the current network configuration of the SC boards.

The basic configuration of the Mediant 8000 software is typically carried out when the Mediant 8000 is moved to the new IP environment. Common maintenance and configuration tasks are typically performed via more feature-rich management interfaces, i.e EMS GUI or CLI commands.

The basic configuration of the Mediant 8000 software must be performed on both SC boards, located in Slots 1 and 2 correspondingly, and consists of the following steps:

- Performing basic configuration of the Mediant 8000 software on the SC board to operate as the Active board (in Slot 1).
- Performing basic configuration of the Mediant 8000 software on the SC board to operate as the Standby board (in Slot 2).

21.2.1 Performing Basic Configuration of the Mediant 8000 Software on the SC board to Operate as the Active Board

The following configuration should be performed on the SC board to operate as the Active board (in Slot 1) in the following cases:

- When the Mediant 8000 is installed in the customer premises for the 1st time and its pre-installed software version matches the version used by the customer.
- When the Mediant 8000 is moved to the new IP network segment (and IP addresses of SC boards must be changed).
- When the Mediant 8000's Operational mode is changed from non-secure to secure mode (or vice versa)

➤ **To perform the basic configuration of the Mediant 8000 software on the SC board to operate as the Active board (in Slot 1):**

1. Connect to the CLI interface on the SC board to operate as the Active board (in Slot 1). For more information, see Section 'Command Line Interface' on page 107.
2. Login as user **root**. For more information, see Section 'Logging in as a Root User' on page 115.
3. At the prompt, type **install** and press **Enter**.
4. Choose option **3**.

```
client238::~~# install
Found uncompressed Media Gateway installation package...
Verify installation package integrity...
```

```
SC Software Installation & Basic Configuration
```

```
1 - Change network configuration.
2 - Install the software.
3 - Change basic configuration.
4 - Copy basic configuration from Active SC.
5 - Uninstall the software.
0 - Quit.
Choose (0-5) : 3
```

```
System Configuration
```

```
Keyboard shortcuts:
ENTER - leave the default parameter value as is
\      - return to the previous parameter
Ctrl-C - abort the configuration script
```

5. At the **Global SC IP Address** prompt, enter the IP address to be assigned to the Active SC board and used to connect to the Media Gateway's management interface (e.g., from EMS server).

Global SC IP address	[0.0.0.0]: 10.7.13.90

6. At the **1st SC IP address** prompt, enter the private IP address of the SC board in Slot 1 as specified in 'Configuring the Basic IP Network Parameters Of SC Boards' on page 117.

1 st SC IP Address	[0.0.0.0]: 10.7.13.91

7. At the **2nd SC IP address** prompt, enter the private IP address of the SC board in Slot 2 as specified in 'Configuring the Basic IP Network Parameters Of SC Boards' on page 117.

2 nd SC IP Address (or 1.1.1.1 if none)	[0.0.0.0]: 10.7.13.92



Note: Parameters **1st SC IP Address** and **2nd SC IP Address** are used to identify the SC boards in Slot 1 and 2 correspondingly and not to change their existing network configuration. The Software installation will fail if these parameters do not match the IP addresses currently configured on both SC boards. If you wish to change the private IP address of the SC board, see "Configuring the Basic IP Network Parameters of SC Boards" on page 117.

8. At the **Time Zone** prompt, enter the local time zone where the Media Gateway resides.

The time zone may be specified as an offset from the **Greenwich Mean Time (GMT)** (e.g. **GMT-2** or **GMT+3**) or as a name of a geographical area where Media Gateway resides (e.g. **Europe/Paris** or **America/Denver**). In the latter case, Daylight Saving Time will be activated if the specific time zone supports it.

Time Zone	[GMT]: Europe/Paris

The name of the time zone uses standard **UNIX tz/zoneinfo** format. Geographical Locations are identified by continent or ocean and then by the name of the location, which is typically the largest city within the region. For example, **America/New_York** represents most of the US eastern time zone and **America/Phoenix** represents most of Arizona, which uses mountain time without daylight saving time (DST).

For major US and European cities, short time zone name (without continent name) is supported as well – e.g. **Paris** instead of **Europe/Paris**.

See 'Timezone Converter' '<http://www.timezoneconverter.com>' for a complete list of valid time zone names, their DST settings and current time in each time zone. Alternatively, use the following commands on the SC board to view the complete list of supported time zone names:

```
cd /usr/share/lib/zoneinfo
find . -type f,l -print | grep -v src | cut -b 25-
```


9. At the **Enable Security** prompt, type **1** to enable the Mediant 8000 software operate in Secure Mode or **0** to leave Mediant 8000 software in its default mode. For more information, see Section 'Secure Operation Mode' on page 306.

```
Enable Security (0-no, 1-yes)                [0]:0
```



Note: If your system uses SC- Rev.2 boards (with the Linux OS), the “Enable Security” prompt does not appear as the software always operates in a Secure Mode. See 'Secure Operation Mode' on page 306 for details.

10. At the **SC Root Password** prompt, enter the new password for user **root** or press **Enter** to leave it unchanged. Re-enter the new password when prompted. Use the following rules when specifying a new **root** password:
- Password must have at least 8 characters.
 - Password must contain at least two alphabetic characters and at least one numeric or special character. In this case, "alphabetic" refers to all upper or lower case letters.
 - Password must differ from the user's login name (**root**) and any reverse or circular shift of that login name.

```
SC Root Password                [leave unchanged]: *****
```



Note: For security reasons, it is strongly recommended to change **root** password from it's default value. Make a note of the new password you enter and keep it in a secure location for future reference.

11. After all basic configuration parameters are prompted, a summary of the settings is displayed.

Configuration Summary:

```
Global SC IP Address           : 10.7.13.90
1st SC IP Address              : 10.7.13.91
2nd SC IP Address              : 10.7.13.92
Enable Security                 : 0 (no)
SC Root Password                : *****
```

12. You are prompted to **start configuring**. To commence the configuration, type **y** and press **Enter**.

```
Start configuring ([y]/n) [n]: y
>>> Configure INET services ...
>>> Update /etc/inet/inetd.conf file ...
>>> Restore file /etc/inet/inetd.conf from the backup ...
>>> Update /etc/inet/services file ...
(This sequence is abbreviated)
```

13. After the configuration successfully completes, you will be prompted to reboot the SC board.

```
SC board must be rebooted to complete the re-configuration.
```

IMPORTANT: If you re-configure the Media Gateway software on both SC boards, do not reboot the SC board in slot 1 until the re-configuration of the SC board in slot 2 is completed.

```
REBOOT now (n/y) [y]: y
Are you sure (n/y) [y]: y
```

If you are performing a basic configuration of the Mediant 8000 software on both SC boards, do not reboot the SC board to operate as the Active board (the board that you are currently configuring) until you complete the configuration of the other SC board (to operate as the Standby board).

When both SC boards are ready to be rebooted, reboot them simultaneously by typing **y** and pressing **Enter** on the respective SC board's CLI interfaces.

14. The SC board reboots. It typically takes 2 minutes to complete the reboot process. The Media Gateway software starts automatically after the SC board completes the reboot process.

21.2.2 Performing Basic Configuration of the Mediant 8000 Software on the SC Board to Operate as the Standby Board

The basic configuration of the Mediant 8000 software on the SC board to operate as the Standby board (in Slot 2) should be performed after completing the basic configuration on the SC board to operate as the Active board (in Slot 1).

The software configuration is copied from the Active SC board, which ensures that the configuration of both SC boards fully matches and reduces the chance of an erroneous configuration.

➤ **To perform the basic configuration of the Mediant 8000 software on the SC board to operate as the Standby board (in Slot 2):**

1. Connect to the CLI interface on the SC board to operate as the Standby board (in Slot 2). For more information, refer to 'Command Line Interface' on page 107.
2. Login as user **root**. For more information, refer to 'Logging in as a Root' on page 115.
3. At the prompt, type **install** and press **Enter**.
4. Choose option 4.

```
client241::~~# install
Found uncompressed Audiocodes installation package...
Verify installation package integrity...
```

SC Software Installation & Basic Configuration

```
1 - Change network configuration.
2 - Install the software.
3 - Change basic configuration.
4 - Copy basic configuration from Active SC.
5 - Uninstall the software.
0 - Quit.
Choose (0-5) : 4
```

5. You will be prompted to enter the IP address of the SC board to operate as the Active board. Enter the corresponding IP address and press **Enter**.

Active SC IP Address [10.7.13.91]: **10.7.13.91**

Verify that Active SC 10.7.13.91 responds to ping...

10.7.13.91 is alive

Configuration will be copied from Active SC 10.7.13.91 via SSH.

6. At the **CLI user name** prompt, enter the name of a regular CLI user on the Active SC board (e.g., **acladmin**). Refer to 'Command Line Interface Users' on page [113](#) for more details.

Please provide CLI user credentials:
CLI user name [acladmin] : acladmin

7. At the **CLI user password** prompt, enter the password of the specific CLI user on the Active SC board (e.g., **pass_1234**).

CLI user password :*****

8. At the **ROOT user password** prompt, enter the password of **root** user on the Active SC board (e.g., **root**).

ROOT user password : *****



Note: If you changed **root** password as part of the Active SC software basic re-configuration, ensure that you enter the new **root** password at this prompt.

9. The configuration is copied from the SC board to operate as the active board and a summary of the settings is displayed.

```
Copying Files...Done!
```

```
Configuration Summary:
```

```
Global SC IP Address      : 10.7.13.90
```

```
1st SC IP Address        : 10.7.13.91
```

```
2nd SC IP Address        : 10.7.13.92
```

```
Enable Security           : 0 (no)
```

```
SC Root Password          : *****
```

10. You are prompted to start configuring. Type **y** and press **Enter** to commence the configuration.

```
>>> Configure INET services ...
>>> Update /etc/inet/inetd.conf file ...
>>> Restore file /etc/inet/inetd.conf from the backup ...
>>> Update /etc/inet/services file ...
>>> Restore file /etc/inet/services from the backup ...
```

```
(This sequence is abbreviated)
```

11. After the configuration successfully completes, you are prompted to reboot the SC board.

```
SC board must be rebooted to complete the re-configuration.
```

```
IMPORTANT: If you re-configure the Media Gateway software on both SC
boards, do not reboot the SC board in slot 1 until the re-configuration
of the SC board in slot 2 is completed.
```

```
REBOOT now (n/y)                      [y]: y
```

```
Are you sure (n/y)                    [y]: y
```

If you are installing the Mediant 8000 software on both SC boards, prior to this installation (on the Standby SC board), you have waited for the SC board to operate as the Active board to complete the reboot process.

Reboot both SC boards simultaneously by typing **y** and pressing **Enter** on the respective SC board's CLI interfaces.

12. The SC board reboots. It typically takes 2 minutes to complete the reboot process. The Media Gateway software starts automatically after the SC board completes the reboot process.

21.3 Starting Mediant 8000 Software

Mediant 8000 software is automatically started after both SC boards are rebooted.

In the default configuration, the SC board in Slot 1 operates as the Active SC board and performs all maintenance and configuration tasks, while the SC board in Slot 2 operates as the Standby SC board and provides redundancy in case of a failure of the SC board in Slot 1.

➤ **To verify that Mediant 8000 software is up and running on specific SC board:**

1. Connect to the CLI interface on the specific SC board. For more information, refer to 'Command Line Interface' on page 107.
2. Login as a regular **CLI** user (e.g. **acladmin**). For more information, refer to 'Logging into Command Line Interface' on page 115.
3. At the prompt, type **tools sc p** command. A list of SC software processes indicates that software is up and running.

```
client241::~~# tools sc p
LIST OF SC SOFTWARE PROCESSES

29510 tg_watch /Project/bin/exe/tg_watchdog

2185 tg_radiu tg_radius
2184 tg_xfer  tg_xfer
2183 tg_syslo tg_syslog
2181 tg_core  tg_core
2180 tg_tftp  tg_tftp
2179 tg_bootp tg_bootp
2178 tg_tpnpc tg_tpnpcif
2177 tg_sat   tg_sat
2176 tg_hbg   tg_hbg
2175 tg_hbm   tg_hbm
```

If the SC software is not running, repeat the Mediant 8000 software installation or basic re-configuration.

21.4 Configuring Connectivity with the EMS Server

After the Mediant 8000 software on both SC boards is up and running, you must configure connectivity between the Mediant 8000 and the EMS Server. This action is performed by running the command **tools ems** on the CLI interface of the Active SC board. For more information, refer to 'Configuring Connectivity between Media Gateway and EMS Server' on page [171](#).

Once you have completed this configuration, open the EMS client, establish connection with the EMS server and verify that the Mediant 8000 Media Gateway is visible in the EMS Media Gateways tree and its main status screen is correctly displayed. Verify the status of all Mediant 8000 components (SC boards, ES boards, power supplies, fan modules etc). Perform lock/unlock action on any board (e.g. standby ES board) and verify that actions are executed as expected and alarms are properly recorded in the EMS alarms browser.

22 Advanced Configuration

Once you have successfully connected the Mediant 8000 to the IP and the PSTN networks, powered it up and established connectivity with EMS management application, you should proceed to the configuration of site-specific features and the Media Gateway applications.

The configuration tasks that must be performed depend on specific applications that must be configured on the Mediant 8000 (SS7, SIP, MGC) and vary for each deployment. Nevertheless, the following configuration tasks should be performed in most of the deployment scenarios:

- Configuring IP network connectivity (subnets, VLANs, interface separation, link aggregation etc)
- Configuring NTP Server
- Configuring IP addresses of Media Gateway boards
- Configuring parameters of Media Gateway Controller (MGC) or SIP Proxy
- Configuring PSTN Connectivity
- Configuring clock synchronization for PSTN interfaces
- Configuring security settings

See 'Configuring & Operating the Media Gateway' on page [155](#) for a detailed description of these and additional configuration tasks.

This page is intentionally left blank.

Part III

Configuring and Operating the Media Gateway (Part 1)

This part describe how to configure and operate the Media Gateway.

23 Overview

The Mediant 8000 configuration consists of 2 parts:

- Basic configuration – a small set of basic configuration parameters (e.g. IP addresses of SC boards and chassis hardware type) that must be changed during the initial installation. Basic configuration is typically not changed unless the Media Gateway is moved from one IP network to another. See 'Performing Basic Configuration of the Mediant 8000 Software' on page 146 for more information.
- Operational configuration – the major part of the configuration that defines the Media Gateway hardware components, available applications and application functionality. The operational configuration of Mediant 8000 is described in this section.

The Mediant 8000 also provides operational information (status) of its hardware components and defined applications. The operational status of the Mediant 8000 is described in this chapter as well.

23.1 Management Interfaces

The operational configuration and status of the Media Gateway are managed via the following management interfaces:

- SNMP interface
- CLI (command line) interface
- Syslog interface

23.2 AudioCodes Element Management System (EMS)

The Mediant 8000 is typically accompanied by the AudioCodes Element Management System (EMS) that is used for managing the Mediant 8000 Media Gateway. The EMS is a universal standards-compliant feature-rich solution that provides management capability for the full line of AudioCodes' Media Gateway/Server products – both digital and analog. It provides user-friendly GUI-based interface and supports fault management, status monitoring and configuration of the managed entities.

The EMS uses both SNMP and CLI interfaces for managing the Mediant 8000 Media Gateway. However the SNMP management interface is used for most of the configuration and management tasks.

The EMS application consists of the following components:

- **EMS server** – manages the main EMS software logic and contains the management database; is typically installed on a dedicated Solaris or Linux based server.
- **EMS client** – a small GUI application, used to connect to the EMS server; is typically installed on the Windows-based PC.

SNMP and CLI management interfaces of the Mediant 8000 Media Gateway are utilized by the EMS server. The EMS client establishes connection with the EMS server (via secured RMI protocol) and never directly connects to the Mediant 8000 SNMP or CLI management interfaces.

For detailed information on using the EMS see the following documents:

- *EMS User's Manual, Document # LTRT 910xx*
- *EMS Release Notes - Document # LTRT-912xx*
- *Mediant 5000 and Mediant 8000 Alarm and Performance Monitoring Guide - Document # LTRT-237xxx*

23.3 SNMP Management Interface

The SNMP management interface is used by the EMS server and/or standards-compliant 3rd party SNMP managers to perform most of the Mediant 8000 management, configuration and status monitoring tasks. For detailed information, see 'SNMP Management Interface' on page [170](#).

23.4 CLI Management Interface

In addition, a CLI (command line) interface may be used for management, configuration and status monitoring. For detailed information, see:

- *CLI Reference - Document # LTRT-892xx*

23.5 Syslog Management Interface

In addition, a Syslog management interface may be used to perform status monitoring. For detailed information, see 'Syslog Management Interface' on page [175](#).

23.6 Managed Objects, Administrative and Operational State

The operational configuration and status of the Mediant 8000 Media Gateway uses an ITU-T X.730/731 compatible data model.

The operational configuration and status of the Mediant 8000 Media Gateway is represented by a set of **Managed Objects (MOs)**, which combine physical and logical resources. Each MO contains multiple attributes that represent different properties of specific resource. Each attribute has access permissions (**read-write** or **read-only**) that indicate whether specific property may or may not be modified by the user.

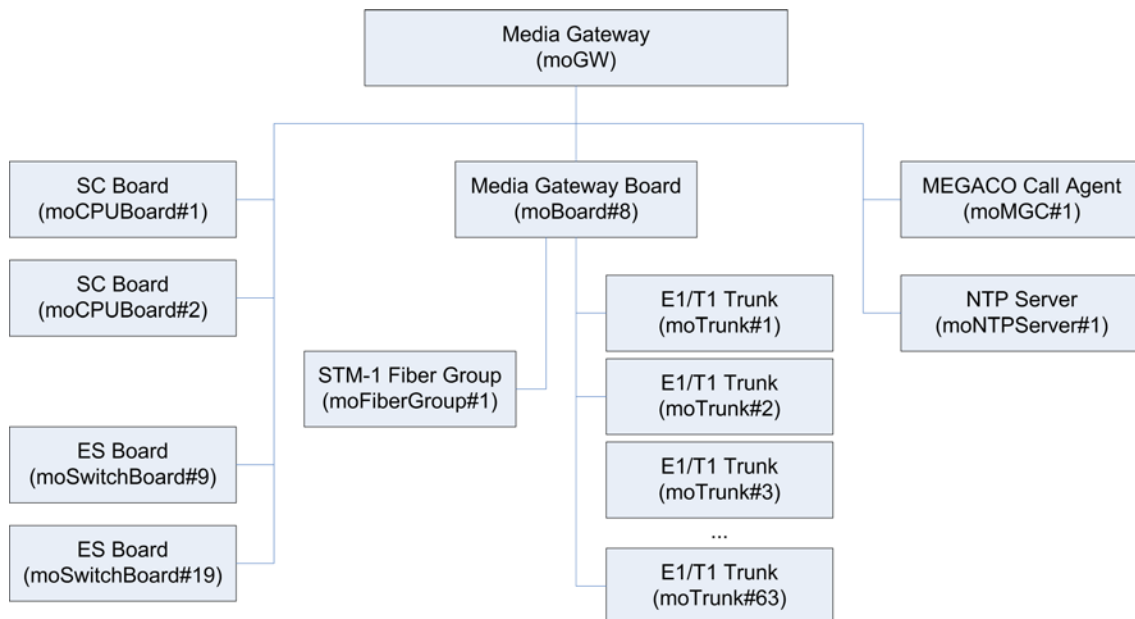
Examples of MOs that represent physical resources are: Media Gateway, Media Gateway Board, and E1/T1 Trunk.

Examples of MOs that represent logical resources are: SS7 Node, Firewall Profile, and Media Gateway Controller (Call Agent).

23.6.1 MO Tree Hierarchy

All MOs are grouped into an MO Tree that represents the hierarchical relationship between different MOs. The Media Gateway MO is located at the top of MO Tree and represents a Gateway Entity.

Figure 23-1: Sample MO Tree Hierarchy



Note: The sample MO Tree Hierarchy, shown above, illustrates only a sample containing the most basic and widely-used MOs. The actual configuration typically contains hundreds of MOs, representing different physical and logical resources.

23.6.2 MO States

Each MO has an **Operational State** and an **Administrative State**.

- **Operational State** – describes the *factual* operability of the corresponding resource. It has two possible values – *enabled* and *disabled*.
- **Administrative State** – describes the *user-desired* operability of the corresponding resource. It has three possible values – *locked*, *shuttingDown* and *unlocked*.

23.6.3 Lock/Unlock Actions

The **Operational State** of the MO cannot be altered. Instead you can alter the **Administrative State** of the MO by performing a **lock** or **unlock** action. If the action succeeds, the **Operational State** is changed to the corresponding value as soon as the *factual* operability is updated.



Note: It may take some time for the operability state of an MO to change – e.g., it takes a few minutes for a Media Gateway board to complete an **unlock** action. In the intermediate state, the **Administrative State** of the corresponding MO is **unlocked**; however, the **Operational State** of the MO is *disabled*. As soon as the Media Gateway board returns to service its **Operational State** is changed to *enabled*.

23.7 Managed Objects (MOs) in the EMS

EMS uses status screens to illustrate the Mediant 8000 Managed Objects (MOs). Two types of status screens are available:

- Graphical status screens – each MO is illustrated by a drawing or an icon which resembles the physical view of the hardware component.
- Textual status screens – each MO is represented by a table entry which typically contains the MO name and its most commonly used properties.

Figure 23-2: Graphical EMS Status Screen

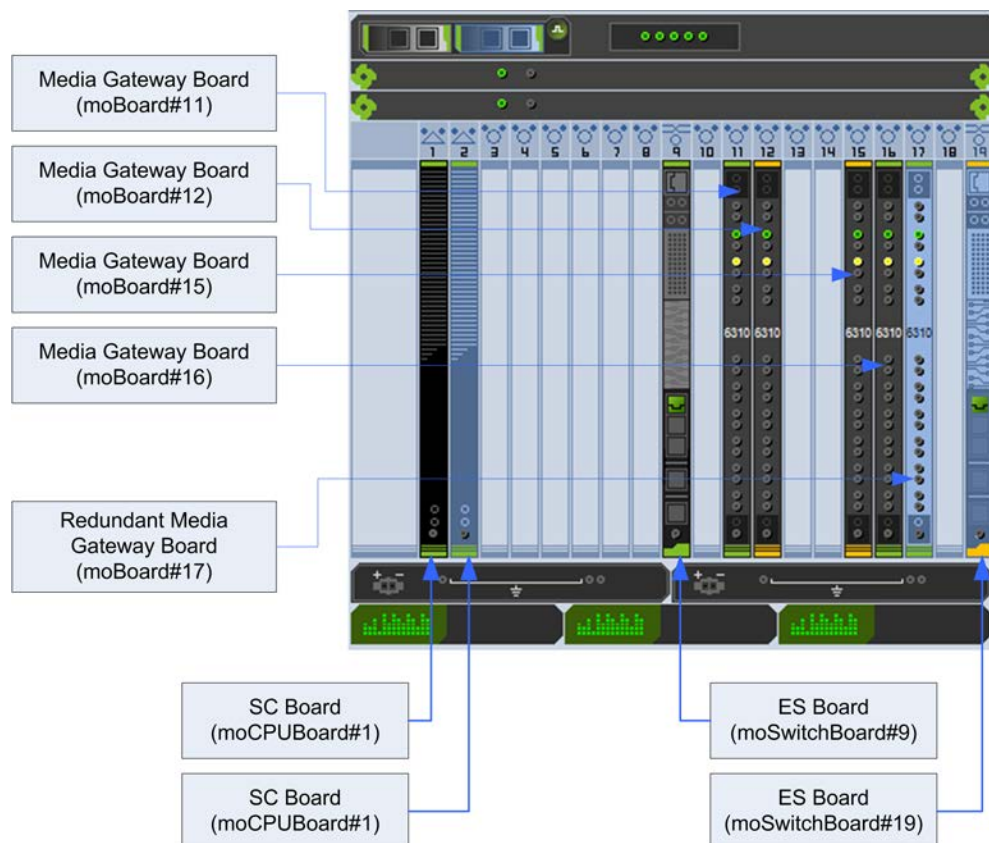


Figure 23-3: Textual EMS Status Screen

Apply Profile Lock Unlock Activate Deactivate Create Loopback Remove Loopback								
DS1 Carriers List								
#	Name	Protocol	DS1 Path	Activity Status	D Channel Status	NFAS ...	Admin State	Oper State
1	Trunk#1	T1Transparent	none	Activated	dChannelNotApplicable	0	Unlocked	Enabled
2	Trunk#2	T1Transparent	none	Activated	dChannelNotApplicable	0	Locked	Disabled
3	Trunk#3	T1Transparent	none	Activated	dChannelNotApplicable	0	Locked	Disabled
4	Trunk#4	T1Transparent	none	Activated	dChannelNotApplicable	0	Locked	Disabled
5	Trunk#5	T1IUA	none	Activated	dChannelNotEstablished	0	Locked	Disabled
6	Trunk#6	T1IUA	none	Activated	dChannelNotEstablished	0	Locked	Disabled
7	Trunk#7	T1IUA	none	Activated	dChannelNotEstablished	0	Locked	Disabled
8	Trunk#8	T1IUA	none	Activated	dChannelNotEstablished	0	Locked	Disabled
9	Trunk#9	T1Transparent	none	Activated	dChannelNotApplicable	0	Locked	Disabled
10	Trunk#...	T1Transparent	none	Activated	dChannelNotApplicable	0	Unlocked	Enabled
11	Trunk#...	T1Transparent	none	Activated	dChannelNotApplicable	0	Locked	Disabled
12	Trunk#...	T1Transparent	none	Activated	dChannelNotApplicable	0	Locked	Disabled

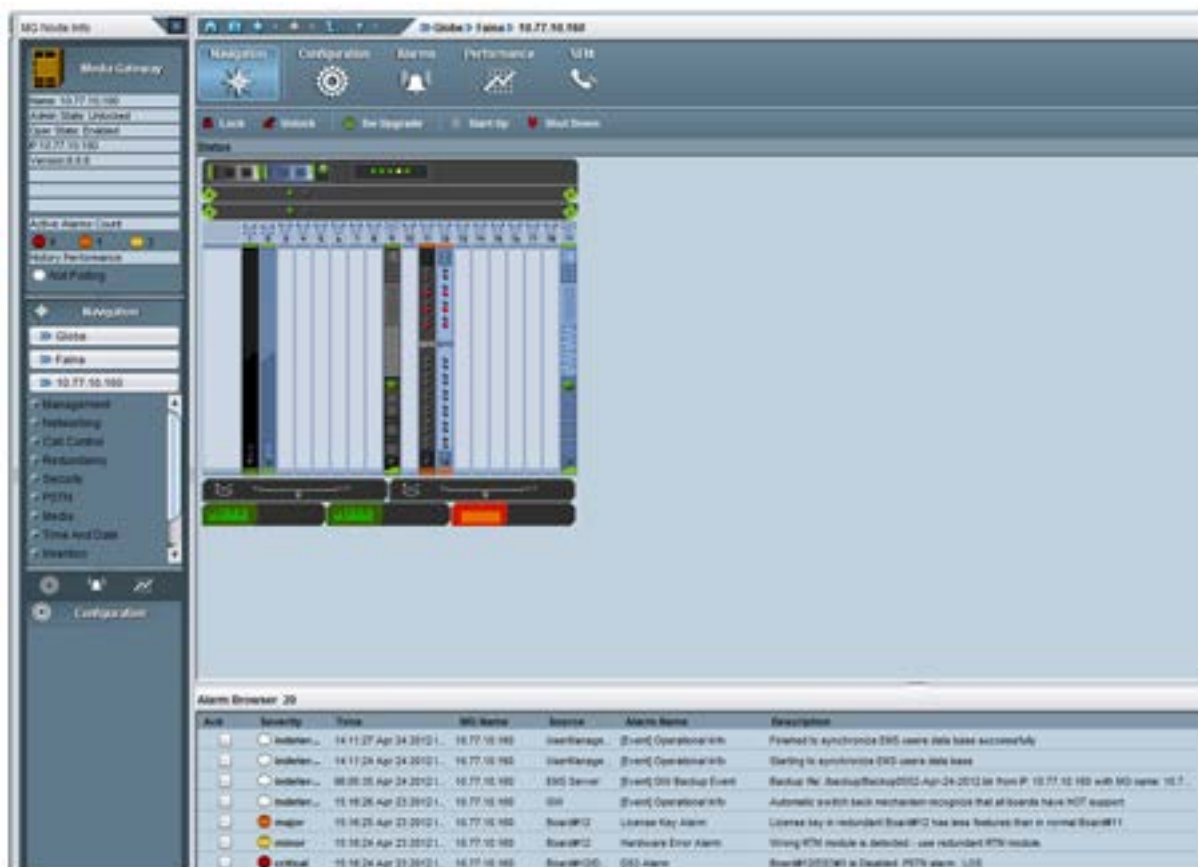
For easy navigation, the EMS GUI divides MOs into group types. For example all security-related MOs are grouped under the “Security” tab.



Note: These navigation tabs are used in the EMS GUI for navigation purposes only. They are not represented in SNMP Alarm sources nor in the CLI management interface.

To navigate between MOs, first select the MO name in the Navigation pane on the left, and then select the MO instance in the corresponding status screen on the right (by clicking on the corresponding drawing in graphical status screens or choosing the table entry in table status screens). Whenever an MO instance is selected, the Navigation pane and Info pane are updated accordingly. Repeat the process until the desired MO instance is selected.

Figure 23-4: Navigation Pane and Info Panel in EMS



23.8 Modifying the Media Gateway Configuration

Each MO contains multiple attributes that represent different properties of corresponding resource. Each attribute has **access permissions** (**read-write** or **read-only**) that indicate whether specific property may or may not be modified by the user.

In addition, **read-write** attributes have a **provisioning type** that indicates under which conditions a specific attribute may be modified. The following provisioning types are supported:

Table 23-1: MO Attribute Provisioning Types

Provisioning Types	Description	EMS Icon
Instant	The attribute may be configured at any time. No specific state of the corresponding MO is enforced.	None
Online	The corresponding MO must be locked prior to altering the specific attribute.	
Offline	The “father” of the corresponding MO (hierarchical superior) must be locked prior to altering the specific attribute (e.g., an Offline attribute in an MO Trunk requires that the Media Gateway Board, where the trunk is located, must be locked.)	
Offline_create	The attribute behaves as an <i>Instant</i> attribute after the MO is initially created. However, the attribute turns into an Offline attribute as soon as the MO is unlocked .	none or  (depending on the state)

➤ **To modify Media Gateway configuration via the EMS:**

1. Use the Navigation pane to navigate to the specific MO.
2. In the Configuration pane (located below the Navigation pane), select the specific settings screen.

3. In the settings screen, configure parameters and click Apply to apply the new configuration.

Figure 23-5: EMS Configuration Pane

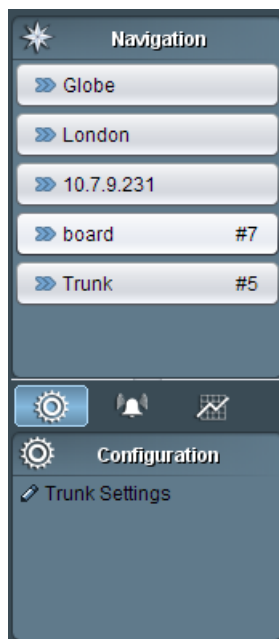
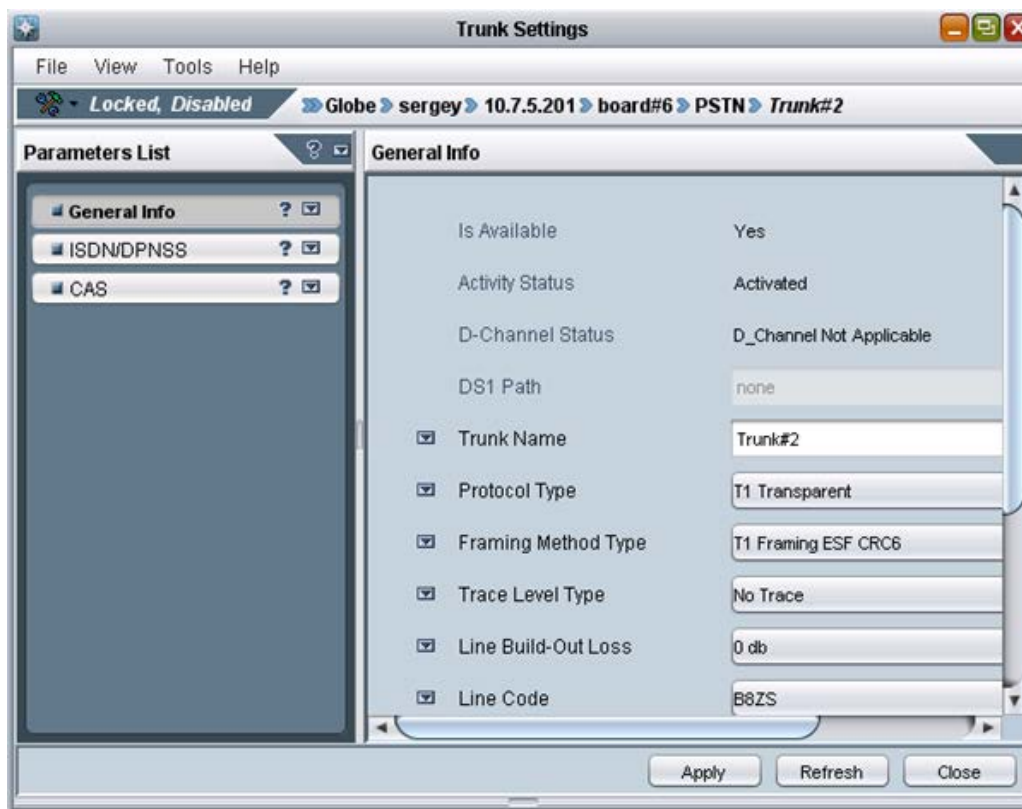


Figure 23-6: Example Settings Screen-Trunk Settings



23.9 Faults and Alarms Monitoring

Gateway functionality and service status can be monitored in one of the following ways:

- Polling the status attributes of corresponding MOs
- Processing trap notifications issued by the Media Gateway

Trap notifications are issued by the Media Gateway when a fault or an event occurs that may affect service provided by the Media Gateway or its specific application. Trap notifications are sent to the SNMP managers (e.g., EMS) and recorded in the trap log file accessible via the CLI interface.

Trap notifications may be one of the following two types:

- **Alarms** – indicates the problem that currently affects the specific Media Gateway component; alarms are raised when problem occur and are cleared when the problem is gone; only alarms that are currently raised are displayed in the EMS Alarm Browser screen by default.
- **Events** – provides information about a specific event that occurred in the past and is not necessarily currently relevant to the system; events are not cleared and therefore should be used for logging purposes only; the EMS Alarm Browser may be configured to either sort events from alarms or to filter events from the alarm browser view.

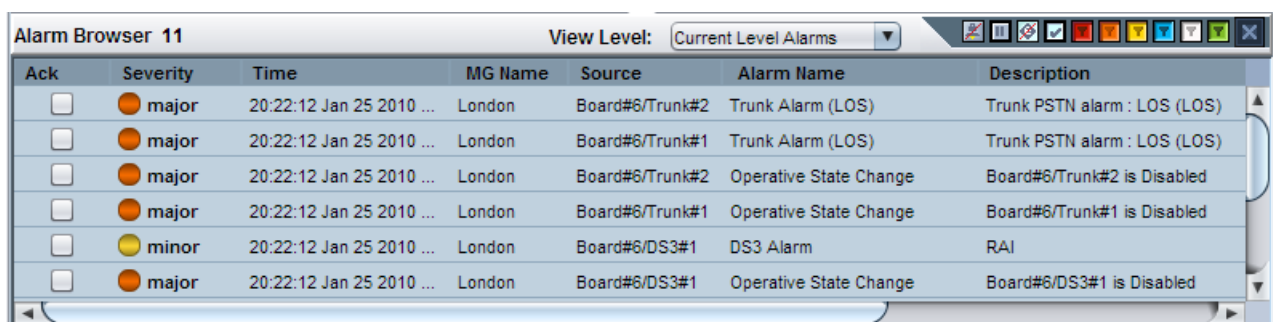
Each trap notification contains the following data:

- **Name** – trap name
- **Textual Description** – detailed description of the problem or informational event
- **Source** – MO where the problem or event occurred
- **Severity** – problem or event severity
- **Type** – generic trap type
- **Probable Cause** – probable problem or event cause
- **AdditionalInfo1-3** – additional information about the problem or informational event

In the EMS, trap notifications are displayed in the Alarm Browser located at the bottom of the screen. The Alarm browser is context-sensitive and displays only alarms that belong to the selected MO and it's children. To display all available trap notifications,

click the  button to access the Media Gateway status screen.

Figure 23-7: EMS Alarm Browser



Ack	Severity	Time	MG Name	Source	Alarm Name	Description
☐	major	20:22:12 Jan 25 2010 ...	London	Board#6/Trunk#2	Trunk Alarm (LOS)	Trunk PSTN alarm : LOS (LOS)
☐	major	20:22:12 Jan 25 2010 ...	London	Board#6/Trunk#1	Trunk Alarm (LOS)	Trunk PSTN alarm : LOS (LOS)
☐	major	20:22:12 Jan 25 2010 ...	London	Board#6/Trunk#2	Operative State Change	Board#6/Trunk#2 is Disabled
☐	major	20:22:12 Jan 25 2010 ...	London	Board#6/Trunk#1	Operative State Change	Board#6/Trunk#1 is Disabled
☐	minor	20:22:12 Jan 25 2010 ...	London	Board#6/DS3#1	DS3 Alarm	RAI
☐	major	20:22:12 Jan 25 2010 ...	London	Board#6/DS3#1	Operative State Change	Board#6/DS3#1 is Disabled

EMS displays both alarms and events in the Alarm Browser by default. Cleared alarms are removed from the Alarm Browser, however, may still be viewed by selecting **Faults -> Alarms History** in the EMS main menu. Events are never cleared; however, may be manually removed from the Alarm Browser by pressing the  button in the icon bar located at the top-right corner of the Alarm Browser.

EMS uses the following table to color-code alarms based on their severity:

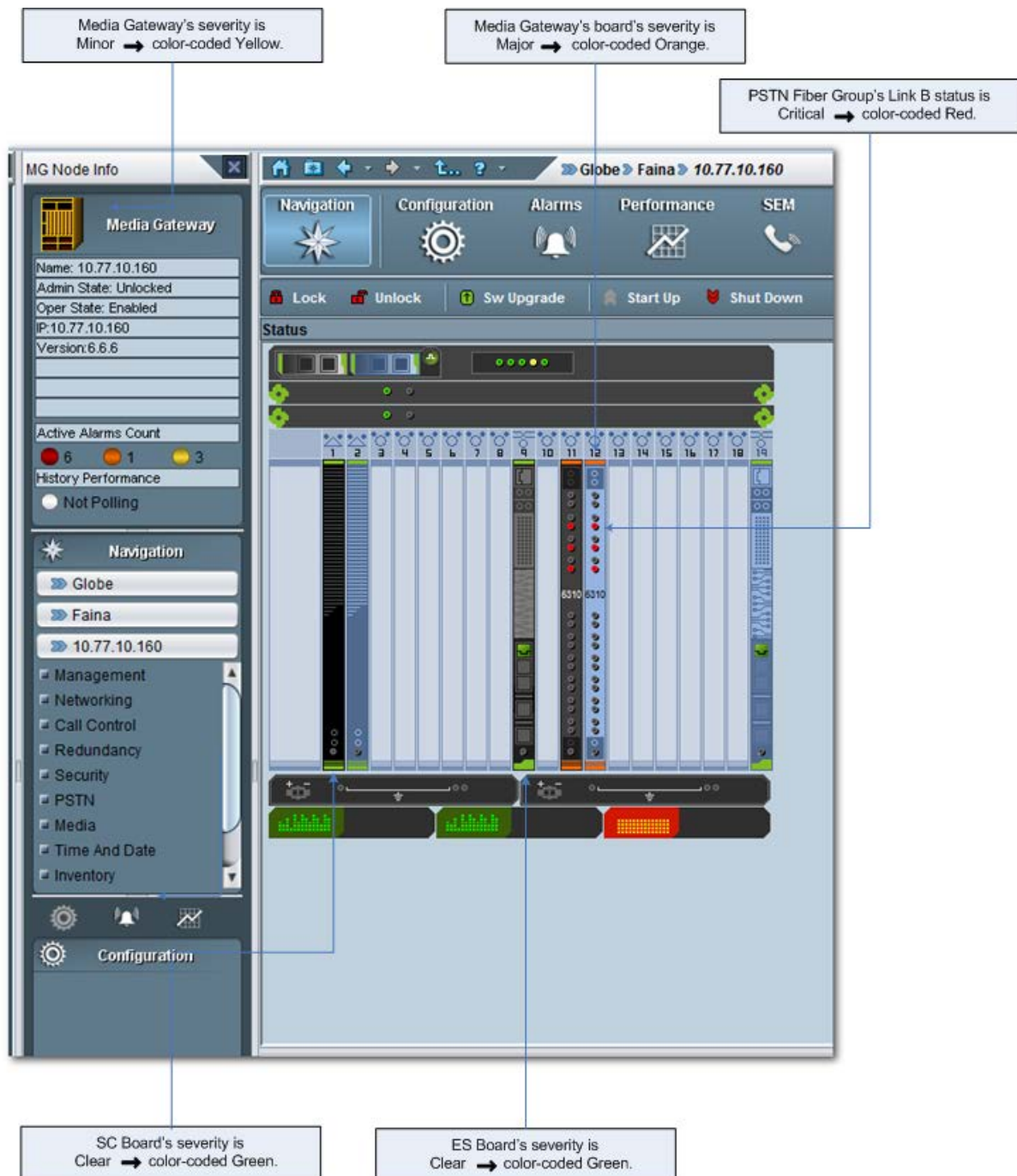
Table 23-2: EMS-Alarm Severity Color

Severity	Color
Clear	Green
Indeterminate	White
Minor	Yellow
Warning	Blue
Major	Orange
Critical	Red

When an alarm is raised on the MO, the severity attribute of the MO itself is updated accordingly. In addition, the severity attribute of the “father MO” may be updated as well. For example, when a major PSTN alarm is raised on Trunk, the severity of the Trunk is set to major and the severity of the Media Gateway board where this trunk resides is set to minor. The alarm propagation behavior is pre-configured and properly tuned for each and every alarm.



Note: Events lack a clearing mechanism and do not necessarily indicate a problem that is still relevant; therefore their severity is typically set to indeterminate and they do not affect the severity of the corresponding MO.

Figure 23-8: MOs in the EMS Color-Coded according to their Severity

EMS color-codes MOs according to their Severity attribute, using a similar logic as for alarms. However it also takes into account the **Operational State** and **Administrative State** of the MO. The MOs color-coding is described as follows:

Table 23-3: MO Severity Colors in the EMS

Administrative State	Operational State	Severity	Color
Unlocked	Enabled	Clear	Green
Unlocked	Enabled	Indeterminate	White
Unlocked	Enabled	Warning	Blue
Unlocked	Enabled	Minor	Yellow
Unlocked	Enabled	Major	Orange
Unlocked	Enabled	Critical	Red
Unlocked	Disabled	-	Dark Red
Locked	-	-	Grey

You can view problems by identifying components in the EMS status screen that have colors other than Grey or Green. When you select a specific component, the Alarm Browser screen is updated to display Alarms and Events that are applicable for the specific component (and all its sub-components) only. Therefore, you can use the Alarm Browser screen to determine the problem that currently applies to the specific component.

23.9.1 Alarm Throttling

In rare circumstances, a specific alarm may be continuously raised and cleared at a high rate (e.g. PSTN alarm on a Trunk may be issued continuously when the Media Gateway is not properly synchronized with the PSTN trunk). If such a scenario occurs, the Media Gateway automatically suppresses alarms from the specific MO for a certain period of time to prevent overload of the EMS of 3rd party SNMP managers (e.g. NMS).

An **Alarm Throttling Limit Exceeded** alarm will be generated when alarm throttling is activated.

24 SNMP Management Interface

The Media Gateway supports Simple Network Management Protocol (SNMP) as a main management interface. SNMP is used by the EMS server to perform configuration, alarms collection and performance monitoring tasks. It may also be used by 3rd party standard-compliant SNMP managers to perform alarms collection and performance monitoring tasks.

The Media Gateway supports the following versions of the SNMP protocol:

- **SNMPv2c** – compliant with RFC 1901 – RFC 1908; uses UDP transport and simple community-based security scheme
- **SNMPv3** – compliant with RFC 3411 – RFC 3418; uses enhanced User Security Model (USM) and supports message integrity, authentication and encryption.

The Media Gateway also supports encryption of the SNMPv2c traffic via the IPSEC/IKE security protocols. IPSEC/IKE encryption may be enforced for all SNMP managers, or, alternatively, configured for specific SNMP managers only.

24.1 Configuring Connectivity between the Media Gateway and the EMS Server

After initial Media Gateway software installation or when parameters of the EMS Server or of the SNMP management protocol are modified, use the following procedure to configure connectivity between the Media Gateway and the EMS Server.

The new configuration is applied immediately without any disruption to the Media Gateway service.

➤ **To configure connectivity between Media Gateway and EMS Server:**

1. Connect to the CLI interface on the Active SC board. For more information, see Section 'Connecting to the CLI via the IP Network' on page [111](#).
2. Log in as a CLI user with administrative privileges (e.g. **acladmin**). For more information, see Section 'Logging into Command Line Interface' on page [115](#).
3. At the prompt, type **tools ems** and press **Enter**.
4. At the **Choose submenu** prompt, type **conf** and press **Enter**.

```
client224::/# tools ems
```

```
EMS Server and SNMP Management Configuration
```

```
conf    -- CONFIGURE: configure parameters
view    -- VIEW: view current configuration
```

```
Choose submenu : conf
```

5. The Media Gateways SNMP management interface may operate in one of the following modes:
 - **SNMPv2** – a simple default management mode widely deployed in many closed networks, has a relatively weak security model based on the plain-text read and write community strings and therefore is a security threat for systems connected to the public networks (e.g. Internet): IPSEC/IKE encryption may be optionally configured for specific SNMP managers (see 'Configuring IPSEC/IKE for Management Interfaces (on SC boards)' on page 341; however, it is not enforced on the incoming SNMP port 161.
 - **SNMPv2 + IPSEC** – a secure version of the SNMPv2 management mode; communication between the Media Gateway and all SNMP managers (including the EMS server) is secured via the IPSEC/IKE protocol with a pre-shared key; use of the IPSEC/IKE is enforced on the incoming SNMP port 161, therefore all SNMP managers (EMS, NMS, OSS) must have a proper IPSEC/IKE association configured.
 - **SNMPv3** – the latest and secure version of the SNMP management protocol:
6. At the **SNMP mode** prompt, choose the SNMP management mode to be used by the Media Gateway.

```
SNMP Mode (0-SNMPv2, 1-SNMPv3, 2-SNMPv2+IPSEC)      [0]: 0
```

7. At the **EMS Server IP Address** prompt, enter the IP address of the EMS server.

```
EMS Server IP Address                               [10.7.6.21]: 10.7.6.21
```

8. If you have chosen SNMPv3 mode, you must enter **EMS Security Name**, **EMS Authentication Protocol**, **EMS Authentication Key**, **EMS Privacy Protocol** and **EMS Privacy Key** parameters.
 - a. At the **EMS Security Name** prompt, enter the SNMPv3 User Name that will be used by EMS Server when connecting to the Media Gateway.

```
EMS Security Name                                  [EMSUser]: EMSUser
```

- b. At the **EMS Authentication Protocol** prompt, enter the SNMPv3 Authentication Protocol that will be used between the EMS server and the Media Gateway. Authentication protocol ensure that SNMP messages exchanged between the participants are from a valid source.

```
EMS Authentication Protocol (0-No, 1-MD5, 2-SHA1)  : 1
```

- c. At the **EMS Authentication Key** prompt, enter the key that will be used to ensure authentication of SNMPv3 messages.

```
EMS Authentication Key                             [leave unchanged]: *****
```

- d. At the **EMS Privacy Protocol** prompt, enter the SNMPv3 Privacy Protocol that will be used between the EMS Server and the Media Gateway. Privacy protocol performs encryption of the SNMP packets to prevent snooping by unauthorized source.

EMS Privacy Protocol (0-No, 1-DES) : **1**

- e. At the **EMS Privacy Key** prompt, enter the Key that will be used to ensure privacy of SNMPv3 messages.

EMS Privacy Key [leave unchanged]: *********

9. If you have chosen the SNMPv2 or SNMPv2+IPSEC mode, you must enter the **SNMP Read Community** and the **SNMP Write Community** parameters.
 - At the **SNMP Read Community** prompt, enter the **Read Community** string used to authorize read operations performed by the EMS server and other SNMP managers. Press **Enter** to leave current SNMP Read Community string unchanged. Default value for SNMP Read Community string is **public**.

SNMP Read Community [leave unchanged]: **public**

- At the **SNMP Write Community** prompt, enter the **Write Community** string used to authorize write operations performed by the EMS server and other SNMP managers. Press **Enter** to leave current SNMP Write Community string unchanged. Default value for SNMP Write Community string is **private**.

SNMP Write Community [leave unchanged]: **private**

10. If you have chosen the SNMPv2+IPSEC mode, you must configure the IPSEC/IKE association between the Media Gateway and the EMS server. To configure the transport mode IPSEC/IKE association between the Media Gateway and the EMS server, enter the EMS IKE Pre-Shared Key parameter. To configure the tunnel mode IPSEC/IKE association, press Enter and use the EMS GUI or CLI to configure the SC IPSEC Rules table (see 'Configuring IPSEC/IKE for Management Interfaces (on SC boards)' on page 341).

To configure IPSEC/IKE association in transport mode between Media Gateway and EMS server, enter Preshared Key now. Otherwise, press ENTER and use EMS GUI or CLI to configure the SC IPSEC Rules table (moSCIPSECRule).
 EMS IKE Pre-Shared Key [don't configure]: *********

11. A summary of the settings is displayed. You are prompted to **Start configuring**. To commence the configuration, type **y** and press **Enter**.

Configuration Summary:	
Enable IPsec	: 0 (No)
SNMP Mode	: 0 (SNMPv2)
EMS Server IP Address	: 10.7.6.21
SNMP Read Community	: *****
SNMP Write Community	: *****
Start configuring ([y]/n) [n]: y	
<pre>>>> configure IPSEC... >>> configure SNMP V2... >>> creating new cli_server configuration file...</pre>	

After completing the SNMP protocol configuration on the Media Gateway, you must configure the EMS Server in exactly the same way. Do it as follows:

- If Media Gateway is already listed in the MG Tree, right-Click it and choose **Details** from the menu. Otherwise add Media Gateway to the MG Tree by right-clicking on the proper Region and choosing **Add MG** from the menu.
- In **MG Information** screen, configure SNMP parameters of the Media Gateway. Provide the same answers as entered when running the **tools ems** script on the Media Gateway. Press **OK** button when finished.



Note: EMS Server will be able to successfully connect to the Media Gateway, only when the SNMP Protocol parameters configured in the Media Gateway via the **tools ems** script fully match SNMP parameters configured in the EMS in the **MG Information** screen.

24.2 Configuring Connectivity between the Media Gateway and Additional SNMP Managers

Standard-compliant 3rd party SNMP managers (e.g. HP OpenView) may be used to perform the following basic management tasks on the Mediant 8000 Media Gateway:

- Trap notifications (alarms and events) collection
- Monitoring of the Mediant 8000 status and configuration via standard MIBs (e.g. IF-MIB or ENTITY-MIB)

For additional information see *Programmer's User Manual - Document # LTRT-914xx*.

Configuration of the additional SNMP managers may be performed as follows:

- Up to two additional SNMP managers (called **NMS** and **OSS**) may be configured via the **Media Gateway Management Settings** configuration screen in the EMS. For each server, an IP address and trap port must be specified.
- For the SNMPv3 protocol mode, additional SNMP managers may be configured via the standard SNMP USM tables. This configuration may be performed directly via the USM MIB or, alternatively, via the **SNMPv3 Users Settings** and **SNMPv2 Notification Settings** tabs in the **Media Gateway Management Settings** configuration screen in the EMS.

If you chose to secure SNMP traffic via IPSEC/IKE protocols, in addition to the above described configuration, you must create corresponding SC IPSEC Rules. For more information, see Section 'Configuring IPSEC/IKE for Management Interfaces (on SC boards)' on page [341](#).

This page is intentionally left blank.

25 Syslog Management Interface

The Media Gateway supports Syslog as an additional management interface. The Syslog interface may be used by 3rd party managers (Syslog servers) for trap notifications (alarms and events) collection. Configuration and performance monitoring tasks are not supported via the Syslog management interface (use the SNMP or CLI interfaces instead).

Syslog messages generated by the Media Gateway are compliant with RFC-3164. They have *Facility* element set to 16 (local0). The **Severity** element that is mapped from the corresponding SNMP alarm severity as described in the table below:

Table 25-1: SNMP to Syslog Severity Mapping

SNMP Severity	Syslog Severity
cleared	info
indeterminate	info
warning	notice
minor	warning
major	error
minor	warning
major	error
critical	critical

25.1 Configuring Connectivity between the Media Gateway and the Syslog Server

➤ To configure connectivity between the Media Gateway and the Syslog server:

1. Click  to access the Media Gateway status screen.
2. In the Navigation pane, click **Management** and in the Configuration pane click **Management Settings**; the Management Settings screen is displayed.
3. Configure the following parameters:
 - **External Syslog Server**
 - **External Syslog Server IP Address**
 - **External Syslog Server Port**

25.2 Securing the Syslog Management Interface

For improved security, Syslog traffic from Media Gateway may be encrypted via IPSEC/IKE security protocols. This is performed by configuring the corresponding SC IPSEC Rule, as described in 'Configuring IPSEC/IKE for Management Interfaces (on SC boards)' on page [341](#).

26 Connecting the Media Gateway to the IP Network

The Mediant 8000 must be connected to one or more IP networks to ensure its normal operation.

IP network architectures may strongly differ from one site to another. Separate network segments may be used for carrying different types of the traffic (e.g. dedicated network segments – subnets – may be created to transmit OAM, call control and media traffic). Subnets may be separated either physically (by using different network interfaces) or via the use of tagged VLANs. Link aggregation may be used to achieve engineered data throughput on specific subnet links. Quality of Service features may be configured to control traffic flow.

The Mediant 8000 provides a very flexible and extensive configuration of its IP Networking subsystem ensuring that the Mediant 8000 may be deployed in the widest possible range of IP network environments. This configuration can be easily implemented in a step-by-step manner as described in this manual.

Perform the Mediant 8000 IP Network configuration in the following order:

- Establish connectivity between the Mediant 8000 and EMS server as described in 'Establishing Connectivity with the EMS Server' on page 180. Connect the Mediant 8000 to the OAM subnet and configure basic network parameters on SC boards (IP addresses and OAM VLAN tagging, if applicable). The network configuration at this point in time may differ from the final one – e.g. it will use one network interface only, while final configuration may use multiple interfaces.
- Configure IP network topology as described in 'Configuring Network Topology' on page 182. Determine the relevant network subnets to which the Mediant 8000 must be connected and connection types (separate network interfaces and/or VLANs). Configure the **Interfaces** parameter accordingly and define **VLAN Tags** for all applicable VLANs. Configure **Link Aggregation** for the Media subnet, if applicable.
- Configure IP Network connectivity on SC boards as described in 'Configuring IP Network Connectivity on SC Boards' on page 195. Most of the parameters (IP addresses and OAM VLAN tagging, if applicable) were already configured in the 1st step. However additional OAM subnet parameters, such as OAM static routes and quality of service (QoS) settings, may be required.
- Configure IP Network connectivity on Media Gateway boards as described in 'Configuring IP Network Connectivity on Media Gateway Boards' on page 197. Configure Media and Call Control subnet properties. Configure Network Profiles and attach them to the Media Gateway boards. Configure IP addresses for Media Gateway boards. Configure additional Media and Control subnet parameters, such as Media and Control static routes and quality of service (QoS) settings.
- Apply the new network configuration. This may require lock/unlock of the ES boards, which should be performed "one board at a time". Re-connect network cables (or connect additional network cables) to match the final network configuration.

In addition to the below description, an example of the IP networking subsystem configuration for specific scenarios is provided in 'Appendix : Examples of IP Network

Connectivity Configuration' on page 877. It is recommended that you read this chapter to become familiar with the terminology used, as well as general principles of the Mediant 8000 network configuration, prior to reviewing (and implementing) the examples described in this appendix.

26.1 Establishing Connectivity with the EMS Server

IP network configuration is a relatively complicated task that is ideally performed via the EMS GUI. Therefore, prior to starting the IP network configuration, the connectivity between the Mediant 8000 and the EMS server should be established as described below.



Note: If the connection between the Mediant 8000 and the EMS server is already established (e.g. after the initial Mediant 8000 installation), proceed to the next section.

To establish connectivity between the Mediant 8000 and the EMS server, you may need to reset both Ethernet Switch (ES) boards by performing **lock** and **unlock** maintenance actions on them. The ES board is reset as part of the **unlock** action and may take up to 10 minutes till it completes the reset and returns to service. Lock/unlock actions must be performed on ES boards sequentially (one at a time) in the following order:

- Lock the ES boards in both Slot 9 and 19
- Unlock the ES board in Slot 9 and wait till it completes the restart and returns to service.
- Unlock the ES board in Slot 19 and wait till it completes the restart and returns to service.

➤ To establish connectivity between Mediant 8000 and EMS Server:

1. Connect the Mediant 8000 to the OAM subnet only (using a single network interface) and configure basic IP network parameters of SC boards. See 'Connecting to the IP Network' on page 116 for details.
2. Connect to the Mediant 8000 CLI interface and run the **tools ems** command to configure connectivity between the Media Gateway and the EMS server. See 'Configuring Connectivity between the Media Gateway and the EMS Server' on page 171 for details.
3. Open the EMS GUI and add the Media Gateway to the MG Tree. If a connection is established and the Mediant 8000 status screen is properly displayed in the EMS, proceed to the next section.
4. Connect to the CLI interface on the Active SC board (typically located in Slot 1). Use the RS-232 serial console if IP connectivity with the Mediant 8000 is unavailable. For more information, see Section 'Connecting to the CLI via an RS-232 Serial Console' on page 109.

5. Login as a CLI user with administrative privileges (e.g. **acladmin**). For more information, see Section section 'Logging into the Command Line Interface' on page 115.
6. Type the following command to reset the IP network configuration to default:

```
SC-1 -- ~ -- /moGW
• modify Interfaces=0
```

7. If the OAM network uses VLAN tagging, type the following command to configure the OAM VLAN Tag ID (replace 84 by actual VLAN Tag value):

```
SC-1 -- ~ -- /moGW
• modify OAMTagID=84
```

8. Type the following commands to lock both ES boards; type **y** to confirm the lock maintenance action:

```
SC-1 -- ~ -- /moGW
• lock esboard#9
```

```
Do you really want to lock /moGW/moSwitchBoard# 9 ? [y/n] y
Performing lock action on /moGW/moSwitchBoard# 9 - OK!
```

```
• lock esboard#19
```

```
Do you really want to lock /moGW/moSwitchBoard#19? [y/n] y
Performing lock action on /moGW/moSwitchBoard#19 - OK!
```

9. Type the following command to unlock the ES board in slot 9:

```
SC-1 -- ~ -- /moGW
• unlock esboard#9
Performing unlock action on /moGW/moSwitchBoard#9 - OK!
```

10. Wait up to 10 minutes until the ES board in slot 9 completes the restart and returns to service. Use the following command to determine whether the ES board has completed the restart. Value *Enabled(1)* indicates that the ES board is back in service:

```
SC-1 -- ~ -- /moGW
• show esboard#9 param OperationalState
OperationalState=Enabled(1)
```

11. Type the following command to unlock the ES board in slot 19:

```
SC-1 -- ~ -- /moGW
• unlock esboard#19
Performing unlock action on /moGW/moSwitchBoard#19 - OK!
```

12. Wait up to 10 minutes until the ES board in slot 19 completes the restart and returns to service. Use the following command to determine whether the ES board has completed the restart. Value **Enabled(1)** indicates that the board is back in service:

```
SC-1 -- ~ -- /moGw
```

```
• show esboard#19 param OperationalState
OperationalState=Enabled(1)
```

13. If after completing the above procedure, there is still no network connectivity between the EMS server and the Mediant 8000, contact the on-site network administrator and verify that the physical network topology and configuration of the external Layer 3 Switches / Routers to which the Mediant 8000 is connected is correct.

26.2 Configuring Network Topology

This section describes how to configure network topology.

26.2.1 Types of IP Network Traffic and Network Subnets

IP network traffic processed and/or generated by the Mediant 8000 may be divided into the following categories:

- Management (OAM) traffic – including SNMP, SSH (CLI) and NTP (time and date synchronization) protocols
- Call Control traffic – including MGCP, MEGACO and SIP protocols
- Media traffic – including RTP and RTCP protocols

The IP network on site, where the Mediant 8000 is installed, may be configured to either pass all types of the IP traffic via the same network segment (the simplest and default network configuration). Or, alternatively, use different network segments that are dedicated to the transmission of a specific traffic type.

Each network segment (subnet) has its own address space (e.g. the OAM subnet may use **10.7.x.x** addresses, while the Control subnet may use **10.8.x.x** addresses). This requires the Mediant 8000 to have multiple IP addresses – at least one address for each subnet to which it is connected.



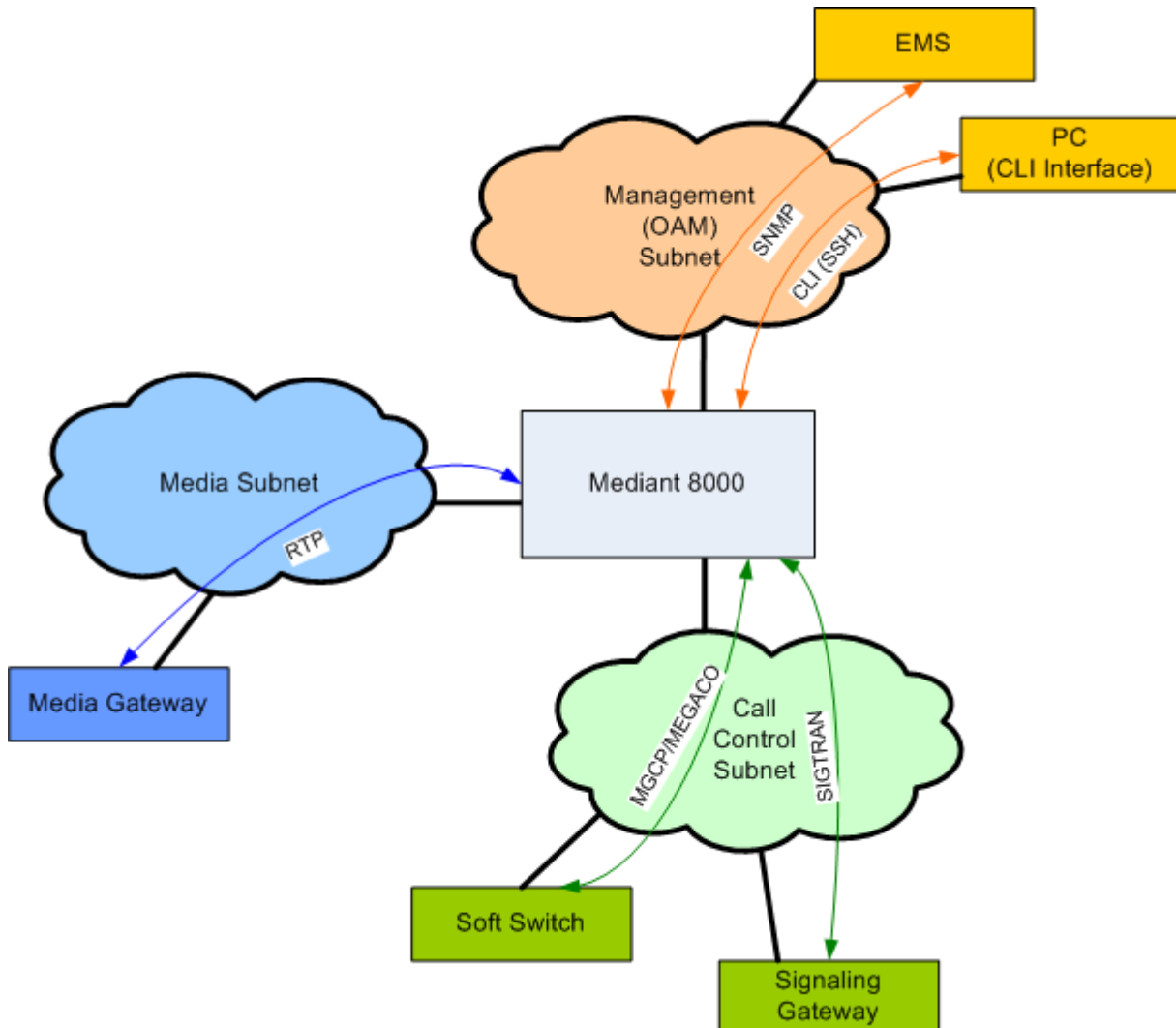
Note: Some network administrators may use the term **VLAN** instead of **Subnet** to see the segment of the IP network. These terms are interchangeable.

Subnets may be separated via the following methods:

- **Physical interface separation** – different Ethernet interfaces (cables) are used for each subnet.
- **Quasi-physical separation via use of tagged VLANs** – the same Ethernet interfaces (cables) are used for transmitting the traffic that belongs to different subnets; packets are separated via the use of a VLAN tag placed inside the IP packet header.

In both cases, separation between subnets helps to isolate one type of IP traffic from another, which provides both quality of service (QoS) and security features. For example, users connected to the OAM subnet may not in any possible way examine or affect call control and/or media traffic that flows in the separate subnets. This prevents possible call tapping and/or hijacking and protects call control and media subnets from possible denial of service (DoS) attacks that may be launched by users connected to the OAM subnet.

Figure 26-1: Network Subnets



26.2.2 Use of OAM, Control and Media Subnets by Mediant 8000 Boards

The Mediant 8000 supports multiple subnets for OAM, call control and media traffic.

OAM traffic mainly passes through the SC boards, located in Slots 1 and 2. This includes SNMP traffic between the Mediant 8000 and EMS (or 3rd party SNMP managers), as well as SSH traffic used for connecting to the Mediant 8000 CLI interface. Specific OAM traffic also passes through the Mediant 8000 boards, located in slots 3-8 and 10-18 – for example, the HTTPS traffic used for connecting to the WEB-based debug interface on the Media Gateway boards.

Media and Control traffic passes through the Media Gateway boards only. All VoP-related communication is performed directly between the Gateway boards and the corresponding external entities (i.e. Soft Switches, Media Gateway and Signaling Gateways). The SC boards are not involved in this type of traffic in any possible way.

26.2.3 Connecting Mediant 8000 to IP Network

The Mediant 8000 must be connected to each relevant subnet existing on site.

Connection details depend on the amount of available subnets and the type of their separation. In the simplest default configuration, when a single subnet is used for all types of IP traffic, two uplinks – one from each Ethernet Switch board (residing in slots 9 and 19) – should be connected to the external equipment. See 'External Layer 3 Ethernet Switches or Routers' in Section 'Connecting the Mediant 8000 to the IP Network' on page 217 for details on how the external equipment should be configured.

When multiple subnets are available, connection options depend on whether subnets are separated via the use of separate network interfaces (cables) or via the use of the tagged VLANs. In the former case (subnets separated via the use of separate network interfaces), multiple network cables should be connected to each ES board – one cable per each relevant subnet. In the latter case (subnets separated via the use of tagged VLANs) – a single cable should be connected to each ES board for multiple subnets.

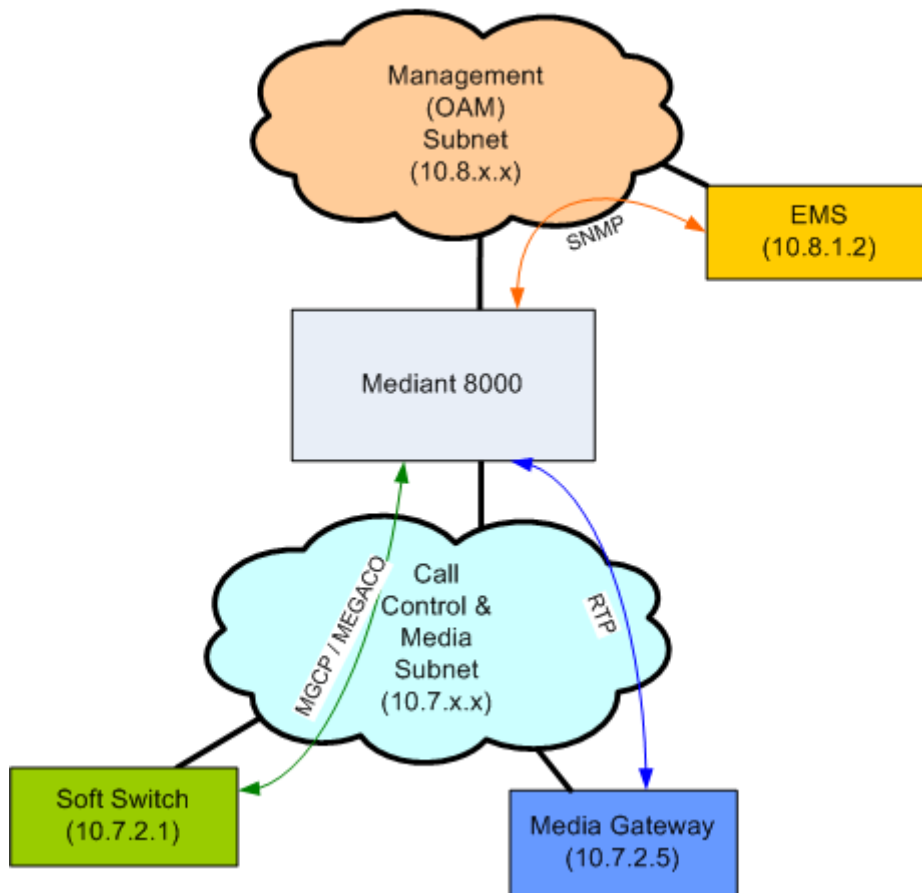
In any case, to ensure a fully redundant IP network connection, make sure that for each network cable connected to the ES board in slot 9, a redundant cable is connected to the corresponding port on the ES board in slot 19.

26.2.4 Configuring IP Network Interfaces

The Mediant 8000 supports connection to the physically-separated subnets via the use of separate network cables, each cable being connected to its own subnet. The following physical network interfaces configurations are supported:

- *"One: OCM"* – one network interface is used for carrying all types of IP traffic, including OAM (management), Call Control and Media traffic; subnet separation is possible within the interface via the use of VLAN tagging.
- *"Two: OC & M"* – two network interfaces are used, one carrying OAM (management) and Call Control traffic and another one carrying Media traffic; additional subnet separation (on both interfaces) is possible via the use of VLAN tagging.
- *"Two: O & CM"* – two network interfaces are used, one carrying OAM (management) traffic and another one carrying Call Control and Media traffic; additional subnet separation (on "CM" network interface) is possible via the use of VLAN tagging.
- *"Three: O & C & M"* – three network interfaces are used, each one dedicated to a corresponding traffic type – OAM (management), Call Control and Media correspondingly; additional sub-subnet separation is possible via the use of VLAN tagging (e.g. for multiple Media subnets).
- *"Two: OLAN & WAN"* – two network interfaces are used, one carrying OAM (management), Call Control and Media traffic ("OLAN" interface) and another one carrying Call Control and Media traffic ("WAN" interface); additional subnet separation (on both interfaces) is possible via the use of VLAN tagging.
- *"Three: O & LAN & WAN"* – three network interfaces are used, one carrying OAM (management) traffic and another two carrying both Call Control and Media traffic ("LAN" and "WAN" interfaces); additional subnet separation (on "LAN" and "WAN" interfaces) is possible via the use of VLAN tagging.

See 'Ethernet ports allocation on ES boards' on page [217](#) for the exact numbers of network interfaces (ES board ports) used for connecting Mediant 8000 to the external network equipment in each network interfaces configuration.

Figure 26-2: An Example of “Two O & CM” Subnet Configuration

In order to change the IP Network Interfaces configuration, the Media Gateway must be locked and all service on it must be stopped. The new IP network interfaces configuration is not applied immediately; instead you must lock/unlock ES boards and then unlock the Media Gateway as described in 'Activating New Network Interfaces Configuration' on page 214.

➤ **To configure IP Network Interfaces:**

1. Click  to access the Media Gateway status screen.
2. Lock the Media Gateway by clicking **Lock** in the toolbar. In the pop-up dialog, confirm the type of Lock action and click **Yes**.
3. In the Navigation pane, click **Networking** and in the Configuration pane, click **Network Settings**; the Network Settings screen is displayed.
4. In the **Interfaces and VLAN Settings** tab, configure the **Interfaces** parameter.



Note: VLAN table configuration is required only for the ES/6600 switch.

Proceed to the next section 'Working with VLANs' on page [188](#) to define the applicable VLAN IDs for each network interface. Keep the Media Gateway locked, until you complete the network configuration. Apply the new configuration by locking/unlocking ES boards and then unlocking the Media Gateway as described in 'Activating New Network Interfaces Configuration' on page [214](#).

26.2.5 Working with VLANs

A virtual LAN (VLAN) is a logical grouping of nodes which communicate as if they were attached to the broadcast domain, regardless of their physical location. A VLAN has the same attributes as a physical LAN; however it allows end stations to be grouped together even if they are not located on the same network switch.

VLANs are created to provide the segmentation services traditionally provided by routers in LAN configurations. They address the following issues:

- **Scalability** – VLANs facilitate moves, additions, and changes for devices on networks without the need to add additional hardware
- **Security** – Devices in a VLAN can only communicate with devices on the same VLAN.

When working within a VLAN, each Ethernet frame in the VLAN is marked with a VLAN ID (tag). The VLAN ID may be generated by the end-station and carried in the Ethernet frame itself. Or, alternatively, it may be assigned by the Layer 3 switch, based on the port used.

26.2.5.1 Using Tagged VLANs for Subnet Separation

Tagged VLANs may be used to separate traffic belonging to different subnets, transmitted via the same Ethernet cable (port), based on the VLAN ID tag in the Ethernet frame. In addition, the Mediant 8000 may be connected to the IP network that uses VLAN tagging for all Ethernet frames transmitted through it – even though subnet separation is achieved via the use of a separate network interface as described in Configuring IP Network Interfaces.

26.2.5.2 Configuring VLAN Tags

The chapters below describe how to configure VLAN tags for OAM, Media and Control Subnets.

The VLAN tags configuration is handled differently according to the configured ES board:

- **ES/6600:** The new VLAN tags configuration is not applied immediately. Instead you must lock/unlock ES boards and then unlock the Media Gateway as described in 'Activating New Network Interfaces Configuration' on page [214](#).
- **ES-2:** The new VLAN tags are configured in the Subnets entity (see Section 'Configuring VLAN Tags for Media and Control Subnets' on page [189](#) and applied immediately (except for the OAM subnet, which is read automatically from the OAM Tag ID configuration-see Section 'Configuring VLAN Tags for OAM Subnet' on page [189](#)).



Note: When configuring Control and Media Subnets, there is no need to lock/unlock ES boards and then unlock the Media Gateway as described in 'Activating New Network Interfaces Configuration' on page 214.

26.2.5.3 Configuring VLAN Tags for OAM Subnet

VLAN tagging for the OAM subnet primarily affects management traffic carried by SC boards and is typically configured via the CLI interface, while establishing connectivity with EMS server, as described in 'Establishing Connectivity with the EMS Server' on page 180. However, it may also be configured via the EMS GUI as described below:

➤ **To configure VLAN Tags for the OAM Subnet:**

1. Click  to access the Media Gateway status screen.
2. In the Navigation pane, click **Networking** and then in the configuration pane,, click **Network Settings**; the Network Settings screen is displayed.
3. In the **Interfaces and VLAN Settings** tab, configure the **OAM Tag ID** parameter.

26.2.5.4 Configuring VLAN Tags for Media and Control Subnets

VLAN Tagging for Media and Control subnets applies to Media Gateway boards only and doesn't affect SC boards. The Media and Control Subnets VLAN Tags table is used to configure Media and Control VLAN Tagging.

The Media and Control Subnets VLAN tags configuration is handled differently according to the configured ES board:

■ **ES/6600**

For each Media and Control network interface, an entry in the VLAN tags table should be created. This entry indicates the VLAN tag used. For untagged traffic, a default 0 (zero) VLAN tag entry is used. Multiple VLAN tag entries may be created for the same network interface to allow multiple VLAN tags to be carried on the same network interface.

■ **ES-2**

The Media and Control Subnets VLAN tags table is not relevant for this ES board; you cannot configure this table in the Networks Settings screen.

For each Media and Control network interface, an entry in the Subnet table should be created. This entry indicates the VLAN tag used. For untagged traffic, a default 0 (zero) VLAN tag entry is used. Multiple Subnet entries may be created for the same network interface to allow multiple VLAN tags to be carried on the same network interface.

➤ **To configure VLAN Tags for Media and Control Subnets for ES/6600:**

1. Click  to access the Media Gateway status screen.
2. In the Navigation pane, click **Networking** and then in the configuration pane, click **Network Settings**; the Network Settings screen is displayed.

3. In the Interfaces and VLAN Settings tab, go to the Media And Control Subnets VLAN tags section.
4. Use  or  buttons to add or remove VLAN tag entries.
5. For each VLAN tag entry, configure VLAN tag ID and corresponding Network Interface.



Note: The VLAN Tags configuration requires locking of the Media Gateway and consequent locking/unlocking of the ES boards, as described in 'Activating New Network Interfaces Configuration' on page 214. Therefore, consider configuring additional (spare) VLAN tags reserved for future use, to minimize system downtime in case of future network..

➤ To configure VLAN Tags for Media and Control Subnets for ES-2

1. Click  to access the Media Gateway status screen.
2. In the Navigation pane, click **Networking** and then in the configuration pane, click **Subnets**; the Subnet Setting screen is displayed.
3. Use  or  buttons to add or remove VLAN tag entries.



Note: The first Subnet is for the OAM and cannot be removed. In addition, it takes the VLAN Tag ID from the Network Settings configuration (see 'Configuring Network Settings').

4. For each Subnet entry, configure VLAN Tag ID and corresponding Network Interface.



Note: The Subnet configuration does not require the locking of the Media Gateway and consequent locking/unlocking of the ES boards. Only in the event of a change in the OAM VLAN Tag ID at the gateway level requires the locking and unlocking of the gateway.

26.2.6 Media Link Aggregation

The Mediant 8000 uses 1 Gb Ethernet copper ports for connection to IP networks.

When five or more TP-6310 or TP-8410 Media Gateway boards are installed in the chassis, the volume of the generated Media traffic may exceed the capacity of a single 1 Gb Ethernet port. Under such circumstances, link aggregation is supported.

Link aggregation allows up to three physical ports to be aggregated together to form a Link Aggregation Group. This aggregation can then function as if it were a single link, which means that constituent links that would otherwise be blocked as redundant by the Spanning Tree can continue providing increased link capacity. Link Aggregation implementation fully conforms to the *IEEE 802.3ad* specification.

26.2.6.1 Benefits

By taking multiple LAN connections and treating them as a single, aggregated link, the following benefits may be achieved:

- **Increased link capacity:** The total capacity of the aggregated links is the sum of the capacities of the individual links composing the aggregate.
- **Higher link availability:** A properly designed link aggregation scheme will prevent the failure of any single component link from disrupting communication between the interconnected devices. For the Mediant 8000, this additional link availability supplements the regular failover between the redundant links connected to both ES boards.

26.2.6.2 Distribution Rules

The Mediant 8000 supports six different rules for distributing the traffic across the aggregated links. All rules are based on analysis of the specific three bits of the IP packets generated by the Mediant 8000 and must be configured according to the specific details of the IP network to which the Mediant 8000 is connected.

For example, when the **Source IP** distribution rule is configured and two aggregation links are available, packets originating from IP addresses 10.7.1.9 (last three bits 001) and 10.7.1.19 (last three bits 011) will be sent via the first aggregated link, while packets originating from IP addresses 10.7.1.2 (last three bits 010) and 10.7.1.24 (last three bits 000) will be sent via the second aggregated link.

The distribution algorithm for three aggregated links uses proprietary hash-based algorithms to determine links to be used. The algorithm is not configurable by the user; however, ensures that for evenly distributed IP addresses, traffic will be evenly distributed across aggregated links.



Note: It is imperative that you configure the aggregated link distribution rules that match the specific details of the network, where the Mediant 8000 is installed and that ensures that traffic is actually distributed across links. When in doubt, use the recommended settings – **Source IP** – as described below.

Improperly configured distribution rules may lead to all traffic being transmitted via the same single link, leaving other links in the aggregation group unused. This essentially degrades the capacity of the Aggregated Links Group to a single link, which defeats the purpose of the link aggregation.

Aggregated link distribution rules must be configured both on the Mediant 8000 (for outgoing traffic) and on the next-hop network element – Layer 3 switch to which the Mediant 8000 is connected (for incoming traffic). Configuration on the next-hop network element – Layer 3 switch – must be "the opposite of" the Mediant 8000 configuration. For example, if the Mediant 8000 is configured to distribute traffic using the **Source IP** address, the next-hop network element – Layer 3 switch – should be configured to distribute the traffic according to the **Destination IP** address.

The following distribution rules are supported:

- **Source MAC** – packets are distributed based on the last three bits of the Source MAC address; this rule is not recommended for use, since source MAC addresses (of Media Gateway boards) may not be controlled by the user and may not be evenly distributed.
- **Destination MAC** – packets are distributed based on the last three bits of the Destination MAC address; this rule is not recommended for use, since usually the next network element (hop) is a router which is represented by a single MAC address. In such cases, all traffic will be routed via a single link.
- **Source XOR Destination MAC** – packets are distributed based on the last three bits of the Source MAC address XOR'ed with the last three bits of the Destination MAC address; this rule is not recommended for use for the same reasons, the **Source MAC** and **Destination MAC** rules are not recommended for use.
- **Source IP** – packets are distributed based on the last three bits of the Source IP address; this is the recommended distribution policy, assuming that the IP addresses of the Media Gateway boards are allocated consecutively.



Note: Allocate IP addresses for the Media Gateway boards sequentially – e.g. 10.7.1.9, 10.7.1.10, 10.7.1.11 etc. – to ensure optimal traffic distribution across the aggregated links when **Source IP** distribution policy is configured. Do not use any "pattern" in IP addresses allocation. For example, the use of odd IP addresses only – 10.7.1.3, 10.7.1.5 and 10.7.1.7 – will cause an uneven distribution of traffic across the aggregated links. Don't forget to configure "the opposite" distribution policy – based on the **Destination IP** – on the next-hop network element – Layer 3 switch to which the Mediant 8000 is connected.

- **Destination IP** – packets are distributed based on the last three bits of the Destination IP address; this rule is recommended for use when there is communication with a large number of Media Gateway and/or endpoints and their destination IP addresses are evenly distributed.
- **Source XOR Destination IP** – packets are distributed based on the last three bits of the Source IP address XOR'ed with the last three bits of the Destination IP address; this rule is not recommended for use, due to its complexity.

26.2.6.3 Link Aggregation Control Protocol

Link Aggregation Control Protocol (LACP) provides a standardized means of exchanging information between Partner Systems on a link, allowing each system to reach agreement on the identity of the Link Aggregation Group to which the link belongs. Transmission of LACPDUs occurs either as a result of a periodic transmission or as a result of changes to the Actor's state information, which needs to be communicated to the Partner. The periodic transmission may occur at a Short timeout (1 sec.) or a Long timeout (30 sec.), which is determined by the **Link Aggregation Timeout** configuration parameter.



Note: This protocol is only supported for the ES/6600 switch, not for the ES-2 switch.

26.2.6.4 Aggregated Link Failure Detection

Use of aggregated links provides additional availability for an IP network connection. This feature supplements the regular high availability mechanism that switches from one Ethernet Switch (ES) board to another when an uplink failure is detected. For aggregated links, failure detection is performed as follows:

Table 26-1: Aggregated Link Failure Detection

Initial State	Event	Taken Action & New State
1 st ES board is active All 3 aggregated links are up on both ES boards.	Failure of one of the aggregated links on the 1 st ES board.	Switchover to the 2 nd ES board (where all aggregated links are up)
2 nd ES board is active 2 of 3 aggregated links are up on 1 st ES board; all aggregated links are up on the 2 nd ES board.	Failure of one of the aggregated links on the 2 nd ES board.	The Mediant 8000 continues to use the 2 nd ES board as active.
2 nd ES board is active 2 of 3 aggregated links are up on both ES boards.	Failure of another (second) aggregated link on the 2 nd ES board.	The Mediant 8000 continues to use the 2 nd ES board as active (even though the amount of available aggregated links on the 1 st ES board is higher than on the 2 nd ES board).

Initial State	Event	Taken Action & New State
2 nd ES board is active 2 of 3 aggregated links are up on both ES boards.	Failed link on the 1 st ES board returns to service.	Switchover to the 1 st ES board (where all aggregated links are up).

26.2.6.5 Configuring Media Link Aggregation

This section describes how to configure Media Link Aggregation.

➤ To configure media link aggregation:

1. Click  to access the Media Gateway status screen.
2. In the Navigation pane, click **Networking** and then in the configuration pane, click **Network Settings**; the Network Settings screen is displayed.
3. In the **Interfaces and VLAN Settings** tab, configure the link aggregation parameter as described in the table below.

Table 26-2: Media Link Aggregation Settings

Parameter Name	Type	Provisioning Type	Description
Media Aggregation Enable	Enum Disable, Aggregate2, Aggregate3	Online	Defines link aggregation mode for media subnets: ▪ Disable – disable link aggregation (use this configuration when four or less TP-6310 or TP-8410 Media Gateway boards are installed in the chassis) ▪ Aggregate2 – use 2 aggregated links (use this configuration when five to six TP-6310 or TP-8410 Media Gateway boards are installed in the chassis) ▪ Aggregate3 – use 3 aggregated links (use this configuration when more than six TP-6310 or TP-8410 Media Gateway boards are installed in the chassis)

Parameter Name	Type	Provisioning Type	Description
Link Aggregation Distribution Rule. (For ES/6600)	Enum Source MAC, Destination MAC, Source XOR Destination MAC, Source IP, Destination IP, Source XOR Destination IP	Online	Defines rules for traffic distribution across aggregated links.
Aggregation Distribution Rule –For ES-2	Enum Source MAC, Destination MAC, Source XOR Destination MAC, Source IP, Destination IP, Source XOR Destination IP.	Instant	Defines rules for traffic distribution across aggregated links.
Link Aggregation Timeout – for ES/6600 only.	Enum Short, Long	Online	Defines the Link Aggregation Control Protocol (LACP) timeout value: ▪ Short – short timeout (1 sec) ▪ Long – long timeout (30 sec)

26.3 Configuring IP Network Connectivity on SC Boards

The SC boards participate in IP traffic exchange with the management equipment only (EMS server, additional SNMP managers, CLI clients etc). Therefore, they are connected to the OAM (management) subnet only.

Configuration of the SC board's IP network connectivity is performed via the following steps (typically completed as part of establishing connectivity between the Mediant 8000 and the EMS Server:

- Configuring the basic IP network parameters of the SC board – this step configures basic parameters of the OAM subnet (i.e. subnet IP address, mask and default gateway) as well as the private IP addresses of each SC board. See 'Configuring the Basic IP Network Parameters of SC Boards' on page 117 for details.
- Configuring the global (virtual) IP address for SC boards – this step configures the global (virtual) IP address to be used by the active SC board. The address moves from one SC board to another, as their activity is switched over, and is used as a "single point of contact" by all management entities (e.g. EMS or additional SNMP managers). See 'Performing Basic Configuration of the Mediant 8000 Software' on page 146 for details.
- Configuring VLAN tagging for the OAM subnet (if applicable). See 'Configuring VLAN Tags for OAM Subnet' on page 189 for details.



Note: Basic IP Network connectivity on SC boards is typically configured during the Mediant 8000 software installation or initial configuration. There is no need to repeat the configuration, if it has already been completed.

26.3.1 Additional OAM Subnet Configuration

In addition to the above-described configuration, the following additional OAM Subnet parameters may be configured on the Mediant 8000.

The Mediant 8000 may be configured for two additional OAM (management) subnet segments. For each segment, the following parameters must be configured:

- VLAN Tag ID – VLAN tag to be used by this additional OAM (management) subnet segment.
- Subnet Mask – subnet mask of this additional OAM (management) subnet segment.
- SC1 and SC2 IP Addresses – private IP addresses of the SC boards located in Slots 1 and 2 correspondingly in this additional OAM (management) subnet segment.
- Global IP Address – global (virtual) IP address assigned to the active SC board in this additional OAM (management) subnet segment.

➤ **To perform additional configuration of OAM subnet:**

1. Click  to access the Media Gateway status screen.
2. In the Navigation pane, click **Networking** and then in the configuration pane, click **Network Settings**; the Network Settings screen is displayed.
3. In the **Additional OAM Subnet** tab, configure additional OAM subnet parameters as described above.

In addition, Quality of Service (QoS) may be configured for the OAM subnet. See 'Quality of Service' on page 206 for details.

26.4 Configuring IP Network Connectivity on Media Gateway Boards

Media Gateway boards (TP-6310 or TP-8410) send and receive all types of IP traffic: OAM (management), Call Control and Media.

Configuration of the Media Gateway board's IP network connectivity is performed via the following steps:

- Configuring IP subnets for each network segment (subnet) to which the Mediant 8000 is connected. See 'IP Subnets' on page 198 for details.
- Grouping IP subnets into Network Profiles. See 'IP Network Profiles' on page 200 for details.
- Attaching each Media Gateway board to a corresponding Network Profile. See 'Attaching IP Network Profile to the Media Gateway Board' on page 201 for details.
- Configuring Media Gateway board's IP Addresses for each subnet included in the corresponding Network Profile. See 'Configuring Media Gateway Board's IP Addresses' on page 202 for details.

26.4.1 IP Subnets

In the simplest (default) IP network configuration, a single network segment (subnet) is used to transmit all IP traffic to and from the Mediant 8000.

However in more complicated IP network architectures, different segments (subnets) may be used to transmit different types of traffic, as described below:

- **OAM Subnet** – used to transmit management traffic, e.g. SNMP, CLI (SSH), Syslog and NTP.
- **Control Subnets** – used to transmit call control traffic, e.g. MGCP, MEGACO and SIP
- **Media Subnets** – used to transmit media traffic, e.g. RTP.

The Mediant 8000 may be connected to one OAM Subnet, and up to ten Control and Media Subnets. Mixed subnets may be used as well – e.g. a single subnet may be used to transmit both OAM and Control types of traffic. See Types of IP Network Traffic and Network Subnets for details.

For each IP network subnet available on the site to which the Mediant 8000 must be connected, a corresponding configuration object – **Subnet** – must be defined. Each **Subnet** configuration object defines the basic IP subnet properties, such as subnet IP address, subnet mask and default gateway.

Since OAM subnet parameters are configured as part of basic network configuration on SC boards (see 'Configuring IP Network Connectivity on SC Boards' on page 195 for details); a corresponding **Subnet** configuration object (with index 1) is created automatically. This first **Subnet**, describing the OAM subnet, may not be deleted by the user and only its traffic type may be configured as described below.

26.4.1.1 Configuring IP Subnets

This section describes how to configure IP Subnets.

➤ **To configure IP Subnet:**

1. Click the  to access the Media Gateway status screen.
2. In the Navigation pane, select **Networking** ➤ **Subnets**; the Subnets list is displayed.
3. Use  or  buttons to add or remove entries.
4. Select a specific row and then in the configuration pane, click **Subnet Settings**; the Subnet Settings screen is displayed.
5. Configure the Subnet properties according to the 'Subnet Properties' table below.

Table 26-3: Subnet Properties

Parameter Name	Type	Provisioning Type	Description
Subnet Name	String Up to 16 chars.	Online	Defines the textual name assigned to the Subnet, enabling it to be easily identified.
Interface	Enum OCM, CM, OC, C, M, OLAN, LAN, WAN, OAM	Online	Defines the network interface used to connect Mediant 8000 to the specific IP subnet.
Subnet Type	Enum OAM(0), Media(1), Control(2), OAM & Control(4), Media & Control(5), All(6)	Online	Defines type of the IP traffic carried by the subnet.
Interface Mode	Enum IPv4, IPv6	Online	Defines IPv6 or IPv4 address mode.
Subnet IP	String Up to 40 chars.	Online	Defines the subnet IP address.

Parameter Name	Type	Provisioning Type	Description
Subnet Prefix Bit Length	Integer 0-120	Online	Defines the subnet prefix bit length. For IPv4 this is equivalent to specifying Subnet Mask, e.g. Prefix Bit Length = 8 corresponds to Class A Subnet Mask 255.0.0.0.
VLAN Tag ID	Integer 0-3999	Online	Defines the VLAN Tag ID. 0 = untagged 1 – reserved for internal use 2-3999 – VLAN tag to be used
Default Gateway	String Up to 40 chars.	Online	Defines the subnet's default gateway.

26.4.2 IP Network Profiles

The Mediant 8000 uses the term **Network Profile** to describe a set of IP network properties (configurations) that may be assigned to one or more Media Gateway board. This set consists of the following:

- One or more Subnets to which the specific Media Gateway board is connected
- Quality Of Service (QoS) settings
- Media and Control Static Routes table

The same **Network Profile** may be used for all Media Gateway boards (which implies that all Media Gateway boards are connected to the same Control and Media networks). Or alternatively, different **Network Profiles may be used** for different Media Gateway boards (in this case, each board will be connected to its own Control and Media subnets).

The Mediant 8000 installation creates a default **Network Profile** configuration object to which all Media Gateway boards are attached. All **Network Profiles** (both default and added by user) contain first^t **Subnet** configuration object (with index 1) that corresponds to the OAM subnet.

26.4.2.1 Creating IP Network Profile

➤ To define a new Network Profile:

1. Click  to access the Media Gateway status screen.
2. In the Navigation pane, select **Networking** ► **Network Profiles**; the Network Profiles list is displayed.
3. Use the  or  buttons to add or remove entries.
4. Select a specific row and then in the configuration pane, click **Network Profile Settings**; the Network Profile Settings screen is displayed.
5. In the **Network Settings** tab, use the  or  buttons to choose all Subnets that should be part of this network profile.
6. In the **Quality Of Service** tab, configure quality of service (QoS) settings as described in 'Quality of Service' on page 206.

26.4.2.2 Attaching IP Network Profile to the Media Gateway Board

A newly created IP Network Profile must be attached to the corresponding Media Gateway boards.



Note: If you use a similar network configuration for all Media Gateway boards, and therefore use a single Network Profile (created by default), then you do not need to complete the following procedure.

➤ To attach a IP Network profile to the Media Gateway Board:

1. Click  to access the Media Gateway status screen.
2. Select the desired Media Gateway board.
3. In the Actions bar, click **Lock** to stop the service on the Media Gateway board.
4. In the Navigation pane, click **Networking** and then in the configuration pane, click **Network Settings**; the Network Settings screen is displayed.
5. Select the corresponding Network Profile configuration object to be attached to the Media Gateway board.

26.4.3 Configuring Media Gateway Board's IP Addresses

The Media Gateway board must be configured with IP addresses for each IP subnet included in the **Network Profile** attached to it.

➤ To configure Media Gateway Board's IP addresses:

1. Click the  to access the Media Gateway status screen.
2. Select the desired Media Gateway board.
3. In the Actions bar, click **Lock** to stop the service on the Media Gateway board.
4. In the Navigation pane, click **Networking** and then in the configuration pane, click **Network Settings**; the Network Settings screen is displayed.
5. Configure IP addresses for each subnet included in the **Network Profile**, attached to the board (the table is automatically updated when/if the network profile is changed).
6. Configure Primary and Secondary DNS Server if required for each subnet included in the **Network Profile** attached to the board.

26.5 Additional Network Settings

This section describes additional network settings.

26.5.1 Static Routes

Static routes may be used to configure IP routing with entities or network segments to which the Mediant 8000 communicates on a regular basis. Starting from v6.2, default gateways may be configured for each IP subnet, which significantly reduces the need for configuring static routes. Nevertheless, the configuration is still supported for complicated network setups.

Static routes are configured separately for SC and TP boards – as described below. The configuration may be applied instantly – without any adverse effect on the Media Gateway service, by unlocking the corresponding configuration objects.



Note: When the Mediant 8000 wishes to send an IP packet, it scans the static routes table starting from the lowest index; the first entry that matches the IP packet's destination IP address is chosen. Therefore, the order of the entries in the static routes table is very important.

26.5.1.1 Static Routes for SC Boards

Static routes for SC boards are applied simultaneously to both Active and Standby SC boards

➤ **To configure Static Routes for SC Boards:**

1. Click  to access the Media Gateway status screen.
2. In the Navigation pane, select **Networking** ➤ **SC Static Routes**; the SC Static Routes list is displayed.
3. Use the  or  buttons to add or remove entries.
4. Select a specific row and then in the configuration pane, click **SC Static Route Settings**; the Static Route Settings screen is displayed.
5. Configure SC Static Route parameters according to the table below.
6. Click the Maintenance icon  and select **Unlock** to activate the configuration.

Table 26-4: SC Static Route Properties

Parameter Name	Type	Provisioning Type	Description
Destination IP Address	String Up to 40 chars.	Online	Defines the IP Address of the destination entity.
Destination Prefix Length	Integer 0-120	Online	Defines the Prefix Length of the destination entity (for IPv4 addresses this is equivalent to subnet mask). When the Mediant 8000 wishes to send an IP packet, it compares the packet's destination address with the Destination IP Address of each available static route using a Destination Prefix Length for XOR operation on both. If a match is found, the packet will be sent to the static route's Gateway IP Address.
Gateway IP Address	String Up to 40 chars.	Online	Defines the Gateway IP Address to which packets to the destination entity will be routed.
Comment	String Up to 200 chars.	Instant	Defines the user-defined comment for specific static route.

26.5.1.2 Static Routes for Media Gateway (TP) Boards

Static routes for Media Gateway (TP) boards are defined as part of **Network Profile** and applied to all Media Gateway boards attached to the specific Network Profile.



Note: Starting from v6.2, Media Gateway (TP) boards implement 'strong-end' routing behavior, making routing decision based on the source subnet/VLAN. This implies that the TP board's static routes may not be used to "leak" packets from one subnet/VLAN to another.

➤ To configure Static Routes for Media Gateway (TP) Boards:

1. Click  to access the Media Gateway status screen.
2. In the Navigation pane, select **Networking** ➤ **Network Profiles**; the Network Profiles list is displayed.
3. Select a specific Network Profile.
4. In the Navigation pane, click **TP Static Routes**; the TP Static Routes list is displayed.

5. Use the  or  buttons to add or remove entries.
6. Select a specific row and then in the configuration pane, click **TP Static Route Settings**; the Static Route Settings screen is displayed.
7. Configure TP Static Route parameters according to the table below.
8. Click the Maintenance icon  and select **Unlock** to activate the configuration.

Table 26-5: TP Static Route Properties

Parameter Name	Type	Provisioning Type	Description
Network Subnet	Integer 0-10	Instant	Defines the Network Subnet to which the specific static route applies.
Destination IP Address	String Up to 40 chars.	Instant	Defines the IP Address of the destination entity.
Destination Prefix Length	Integer 0-128	Instant	Defines the Prefix Length of the destination entity (for IPv4 addresses this is equivalent to subnet mask). When the Mediant 8000 wishes to send an IP packet, it compares the packet's destination address with the Destination IP Address of each available static route using a Destination Prefix Length for XOR operation on both. If a match is found, the packet will be sent to the static route's Gateway IP Address.
Gateway IP Address	String Up to 40 chars.	Instant	Defines the Gateway IP Address to which packets to the destination entity will be routed.
Comment	String Up to 200 chars.	Instant	Defines the user-defined comment for specific static route.

26.5.2 Quality of Service

Quality of Service (QoS) features are used in multi-service networks to distribute available (limited) network resources across multiple applications and to guarantee the best applicable service to all of them. The Mediant 8000 supports the following QoS features:

- Ethernet frame priority header – as per IEEE 802.1p and 802.1q
- Differentiated Services (DiffServ) – as per RFC 2747, 2475 and 3260.

The Mediant 8000 adopts commonly-used classification of IP network traffic into "service classes" as follows:

Table 26-6: Network Service Classes

Service Class	Description	Tolerance to:		
		Loss	Delay	Jitter
Critical	Network-to-network device communications within an administrative domain like heartbeats between routers/switches. Not applicable to the Mediant 8000.	Very Low	Very Low	N/A
Network	Communications between network devices within one administrative domain. The following Mediant 8000 management protocols belong to this category: ICMP, DNS, NTP.	Low	Low	N/A
Premium	Telephony service. All call control and media traffic sent/received by the Mediant 8000 belongs to this category.	Very Low	Very Low	Very Low
Platinum	Used for video conferencing and interactive gaming. Not applicable to the Mediant 8000 .	Low	Low	Low
Gold	Used for Voice Streaming, Video on demand Broadcast TV, Video surveillance. HTTP streaming traffic, generated by the Mediant 8000, falls under this category.	Med-Low	Med-High	High
Silver	Used for fast response for TCP and HTTP short lived flows such as Credit card transactions. Not applicable to the Mediant 8000 .	Low	Low-Med	N/A
Bronze	Used for long-lived TCP, and HTTP flows such as Non time-critical OAM&P, Email, Instant Messaging. The following Mediant 8000 management protocols belong to this category: SNMP, SSH (CLI), HTTP (for WEB interface).	Low	Med-High	N/A

Service Class	Description	Tolerance to:		
		Loss	Delay	Jitter
Standard	Used for all traffic that has not been characterized into one of the other service classes and for Best effort applications. Not applicable to the Mediant 8000 .	Med	High	N/A

26.5.2.1 Ethernet Frame Priority Header

The Mediant 8000 supports Ethernet frame Priority header as defined in the IEEE 802.1p and 802.1q standards. 3-bit priority value (from 0 to 7) may be assigned to each network service class, applicable to the Mediant 8000 .

Ethernet Switch (ES) boards are configured to strictly prioritize processed traffic, based on the Priority header. Packets with a higher priority value will be processed prior to packets with a lower priority (within the same VLAN).



Note: Ethernet Frame Priority Header configuration will be activated only when VLAN tagging is enabled for the corresponding subnet. See 'Working with VLANs' on page 188 for details.

The Ethernet Frame Priority Header may be configured as follows:

- For OAM subnet (Network, Gold and Bronze service classes) – open the Media Gateway's **Network Settings** configuration screen and configure parameters in the **Quality Of Service** tab.



Note: This feature is not supported for an SC board configured with the ES-2 switch (only supported for the ES/6600 switch). In the case of the Media Gateway board, both ES boards are supported.

- For Media and Control subnets – open Network Profile's configuration screen and configure parameters in the **Quality Of Service** tab.

26.5.2.2 Differentiated Services (DiffServ)

Differentiated Services (DiffServ) is an alternative QoS architecture that is defined in the following IETF standards:

- RFC 2474 – Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
- RFC 2475 – An Architecture for Differentiated Services
- RFC 3260 – New Terminology and Clarifications for Diffserv

DiffServ utilizes Differentiated Services Field (DS Field) in the IP header to indicate the service level of the corresponding IP packet. The Mediant 8000 supports definition of this DS Field (values from 0 to 63) for each supported network service class.

The DiffServ Field value may be configured as follows:

- For OAM subnet (Network, Gold and Bronze service classes) – open the Media Gateway's **Network Settings** configuration screen and configure parameters in the **Quality Of Service** tab.
- For Media and Control subnets – open the Network Profile's configuration screen and configure parameters in the **Quality Of Service** tab.

Table 26-7: Media Gateway Quality Of Service Settings

Parameter Name	Type	Provisioning Type	Description
Network Service Class Priority	Integer 0 – 7	Online	Defines Layer 2 Class Of Service (as per IEEE 802.1P) for the Network service class, applied to DNS, DHCP, ICMP, etc.
Gold Service Class Priority	Integer 0 – 7	Online	Defines Layer 2 Class Of Service (as per IEEE 802.1P) for the Gold service class applied to voice streaming.
Bronze Service Class Priority	Integer 0 – 7	Online	Defines Layer 2 Class Of Service (as per Q802.1P) for the Bronze service class, applied to the management traffic.
Network Service Class Diff Serv	Integer 0 – 63	Online	Defines Layer 3 Quality Of Service for Network service class, applied to DNS, DHCP, ICMP, etc.
Gold Service Class Diff Serv	Integer 0 – 63	Online	Defines Layer 3 Quality Of Service for Gold service class, applied to voice streaming.

Parameter Name	Type	Provisioning Type	Description
Bronze Service Class Diff Serv	Integer 0 – 63	Online	Defines Layer 3 Quality Of Service for Network service class, applied to management traffic.

Table 26-8: Network Profile Quality Of Service Settings

Parameter Name	Type	Provisioning Type	Description
Premium Control Priority	Integer 0-7	Online	Defines Layer 2 Class Of Service (as per IEEE 802.1P) for the Premium service class, applied to call control traffic.
Premium Control Diffserv	Integer 0-63	Online	Defines Layer 3 Quality Of Service for the Premium service class, applied to call control traffic.
Premium Media Priority	Integer 0-7	Online	Defines Layer 2 Class Of Service (as per IEEE 802.1P) for the Premium service class, applied to media traffic.
Premium Media Diffserv	Integer 0-63	Online	Defines Layer 3 Quality Of Service for the Premium service class, applied to media traffic.

26.5.3 Configuring IPv6

The Internet Protocol version 6 (IPv6) is a next-generation internet protocol version designated as a successor to version 4, IPv4 (also known as IP and the presently dominant implementation used in the Internet and corporate LANs).

The Mediant 8000 currently provides support for IPv6 only in Call Control and Media Subnets.

➤ To configure IPv6 for a Control or Media Subnet, take the following steps:

1. Configure the Control or Media Subnet, as described in 'IP Subnets' on page 198. Set **Interface Mode** to *IPv6* and configure the corresponding **IPv6 Subnet Address** and **Subnet Prefix Bit Length** parameters.
2. Configure the IP Network Profile, as described in 'IP Network Profiles' on page 200. Attach the IPv6 Control or Media Subnet (configured in step 1) to this profile and configure the **IPv6 Default Gateway** parameter.
3. Attach the IP Network Profile to the Media Gateway boards and configure the Media Gateway Board's IPv6 addresses, as described in 'Attaching IP Network Profile to the Media Gateway Board' on page 201.

26.5.4 Configuring Media Realms

Media Subnets may be divided into several Realms, where each realm is specified by an UDP port range. Once the Realm has been created, it can be assigned to other elements – e.g. SIP IP Group.

➤ To configure Media Realms, take the following steps:

1. Click  to access the Media Gateway status screen.
2. Select the desired Media Gateway board.
3. In the Navigation Pane, select **Network** ► **Media Realms**; the Media Realm list is displayed.
4. Use the  or  buttons to add or remove entries.
5. Select a specific row and then in the configuration pane, click **Board Realm Settings**; the Board Realm Settings screen is displayed.
6. Configure the Media Realm parameters according to the 'Media Realm Setting' table below.
7. Click the Maintenance icon  and select **Unlock** to activate the configuration.

Table 26-9: Media Realm Settings

Parameter Name	Type	Provisioning Type	Description
Media Realm Name	String Up to 63 chars	Offline	Defines textual name of the Media Realm enabling user to easily identify it.
IPv4 Subnet	Integer 0-10	Offline	Defines the IPv4 Subnet associated with this Realm.
IPv4 Subnet Name	String Up to 14 chars	Read-Only	Indicates name of the IPv4 Subnet associated with this Realm.
IPv6 Subnet	Integer 0-10	Offline	Defines the IPv6 Subnet associated with this Realm.
IPv6 Subnet Name	String Up to 14 chars	Read-Only	Indicates name of the IPv6 Subnet associated with this Realm.
Port Range Start	Integer -1-60000	Offline	Defines the starting port for the range of Media Subnet UDP ports. Value -1 defines Media Realm without port range. Notes: All Media Realms must be configured either with or without a port range (not specific realms with a port range and specific realms without) Ranges of Media Realms must not overlap.
Media Session Amount	Integer -1-6000	Offline	Defines the number of media sessions associated with the range of ports. Ports are allocated in groups of 10. Hence, for example, 10 media sessions correspond to 100 ports.
Port Range End	Integer -1-60000	Read-only	Displays the ending port for the range of Media Subnet UDP ports
Is Default	Enum No, Yes	Offline	Enables the user to determine whether or not a Media Realm is set as default.

26.6 Additional Network Services and Settings

The tables below describe additional network settings that may be configured in the Media Gateway or Media Gateway board's network configuration screens.

Table 26-10: Additional Media Gateway Board Network Settings

Parameter Name	Type	Provisioning Type	Description
ARP Table Max Entries	Integer 64 – 2084	Instant	Defines the maximum number of entries in the TCP/IP Address Resolution Protocol (ARP) table. The entries show the mappings of IP addresses to MAC addresses.
DNS Request Timeout Seconds	Integer 1 – 100	Instant	Determines the time (in seconds) to wait before retransmitting a DNS request.
Number of DNS Request Retries	Integer 1 – 100	Instant	Determines the number of times to retransmit DNS requests; after this number of retries, the gateway attempts to connect to the secondary DNS server IP.
ARP Aging	Enum Disable, Enable	Instant	Defines whether the aging mechanism is applied to the entries in the Address Resolution Protocol (ARP) table as described below. If disabled, the ARP (Address Resolution Protocol) table will be static and no ageing occurs. A MAC address entered into the table will never be dropped from it, until the board is reset. When the table is full (when the value defined for parameter ARP Table Max Entries is exceeded), the board will not learn new MAC addresses. If enabled, old addresses are 'aged out' and discarded.
Media ARP Cache override	Enum Disable, Enable Media, Enable GARP, Enable Media Or GARP	Online	Defines whether the board should override (update) the ARP cache on detection of an incoming RTP stream from a changed remote MAC address and/or detection of GARP message.
SCTP Checksum Method	Enum Adler 32, CRC32c	Online	Defines the SCTP checksum method.

Parameter Name	Type	Provisioning Type	Description
NAT Mode	Enum Enabled, Disabled	Instant	Enables / disables the Network Address Translation (NAT) mechanism. Note: The compare operation that is performed on the IP address is enabled by default and is controlled by the parameter IP Address Translation. The compare operation that is performed on the UDP port is disabled by default and is controlled by the parameter UDP Port Translation.
IP Address Translation	Enum Disable, Enable	Instant	Enables / disabled the IP address translation for RTP, RTCP, and T.38 packets. When enabled, the device compares the source IP address of the first incoming packet to the remote IP address stated in the opening of the channel. If the two IP addresses don't match, the NAT mechanism is activated. Consequently, the remote IP address of the outgoing stream is replaced by the source IP address of the first incoming packet. Note: for this parameter to take effect the NAT mechanism must be enabled (via the parameter NAT Mode).
UDP Port Translation	Enum Disable, Enable	Online	Enables / disabled the use of UDP port when performing IP address translation for RTP, RTCP, and T.38 packets. Note: for this parameter to take effect, the NAT mechanism must be enabled (via the parameter NAT Mode) and the IP address translation must be enabled (via the parameter IP Address Translation).

26.6.1 Activating New Network Interfaces Configuration

The new IP network configuration is activated by unlocking all relevant entities (e.g. Media Gateway, Media Gateway boards) etc. To simplify the network configuration, all "intermediate" configuration objects (e.g. **Subnet** and **Network Profiles**) do not require an explicit unlock – instead, they are automatically unlocked when the corresponding Media Gateway board is unlocked.

26.6.1.1 Offline Network Configuration of ES/6600

Configuration of network interfaces separation and VLAN tags must be performed when the Media Gateway is locked. It is not applied immediately –only when **lock** and **unlock** maintenance actions are performed on both Ethernet Switch (ES) boards. Users who modify the affected configuration will be forced to perform lock/unlock of the ES boards prior to unlocking the Media Gateway (EMS and CLI management interfaces will produce a corresponding warning when the user attempts to unlock the Media Gateway).

The ES board is reset as part of the **unlock** action and it may take up to 10 minutes till it completes the reset and returns to service. Lock/unlock actions must be performed on ES boards sequentially (one at a time) in the following order:

- Lock the ES boards in both Slots 9 and 19
- Unlock the ES board in Slot 9 and wait until it completes the restart and returns to service.
- Unlock the ES board in Slot 19 and wait until it completes the restart and returns to service.

See 'Activating Offline Network Configuration' on page [216](#) for details.

26.6.1.2 Offline Network Configuration of ES-2

Configuration of network interfaces separation and the OAM VLAN tag must be performed when the Media Gateway is locked. After you then unlock the Media Gateway, the OAM VLAN tag is applied immediately to all unlocked ethernet switches (Locked ethernet switches are not configured).



Note: It is recommended to lock both ethernet switches before changing such a configuration; however, in the case of expert users the ESs boards can remain unlocked. In the latter case, when unlocking the Media Gateway board, both ESs are automatically configured with the new QAM VLAN Tag ID. As a consequence, connection with the external Switch/Router is lost until the VLAN ID is configured on the external Switch/Router side.

➤ **To activate the OAM VLAN tags:**

■ **While both ESs are unlocked (for expert users):**

When unlocking the Media Gateway, both ethernet switches are configured with the new OAM VLAN tag. The user must then separately configure the external Switch/Router to support the same VLAN ID (the connection with the chassis is lost until the user configures the external Switch/Route with the new VLAN ID).

■ **While both ES are locked:**

1. Lock the ES boards in both slots 9 and 19.
2. Configure the OAM VLAN Tag (see Section 'Configuring VLAN Tags for OAM Subnet' on page 189).
3. Unlock the ES board in slot 9 (variable needed) and wait until it completes the restart and returns to service.
4. Unlock the ES board in slot 19 (variable needed) and wait until it completes the restart and returns to service.

See Section 'Activating Offline Network Configuration' on page 216 for details.

26.6.1.3 Online Network Configuration

The remainder of the network configuration may be performed online, with minimal affect on the Media Gateway service. Only the entities to which the modified configuration applies are affected (and typically must be locked and unlocked to activate the new configuration). The rest of the Media Gateway entities remain unlocked and continue to provide the service.

The following examples demonstrate the online network configuration capabilities of the Mediant 8000:

- Changing the IP address of the specific IP subnet – only the Media Gateway boards, attached to the specific IP subnet are affected.
- Modifying static routes table – configuration is performed instantly without the need to stop service on either the SC or TP boards.

26.6.2 Activating Offline Network Configuration

➤ To activate the offline network configuration:

1. Click the  button to access the Media Gateway status screen.
2. Right-click the ES board in slot 9 and choose **Maintenance -> Lock**.
3. Right-click the ES board in slot 19 and choose **Maintenance -> Lock**.
4. Right-click the ES board in slot 9 and choose **Maintenance -> Unlock**. The board will be reset and its **Operational State** will be changed to *Disabled* (board will be colored *Red* in the EMS GUI).
5. Wait till the ES board in slot 9 completes the restart. This may take up to 10 minutes. When the ES board returns to service, its **Operational State** is changed to *Enabled* and the board's color is changed to *Green* in the EMS GUI.
6. Repeat steps 4-5 on the ES board in slot 19.



Note: After applying the new IP network configuration, connectivity between the Mediant 8000 and the EMS server may be lost, due to the changes in interface separation configuration and consequent changes in the ES board's Ethernet ports allocation. If such a change occurs, connectivity will be lost as soon as you unlock the 2nd ES board. To restore connectivity, re-connect IP network cables to appropriate ES board's Ethernet ports as described in 'Connecting the Mediant 8000 to the IP Network' on page [217](#).

26.7 Connecting the Mediant 8000 to the IP Network

After completing the new network configuration and activating it, re-connect the network cables to the appropriate ES board's Ethernet ports and/or connect additional cables to match the configured interface separation as described in 'Configuring Network Topology' on page 182.

26.7.1 Ethernet Ports Allocation on the ES/6600 Board

Each ES board features six 1Gb Ethernet copper ports, available on the corresponding ES/6600/RTM board, located in the rear of the chassis. Use of the Ethernet Ports depends on the configured interface separation as described in 'Configuring Network Topology' on page 182.

Table 26-11: Ethernet Ports Allocation on ES/6600 Boards

Interface Separation	ES boards Ports Allocation
"One: OCM" (default configuration)	Use Port 20 for connection to the IP network. If Link Aggregation is enabled, use Ports 21 and 22 for additional connection to the IP network.
"Two: OC & M"	Use Port 18 for connection to the OAM (management) and Call Control network. Use Port 20 for connection to the Media network. If Link Aggregation is enabled, use Ports 21 and 22 for additional connection to the Media network.
"Two: O & CM"	Use Port 18 for connection to the OAM (management) network. Use Port 20 for connection to the Call Control and Media network. If Link Aggregation is enabled, use Ports 21 and 22 for additional connection to the Call Control and Media network.
"Three: O & C & M"	Use Port 18 for connection to the OAM (management) network. Use Port 19 for connection to the Call Control network. Use Port 20 for connection to the Media network. If Link Aggregation is enabled, use Ports 21 and 22 for additional connection to the Media network.

Interface Separation	ES boards Ports Allocation
Two: OLAN & WAN	Use Port 20 for connection to the LAN network, that carries OAM (management), Call Control and Media traffic. Use Port 22 for connection to the WAN network, that carries Call Control and Media traffic. If Link Aggregation is enabled, use Port 21 and for additional connection to the LAN network.
Three: O & LAN & WAN	Use Port 18 for connection to the OAM (management) network. Use Port 20 for connection to the LAN network, that carries Call Control and Media traffic. Use Port 22 for connection to the WAN network, that carries Call Control and Media traffic. If Link Aggregation is enabled, use Port 21 and for additional connection to the LAN network.

26.7.2 Ethernet Ports Allocation on ES-2-SINGLE boards

Each ES board features nine 1Gb Ethernet copper ports, available on the corresponding ES-2 /RTM board, located in the rear of the chassis. Use of the Ethernet Ports depends on the configured interface separation as described in 'Configuring IP Network Interfaces'.

Table 26-12: Ethernet Ports Allocation on ES-2 Boards

Interface Separation	ES boards Ports Allocation
"One: OCM" (default configuration)	Use Port 1 for connection to the IP network. If Link Aggregation is enabled, use Ports 2 and 3 for additional connection to the IP network.
"Two: OC & M"	Use Port 1 for connection to the OAM (management) and Call Control network. Use Port 3 for connection to the Media network. If Link Aggregation is enabled, use Ports 4 and 5 for additional connection to the Media network.
"Two: O & CM"	Use Port 1 for connection to the OAM (management) network. Use Port 3 for connection to the Call Control and Media network. If Link Aggregation is enabled, use Ports 4 and 5 for additional connection to the Call Control and Media network.
"Three: O & C & M"	Use Port 1 for connection to the OAM (management) network. Use Port 2 for connection to the Call Control network. Use Port 3 for connection to the Media network. If Link Aggregation is enabled, use Ports 4 and 5 for additional connection to the Media network.
Two: OLAN & WAN	Use Port 1 for connection to the LAN network, that carries OAM (management), Call Control and Media traffic. Use Port 5 for connection to the WAN network, that carries Call Control and Media traffic. If Link Aggregation is enabled, use Port 2 and for additional connection to the LAN network.

Interface Separation	ES boards Ports Allocation
Three: O & LAN & WAN	Use Port 1 for connection to the OAM (management) network. Use Port 2 for connection to the LAN network, that carries Call Control and Media traffic. Use Port 5 for connection to the WAN network, that carries Call Control and Media traffic. If Link Aggregation is enabled, use Port 3 and for additional connection to the LAN network.

26.7.3 External Layer 3 Ethernet Switches or Routers

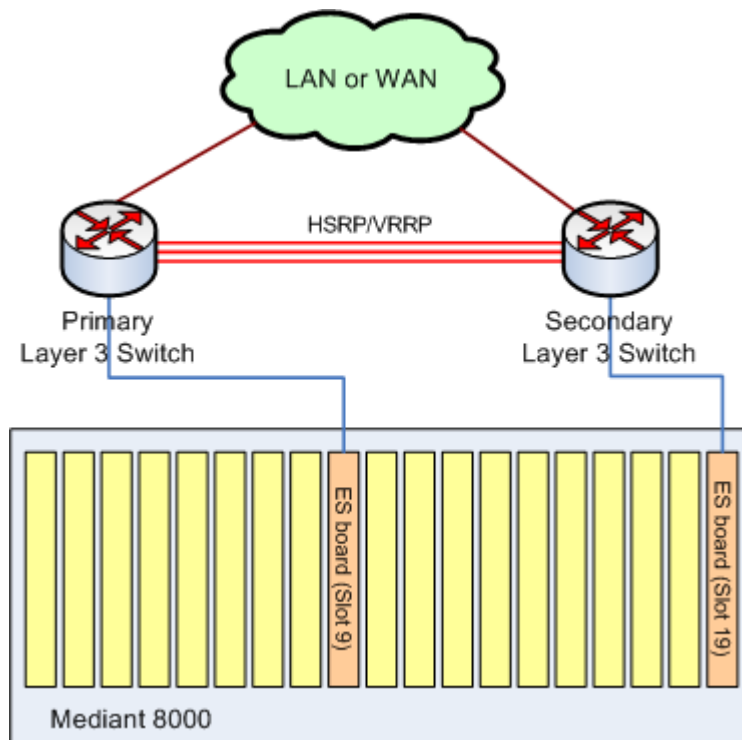
At least two external fully-redundant Layer 3 ethernet switches or routers are required for connecting the Mediant 8000 to the IP network.



Note: When multiple physically-separated subnets are used, it is possible to either use the same properly-configured external Layer 3 switch for multiple subnets or use separate Layer 3 switches for each subnet.

Uplinks of the two available Ethernet Switch (ES) boards (located in slots 9 and 19) must be connected to a corresponding external Layer 3 Switch or Router as shown in the figure below. Ensure that you connect all relevant uplinks on both ES boards, as described in 'Ethernet ports allocation on ES boards' on page 217.

Figure 26-3: Ethernet Port Allocation



External Layer 3 switches or routers must be configured with the same IP addresses. They must be interconnected at Layer 2 and support non-disruptive failover of IP traffic in case of the failure of one of them. HSRP (Hot Standby Router Protocol – as per RFC 2281) or VRRP (Virtual Router Redundancy Protocol – as per RFC 3768) should be configured on the external Layer 3 Switch or Router for this purpose.



Note: In a temporary lab environment, it is possible to connect uplinks of both ES boards to the same external Layer 3 Switch or Router. However such a configuration does not provide redundant IP network connection for the Mediant 8000 and therefore should not be used for live deployments.

26.7.3.1 Configuring HSRP/VRRP Protocols on External Layer 3 Switches

The following HSRP/VRRP configuration should be performed on the external Layer 3 switches to which the Mediant 8000 is connected:

- The HSRP/VRRP routing between the external Layer 3 switches should be configured per VLANs and not per port.
- The HSRP/VRRP switches priority should be configured with the outside network ports (connected to the WAN) and not with the inside network ports (connected to the Mediant 8000). This configuration ensures the proper Layer 3 switches activity switchover in case of a switch failure. When the priority is properly set and both external Layer 3 switches are up, the switch with the higher priority assigned, functions as the "active switch".

For detailed instructions on the HSRP/VRRP configuration on external Layer 3 switches, see the vendor-specific documentation of the equipment being used.

See 'Appendix - Configuring HSRP/VRRP' on page 889 for an example configuration of a CISCO Layer 3 switch network.

26.7.3.2 Configuring the Mediant 8000 for the HSRP Protocol

When the Mediant 8000 is connected to the Layer 3 switches clustered via the HSRP protocol, configure **Media ARP Cache Override** parameter to *Enable GARP* in the Media Gateway board's Network Settings configuration screen. This setting ensures that Media Gateway board's ARP cache is updated only when Gratuitous ARP packets are received and avoids excessive CPU utilization on Media Gateway boards in case of ES boards or external Layer 3 switches failover.

27 Working with the SC Boards

The SC (System Controller) boards provide a management interface to the Mediant 8000 and are responsible for system configuration, status monitoring and high-availability operations.

SC boards do not participate in VoP (call control and media) traffic, handled by the TP-6310 and the TP-8410 Media Gateway boards. Instead they operate as a “host” of the Mediant 8000 chassis, managing the configuration of all chassis elements (including Media Gateway boards), constantly monitoring the health status of all hardware components and reporting any malfunction to the management stations. All management operations (configuration, fault and status monitoring) are performed through the SC boards.

See the 'System Controller (SC) Board' for a detailed description of the SC board's hardware.

27.1 Redundancy Mode

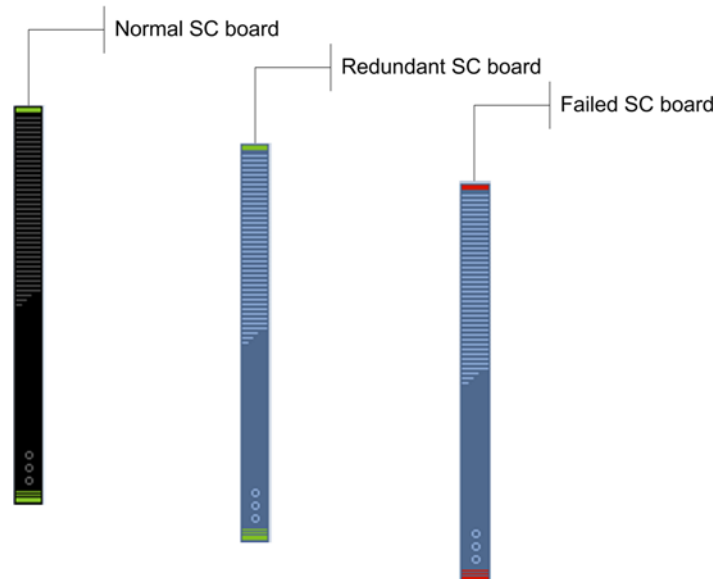
There are two SC boards in the chassis, installed in slots 1 and 2. Each board has a local IP address (in the OAM subnet). The two SC boards operate in an asymmetric 1+1 redundant mode. At any time, one of the SC boards operates as the Active board and performs chassis management tasks, while the other SC board operates as the Standby board. A Global IP address (also belonging to the OAM subnet) is assigned to the Active SC board to provide a "single point of contact" for SNMP and CLI management.

When the Active SC board fails, the Standby SC board takes over activity and becomes the Active one. The Global IP address is moved to the new Active SC board during activity switchover.

27.2 SC Boards in the EMS

In the EMS, the Active SC board is colored *black*, while the Standby SC board is colored *blue-gray*. The SC board in slot 1 is initially the Active SC board (upon chassis power up) and the SC board in slot 2 is initially the Standby SC board.

Figure 27-1: SC Boards in EMS



The status of the SC boards is represented by a standard **Operational State**, **Administrative State** and **Severity** attributes.

- When the SC board is functioning properly, its **Operational State** is set to *Enabled*, **Severity** is set to *Clear* and in the EMS, the SC board is colored *green*.
- When the SC board's functionality is degraded, an alarm indicating the problem details is generated and board's **Severity** is set according to the alarm's severity. In the EMS board is colored *blue*, *yellow* or *orange*, according to the *Severity* value.
- When the SC board is not functioning properly (or is absent), its **Operational State** is set to *Disabled* and in the EMS, the SC board is colored *red*.
- When the SC board is locked, its **Administrative State** is set to **Locked** and in the EMS, the SC board is colored *grey*.

27.3 SC Board Actions

The following actions can be performed on an SC board and are available in the EMS when you right-Click the specific SC board in the Media Gateway status screen:

- **Switchover** – applicable to the Active SC only. The activity of the SC boards is switched; the Standby SC becomes the Active SC). The software on the initially Active SC board is re-started during the switchover action. It may take up to 2 minutes before it returns back to service (as the Standby SC board).
- **Lock** – take the SC board out of service.



Note: The locked SC board permanently stays in the Standby state, even when another SC board fails. Therefore, use the lock action with great caution.

- **Unlock** – bring locked SC board back to service. SC board is rebooted during the **unlock** action and it may take up to 5 minutes before it returns back to service.

27.4 SC Board Hardware Revisions

The following hardware revisions of the SC boards may be installed in the Mediant 8000 chassis:

- SC Rev.1 board – based on the SUN CP2300 SBC and using the SUN Solaris OS
- SC Rev.2 board – next-generation SC board, based on the Intel CPU and using the Linux OS

See 'System Controller (SC) Board' on page 63 for details.

To determine the hardware revision of SC boards installed in your chassis, open the SC Board Provisioning frame, by double-clicking on the SC board in the EMS main status screen, and verify the **OS Name** parameter value. Value “SunOS” corresponds to the SC Rev.1. Value “Linux” corresponds to the SC Rev.2.



Note: Both SC boards installed in the chassis must be of the same hardware revision. Do not mix SC boards of different hardware revisions (SC Rev.1 and SC Rev.2) in the same chassis.

27.5 The Operating System on the SC Boards

Each SC board has a generic operating system installed on it. The exact version of the operating system (OS) depends on the hardware revision of the specific SC board:

- SC board Rev.1 (SC Rev.1) – uses the SUN Solaris 9 OS
- SC board Rev.2 (SC Rev.2) – uses the Linux OS

The Operating system is installed on the SC boards during the manufacture process and is specifically configured for optimal performance of the Mediant 8000 software. The Mediant 8000 software automatically configures all required OS services and provides optimized user-friendly CLI commands for optional configuration (e.g. the tools user command is provided for user management). No additional “administration tasks” are required on the SC boards. Moreover, any attempt to modify the default OS configuration or install additional software on SC boards will be dealt with as a malicious action and reported as a “Security Alarm” – since it may potentially affect the normal operation of the Mediant 8000 software (see 'File System Integrity Check' on page 316 for details).



Note: Do not perform any “generic OS administration” on the SC boards (e.g. do not enable/disable OS services and do not modify the default OS configuration files). The Mediant 8000 software automatically configures the underlying OS for optimal performance and may not be able to operate correctly if the OS configuration is modified.

All relevant OS security and bug fixes are delivered as part of the Mediant 8000 software installation package. See 'Installing Mediant 8000 Software' on page 129 and 'Online Software Upgrade' on page 811 for details.

The OS (re)installation on the SC board is therefore a very uncommon process that is typically performed in the following cases:

- During the initial SC board installation (typically in a production environment or after hard disk replacement).
- When the OS installation and/or configuration is damaged by a malicious user or virus software.

27.6 Installing the Solaris OS on the SC Rev.1 Board

The SC Rev.1 boards uses a special version of the SUN Solaris 9 TM operating system, provided by AudioCodes and configured for optimal Mediant 8000 hardware and software performance. For a typical SC board that is preinstalled with a correct version of the SolarisTM OS, there is no need to re-install it.



Note: When it becomes necessary to re-install the SolarisTM OS on SC boards, it is important to use the Solaris OS installation image that is provided by AudioCodes.

27.6.1 Verifying the Current Version of the Solaris OS on the SC Board

Version 6.6 of the Mediant 8000 software requires the SUN Solaris 9 TM version 9/04 or later.

➤ **To access the current version of the SolarisTM OS:**

1. Connect to the SC board's CLI Interface. For more information, see Section 'Command Line Interface' on page [107](#).
2. Login as **root** user. For more information, see Section 'Logging in as a Root User' on page [115](#).
3. At the prompt, type **cat /etc/version** and press **Enter**. The current SolarisTM OS version is displayed.
4. Verify that the SolarisTM OS version matches the version required by the specific Mediant 8000 software.

27.6.2 Installation Requirements

Installation of the Solaris™ OS on SC boards is performed via the network. The Solaris™ OS Installation image must be placed on an Install Server that fulfills the following requirements:

- Solaris™ 8 2/02 or later
- CD-ROM Drive
- At least 2 Gb free disk space in the root file system
- Resides on the same subnet as the Mediant 8000

AudioCodes recommends using the EMS server as the *Install server*.



Note: The Install server must reside on the same LAN subnet as the Mediant 8000 (i.e., it must be connected to the same Ethernet Switch).

The installation is to be performed on the SC board while it resides in the Mediant 8000 chassis. In addition, the SA/RTM must also be in place behind the SC board during the installation process.

27.6.3 Preparing the 'Install Image' on the Install Server (EMS)

Prior to installing the Solaris OS on the SC board for the first time, the "Install Image" must be created on the Install server (EMS). Once created, the "Install Image" may be used for multiple SC board installations.

➤ **To prepare the 'Install Image':**

1. Insert the Solaris™ 9 OS 'Install Image' CD into the Install Server's (EMS) CD-ROM drive.
2. Login to the Install Server (EMS) via Telnet, SSH or X-terminal as the **root** user.
3. At the prompt, change the directory to the CD-ROM's root.

```
EMS-Server8:/ [root] => cd /cdrom/cdrom0
```

4. If there is no directory, "cdrom0", type the command, eject and try again.

```
EMS-Server8:/ [root] => eject
```

5. To run the 'install' script, at the prompt, type **./install** and press **Enter**.

```
EMS-Server8:/cdrom/cdrom0 [root] => ./install
```

The Install image creates a **/jumpstart** directory that is shared over the network.



Note: For correct Install server operation, the following services must be enabled on it:

- TFTP
- RARP
- BOOTPARAMS
- TIME

If you use the EMS server as the Install server, login to the EMS server and in the EMS Server Manager, choose the option “Enable Jumpstart Server” to enable these services.

If you use the EMS server as the Install server, use the options in the EMS Manager to enable these services.

27.6.4 Installing the Solaris 9 OS on the SC Board

➤ **To install the Solaris™ 9 OS on the SC boards:**

1. Connect to the Active SC board's CLI interface via RS-232 Console. For more information, see Section 'Command Line Interface' on page 107.
2. Login as the **root** user (the default password is **root**).
3. Type **ifconfig -a** and press **Enter** to identify the SC hostname, IP address and MAC address of the SC board.

Sample values are shown in red in the example below.

```
client224:~# ~ => ifconfig -a
lo0: flags=1000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
inet 127.0.0.1 netmask ff000000
dmfe0: flags=1000863<UP,BROADCAST,NOTRAILERS,RUNNING,MULTICAST,IPv4> mtu
1500 index 2
inet 10.7.13.94 netmask ffff0000 broadcast 10.7.255.255
ether 0:3:ba:78:8e:65
```

4. Type **sync**; halt and press **Enter** to drop the SC board to the OpenBoot level prompt (**ok>**).

```
client224:~# ~ => sync; halt
ok>
```



Note: If after connecting to the SC board's RS-232 console, the OpenBoot level prompt (**ok>**) prompt appears instead of the Solaris OS login prompt, type **banner** and press **Enter** to identify the SC board's MAC address. Consult with your network administrator to allocate the hostname and the IP address for the new SC board.

5. Login to the Install server (EMS) as the **root** user via Telnet, SSH or X-terminal (when connecting to the EMS server, you may need to login as **acems** user first, and then switch to **root** user via the **su – root** command).
6. In the Install server (EMS), define the SC board as the "jumpstart client" (use the SC hostname, IP address and MAC address defined in step 3)

```
EMS1:/ [root] => cd /jumpstart/Solaris_9_for_v6.6
EMS1:/ [root] => ./add_client.sh client224 10.7.13.94 0:3:ba:78:8e:65
```

7. Return to the RS-232 console terminal connected to the SC board and at the prompt, type **boot net - install** and press **Enter**. Make sure to separate each word with a space.

```
ok> boot net - install
```

The Solaris™ 9 OS installation takes between 10 to 30 minutes (depending on the IP network bandwidth and throughput). During this process, the SC board is rebooted. A message appears when the installation is complete and a login prompt is displayed.

8. When the Solaris OS installation has completed, re-login to the Install Server (EMS) as the **root** user via Telnet, SSH or X-Terminal and remove the SC board's "jumpstart client" definitions (replace **client224** with the actual SC name).

```
EMS1:/ [root] => cd /jumpstart/Solaris_9_904_v6.6/Solaris_9/Tools
EMS1:/ [root] => ./rm_install_client client224
```

27.7 Installing the Linux OS on the SC Rev.2 Board

The SC Rev.2 boards use a special version of the Linux operating system, provided by AudioCodes and configured for optimal Mediant 8000 hardware and software performance. For a typical SC board that is preinstalled with a correct version of the Linux OS there is no need to re-install it.



Note: When it becomes necessary to re-install the Linux OS on SC boards, it is important to use the Linux OS installation image provided by AudioCodes.

27.7.1 Verifying the Current Version of the Linux OS on the SC Board

Version 6.6 of the Mediant 8000 software requires the Linux OS version 5.3 or later.

➤ **To access the current version of the Linux™ OS:**

1. Connect to the SC board's CLI interface. For more information, see Section 'Command Line Interface' on page [107](#).
2. Login as **root** user. For more information, see Section 'Logging in as a Root User' on page [115](#).
3. At the prompt, type **cat /etc/version** and press **Enter**. The current Linux OS version is displayed.
4. Verify that the Linux OS version matches the version required by the specific Mediant 8000 software.

27.7.2 Linux OS Installation Requirements

The Mediant 8000 software supports four different mechanisms for Linux OS (re)installation. The following table provides a summary of each available option, its applicability and installation requirements. The options are listed in a descending preference order.

Table 27-1: Linux OS Installation Requirements

OS Installation Mechanism	Installation Summary	Installation Requirements
OS re-installation via the remote network connection	The OS is re-installed from a local copy of the OS installation image that was created during the initial OS installation on the SC board and is stored on a hidden partition. The network configuration is preserved and the installation may be performed from the remote network connection (via SSH) – i.e. without the need for an RS-232 serial console.	The SC board must be able to boot the currently installed version of the Linux OS (even if partially broken or compromised) and a hidden partition that holds a local copy of installation image must be undamaged. Network connection to the SC board (via SSH) is required.
OS re-installation via the RS-232 console	The OS is re-installed from a local copy of the OS installation image that was created during the initial OS installation on the SC board and is stored on a hidden partition. The RS-232 serial console is used to perform re-installation.	The SC board's bootloader and a hidden partition that holds a local copy of installation image must be undamaged. Note that the currently installed version of the Linux OS may be damaged to the extent that the SC board is unable to boot. The RS-232 serial connection to the SC board is required.
OS installation from the USB Flash Drive via the RS-232 console.	The OS is installed from the USB Flash Drive that must be connected to the USB port on the SC board's front panel and must contain a bootable copy of "Linux OS for SC boards" installation image. Installation is performed via the RS-232 serial console.	No requirements for any data preserved on the local drive– it may be completely wiped out. 1GB or bigger USB flash drive is required (should be provided by the customer). A bootable copy of "Linux OS for SC boards" installation image must be created on the USB flash drive as described below. An RS-232 serial connection to the SC board is required.

OS Installation Mechanism	Installation Summary	Installation Requirements
OS installation from the USB CD/DVD drive via the RS-232 console	The OS is installed from a bootable "Linux OS for SC boards" CD-ROM to be inserted into the USB CD/DVD drive. The installation is performed via the RS-232 serial console,	USB CD-ROM drive (to be provided by the customer) is required. An RS-232 serial connection to the SC board is required.

27.7.3 Re-installing the Linux OS via the Remote Network Connection

When the SC board that needs to be re-installed is able to boot the currently installed version of the Linux OS (even if it's partially broken or compromised), use the following method to perform Linux OS re-installation via the remote network connection (via SSH).

The Linux OS will be re-installed from a local copy of the OS installation image that was created during the initial OS installation on the SC board and is stored on a hidden partition. The re-installation may be performed via the remote network connection to the CLI interface (via the SSH) and does not require connection to the SC board's RS-232 serial console.

➤ **To re-install Linux OS via the Remote Network Connection:**

1. Connect to the SC board via the SSH (see 'Command Line Interface' on page 107).
2. Login as **root** user (see 'Logging in as a Root User' on page 115).
3. At the prompt, type **reinstall-linux** and press **Enter**.

```
[root@sc2-linux ~]# reinstall-linux
```

```
Re-install Linux OS from the recovery partition
```

```
This utility allows you to re-install Linux OS from a hidden recovery partition on the SC board. All data on the disk will be lost (including Media Gateway software and its configuration).
```

```
Make sure that you have Media Gateway software installation package and configuration backup prior to proceeding with the re-installation.
```

4. When prompted to proceed with the Linux OS re-installation, type **y** and press **Enter**.

```
Do you wish to proceed with Linux OS re-installation? (y/n) : y
```

5. The current IP network configuration is displayed. This configuration is preserved after the Linux OS re-installation. Verify that the configuration is correct and type **y** and press **Enter** to proceed with the re-installation.

```
This SC board has the following IP configuration:
  Hostname           : sc2-linux
  IP Address         : 10.7.21.4
  Network Mask       : 255.255.0.0
Default Gateway     : 10.7.0.1
This configuration will be preserved after the Linux OS re-installation
and you will be able to re-connect to the SC board's IP address
(10.7.21.4) via the SSH.
Is the above IP configuration correct? (y/n) : y
```

6. After the Linux OS re-installation, only **acladmin** and **root** users will remain on the SC board. You will be prompted to enter the default password for each user. Enter the passwords as prompted and use them to re-connect to the SC board when the Linux OS re-installation has completed.

```
After Linux OS re-installation only the following 2 users will remain on
the SC board:
1) acladmin
2) root
When Linux OS re-installation completes, you should re-establish SSH
connection with the SC board, login as user "acladmin" and then, if
required, type "su -" command to switch to the "root" user.
You will now be prompted for the default passwords that will be used
after Linux OS re-installation.
Enter default password for "acladmin" user : pass_1234
Enter default password for "root" user : root
```

7. When prompted to start the Linux OS re-installation, type **y** and press **Enter**.

```
Ready to perform Linux OS re-installation.
SC board will now be rebooted and Linux OS will be re-installed on it.
Re-installation will take approximately 15 minutes and will be performed
in a fully automatic mode. During the re-installation SC board will be
inaccessible via the network (i.e. all SSH connections will be dropped).
You may optionally use RS-232 serial console to monitor re-installation
progress.
When re-installation completes, SC board will be rebooted and you will be
able to connect to it via the SSH.
Start Linux OS re-installation? (y/n) : y
```

8. The SC board will reboot and the Linux OS will be automatically re-installed on it. The re-installation process will typically take approximately 15 minutes. During this time, the SC board will be inaccessible via the network and you may optionally use the RS-232 console to monitor the re-installation progress. When the re-installation has completed, the SC board will reboot again and you will be able to connect to it via the IP network using the IP address and passwords provided in previous steps.

27.7.4 Re-installing the Linux OS via the RS-232 Serial Console

When the SC board that is required to be re-installed is unable to boot the currently installed version of the Linux OS, however its bootloader is not damaged (the GRUB menu is displayed in the RS-232 console when the SC board attempts to boot), use the method described in this section to perform Linux OS re-installation via the RS-232 serial console.

The Linux OS will be re-installed from a local copy of the OS installation image that was created during the initial OS installation on the SC board and is stored on a hidden partition. An RS-232 serial console connection to the SC board is required to perform this type of OS re-installation.

➤ To re-install the Linux OS via the RS-232 Serial Console:

1. Connect to the SC board via the RS-232 Serial Console (see 'Command Line Interface' on page 107).
2. Restart the SC board by pressing the hidden "Reset" pin, located on the SC board's front panel or by extracting and re-inserting the SC board into the Mediant 8000 chassis slot.
3. When the GRUB menu is displayed, press the **Space** key to pause the boot process. Make sure to press the key within 5 seconds after the menu is displayed, otherwise the boot process will continue as normal.

```
GNU GRUB  version 0.97  (629K lower / 2083729K upper memory)
```

```
+-----+
| CentOS (2.6.18-128.1.14.el5)          |
| Re-install Linux OS                   |
| Rescue Console                       |
|                                     |
|                                     |
+-----+
```

```
Use the ^ and v keys to select which entry is highlighted.
Press enter to boot the selected OS or 'p' to enter a
password to unlock the next set of features.
```

4. Press **p** and enter the GRUB security password (**grub_12345** by default) to unlock the advanced GRUB features.

```
Password: *****
```

5. Press the "Down" arrow key to choose the "Re-install Linux OS" menu item and press **Enter** to activate it.

```
Booting 'Re-install Linux OS'
root (hd0,0)
Filesystem type is ext2fs, partition type 0x83
lock
cat /INSTALL/reinstall.txt
```

• W A R N I N G ! ! ! *

You are going to re-install Linux OS on the SC board.
The hard disk will be formatted and all data on it
(including Media Gateway binaries and configuration)
will be lost.
To proceed with the installation, press any key.
To abort the installation, reboot SC board now.

6. At the warning prompt, press any key to proceed with the re-installation.
7. The re-installation will take approximately 15 minutes and will be performed in a fully automatic mode. The re-installation progress will be reported on the RS-232 serial console as follows:

```
+-----+ Package Installation +-----+
|
| Name   : parted-1.8.1-23.el5-i386
| Size   : 1354k
| Summary: The GNU disk partition manipulation program.
|
|
|                                     38%
|
| Packages      Bytes      Time
| Total        :      237      503M      0:04:15
| Completed:    :      205      396M      0:03:21
| Remaining:    :       32      107M      0:00:54
|
|                                     78%
|
|
+-----+
```


8. When the re-installation has completed, the SC board will be rebooted. After the Linux OS re-installation via the RS-232 console, the SC board will be inaccessible from the IP network (it will be assigned a non-routable local link IP address) and only the following default users with default passwords will be defined on it:

Default Username	Default Password
root	root
acladmin	pass_1234

Therefore you must use the following procedure to change the default user passwords and make the SC board accessible via the IP network by configuring the basic SC board's network parameters.

➤ **To configure the basic SC board's network parameters after the Linux OS re-installation:**

1. Use the RS-232 serial console to connect to the SC board's CLI interface. For more information, see 'Command Line Interface' on page 107.
2. Login as the **root** user. For more information, see Section 'Logging in as a Root User' on page 115.
3. To change the default password for **acladmin** user, type **passwd acladmin** and enter the new password. To change the default password for **root** user, type **passwd root** and enter the new password.
4. To configure the SC board's IP network parameter, at the prompt type **network-config** and press **Enter**.

```
[root@sc-board ~]# network-config
```

5. The current SC board's network configuration is displayed and you will be prompted to change it. Type **y** and press **Enter**.

```
Current network configuration:
```

```
Hostname           : sc-board
```

```
IP Address          : 169.254.100.1
```

```
Subnet Mask         : 255.255.0.0
```

```
Default Gateway     : 169.254.0.1
```

```
Do you wish to change it? (y/[n]) : y
```

6. When prompted, enter the **Hostname**, **IP Address**, **Subnet Mask** and **Default Gateway** for the SC board. It is strongly recommended to provide the same values as were defined prior to the Linux OS re-installation.

```
Hostname           : sc2-linux
```

```
IP Address          : 10.7.21.4
```

```
Subnet Mask         : 255.255.0.0
```

```
Default Gateway     : 10.7.0.1
```

7. When prompted to apply the new network configuration, type **y** and press **Enter**.

```
Apply new configuration? ([y]/n) : y
```

```
SC board must be rebooted to activate the new
network configuration.
```

```
Reboot now? ([y]/n) : y
```

8. The SC board will be rebooted and will become accessible via the IP network.

27.7.5 Installing the Linux OS from the USB Flash Drive via the RS-232 Serial Console

When the SC board is damaged to the extent that its bootloader does not operate correctly or a hidden partition that stores a local copy of the OS installation package is damaged. Or, alternatively, when a new OS installation image must be installed on the SC board, use the following method to perform the Linux OS installation from the USB Flash Drive via the RS-232 serial console.

An empty 1 GB or larger USB Flash Drive (to be provided by the customer) is required to perform this type of OS installation. The drive must be formatted and a bootable copy of "Linux OS for SC boards" installation image must be installed on it, as described below. A Windows XP/2003/Vista based PC is required to complete these USB Flash Drive preparations.

The RS-232 serial console connection to the SC board is required to perform this type of OS installation.

27.7.5.1 Preparing the USB Flash Drive

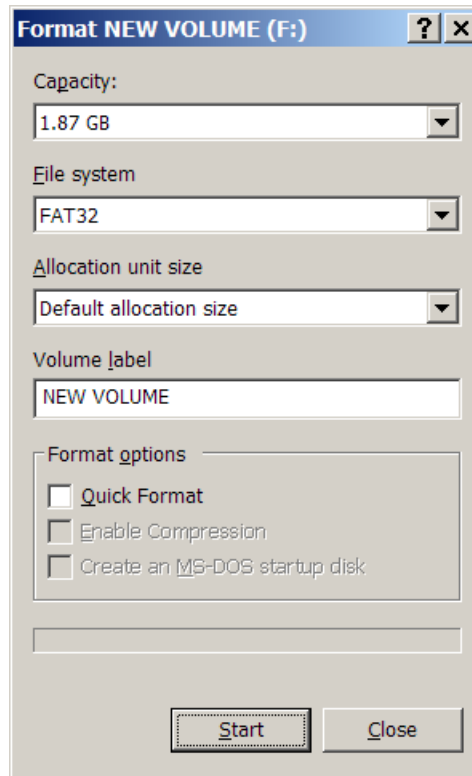
Prior to installing the Linux OS from the USB Flash Drive, you must prepare a bootable USB Flash drive with the OS installation image.

➤ **To prepare a bootable USB Flash Drive with the OS installation image:**

1. Connect the USB Flash Drive to a free USB port on your Windows-based PC.
2. Open "My Computer", right-click the entry that corresponds to the USB Flash Drive and choose **Format**.

3. Choose **FAT** or **FAT32** File System and press **Start** to start the formatting.

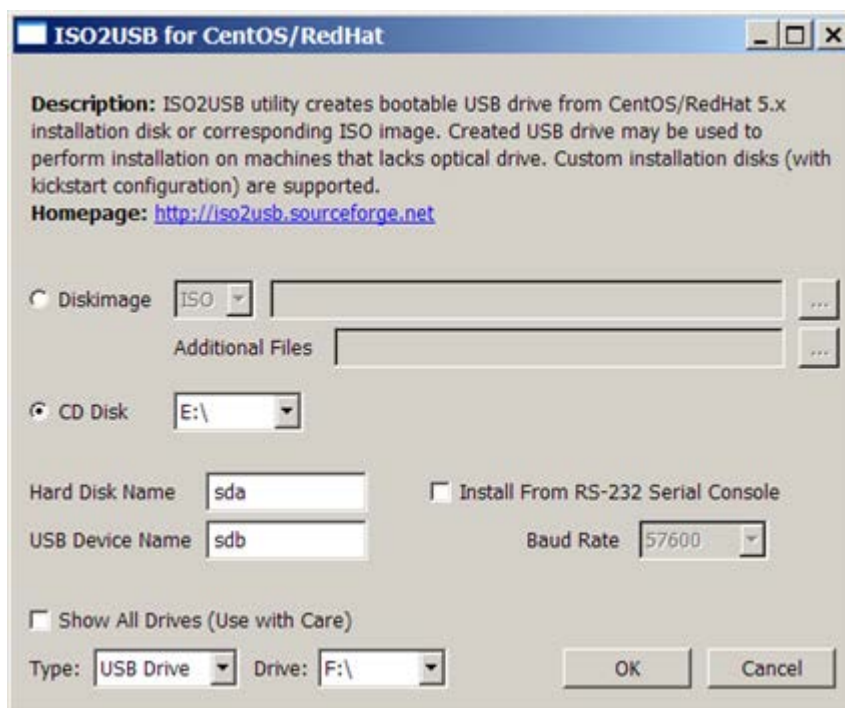
Figure 27-2: Format New Volume



4. When the formatting has completed, insert “Linux OS for SC Board” CD-ROM into the CD/DVD drive on your Windows PC.
5. Open “My Computer” and double-click the entry that corresponds to the CD/DVD drive. The “Linux OS for SC Board” CD-ROM content is displayed.

6. Open the **iso2usb** folder and run **iso2usb.exe** file by double-clicking on it.

Figure 27-3: ISO2USB



7. Click the “CD Disk” radio button and choose the drive letter that corresponds to the CD/DVD drive where “Linux OS for SC Board” CD-ROM is inserted.
8. In the “USB Drive” combo box, choose the drive letter that corresponds to the USB Flash Drive.
9. Press **OK** to create a bootable OS installation image on the USB Flash Drive.
10. Wait patiently while the image is created (it may take up to 15 minutes, depending on the write speed of the USB Flash Drive that you use).


```

+-----+ Error downloading kickstart file +-----+
|
| Unable to download the kickstart file. Please modify the
| kickstart parameter below or press Cancel to proceed as an
| interactive installation.
|
| hd:sdb1:/custom/ks-cd.cfg_____
|
|           +-----+           +-----+
|           | OK |           | Cancel |
|           +-----+           +-----+
|
+-----+

```

7. Wait 5 seconds and press **Enter** twice to continue with the installation.
8. The OS installation will continue. It will take approximately 15 minutes to complete and will be performed in a fully automatic mode. The installation progress will be reported on the RS-232 serial console as follows:

```

+-----+ Package Installation +-----+
|
| Name   : parted-1.8.1-23.el5-i386
| Size   : 1354k
| Summary: The GNU disk partition manipulation program.
|
|
|           38%
|
|           Packages      Bytes      Time
| Total       :          237      503M    0:04:15
| Completed:          205      396M    0:03:21
| Remaining:          32       107M    0:00:54
|
|           78%
|
+-----+

```

9. When the installation is complete, you will be prompted to reboot the SC board. Press **Enter** to perform the reboot.

After the Linux OS installation, the SC board will be inaccessible from the IP network (it will be assigned a non-routable local link IP address) and only the following default users with default passwords will be defined on it:

Default Username	Default Password
root	root
acladmin	pass_1234

Therefore, you must use the following procedure to change the default user passwords and make the SC board accessible via the IP network by configuring the basic SC board's network parameters.

➤ **To configure the basic SC board's network parameters after the Linux OS installation:**

1. Use the RS-232 serial console to connect to the SC board's CLI interface (see 'Command Line Interface' on page 107).
2. Login as **root** user (see 'Logging in as a Root User' on page 115).
3. To change the default password for **acladmin** user, type **passwd acladmin** and enter the new password. To change the default password for **root** user, type **passwd root** and enter the new password.
4. To configure the SC board's IP network parameter, at the prompt type **network-config** and press **Enter**.

```
[root@sc-board ~]# network-config
```

5. The current SC board's network configuration will be displayed and you will be prompted to change it. Type **y** and press **Enter**.

```
Current network configuration:
```

```
Hostname           : sc-board
```

```
IP Address         : 169.254.100.1
```

```
Subnet Mask        : 255.255.0.0
```

```
Default Gateway    : 169.254.0.1
```

```
Do you wish to change it? (y/[n]) : y
```

6. When prompted, enter the **Hostname**, **IP Address**, **Subnet Mask** and **Default Gateway** for the SC board. It is strongly recommended to provide the same values that were defined prior to the Linux OS re-installation.

```
Hostname           : sc2-linux
```

```
IP Address         : 10.7.21.4
```

```
Subnet Mask        : 255.255.0.0
```

```
Default Gateway    : 10.7.0.1
```

7. When prompted to apply the new network configuration, type **y** and press **Enter**.

```
Apply new configuration? ([y]/n) : y
```

```
SC board must be rebooted to activate the new
network configuration.
```

```
Reboot now? ([y]/n) : y
```

8. The SC board will be rebooted and will become accessible via the IP network.

27.7.6 Installing the Linux OS from the USB CD/DVD Drive via the RS-232 Serial Console

Instead of a bootable USB Flash Drive, a USB CD/DVD drive (to be provided by the customer) may be used to perform the Linux OS installation on the SC board. The installation instructions for both mechanisms are very similar.

➤ To start the OS installation:

1. Connect the USB CD/DVD drive to one of the available USB ports on the SC board's front panel.
2. Insert the "Linux OS for SC Boards" installation CD-ROM into the CD/DVD drive.
3. Connect to the RS-232 serial console on the SC board, reboot the SC board and proceed with the installation from step 2 as described in 'Installing the Linux OS from the USB Flash Drive via the RS-232 Serial Console' on page [238](#).

28 Working with the Media Gateway Boards (TP-6310 and TP-8410)

The Media Gateway boards (TP-6310 and TP-8410) provide “voice over packet” (VoP) functionality and process both signaling (call control) and media streams. Each Media Gateway board operates as a standalone Media Gateway. It has its own set of IP addresses and directly communicates with external VoP entities – e.g. Soft Switches, other Media Gateway or SIP agents.

28.1 Redundancy Model Overview

Media Gateway boards are grouped into Redundancy Groups. Each Redundancy group operates in an asymmetric N+1 redundant mode. One of the Media Gateway boards in the Redundancy Group is configured as a Redundant Board and is accompanied by a designated redundant RTM module (behind it).

When a failure occurs on any Media Gateway board, the Redundant board takes over the activity of the failed one and all channels (both signaling and media) are re-routed to it via the chassis mid-plane and redundant RTM. Depending on the configuration, this activity switchover may or may not affect established calls.

To restore High Availability, you must attend to the failed Media Gateway board as soon as possible. As soon as the problem is fixed (e.g. by replacing the failed board with a functional Media Gateway board, as described in 'Replacing the Failed Media Gateway Board' on page 795), you perform an activity switchback, in which the functional Media Gateway board is returned to service and resumes handling the traffic as usual. As soon as the switchover takes place, the Redundant Media Gateway board is released and the Media Gateway boards' redundancy service is restored.



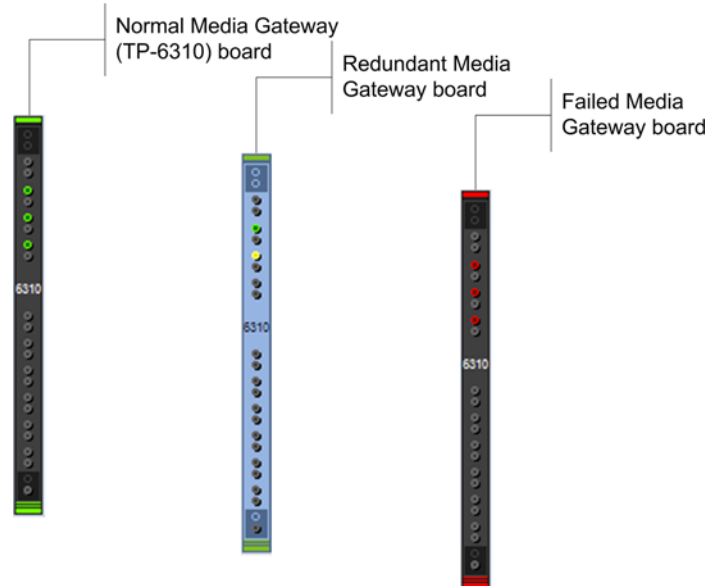
Note: There is an unmarked pinhole on the front panel of the Media Gateway board. This pinhole should never be used when the Media Gateway board is inserted into the Mediant 8000 chassis. In particular, this pinhole should never be used to simulate the Media Gateway board failure/switchover (since switchover may not be properly performed upon such hardware misuse). The correct methods to simulate Media Gateway board switchover are as follows:

- Perform switchover via EMS GUI or CLI
- Extract Media Gateway board from the chassis

28.2 Media Gateway Boards in the EMS

In the EMS, an Active Media Gateway board is colored *black*, while the Redundant Media Gateway board is colored *blue-grey*.

Figure 28-1: Media Gateway Boards in the EMS



The status of the Media Gateway boards is represented by standard **Operational State**, **Administrative State** and **Severity** attributes.

- When the Media Gateway board is functioning properly, its **Operational State** is set to *Enabled*, **Severity** is set to *Clear* and in the EMS, the board is colored *green*.
- When the Media Gateway board's functionality is degraded, an alarm indicating the problem details is generated and board's **Severity** is set according to the alarm's severity. In the EMS board is colored *blue*, *yellow* or *orange*, according to the **Severity** value.
- When the Media Gateway board is not functioning properly (or is absent), its **Operational State** is set to *Disabled* and in the EMS, the board is colored *red*.
- When the Media Gateway board is locked, its **Administrative State** is set to *Locked* and in the EMS, the board is colored *grey*.

28.3 Hardware and Application Types

The capabilities of the Media Gateway board are defined according to two parameters that must be specified at the time when the new board is defined (via **AddBoard** action):

- Hardware Type – defines the type of the Media Gateway board's hardware:
 - TP-6310 OC-3/STM-1
 - TP-6310 T3
 - IPM-6310
 - TP-8410 E1/T1
 - IP-to-IP TP-6310
- Application Type – defines the type of the software application that runs on the Media Gateway board:
 - Gateway
 - SIP Gateway
 - Media Server
 - SIP Media Server

It is possible to combine Media Gateway boards of different hardware and application types in the same chassis. However, the following restrictions apply:

- A combination of TP- 6310 and TP-8410 boards is not supported.
- A combination of OC-3/STM-1 and T3 boards is supported; however, multiple Redundancy Groups may be required to provide high-availability for all boards. See 'Multiple Redundancy Groups' on page 255 for more information.

28.4 Media Gateway Board Actions

The following actions can be performed on a Media Gateway board and are available in the EMS when you right-Click the specific board in the Media Gateway status screen (or on the empty slot – for an AddBoard action):

- **Add Board** (on the empty slot) – add Media Gateway board. You are prompted to choose the **Hardware Type** and **Application Type** of the new Media Gateway board. Ensure to choose the hardware type that matches the physical type of the board that is actually inserted into the slot.
- **Remove** – removes a Media Gateway board. The board must be **locked** prior to performing this action.
- **Lock** – stops service on the Media Gateway board. Board is reset and all calls established on it are dropped.

- An optional **timeout** parameter allows the performance of a **Graceful Lock** on a Media Gateway board – in this case, calls are not torn down immediately; however, the Media Gateway Controller (MGC) or remote SIP agent are informed that the Media Gateway board is to be closed within a specified timeout period. New calls are not accepted after starting the **Graceful Lock** sequence, but existing calls are allowed to proceed and terminate normally. When the graceful timeout expires, all remaining calls are terminated and the board is reset. If all calls are terminated prior to the graceful timeout, the board is immediately reset.
- **Unlock** – restores service on the Media Gateway board. The board is rebooted and the service is restored. It may take up to 5 minutes before the service is restored (and the **Operational State** of the Media Gateway board is updated accordingly).
- **Make Board Redundant** – makes a regular Media Gateway board into the Redundant board. For more information, see Section 'Configuring Redundant Media Gateway Board' on page [249](#).
- **Make Board Non-Redundant** – makes a Redundant board into a regular board.
- **Switchover** – available on the regular board only; forces an activity switchover to the Redundant board. The regular board remains in **disabled** state after a manual switchover action until user explicitly executes **unlock** action on it.
- **Switchback** – available on the Redundant board after switchover only; forces activity switchback to the regular board. Redundant board is automatically reset and returns to service.
- **Move TP board** – available on VoP boards (TP-6310 / TP-8410). TP boards may be moved from an existing slot to a free slot, along with their entire configuration. This feature may be used for system troubleshooting or due to changes in PSTN cabling.
- **Clone TP board** – available on VoP boards (TP-6310 / TP-8410). TP boards may be cloned from an existing slot to a free slot, along with their entire configuration. This feature may be used for copying a working configuration to a new board.

28.5 The Redundancy Model

Media Gateway boards are grouped into Redundancy Groups. Each redundancy group has a dedicated redundant board (equipped with a redundant RTM module) that provides hot redundancy protection for the active boards within the group.

By default, a single Redundancy Group is created and all Media Gateway boards are assigned to it.

28.5.1 Configuring Redundant Media Gateway Board

The redundant board is typically pre-defined on a Media Gateway shipped to customers. However, you may start working with a Media Gateway without redundancy, and then add a redundant board later in the process. In this case, use the **Add Board** action (as described in 'Media Gateway Board Actions' on page 247) to add a new board and then follow the procedure described below. Ensure that your redundant board is equipped with the redundant RTM module.

Use the procedure below to configure the Redundant board under the following circumstances:

- After adding a new Redundant board
- After changing the configuration of the active boards (to ensure the availability of the best possible Redundancy Mode for all boards)

➤ **To configure the Redundant Media Gateway board:**

1. Click the  button to access the Media Gateway status screen.
2. Select a Media Gateway board to be configured as the Redundant board (note that redundant board must be equipped with the redundant RTM module).
3. Right-Click the selected Media Gateway board and, from the popup menu, select **Maintenance> Make Board Redundant**; the Board Redundancy dialog box is displayed.
4. From the **Select Board** drop-down list, select the regular board from which the configuration is to be copied. For more information, see Section 'Actual Redundancy Mode' on page 252.

Complete the configuration of the Redundant Board by provisioning its IP addresses via the Network Settings screen.

Finally, perform the **Unlock** action on the Redundant board to bring it into service. Wait for a few minutes till the action completes (the board is restarted as part of this process; when the process completes, the board's **Operational State** is changed to *Enabled*). Open the Boards Redundancy screen (as described in 'Actual Redundancy Mode' on page 252) and verify redundancy modes for each regular Media Gateway board.

28.5.2 Redundancy Modes

Each Media Gateway board may have different levels of protection, depending on the configuration of the Redundancy Group that it is assigned to and the configuration of the board itself.

The following levels of protection (also called "Redundancy Modes" or "HA Modes") are available:

- **Hot Redundancy**

The Media Gateway board is fully backed-up by the Redundant board. When a Media Gateway board fails or a user-initiated switchover occurs, the service is restored on the Redundant board without service interruption. Both channel capacity and active calls connection is preserved.

- **Warm Redundancy**

The Media Gateway board is only partially backed-up by the Redundant board. When a Media Gateway board fails or a user-initiated switchover occurs, the service is restored on the Redundant board, preserving the channels capacity; however, active calls are dropped. Service may be interrupted for a few minutes after the switchover.

- **No Redundancy**

The Media Gateway board is not protected by the Redundant board. When a Media Gateway board fails, the service is completely dropped. This mode may occur, for example, in case of a double failure – i.e. when two Media Gateway boards fail consequently, the Redundant board is used to protect the first failed board, and no protection is provided for the second failed board.

28.5.3 Desired Redundancy Mode

Desired Redundancy Mode determines the highest level of protection requested by the user. The Desired Redundancy Mode may be configured for the Redundancy Group (and thus affect all Media Gateway boards associated with the specific group) or for each specific Media Gateway board.

➤ **To configure the desired Redundancy mode for a Redundancy group:**

1. Click  to access the Media Gateway status screen.
2. In the Navigation pane, select **Redundancy** ► **Redundancy Groups**; the Redundancy Groups list is displayed.
3. Select a specific row and then in the configuration pane, click **Redundancy Group Settings**; the Redundancy Group Settings screen is displayed.
4. Set **Redundancy Mode** parameter to *Not Protected*, *Hot* or *Warm*.

➤ **To configure desired Redundancy mode for a specific Media Gateway board:**

1. Click  to access the Media Gateway status screen.
2. Select the specific Media Gateway board.
3. In the Navigation pane, select **Redundancy** and then in the configuration pane, click **Redundancy Settings**; the Redundancy Settings screen is displayed.
4. Configure **Desired HA Mode** parameter as follows:
 - a. To use Redundancy Group configuration, set **Desired HA Mode** parameter to *Use RG Configuration*
 - b. To configure Desired HA Mode for a specific Media Gateway board, set **Desired HA Mode** parameter to *Not Protected*, *Hot* or *Warm*.

28.5.4 Actual Redundancy Mode

The Actual Redundancy mode indicates the actual level of protection provided for the specific Media Gateway board. The Actual Redundancy mode may provide a lower level of redundancy to the Desired Redundancy mode, configured by the user, due to the following factors:

- Mismatches in configuration of the normal and redundant Media Gateway boards
For each parameter that is configured with different values on the normal and redundant Media Gateway boards, *Redundancy Type* of the parameter is used to determine whether this mismatch affects the Actual Redundancy mode. The following parameter redundancy types are available:
 - ◆ **Hot** – mismatch in this parameter between the active and redundant Media Gateway boards has no affect on the Actual Redundancy mode; most of the configuration parameters belong to this type;
 - ◆ **Warm** – mismatches in a parameter value between the Active and the Redundant Media Gateway boards, degrade the Actual Redundancy mode to *Warm* value; when a parameter is set to the same value on the Active and Redundant Media Gateway boards, there is no affect on the Actual Redundancy mode; parameters of this type are marked with  icon in EMS configuration screens.
- Mismatches in Hardware and Application Types of normal and redundant Media Gateway boards
Mismatch in the Hardware and/or Application Types of normal and redundant Media Gateway boards may degrade Actual Redundancy Mode to *Warm* or *No Redundancy* value.
- Current state of the normal and redundant Media Gateway boards
Actual Redundancy mode will be downgraded to *No Redundancy* value when normal or redundant Media Gateway boards are out of service
- Current state of the Redundancy group
Actual Redundancy mode will be downgraded to *No Redundancy* value when another Media Gateway board is currently "backed up" by the Redundant board
- Mismatches in License Keys of Normal and Redundant Media Gateway boards
Actual Redundancy mode will be downgraded to *No Redundancy* value when critical mismatches are detected in the License Keys of normal and redundant Media Gateway boards.

The Actual Redundancy mode is independently determined for each Media Gateway board . At any point in time, in the same Redundancy group, the Actual Redundancy mode of one board may differ from the Actual Redundancy mode of another board (due to the difference in their state or configuration).

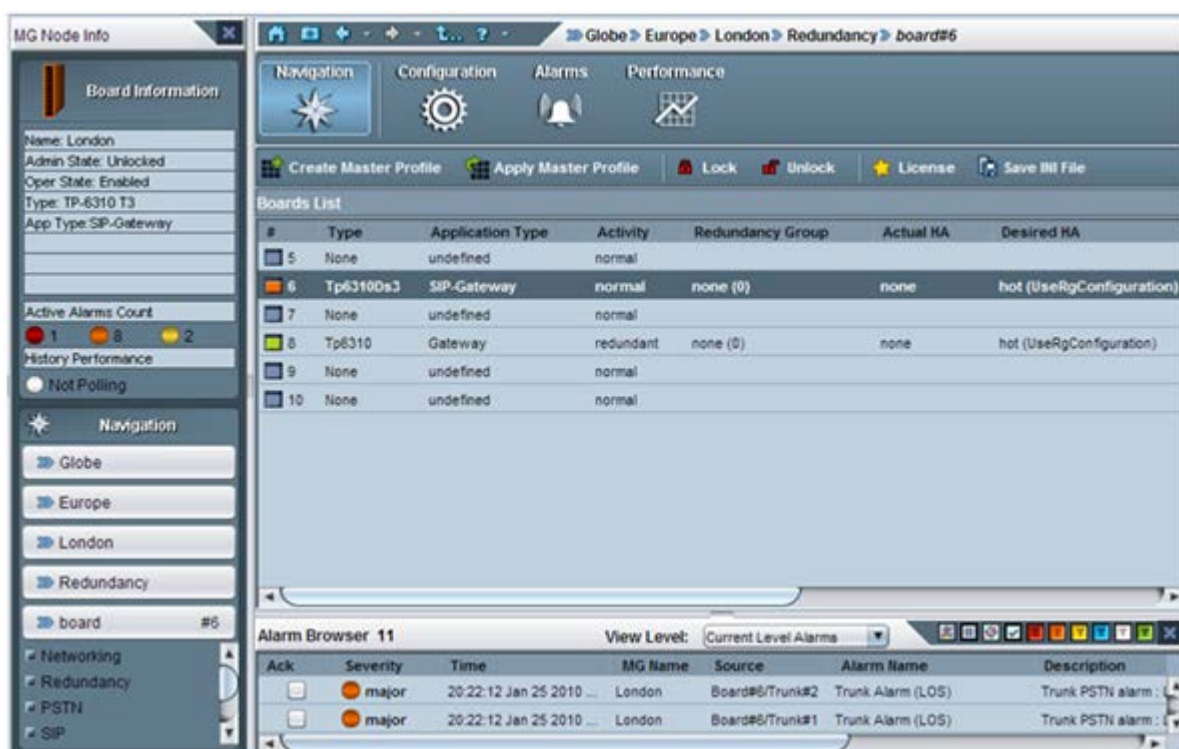
In the Boards Redundancy Status screen, the HA Reason column indicates the exact reason for the current value of the Actual Redundancy mode. For example, if a specific configuration parameter differs between the specific Media Gateway board and the Redundant board, its name will be specified in the HA Reason column.

It is recommended that you periodically inspect the value of the Actual Redundancy mode for all Media Gateway boards to ensure that the system is configured to provide proper protection in case of board failure.

➤ To view the redundancy mode for all Media Gateway boards:

1. Click  to access the Media Gateway status screen.
2. In the Navigation pane, select **Redundancy ▶ Boards Redundancy Status**; the Boards Redundancy list is displayed.

Figure 28-2: Board Redundancy Status



The screenshot displays the 'MG Node Info' window for a node named 'London'. The left navigation pane shows the hierarchy: **Redundancy ▶ Boards Redundancy Status**. The main content area features a 'Boards List' table with the following data:

#	Type	Application Type	Activity	Redundancy Group	Actual HA	Desired HA
5	None	undefined	normal			
6	Tp6310Ds3	SIP-Gateway	normal	none (0)	none	hot (UseRgConfiguration)
7	None	undefined	normal			
8	Tp6310	Gateway	redundant	none (0)	none	hot (UseRgConfiguration)
9	None	undefined	normal			
10	None	undefined	normal			

Below the table is the 'Alarm Browser' showing 11 alarms. The first two are major alarms:

Ack	Severity	Time	MG Name	Source	Alarm Name	Description
☐	major	20:22:12 Jan 25 2010 ...	London	Board#6/Trunk#2	Trunk Alarm (LOS)	Trunk PSTN alarm :
☐	major	20:22:12 Jan 25 2010 ...	London	Board#6/Trunk#1	Trunk Alarm (LOS)	Trunk PSTN alarm :

28.5.5 Activity Switchover

When a failure occurs on the Media Gateway board, one of the following actions are performed:

- If the Redundant Media Gateway board is available, activity switchover to the Redundant board is performed and service is restored on it. The failed board is not automatically restarted until you explicitly perform an **Unlock** action on it. The effect on the Media Gateway board's service depends on the Redundancy mode available to the specific board prior to the failure. See 'Configuring Redundant Media Gateway Board' on page 249.
- If the Redundant Media Gateway board is not available (it's either not configured or is currently used for back-up for another board), the failed board is automatically restarted. Service is typically restored on the failed board when it completes the restart.

When the Media Gateway board fails and then there is an activity switchover to the Redundant board, the operator should attend to the relevant Media Gateway and perform the following maintenance tasks:

- Identify the reason for the failure, collect relevant logs and record all maintenance or operational events that preceded the failure.
- **Lock** and **unlock** the failed Media Gateway board. Wait until the board's **Operational State** is changed to *Enabled* – this indicates that the board is ready for operation.
- Perform **SwitchBack** action to switch activity back from the Redundant board to the regular board.
- Wait until the Redundant board completes restart and its **Operational State** is changed to *Enabled*.
- Open the Board's Redundancy screen and verify the Redundancy modes for all regular Media Gateway boards.

28.5.6 Multiple Redundancy Groups

Multiple redundancy groups may be used to provide adequate protection in the following cases:

- Media Gateway boards installed in the chassis have different hardware or application types.
- Media Gateway boards have different configurations, which makes it impossible to provide Hot redundancy for all boards by a single redundancy group.

Each redundancy group has its own redundant board, accompanied by a redundant RTM module, which is capable of protecting service on a failed regular board within the group. However, at any one time only one redundancy group may be in a switchover state – i.e. when one of the redundancy groups switches activity to their respective redundant board, another group may not perform switchover until the 1st group switches back.

➤ To add and configure a new Redundancy Group:

1. Click  to access the Media Gateway status screen.
2. In the Navigation pane, select **Redundancy** ➤ **Redundancy Groups**; the Redundancy Groups list is displayed.
3. Use the  or  buttons to add or remove entries.
4. Select a specific row and then in the configuration pane, click **Redundancy Group Settings**; the Redundancy Group Settings screen is displayed.
5. Configure Redundancy Group parameters according to the table 'Redundancy Group Parameters' below.

After adding a new Redundancy Group, associate specific Media Gateway boards to it by performing the procedure described below. Ensure that you define a redundant Media Gateway board for each Redundancy Group and configure it as described in 'Configuring Redundant Media Gateway Board' on page 249.

➤ To associate a Media Gateway board with a Redundancy Group:

1. Click  to access the Media Gateway status screen.
2. Select the specific Media Gateway board.
3. In the Navigation pane, select **Redundancy** and then in the configuration pane, click **Redundancy Settings**; the Redundancy Settings screen is displayed.
4. Configure Media Gateway board's redundancy parameters according to the table 'Media Gateway board's Redundancy Parameters' below. Set **Redundancy Group** parameter to match the specific Redundancy Group.

Table 28-1: Redundancy Group Parameters

Parameter Name	Type	Provisioning Type	Description
Redundancy Mode	Enum Not Protected, Hot, Warm	Instant	Defines the Desired Redundancy mode for all Media Gateway boards assigned to this group. The Actual Redundancy mode for each Media Gateway board may never be higher than the value indicated by this parameter. Therefore this parameter may be used to force warm or not protected redundancy modes on all Media Gateway boards.
Protected Boards	String Up to 80 chars	Read-Only	Indicates all Normal Media Gateway boards currently associated with this Redundancy Group.
Redundant Board	String Up to 80 chars	Read-Only	Indicates the Redundant Media Gateway board that is currently associated with this Redundancy Group.
Redundant Board In Use	Enum Unused, Used	Read-Only	Indicates whether the Redundant board is currently used for back-up of a specific normal board.
Failed Board	Integer -1 – 19	Read-Only	Indicates the number of the failed Media Gateway boards that are currently being backed-up by the Redundant board.
Failed Board Behavior	Enum Recover Service, Stop Service, Debug Mode	Instant	Defines the default behavior in case of Media Gateway board failure. The following values are available: Recover Service – attempts to recover service provided by the failed board by performing switchover to the Redundant board (if it's available) or restarting the failed board. Stop Service – keep the failed board reset until the user manually attends to it, solves the problem (e.g. by replacing the board) and performs UNLOCK action) Debug Mode –special mode used for debugging the redundancy mechanism; suitable for lab environment only.
Detection Time For Hot	Enum Normal, Extra	Instant	Defines the failure detection time for boards that have the Actual Redundancy

Parameter Name	Type	Provisioning Type	Description
Redundancy	Safe		mode set to Hot . Normal – normal detection time ExtraSafe – detection time of board failure is longer; however, false detections (e.g. due to the unstable network) are prevented.

Table 28-2: Media Gateway board Redundancy Parameters

Parameter Name	Type	Provisioning Type	Description
Activity	Enum Normal, Redundant	Read-Only	Indicates whether this Media Gateway board is a Redundant board.
Redundancy Group	Integer 0 – 3	Instant	Indicates the Redundancy Group to which this Media Gateway board is associated.
Actual HA Mode	Enum None, Hot, Warm	Read-Only	Indicates the actual level of protection provided for this Media Gateway board.
Desired HA Mode	Enum Not Protected, Hot, Warm, Use RG Configuration	Instant	Defines the Desired Redundancy mode for the specific Media Gateway board. Value Use RG Configuration defines that the Redundancy mode defined in the Redundancy Group is used.
HA Reason	String Up to 255 chars	Read-Only	Indicates the exact reason for the current value of the Actual Redundancy mode. For example, if a specific configuration parameter differs between the specific Media Gateway board and the Redundant board, its name is specified in the HA Reason parameter.

28.5.7 Automatic Switchback

The Media Gateway may be configured to perform automatic activity switchback from the Redundant Media Gateway board back to the failed board, as soon as the later returns to service. This configuration reduces the manual workload performed by the operator upon the Media Gateway board switchover. It also releases the Redundant board and therefore restores redundancy for the rest of the Media Gateway boards.

When automatic switchback is configured, the failed Media Gateway board is automatically restarted after the switchover. When the Media Gateway board returns to service, its functionality is verified for a specified time period. If within that time period, the Media Gateway board is stable, automatic switchback is performed.

Additional configuration parameters are provided to ensure that overall system stability is not compromised by this feature.

➤ To configure Automatic Switchback:

1. Click  to access the Media Gateway status screen.
2. In the Navigation pane, select **Redundancy** ➤ **Redundancy Groups**; the Redundancy Groups list is displayed.
3. Select a specific row and then in the configuration pane, click **Redundancy Group Settings**; the Redundancy Group Settings screen is displayed.
4. In the **Automatic Switchback** tab, configure Automatic Switchback parameters according to the table 'Automatic Switchback Parameters' below.

Table 28-3: Automatic Switchback Parameters

Parameter Name	Type	Provisioning Type	Description
Automatic Switchback	Enum Disabled, Enabled	Instant	Defines whether automatic switchback functionality is enabled.
Automatic Switchback Timeout	Integer 15-10080	Instant	Defines the sanity time (in minutes) prior to performing the automatic switchback. The switchback is performed only if after the failure Media Gateway board successfully completes the restart, passes all sanity tests and is stable for this pre-defined time period.
Max Auto Switch Back Per a Day	Integer 1-100	Instant	Defines the maximum amount of automatic switchbacks per day. Use this parameter to prevent the system from continuously switching between the failed and redundant boards, in case a problem on the failed board is not resolved.
Auto Switch Back	Integer	Read-Only	Indicates the number of Automatic Switch

Parameter Name	Type	Provisioning Type	Description
Counter	0 – 2147483647		Backs performed during the last 24 hours.
Timeout Left	Integer 0 – 2147483647	Read-Only	Indicates the time left (in seconds) to complete the Automatic Switch Back.
State	Enum	Read-Only	Indicates the internal state of the Automatic Switch Back state machine.

28.6 Updating License Key

The License Key defines a list of features and applications available on the Media Gateway board (e.g., the maximum allowed number of MTP2 SS7 links or the availability of G.729 voice coder).

You can access the current License Key, its status and an explicit list of enabled features by selecting the **License Key** tab in the Media Gateway board's Properties screen.

All Media Gateway boards are preloaded with a License Key according to the specific customer order. However customers may upgrade the License Key in the future to gain access to additional functionality (e.g., to increase the amount of available MTP2 SS7 links).

To upgrade the License Key, contact your AudioCodes Account Team and provide detailed information on the specific new features that you wish to activate. You will receive a License Key file that contains licenses for one or more Media Gateway boards. These licenses must be applied to Media Gateway boards via the Update License Key action. The Media Gateway board must be restarted (locked/unlocked) to complete the License Key update.

➤ To update License Key of specific Media Gateway board:

1. Upload the License Key file to the EMS Software Manager:
 - a. From the **Tools** menu, select **Software Manager**. The Software Manager screen is displayed.
 - b. In the upper left corner, click . The add Files screen is displayed.
 - c. In the **Auxiliary** tab, click  and navigate to the desired **License Key** file.
 - d. Click **OK**. The file name is displayed in the **License Key** field.
 - e. In the **Description** field, type a meaningful description.
 - f. Click **OK**. The file is uploaded to the EMS.

2. Click the  button to access the Media Gateway status screen.
3. Right-Click the desired Media Gateway board and from the popup menu, select **Maintenance> License Keys Update**.
4. Select the **License Key** file as added in step 1.
5. **Lock** and **unlock** the Media Gateway board. The newly added License Key file is applied.
6. Repeat this procedure for all of the Media Gateway boards that require the License Key update.

If multiple Media Gateway boards in the chassis require License Key updating, you can use the Gateway-level License Keys Update action instead. Software automatically applies the new License Keys to all applicable Media Gateway boards.

- Click the  Maintenance Actions icon located at the top-right corner of the Media Gateway status screen and from the popup menu, select **License Keys Update**.

29 Working with the ES Boards

The Ethernet Switch (ES) boards provide IP network connectivity for all of the boards inside the Mediant 8000 chassis (i.e., the SC and Media Gateway boards).

29.1 ES Redundancy Mode

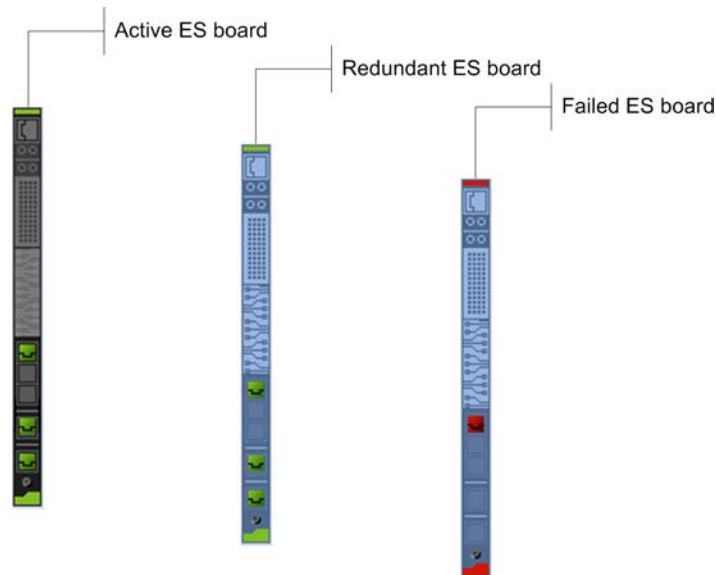
There are two ES boards in the chassis. Each board should be independently connected to the external IP network. The two ES boards operate in an asymmetric 1+1 redundant mode. At any time, one of the ES boards is Active and provides connectivity for the rest of the chassis' boards, while the other ES board is Standby. When the Active ES board fails, the Standby ES board takes over activity and becomes the Active ES board.

An Internal link (F-Link) interconnects between the two ES boards and provides internal communications between the boards inside the chassis.

29.2 ES Boards in the EMS

In the EMS, the Active ES board is colored *black* and the Standby ES board is colored *blue-gray*. The ES board in slot 9 is initially the Active ES board (upon chassis power up) and the ES board in slot 19 is initially the Standby ES board.

Figure 29-1: ES Boards in the EMS



The status of the ES boards is represented by standard **Operational State**, **Administrative State** and **Severity** attributes.

- When the ES board is functioning properly, its **Operational State** is set to *Enabled*, **Severity** is set to *Clear* and in the EMS the board is colored *green*.
- When the ES board's functionality is degraded, an alarm indicating the problem details is generated and the board's Severity is set according to the alarm's severity. In the EMS, the board is colored *blue*, *yellow* or *orange*, according to the Severity value.

- When ES board is not functioning properly (or is absent), its **Operational State** is set to *Disabled* and in the EMS, the ES board is colored *red*.
- When ES board is **locked**, its **Administrative State** is set to *Locked* and in the EMS, the ES board is colored *grey*.

29.3 ES Board Actions – ES/6600

The following actions can be performed on an ES board and are available in the EMS when you right-click the specific ES board in the Media Gateway status screen:

- **Lock** – stops service on the ES board. The locked board cannot be used for providing network connectivity to the chassis, therefore if both ES boards are **locked** simultaneously, the Media Gateway boards lose IP connectivity and the service provided by the Media Gateway is interrupted. The same scenario may happen in the rare case of a 2nd ES board becoming unavailable (e.g., after a board failure) and the 1st ES board being **locked**.
- **Unlock** – restores service on the ES board. The ES board is restarted during the **unlock** action and it may take up to 10 minutes before the service is restored (and the **Operational State** of the ES board is updated accordingly).
- **Align All Boards To Me** – forces all boards inside the chassis (Media Gateway boards and SC boards) to use a specific ES board. When performed on the Standby ES board, it causes the ES boards' activity switchover.
- **Clear Severity** – clears Minor severity on the ES board that may be turned on when the ES board behaves suspiciously (e.g., if for any reason, some of the other boards in the chassis can not communicate with it.)

29.4 ES Board Actions – ES-2

The following actions can be performed on an ES board and are available in the EMS when you right-click the specific ES board in the Media Gateway status screen:

- **Lock** – stops service on the ES board. The locked board cannot be used for providing network connectivity to the chassis, therefore if both ES boards are locked simultaneously, the Media Gateway boards lose IP connectivity and the service provided by the Media Gateway is interrupted. The same scenario may occur in the rare event of a 2nd ES board becoming unavailable (e.g., after a board failure) and the 1st ES board being locked.
- **Unlock** – restores service on the ES board. The ES board is restarted during the unlock action and it may take up to 1 minute before the service is restored (and the Operational State of the ES board is updated accordingly).
- **Align All Boards To Me** – forces all boards inside the chassis (Media Gateway boards and SC boards) to use a specific ES board. When performed on the Standby ES board, it causes the ES boards' activity switchover.

Part IV

Configuring and Operating the Media Gateway (Part 2)

This part describes the configuration and operation of the Media Gateway.

30 Time and Date Configuration

The Media Gateway software requires the precise time and date to be set correctly for normal operations. For example, the following features will not operate correctly when an incorrect time and date are set:

- Secure Call Control and Management protocols that use X.509 certificates (e.g. SIPs and HTTPS) – due to expiration time, included in the X.509 certificate; see 'X.509 Public Key Infrastructure' on page 325 for details.
- Performance measurements – incorrect timestamp and PM values are generated (see 'Performance Monitoring' on page 401).
- Operational and security logs – incorrect timestamp will be used; see 'Internal Software Logs' on page 871 for details.

The Mediant 8000 Media Gateway lacks a hardware clock that is precise enough and can survive a chassis power down/up cycle. Therefore, Network Time Protocol (NTP) is used to synchronize the time and date of the Media Gateway (and all its components) with the external NTP servers.

The Media Gateway operates as an NTP client and has the following capabilities:

- Version 4 of the NTP protocol (as as per the latest draft, available at 'NTP Server' 'http://www.ntp.org') is implemented.
- Backward-compatible with Version 3 of the NTP protocol (as per RFC 1305).
- Up to four external NTP servers are supported.
- EMS server may be used as a NTP server and is configured as such by default.

30.1 Time Zone Settings

NTP protocol synchronizes the “absolute” time and date (i.e time and date of the GMT timezone).

The local time on each machine is determined by applying “time zone offset” to the “absolute” time and date synchronized via the NTP protocol. For example, a machine that resides in New York, applies “-4” offset, and a machine that resides in Paris, applies “+1” offset.

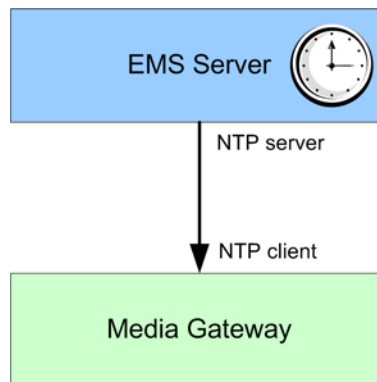
Use of the “time zone offset” enables time and date synchronization between machines that reside in different geographical locations (and therefore different time zones). In the above example, the two machines will have a five hours difference in their local time, while maintaining the precise and synchronized clock values.

The Time Zone of the Mediant 8000 is configured during installation or basic configuration. For detailed description, see 'Installing Mediant 8000 Software' on page 129 and 'Performing Basic Configuration of the Mediant 8000 Software' on page 146.

30.2 Using the EMS Server as the NTP Server

By default, the Media Gateway software uses the EMS server as a pre-configured NTP server and consequently synchronizes its time and date with it. The EMS server is pre-configured to operate as an NTP server and no additional configuration is required.

Figure 30-1: EMS Server Configured as NTP Server



This configuration is suitable for basic lab deployments; however, the EMS server has relatively low clock accuracy. Therefore for field deployments, it is strongly recommended to use the external NTP server for time and date synchronization as described in the following sections.

30.3 Using External NTP Servers

In the field deployments, it is recommended to use external NTP server(s) as a time and date synchronization source for the Media Gateway and EMS server. For redundancy purposes, it is recommended to configure at least two external NTP servers.

If multiple external NTP servers are configured, make sure that all NTP servers derive their clock from the same synchronization source or from the Stratum-0 server. For example, in the figure below both NTP servers derive their clock from the same Stratum-1 NTP server and thus meet this requirement.

There are two possible ways to set up working with external NTP servers. These options are described in the following sections:

- External NTP Servers Setup - Option 1 (see 'External NTP Servers Setup' - Option 1' on page 267).
- External NTP Servers Setup - Option 2 (see 'External NTP Servers Setup' - Option 2' on page 268).

**Notes:**

- If you configure external NTP servers on both the Media Gateway and the EMS server, then you should configure the same NTP servers on both the EMS server and the Media Gateway.
- If you configure external NTP servers on the Media Gateway, it is **not recommended** to use the EMS server as the NTP server clock reference source. Therefore, you should disable the use of the EMS server as an NTP server reference source; in the NTP Servers table, change the **Administrative State** of the EMS server entry (EMS server's IP address) to *Locked* (for more information, see Section 'NTP Synchronization and Status' on page 269).

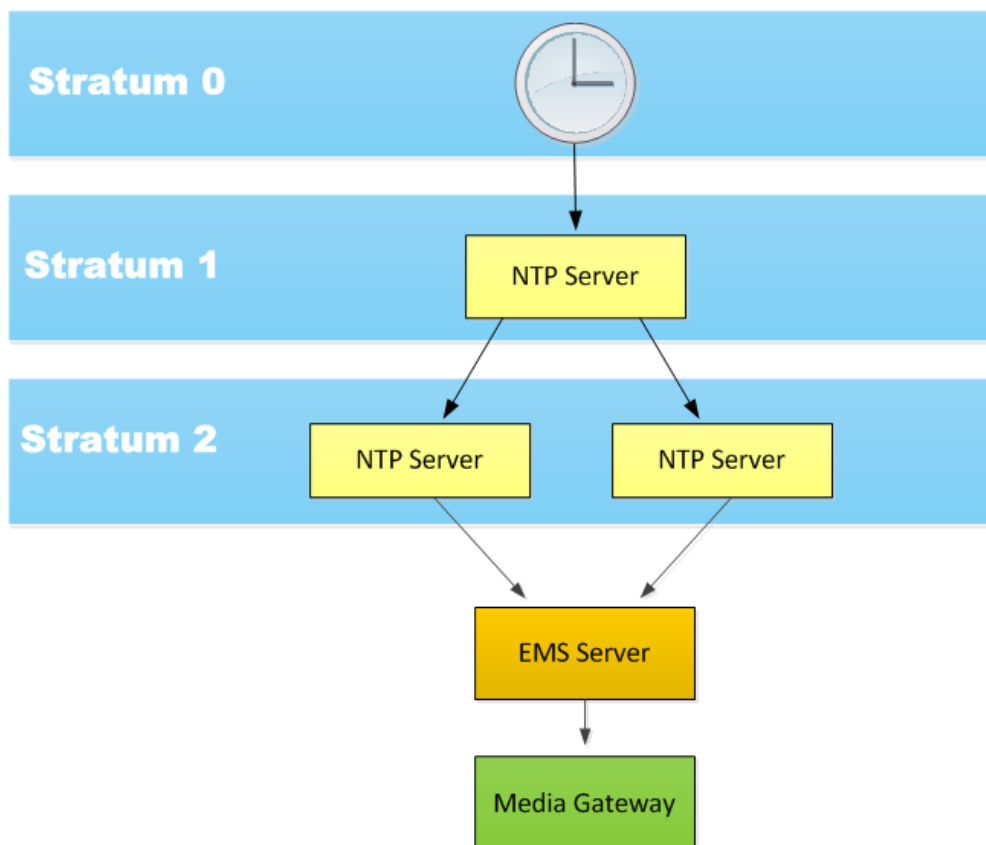
30.3.1 External NTP Servers Setup - Option 1

In the Setup Option 1 below, the EMS server uses two Stratum-2 NTP servers as its NTP clock, and consequently the Media Gateway obtains this NTP clock reference source (when the EMS server is configured as both an NTP server and NTP client).



Note: For information on configuring external NTP servers on the EMS server, refer to the *EMS Server IOM Manual*.

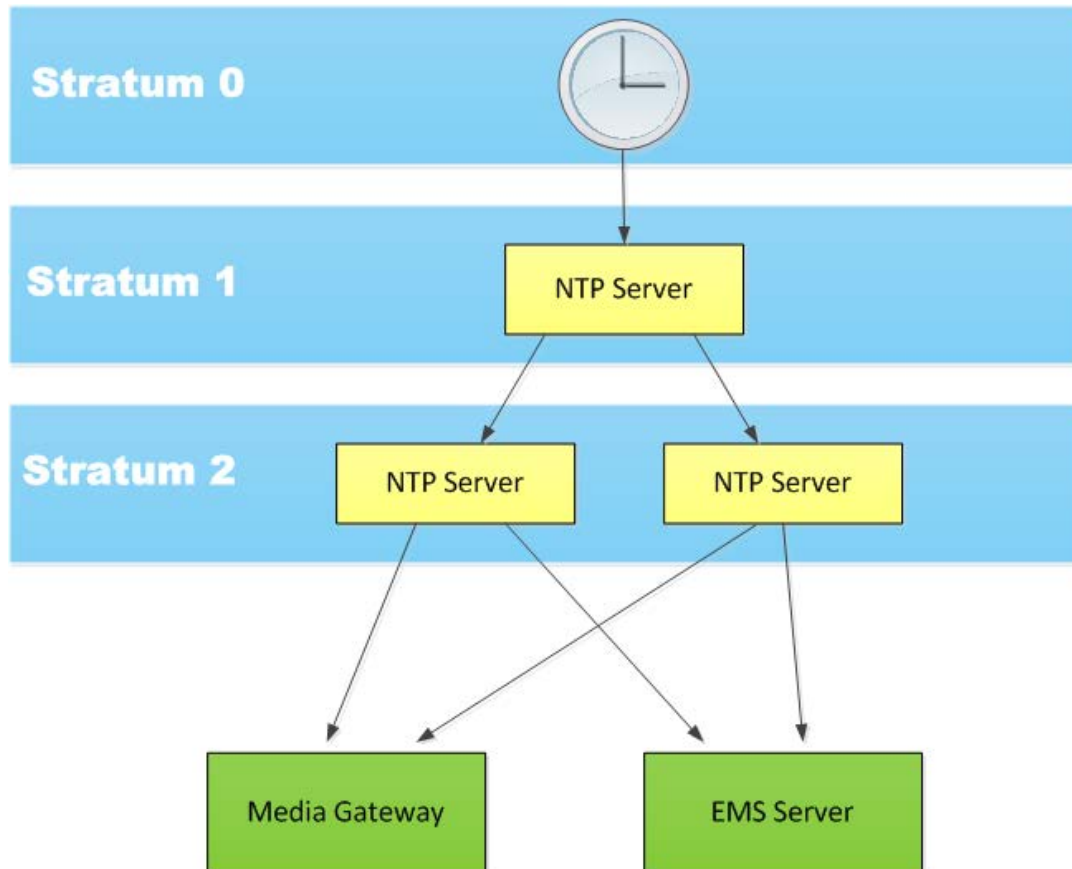
Figure 30-2: External NTP Server Setup - Option 1



30.3.2 External NTP Servers Setup - Option 2

In the Setup Option 2 below, the EMS server uses two Stratum-2 NTP servers as its NTP clock source and the Media Gateway also uses two Stratum-2 NTP servers as its NTP clock source. Therefore, when this setup option is used, both the EMS and the Media Gateway each receive their NTP clock directly from the external NTP server.

Figure 30-3: External NTP Server Configuration - Setup Option 2



30.4 NTP Synchronization and Status

The Media Gateway synchronizes with the NTP server and updates the **Operational State** and **NTP Server Status** attributes accordingly. The **Operational State** attribute indicates whether communication is established with a specific NTP server, while the **NTP Server Status** attribute indicates the “current status” of the specific NTP server, as perceived by a local Media Gateway’s NTP client.

To understand the difference between these two attributes, consider the situation, where two external NTP servers are used to synchronize time and date of the Media Gateway (as shown on the above figure). When communication is established with both servers, their **Operational State** attributes will be set to *Enabled* (and they will be colored *Green* in the EMS GUI). However at any time, only one server will be chosen as the synchronization source – its **NTP Server Status** will be set to *Synchronized*, while another server will be used as an alternative candidate for failover; its **NTP Server Status** will be set to *Candidate*.

Note that due to the nature of the NTP protocol implementation, there may be a significant lag in the update of the **Operational State** and the **NTP Server Status** attributes. For example, when the NTP server is disconnected from the IP network, it may take up to 30 minutes until its **Operational State** is changed to *Disabled* (this delay is introduced to prevent false failure indications in the case of intermittent network problems). In addition, when the connection with the NTP server is re-established, it may take up to 1 hour until the NTP Server is chosen as a synchronization source, and its **NTP Server Status** attribute is updated accordingly.

In addition to the **Operational State** and **NTP Server Status** attributes, additional status and timestamp attributes are maintained for each external NTP server. See Table 'NTP Server Status Parameters' for details. Use these additional attributes (e.g. last sent and received message timestamps) to analyze the current state of the communication with a specific NTP server and to determine possible causes for any malfunction.

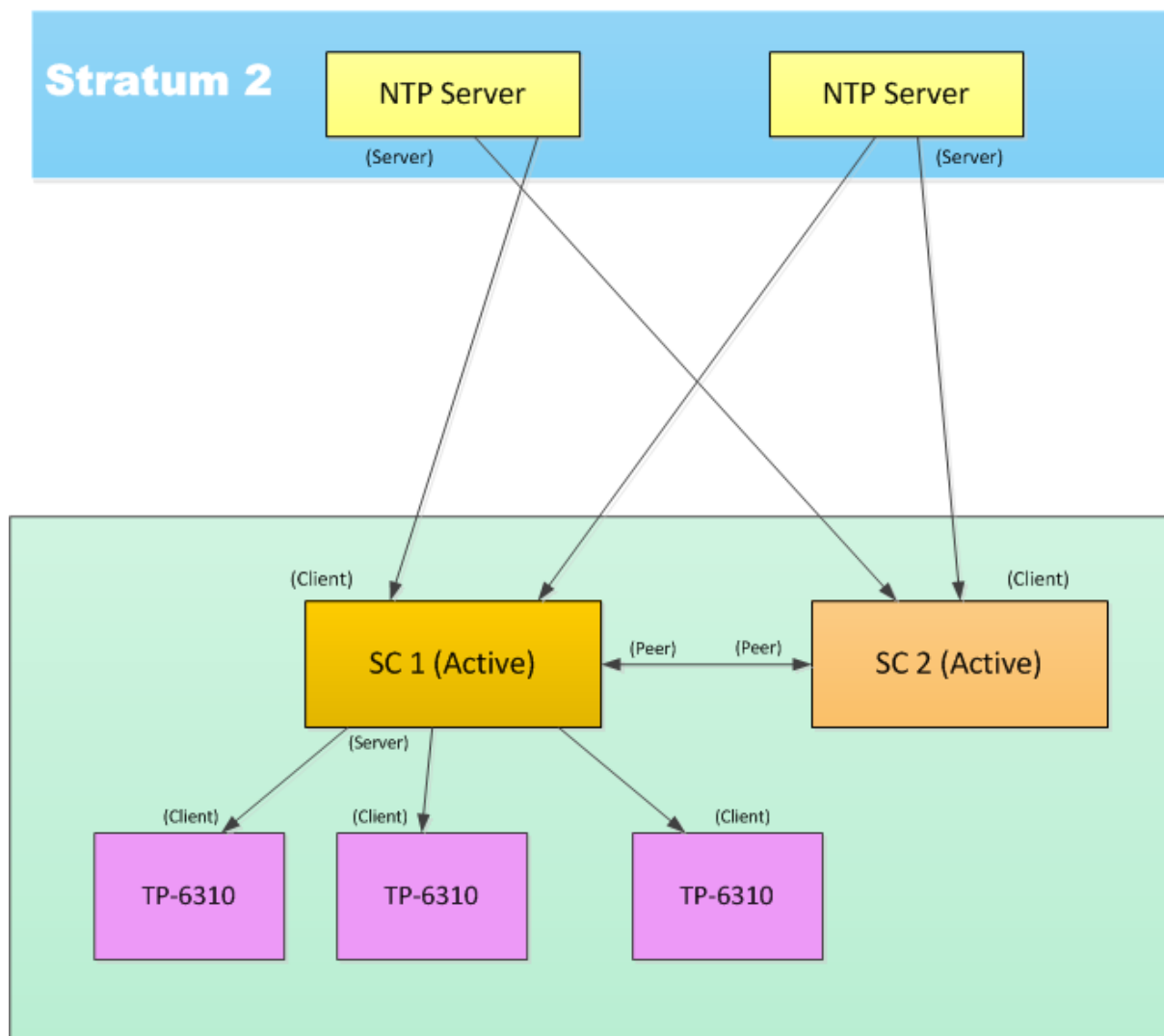
Malfunctioning or suspicious NTP server may be temporarily disabled, by changing its **Administrative State** to *Locked*. The Media Gateway will not establish any communication with locked NTP servers and will not update their **Operational State** or **NTP Server Status** attributes.

30.5 Internal NTP Implementation

The following figure illustrates the internal implementation of the time and date synchronization service inside the Media Gateway chassis. Note the following:

- SC boards operate as NTP clients towards external NTP servers and the EMS server. They also operate as NTP servers for VoP boards inside the chassis, providing time and date synchronization to the latter.
- Peer connection between the SC boards ensures that time and date within the Media Gateway is maintained even when the connection to external NTP servers are not available.
- SC boards are capable of preserving accurate time and date for 7 days in case of the Media Gateway isolation from external NTP servers.

Figure 30-4: Internal NTP Implementation



30.6 Configuring NTP Servers

This section describes how to configure the NTP servers.

➤ **To configure the NTP server:**

1. Click  to access the Media Gateway status screen.
2. In the Navigation pane, select **Time and Date** ➤ **NTP Servers**; The NTP Servers list is displayed.
3. Use the  or  buttons to add or remove entries.
4. Select a specific row and then in the configuration pane, click **NTP Server Settings**; the NTP Server Settings screen is displayed.
5. Configure the NTP Server according to the table 'NTP Server Configuration Parameters' below.
6. Click the Maintenance icon  and select **Unlock** to activate the configuration.
7. Repeat steps 4-6 for additional external NTP Servers that are available.



Note: The NTP Servers List **always** contains the EMS server as its first entry. You may not delete or modify this entry. However you can **lock** or **unlock** this entry thus enabling/disabling synchronization with EMS server.

Table 30-1: NTP Server Configuration Parameters

Parameter Name	Type	Provisioning Type	Description
Name	STRING[40]	Instant	Name of the NTP Server
IP Address	STRING[20]	Online	IP Address of the NTP Server
Burst Mode	ENUM – yes/no	Online	Burst mode for the NTP Server. This mode enables sending of multiple packets instead of a single one when server is reachable.
iBurst Mode	ENUM – yes/no	Online	iBurst mode for the NTP Server. This mode enables sending of multiple packets instead of a single one when server is unreachable.

Parameter Name	Type	Provisioning Type	Description
Prefer Mode	ENUM – yes/no	Online	Prefer this NTP Server to others.
NTP Version	INTEGER 3-4 Default=4	Read-Only	NTP Version number to be used for outgoing NTP packets.

30.7 Viewing NTP Servers' Status

➤ To view NTP servers' status:

1. Click the  button to access the Media Gateway status screen.
2. In the Navigation pane, select **Time And Date** ➤ **NTP Servers**; the NTP Servers list is displayed.
3. Select a specific row and then in the configuration pane, click **NTP Server Settings**; the NTP Server Settings screen is displayed.
4. Select the **General Information** tab to view the status of the NTP server as described in the table below.

Table 30-2: NTP Server Status Parameters

Parameter Name	Type	Provisioning Type	Description
NTP Server Status	Enum Reject, Falsetick, Excess, Outlyer, Selected, Candidate, SysPeer, PpsPeer	Read-Only	Indicates the status of the connectivity between the Media Gateway and the NTP server. The following values are supported: ▪ Reject – server is discarded due to high stratum and/or failed sanity checks ▪ Falsetick – server is designated false ticker by the intersection algorithm ▪ Excess – server is picked out from the end of the candidate list ▪ Outlyer – server is discarded by the clustering algorithm ▪ Selected – server is selected for synchronization, however distance exceeds maximum ▪ Candidate – server is included in the final synchronization selection list ▪ SysPeer – server is selected for synchronization ▪ PpsPeer – server is selected for synchronization; Pulse-per-second (PPS) signal in use
Reference ID	String	Read-Only	Identifies the reference clock of a specific NTP Server. A Reference ID that starts with 127.127 indicates that the NTP Server currently generates the clock from its local clock source (hardware clock).

Parameter Name	Type	Provisioning Type	Description
Administrative State	Enum Locked, Unlocked	Read-Only	Determines whether the Media Gateway uses a specific NTP Server as a synchronization source . If locked, the specific NTP Server is not used for time and date synchronization.
Operational State	Enum Enabled, Disabled	Read-Only	Determines whether the NTP communication with the NTP Server is available. Note that the Enabled NTP Server is not necessarily a valid synchronization source. for more information, see Section the NTP Server Status parameter above .
Stratum	String	Read-Only	Stratum level of the NTP server's local clock
Poll Time	String	Read-Only	Maximum interval between successive messages, in seconds to the nearest power of 2.
Reachability	String	Read-Only	Shift register of 8 bits used to determine the reachability status of the peer, with bits entering from the least significant (rightmost) end. A peer is considered reachable if at least one bit in this register is set to one.
Delay	String	Read-Only	Roundtrip delay of the peer clock relative to the local clock over the network path between them (seconds).
Offset	String	Read-Only	Offset of the peer clock relative to the local clock, (seconds).
Jitter	String	Read-Only	Jitter of the peer clock relative to the local clock, (seconds).
Dispersion	String	Read-Only	Maximum error of the peer clock relative to the local clock over the network path between them (seconds).
Root Delay	String	Read-Only	Total roundtrip delay to the primary reference source at the root of the synchronization subnet (seconds).
Root Dispersion	String	Read-Only	Maximum error relative to the primary reference source at the root of the synchronization subnet (seconds).

Parameter Name	Type	Provisioning Type	Description
Reference Timestamp	String	Read-Only	Local time, in timestamp format, when the local clock was last updated. If the local clock has never been synchronized, the value is zero.
Originate Timestamp	String	Read-Only	Local time, in timestamp format, at the peer when its latest NTP message was sent. If the peer becomes unreachable, the value is set to zero.
Receive Timestamp	String	Read-Only	Local time, in timestamp format, when the latest NTP message from the peer arrived. If the peer becomes unreachable the value is set to zero.
Transmit Timestamp	String	Read-Only	Local time, in timestamp format, at which the NTP message departed the sender.

This page is intentionally left blank.

31 Configuring the MGCP/MEGACO Protocols

This chapter describes configuration of the MEGACO call control protocols on the Mediant 8000. It consists of two major parts:

- The first sections provide an overview of the MGCP/MEGACO protocols and describes the corresponding Mediant 8000 configuration entities.
- 'Configuring MGCP/MEGACO Call Control Settings' on page 283 provides the detailed configuration instructions.

31.1 Media Gateway Controller

The Mediant 8000 can communicate with a number of Media Gateway Controllers / Call Agents via MGCP/MEGACO protocols. In the EMS, each Media Gateway Controller (MGC) is represented by a MGC entity, in which a set of IP addresses and call control protocol parameters are defined.

Media Gateway boards are associated with the MGC entity. Multiple Media Gateway boards may be associated with the same MGC entity. In this case, a single Media Gateway Controller has control over multiple Media Gateway boards.

Multiple MGCs may be used for one of the following reasons:

- Load distribution (e.g., for scalability purposes)
- Traffic engineering
- A mixture of call control protocols

When the MEGACO protocol is used, the Media Gateway board may be divided into Virtual Gateways. Each Virtual Gateway may be associated with a different MGC entity. See 'MEGACO Virtual Gateways' on page 282 for details.

31.1.1 Media Gateway Controller in the EMS

The Status of the Media Gateway Controller is represented by the standard **Operational State** and **Administrative State** attributes:

- The **Operational State** of an MGC entity represents the status of the MGC's configuration inside the Media Gateway and not the **real** status of the Media Gateway Controller equipment. Therefore, in a typical configuration it is **Enabled** even when the Media Gateway Controller is physically disconnected from the network.
- The **Administrative State** of an MGC entity represents the ability to configure its Online parameters and summarizes the **Administrative State** of all of the Media Gateway boards associated with this MGC. When all of the Media Gateway boards are **Locked**, the administrative status of the MGC is also **Locked**. When at least one Media Gateway board is **Unlocked**, the administrative status of the MGC is **Unlocked**.

It is impossible to directly alter the **Administrative State** of an MGC entity by performing **Lock** or **Unlock** actions on it. Instead, perform the **Lock** or **Unlock** actions on the associated Media Gateway boards and the **Administrative State** of the MGC is updated accordingly.

➤ To configure the basic Media Gateway Controller parameters:

1. Click  to access the Media Gateway status screen.
2. Select the specific Media Gateway board.
3. In the Navigation pane, select **Call Control** ➤ **MGCs**; the MGCs list is displayed.
4. Use the  or  buttons to add or remove entries.
5. Select a specific row and then in the configuration pane, click **Call Control Settings**; the Call Control Settings screen is displayed.
6. Configure the MGC parameters according to the table below.
7. Click the Maintenance icon  and select **Unlock** to activate the configuration.

31.2 MGCP Control Protocol

The MGCP (Media Gateway Control Protocol) is a standards-based network control protocol, as defined by IETF RFC 3435 and RFC 3660.

In MGCP architecture, call control intelligence resides outside the Media Gateway and is handled by the external call control element, the Call Agent (Media Gateway Controller). The Media Gateway contains endpoints on which the Call Agent can create, modify and delete connections to establish and control media sessions with other endpoints. In addition, the Call Agent can instruct the endpoints to detect certain events and generate signals. The endpoints automatically communicate changes in service state to the Call Agent. Also, the Call Agent can audit endpoints, as well as the connection on endpoints.

31.3 MEGACO Control Protocol

The Megaco (**ME**dia **GA**teway **CO**ntrol) protocol is a standards-based network control protocol, as defined by IETF RFC 3015 and ITU-T H.248.

Similar to MGCP architecture, in Megaco architecture, call control intelligence resides outside the Media Gateway and is handled by the external call control element, the Media Gateway Controller. On the Media Gateway side, the connection is handled using two elements: Terminations and Contexts.

Termination is the basic element of the call. There is a physical Termination representing a physical entity (e.g., B-channel), and an ephemeral Termination representing the generated stream. To create a connection, a Context is used. A Context contains one or more Terminations and describes the topology between the Terminations. A typical connection creation command creates a new Context and adds into it one physical Termination and one new (ephemeral) Termination. The ephemeral Termination parameters describe the media type and the stream direction (SendReceive, SendOnly or ReceiveOnly).

31.4 Media Gateway Controller Addressing

There are two alternative methodologies for addressing the MGC:

- via FQDN name
- via IP addresses

31.4.1 Via FQDN Name

When the MGC is addressed via **FQDN name**, the FQDN is resolved to the IP address through the DNS server. The DNS server can return a single IP address or a list of up to 10 IP addresses.

The Media Gateway boards' restart procedure is complete only when the DNS server responds to a DNS query successfully. If a DNS resolution fails, the Media Gateway board keeps trying to resolve the FQDN name until the resolution succeeds and a valid set of IP addresses is received. The first IP address returned by DNS is considered to be a **Primary Call Agent** IP address.

Redundant DNS servers may be configured as an alternative means of FQDN name resolution.

31.4.2 Via IP Addresses

If the MGC is to be addressed via IP addresses, you must provision a fixed list of IP addresses. Up to 10 IP addresses may be defined. The priority of the IP addresses is specified via the **Activity Order** parameter – the lower the value, the higher the priority. The IP address with the highest priority (lowest Activity number) is considered to be the **Primary Call Agent IP** and the rest of the addresses are considered to be **Redundant Call Agent IPs**.

The Media Gateway board always sends its events/alarms to the **Primary Call Agent IP**, unless a protocol-specific mechanism is used to modify this default behavior (e.g., Notified Entity element in MGCP messages).

If the **Primary Call Agent IP** address stops responding, the Media Gateway board's retransmission mechanism sends commands to the **1st Redundant Call Agent IP**, then to the **2nd Redundant Call Agent IP**, etc.

31.5 Endpoint Name Provisioning

This section describes the endpoint name provisioning.

31.5.1 Physical Terminations

The **Physical Terminations** are provisioned via the **Phys Term Name Pattern** parameter that contains the Endpoint Name template. Indexes (e.g. Board#, Trunk# and Channel#) are indicated in the template by * (asterisk) character. The exact meaning of each * (asterisk) character is determined according to the **Phys Termination Type** and **Include Board Index** parameters as follows:

- When **Include Board Index** parameter is set to **Yes**, the first * (asterisk) character is substituted by Board#

Remaining * (asterisk) characters are substituted according to the **Phys Termination Type** parameter as follows:

Table 31-1: Physical Termination Types

Phys Termination Type	Pattern Substitution
TGW: Trunk TS	The pattern should contain two additional * (asterisk) characters – to be substituted by Trunk# and Channel# accordingly.
TGW: T3 Trunk TS	The pattern should contain three additional * (asterisk) characters – to be substituted by DS3 Interface#, Trunk# and Channel# accordingly.
V5.2: Interface Port	The pattern should contain two additional * (asterisk) characters – to be substituted by V5.2 Interface# and Port# accordingly.
V5.2: SubRack Card Port	The pattern should contain three additional * (asterisk) characters – to be substituted by V5.2 SubRack#, Card# and Port# accordingly. Division of V5.2 ports into "cards" and "sub-racks" is performed according to the "max count" values set in the MGC Pattern Level table for Port# and Card# indexes, as described below.

The starting number (offset) and maximum count of Trunk#, Channel# and other "index" elements can be controlled via the MGC Pattern Level table, located in the same provisioning frame. The table is populated with entries, according to the value of **Phys Termination Type** parameter and is updated when **Apply** button is clicked.

31.5.2 Ephemeral Terminations (for MEGACO only)

Ephemeral Terminations are provisioned via the **MEGACO RTP Term Name Pattern** parameter. Indexes (Board# and Termination#) are indicated in template by the * (asterisk) character.

- At least one * characters should be present in the template – to be substituted by Termination#.
- If the template contains two * characters – the 1st * is substituted by Board#.

The starting number of Termination# can be controlled via the **MEGACO RTP Term Offset** parameter.

31.5.2.1 Example 1

Phys Term Name Pattern = ds/e1-*/*

Include Board Index = "no"

Phys Termination Type = "TGW: Trunk TS"

Trunk# Offset = 1

TS# Offset = 1

Endpoint name (board 8, trunk 2, channel 10): ds/e1-2/10

31.5.2.2 Example 2

Phys Term Name Pattern = BR*/TR*/TS*

Include Board Index = "yes"

Phys Termination Type = "TGW: Trunk TS"

Trunk# Offset = 1

TS# Offset = 1

Endpoint name (board 8, trunk 2, channel 10): BR8/TR2/TS10

31.5.2.3 Example 3

Phys Term Name Pattern = al/*/*/*

Include Board Index = "no"

Phys Termination Type = "V5.2: SubRack Card Port"

SubRack# Offset = 1

Card# Offset = 1

Card# Max Count = 10

Port# Offset = 1

Port# Max Count = 10

Endpoint name (board 8, V5.2 port# 123): al/1/2/3

31.6 Domain Name Provisioning

The MEGACO endpoint termination identifiers have two components:

- **Endpoint Name** – a local name within the gateway

Domain Name – the domain name of the gateway that is managing the endpoint
These components are delimited by the @ symbol. An example of this is:

<Endpoint Name>@<Domain Name>

For configuring the **Endpoint Name** part, see 'Endpoint Name Provisioning via Termination Name Patterns' above.

The **Domain Name** part may be configured via the **FQDN name** parameter of the Media Gateway board:

- If the **FQDN name** is empty or equals "none" (default configuration), the IP address of the Media Gateway board surrounded by square brackets is used as the domain name.
- If the criteria above is not met, the configured **FQDN name** is used as domain name.

31.7 MEGACO Virtual Gateways

The Mediant 8000 supports MEGACO Virtual Gateway functionality, as defined in the H.248.1 spec, section 11.1 "Multiple Virtual MGs". Each Media Gateway board may be divided into up to three virtual gateways (VGWs). Each virtual gateway registers and operates autonomously with its own controlling MGC(s).



Note: Virtual Gateway functionality is available for MEGACO call control protocol only.

➤ To activate MEGACO Virtual Gateway functionality:

1. Set the Media Gateway Controller's (MGC's) call control protocol to MEGACO.
2. Define Virtual Gateway (VGW) configuration objects for the specific Media Gateway board. Specify E1/T1 trunks that belong to the specific Virtual Gateway.
3. Associate MGC with a specific Media Gateway board.
4. Use the **Virtual GW** parameter in MGC's IP/FQDN address to associate it with a specific Virtual Gateway.

31.8 Configuring MGCP/MEGACO Call Control Settings

To configure MGCP/MEGACO Call Control settings, perform the following tasks:

- Configure Virtual Gateways (if applicable)
- Configure Media Gateway Controllers
- Associate Media Gateway Controllers with Media Gateway Boards and/or Virtual Gateways
- Configure additional MGCP/MEGACO Call Control Settings

31.8.1 Configuring MEGACO Virtual Gateways

When the MEGACO call control is used, the Media Gateway board may be divided into up to three Virtual Gateways. Each virtual gateway registers and operates autonomously with its own controlling MGC(s).

To define Virtual Gateway functionality, up to three Virtual Gateway (VGW) configuration objects may be created for a specific Media Gateway board, as described below. Each VGW configuration object contains a list of E1/T1 trunks and a numeric **Virtual Gateway Index** that is used to associate MGC IP/FQDN addresses with the specific Virtual Gateway. By default, for each Media Gateway board, a single VGW configuration object with index 1, which covers all available trunks for this Gateway board, is created.

➤ To configure MEGACO Virtual Gateways:

1. Click  to access the Media Gateway status screen.
2. In the Navigation pane, select **Call Control** ➤ **Virtual GWs**; the Virtual GWs list is displayed.
3. Use the  or  buttons to add or remove entries.
4. Select a specific row and then in the configuration pane, click **Virtual GW Settings**; the Virtual Gateway Settings screen is displayed.
5. Configure the Virtual Gateway parameters according to the tables below.

Table 31-2: Virtual Gateway Parameters

Parameter Name	Type	Provisioning Type	Description
Name	String Up to 17 chars	Instant	User-defined Virtual Gateway name, used to identify it easily.
Virtual GW Index	Index 1 – 3	Offline	Defines numeric Virtual Gateway index, that is used to associate MGC IP/FQDN addresses with the specific Virtual Gateway.

Parameter Name	Type	Provisioning Type	Description
Network Subnet	Integer 0 – 10	Online	Defines index of the Network Subnet to be used for communication with the specific Virtual Gateway. Default value 0 means that the first Control Subnet will be used.
Local Port	Integer 0 – 65535	Online	Defines the port to be used by the Media Gateway Controller to communicate with this Virtual GW. Default value (0) means that the port is selected according to encoding method (2944, 2945).
Message Identifier	String Up to 200 chars	Online	Defines Message Identifier (MID). If set to not empty value, overrides the MG/Board FQDN. By default, "[IP address]:Port" MID is used.
Load Weight	Integer 1 – 5	Online	Defines the weight of the VGW out of the total load. VGW with higher values process more messages. The priority is applicable between VGW with different network configuration (port, transport type, realm).
Media Realm	Integer 0 – 16	Online	Defines the default Media Realm.
MEGACO Version	Integer 1 – 3	Online	Defines the version of the MEGACO protocol.
Service Change Profile	String Up to 64 chars	Online	Defines the service change profile.
Associated Trunks List	String Up to 64 chars	Online	Defines the list of the E1/T1 trunks that belong to specific Virtual Gateway. Trunks are specified by their number (index). Multiple trunks may be specified using comma delimiter (for enumeration) or dash delimiter (for range definitions). E.g. "1,2,4,10-13". A special line can be used as the default group. This line MUST contain the string DEFAULT LINE. Every trunk which is not defined in one of the other groups will belong to this line. Note that if two default lines are entered, the first one only will be used. Each E1/T1 trunk may belong to one VGW only.

31.8.2 Configuring Media Gateway Controller

The Media Gateway Controller configuration consists of two major parts:

- Configuring generic Media Gateway Controller settings
- Configuring Media Gateway Controller IP/FQDN addresses

When “IP Address” MGC addressing mode is used, up to 10 MGC IP addresses may be defined (for each Virtual Gateway). Priority of the IP addresses is specified via the 'Activity Order' parameter – the lower the Activity Order value, the higher the priority.

When the “FQDN” MGC addressing mode is used, only one MGC FQDN address may be defined (for each Virtual Gateway).

It is impossible to directly modify the administrative state of the Media Gateway Controller (i.e. lock or unlock it). Instead, associate it with specific Media Gateway boards (as described in 'Associating Media Gateway Controller with Media Gateway Boards' on page 288) and lock/unlock the latter. The Media Gateway Controller's Administrative state will be updated as follows:

- If at least one associated Media Gateway board is unlocked, MGC is unlocked.
- If all associated Media Gateway boards are locked, MGC is locked.

➤ To configure the generic Media Gateway Controller settings:

1. Click  to access the Media Gateway status screen.
2. In the Navigation pane, select **Call Control** ➤ **MGCs**; the MGCs list is displayed.
3. Use the  or  buttons to add or remove entries.
4. Select a specific row and then in the configuration pane, click **MGC Settings**; the MGC Settings screen is displayed.
5. Configure the MGC parameters according to the tables below.

Table 31-3: Media Gateway Controller Parameters

Parameter Name	Type	Provisioning Type	Description
MGC Name	String Up to 20 chars	Instant	Defines textual Media Gateway Controller name enabling users to identify it easily.
Control Protocol	Enum None, MEGACO, MGCP	Online	Defines the call control protocol type (MEGACO, MGCP).
MEGACO Check MGC Legality	Enum Disabled, Enabled	Instant	Defines whether the Mediant 8000 rejects MEGACO commands from an MGC with an IP address not included in the provisioned list
MGCP Version	String Up to 32 chars	Online	Defines the MGCP protocol version.

Parameter Name	Type	Provisioning Type	Description
Referenced By	String Up to 255 chars	Read-only	Indicates all the Media Gateway boards associated with this Media Gateway Controller.

Table 31-4: Media Gateway Controller Addressing Parameters

Parameter Name	Type	Provisioning Type	Description
Addressing Type	Enum IP Address, FQDN	Read-only	Indicates the addressing type of the Media Gateway Controller. This parameter is automatically updated upon MGC unlock, according to the Address Format of the configured MGC IP/FQDN addresses.
MGCP – Redundant CA FQDN	String Up to 80 chars	Online	Defines the redundant FQDN name of the Media Gateway Controller. Applicable to the MGCP call control protocol only.

Table 31-5: Media Gateway Controller Endpoint Names Parameters

Parameter Name	Type	Provisioning Type	Description
Phys Term Name Pattern	String Up to 30 chars	Online	Defines the name pattern of the MGC's physical_terminations. See 'Physical Terminations' on page 280 for more details.
Include Board Index	Enum No, Yes	Online	Defines whether the Board Index is included in the physical termination name.
Phys Termination Type	Enum TGW: Trunk TS, TGW: T3 Trunk TS, V5.2: Interface Port, V5.2: SubRack Card Port, Other	Online	Defines the physical termination type..
MEGACO RTP Term Name Pattern	String Up to 30 chars	Online	Defines the name pattern of the MEGACO RTP terminations. See 'Ephemeral Terminations (for MEGACO only)' on page 280 for more details.

Parameter Name	Type	Provisioning Type	Description
MEGACO RTP Term Offset	Integer 0 – 2147483647	Online	Defines the offset to be used in the MEGACO RTP terminations.

➤ **To configure the Media Gateway Controller's IP/FQDN addresses:**

1. Click  to access the Media Gateway status screen.
2. In the Navigation pane, go to **Call Control** ► **MGCs** and select the specific Media Gateway Controller added/configured above.
3. In the Navigation pane, select **CA Address**; the MGC IP/FQDN Addresses list is displayed.
4. Use the  or  buttons to add or remove entries.
5. Select a specific row and then in the configuration pane, click **CA Address Settings**; the MGC IP/FQDN Address Settings screen is displayed.
6. Configure the MGC IP/FQDN Address parameters according to the table below.

Table 31-6: MGC IP/FQDN Address Parameters

Parameter Name	Type	Provisioning Type	Description
Address Format	Enum IPv4(0), DNS(2)	Online	Defines the format of the MGC address. IPv4 – up to 10 IP addresses may be specified (for each Virtual GW); priority of each address is defined by its Activity Order property (lower values correspond to higher priority) DNS – only one MGC FQDN address entry may be defined (for each Virtual GW); the FQDN is resolved to the IP address through the DNS protocol; up to 10 IP addresses may be returned by the DNS
MGC Address	String Up to 30 chars	Online	Defines the MGC Address – IP address or FQDN
MGC Port	Integer 0 – 65535	Online	Defines the IP port number that MGC is listening on.
Transport Type	Enum UDP, TCP, SCTP	Online	Defines the signaling transport type to be used while communicating with this MGC.
Activity Order	Integer 1 – 10	Online	Defines priority of the MGC IP Address within the specified Virtual Gateway. IP addresses

Parameter Name	Type	Provisioning Type	Description
			with lower Activity Number have higher priority. IP address with highest priority will be used as Primary IP, and the rest - as redundant IPs.
Virtual GW Index	Integer 1 – 3	Online	Defines the index of Virtual GW, that this MGC Address applies to. For MEGACO protocol: the value must match a value of Virtual GW Index parameter in one of the Virtual GW configuration objects, defined for associated Media Gateway boards; by default the value is set to 1 and corresponds to a default Virtual GW that represents Media Gateway board "as a whole". For MGCP protocol: leave it at its default (1) to associate the MGC with the default Virtual GW that represents the Media Gateway board "as a whole".

31.8.3 Associating Media Gateway Controller with Media Gateway Boards

This section describes how to associate the Media Gateway Controller with the Media Gateway board.

➤ **To associate the Media Gateway Controller with the Media Gateway board:**

1. Click  to access the Media Gateway status screen.
2. Select the Media Gateway board.
3. In the Navigation pane, select Call Control and in Configuration pane, click **Call Control Settings**; the Call Control Settings screen is displayed.
4. Configure the **MGC Group** parameter to match the index of the Media Gateway Controller configured in the previous section.

31.8.4 Configuring Additional MGCP/MEGACO Settings

This section describes how to configure additional MGCP/MEGACO Settings.

➤ **To configure additional MGCP/MEGACO Settings:**

1. Click  to access the Media Gateway status screen.
2. Select the Media Gateway board.
3. In the Navigation pane, select **Call Control** and then in the configuration pane, click **Call Control Settings**; the **Call Control Settings** screen is displayed.
4. Configure the additional MEGACO parameters as described in the table below.

Table 31-7: Media Gateway Board's Call Control Parameters

Parameter Name	Type	Provisioning Type	Description
Board FQDN	String Up to 40 chars	Online	Defines the FQDN name of the Media Gateway board. If the FQDN name is empty or equals "none", the IP address of the Media Gateway board surrounded by square brackets is used as the domain name when constructing MEGACO/MGCP messages. Otherwise the FQDN name is used instead.
MGC Group	Integer -1 – 14	Online	Defines Media Gateway Controller (MGC) to which this board is associated. Value -1 is used when the MEGACO/MGCP call control protocols are not used for specific board – e.g. in case of SIP application.
Control Protocol	Enum None, MEGACO, MGCP	Read-Only	Indicates the call control protocol of the Media Gateway Controller associated with the specific board.
Call Control Compatibility Profile	Integer 1 – 2147483647	Online	Defines the Call Control compatibility profile.

Parameter Name	Type	Provisioning Type	Description
SDP Behavior	Integer 0 – 2147483647	Instant	Defines a bitmap that determines SDP processing capabilities. ▪ RFC3407, Simple Capabilities support ▪ V.152, VBD Support ▪ Support FRC ▪ Strict Negotiation ▪ T,S,O Line Display ▪ Hard coded (10ms) PTIME for transparent coder ▪ Always reply with Local SDP ▪ Use G711 as the Bypass coder as well ▪ Symmetric payloads ▪ Use Audio port for T38 call ▪ Prefer Remote in SDP Negotiation
H.248.32 Thresholds Hysteresis (%)	Integer 1 – 20	Instant	Defines the Thresholds Hysteresis (in %) for the H.248.32 Package reports.
MEGACO TDM Hairpinning	Enum Disable, Enable	Online	Defines the H.248 2 TDM endpoints connection mode: Disable - connect two TDM terminations through internal IP loopback. In this mode 2 DSP are used and channels will be opened with the default coder and default configuration (according to the board configuration). Enable - connect two TDM terminations through Internal PCM Loop. In this mode no DSP is used.
MEGACO Resources Optimization	Enum Disable 1 DSP, Enable 1 DSP, Enforce Full DSP	Instant	Enables optimization of the IP Media resource usage for MEGACO protocol. Disable 1 DSP – two RTP terminations with the same SDP configuration: no DSP is allocated. On different configurations, two DSPs are allocated. Enable 1 DSP – same as in the previous case, however with one DSP option for two RTP terminations, where at least one termination uses the G.711 coder with "ptime = 20". Enforce Full DSP – enforce two DSP allocations for any SDP configuration (For Statistic report).

Parameter Name	Type	Provisioning Type	Description
MGCP Timeout - 1st ReTx	Integer 50 – 1000	Instant	Defines the MGCP timeout for the first retransmission (in msec). The retransmission intervals thereafter increase exponentially.
MGCP Comm T/out Layer	Integer 1 – 3600	Instant	Defines the maximum time to wait for an MGCP response before declaring a disconnection (in sec). Used for retransmission.
Use Wildcard With RSIP	Enum Trunk, Board Or TPM	Online	This parameter applies to MGCP only. Defines the RSIP Restart messages generation level. When set to <i>Trunk</i> , RSIP Restart messages are generated on a per-trunk basis. When set to <i>Board Or TPM</i> , RSIP Restart messages are generated on a per-board basis.
DLCX by GW	Enum Enable, Disable	Instant	This parameter applies to MGCP only. Enables a Delete connection (DLCX) message from the media gateway side.
Disconnect On Broken Connection	Enum NotConfigured, Disable, Enable	Instant	Defines whether the device releases the call if RTP packets are not received within a user-defined timeout. The timeout is set by the parameter Broken Connection Timeout .
Broken Connection Timeout (100 msec)	Integer 3 – 21474836	Instant	Defines the amount of time (in 100 msec units) an RTP packet isn't received, after which a call is disconnected. Applicable only if Disconnect On Broken Connection parameter is set to <i>Enabled</i> . Currently this feature works only if Silence Suppression is disabled.
Digit Map Name	String Up to 10 chars	Online	Defines the name of the provisioned digit map.
Digit Mapping	String Up to 151 chars	Online	Defines the digit map patterns separated by a vertical bar (), as defined in the MEGACO RFC.

This page is intentionally left blank.

32 V5.2 Access Gateway

32.1 Overview

V5.2 is a standardized protocol suite for the connection of Access Networks (AN) to the Local Exchange (LE) usually implemented in a traditional PSTN Class-5 switch.

V5.2 Access Gateway application implements the LE side of the V5.2 protocol. It aggregates legacy circuit-switched voice from the subscriber side, converts V5.2 protocol messages to H.248 IP protocol and then hands them off to a softswitch and vice versa. The gateway and the softswitch may be used as a replacement for traditional Class 5 PSTN switch.

The V5.2 Access Gateway application implemented on the Mediant 8000 has the following capabilities:

- Support for E1 trunks on TP-8410 Media Gateway boards only.
- Supported by the Mediant 8000 redundancy mechanism (refer to Working with Media Gateway boards -> Redundancy Model for details).
- V5.2 Links: each TP-8410 board features 42 E1 trunks that may be configured as V5.2 links or as E1 transparent trunks (without voice – e.g. for PSTN clock synchronization).
- V5.2 Interfaces: the E1 trunks, configured as V5.2 links, are divided into groups or V5.2 interfaces of 2-16 E1s each. Up to 30 V5.2 interfaces are supported.
- Signaling Channels: a V5.2 interface uses 2 timeslots for signaling (active and standby) in separate V5.2 links called Primary and Secondary links (Protection Group). In both signaling links, the timeslot 16 is dedicated to the V5.2 signaling. Under normal circumstances, a V5.2 interface starts up with the signaling on the Primary link.
- Voice Channels: in all V5.2 links, timeslots 1 to 31 (except for timeslot 16 in signaling links) are used as voice channels.
- User Ports: each TP-8410 board supports up to 10,000 PSTN user ports distributed across the V5.2 interfaces; the number of user ports per V5.2 interface is determined by the following formula: $300 * \text{"Number of Trunks"}$ – e.g. if the V5.2 interface has 16 trunks – up to 4800 user ports may be defined on it.

32.1.1 Working with the V5.2 Access Gateway

The following chapters describe the maintenance actions available on V5.2 entities that may be used to maintain and monitor V5.2 Access Gateway application.

32.1.1.1 V5.2 Interface Status and Maintenance Actions

The V5.2 Interface uses a management model that is slightly different from the other Mediant 8000 entities. The standard **Administrative State** attribute and corresponding **Unlock/Lock** actions are used to add/remove the configuration of the corresponding V5.2 Interface to/from the corresponding Media Gateway board. The following additional attributes are used to indicate the actual and desired state of the service provided by the V5.2 Interface:

- **Interface Admin State** – indicates the desired service state on the V5.2 Interface; valid values are:
 - Offline – indicates the user request to stop the service on the specific V5.2 Interface
 - In Service – indicates the user request to start the service on the specific V5.2 Interface
- **Interface Operational State** – indicates the actual service state on the V5.2 Interface; valid values are:
 - Offline – service is not provided due to local "Offline" request by user
 - Busy – service is not provided due to some communication error with the far-end

In Service – V5.2 Interface is "in service" The following maintenance actions are supported on the V5.2 Interface:

- **Add / Remove** – adds/removes V5.2 Interface
- **Unlock / Lock** – adds/removes the configuration of the corresponding V5.2 Interface to/from the corresponding Media Gateway board (note that it's not enough to **Unlock** the V5.2 Interface to bring it to service – you must also use **In Service** action described below)
- **In Service / Offline** – indicates the user request to start/stop the service on the corresponding V5.2 Interface
- **Protection Switchover** – user-initiated switchover between the primary and the secondary signaling V5.2 links; applicable only when the Interface's Operational State is "In Service". The Mediant 8000 also performs automatic switchover between signaling links when a problem at the physical or data link layers is detected. However there is no automatic switchback when the failed link recovers.

32.1.1.2 V5.2 Link Status and Maintenance Actions

The V5.2 Interface uses an additional attribute – **Link Operational State** – to indicate its precise status. The valid values are:

- Operational – link is "in service"
- Failed – service is not provided due to some communication error with the far-end
- Blocked – service is not provided due to **Block** maintenance request by local user
- Blocked and Failed – service is not provided due to both **Block** maintenance request by local user and a communication error with the far-end

The following maintenance actions are supported on V5.2 Links:

- **Add / Remove** – adds/removes V5.2 Link
- **Unlock / Lock** – adds/removes the configuration of the corresponding V5.2 Interface to/from the corresponding Media Gateway board (note that it's not enough to **Unlock** the V5.2 Link to bring it to service – you must also use **In Service** action on the corresponding V5.2 Interface)
- **Block / Unblock** – temporarily stops/starts the service on the corresponding V5.2 Link; if user port is busy (in call), the **Block** action is deferred until the port goes on-hook; block/unblock actions may also be performed by the soft-switch
- **Link ID Check** – initiates the link identification check that ensures that there is no mismatch between the ends of the link; the link's **Link ID Check Status** attribute is updated accordingly. In addition to the manual initiation (by user), the identification check is automatically performed on a V5.2 link by either peer at startup time or after the link recovers from a physical failure.

32.1.1.3 V5.2 User Ports Status

The Mediant 8000 maintains the current V5.2 User Ports configuration in an auxiliary file named **SlotX_V52_FILE.csv**. The file can be found in auxiliary files repository (refer to 'Auxiliary Files Repository' on page 422) and may be downloaded to your PC and opened in a text or CSV editor to view the current V5.2 User Ports configuration.

➤ **To download the V5.2 User Ports Configuration File:**

1. Click  to access the Media Gateway status screen.
2. In the Navigation pane, select **Management ► Files**; the Files list is displayed.
3. Find an auxiliary file that represents the current V5.2 User Ports configuration on the specific Media Gateway board (it is named **SlotX_V52_FILE.csv**, where X is the slot number, and its file type is "V5 Ports Configuration").
4. Right-click on the auxiliary file and choose **Download File** action.
5. Choose the location where to download the file (either on your PC or on a file server) and press **OK**.

32.1.2 Configuring the V5.2 Access Gateway

Perform the following steps to configure the V5.2 Access Gateway application:

- Configure Media Gateway board's PSTN parameters
- Configure trunks that carry V5.2 links
- Configure V5.2 Interfaces
- Configure V5.2 Links
- Configure V5.2 User Ports
- Complete configuration by bringing V5.2 interfaces "In Service"

32.1.2.1 Configuring Media Gateway board's PSTN parameters

Prior to configuring the Media Gateway board's PSTN parameters, you must configure the PSTN Media Gateway board parameters described in this section.

➤ To configure the Media Gateway board's PSTN parameters:

1. Click  to access the Media Gateway status screen.
2. Select the desired TP-8410 Media Gateway board.
3. In the Navigation pane, select **Media** and in the Configuration pane, click **Media Settings**; the Media Settings screen is displayed.
4. The following Media Gateway board's PSTN parameters should be configured to ensure the proper operation of the V5.2 Access Gateway application:
 - **Default Caller ID** = *ETSI(1)*
 - **Caller ID Transport** = *Relay(1)*
 - **ETSI Caller ID Type** = *ETSIBetweenRings(0)*

32.1.2.2 Configuring Trunks for the V5.2 Access Gateway application

Prior to configuring the V5.2 Access Gateway application, you must configure DS1 Trunks as described in this section.

➤ To configure Trunks for the V5.2 Access Gateway application:

1. Click  to access the Media Gateway status screen.
2. Select a TP-8410 Media Gateway board.
3. In the Navigation pane, select **PSTN ► DS1 Trunks**; the DS1 screen is displayed.
4. Select a specific E1 trunk and in the Configuration pane, select **Trunk Settings**; the Trunk Settings screen is displayed.

5. E1 Trunks that carry V5.2 Links must be configured as follows:
 - **Protocol Type** = V5(43)
 - **V5.2 Number Of C-channels** : for trunks that carry signaling V5.2 links, set the value to 1; otherwise set the value to 0.
 - **V5 Protocol Side** = LE(1)

32.1.2.3 Configuring V5.2 Interfaces

When configuring V5.2 interfaces, for each new V5.2 Interface, configure **Interface ID** and **Variant ID** parameters to match the remote PSTN side.

➤ **To configure V5.2 Interfaces:**

1. Click  to access the Media Gateway status screen.
2. Select the desired TP-8410 Media Gateway board.
3. In the Navigation pane, select **PSTN ▶ V5.2 ▶ V5.2 Interfaces** and in the Configuration pane, click **V5.2 Interfaces**; the V5.2 Interfaces list is displayed.
4. Use the  or  buttons to add or remove entries.
5. Select a specific row and in the Configuration pane, click **V5.2 Interface Settings**; the V5.2 Interface Settings screen is displayed.
6. Configure V5.2 Interface parameters as described in the table 'V5.2 Interface Properties' below.
7. Click the Maintenance icon  and select **Unlock** to activate the configuration.

Table 32-1: V5.2 Interface Properties

Parameter Name	Type	Provisioning Type	Description
V5.2 Interface Name	String Up to 200 chars.	Instant	User-defined name (textual) for the V5.2 Interface, enabling users to identify it intuitively and easily.
Interface ID	Integer 0-16777215	Online	Defines the V5.2 Interface ID towards the peer entity.
Variant ID	Integer 0-127	Online	Identifies a set of configuration parameters.
Logical C-Channel ID	Integer 0-65535	Online	Identifies a set of signaling c-paths.
Trace Level	Integer 0,20-23	Instant	The trace-level indication for the V5.2 protocol.

32.1.2.4 Configuring V5.2 Links

Add new V5.2 Links voice and signaling links as required. Use Trunks and V5.2 Interfaces defined in the previous steps to complete the V5.2 Links configuration. Ensure that for each V5.2 Interface, two signaling V5.2 Links – primary and secondary – are defined.

➤ To configure V5.2 Links:

1. Click  to access the Media Gateway status screen.
2. Select the desired TP-8410 Media Gateway board.
3. In the Navigation pane, select **PSTN ▶ V5.2 ▶ V5.2 Links** and in the Configuration pane, click **V5.2 Links**; the V5.2 Links list is displayed.
4. Use the  or  buttons to add or remove entries.
5. Select a specific row and in the Configuration pane, click **V5.2 Link Settings**; the V5.2 Link Settings screen is displayed.
6. Configure V5.2 Link parameters as described in the table 'V5.2 Link Properties' below.
7. Click the Maintenance icon  and select **Unlock** to activate the configuration.

Table 32-2: V5.2 Link Properties

Parameter Name	Type	Provisioning Type	Description
V5.2 Link Name	String Up to 200 chars.	Instant	User-defined name (Textual), for the V5.2 Link, enabling users to identify it intuitively and easily.
Link ID	Integer 0-127	Online	Defines the V5.2 Link ID within the V5.2 Interface.
V5.2 Interface ID	Integer 0-30	Online	Defines the V5.2 Interface to which the V5.2 Link belongs.
Link Type	Enum Normal, Primary, Secondary	Online	Defines the V5.2 Link Type.

32.1.2.5 Configuring V5.2 User Ports

- The V5.2 user ports are configured via a V5.2 User Ports Configuration File. The file contains commands that allow the addition or removal of user ports belonging to all the V5.2 interfaces.
- The configuration file is constructed by the user (typically using a text editor – e.g. Notepad) and applied to the Mediant 8000 via the **Download V5.2 Configuration Port File** action on the corresponding TP-8410 Media Gateway board. For consistency, it is recommended to use .csv extension for V5.2 User Ports configuration file.

32.1.2.5.1 V5.2 User Port Configuration File Format

The V5.2 User Port configuration file is a CSV comma separated file. Each line in the file might be either:

- The Header or Version Line - It is the first line in the file. It describes the version number as follows:

```
; 1.0 version
```

- A Comment Line - It should start with ";" and may be placed anywhere in the file, but not before the header line.
- A Command Line - A command line configures one PSTN user port or line. This line format is as follows:

```
<command>,<Interface number>, <port number>,<Layer3 address>
```

It should comply with the following rules:

- The command may be "add" or "del".
- Up to 10,000 user ports may be configured on this file.
- An Interface number should be in the range of 0 to 30.
- A Port number should be unique within the V5.2 interface and in range between 0 and 4799.
- An L3 address should be unique within the V5.2 interface and in a range between 0 and 32766.

The following is an example of a V5.2 User Ports Configuration File:

```
; 1.0 version  
; add to V5.2 Interface 12 the port 35 with L3 address 4000  
add,12,35,4000  
; add to V5.2 Interface 17 the port 22 with L3 address 2345  
add,17,22,2345
```

32.1.2.5.2 Downloading the V5.2 User Ports Configuration File

A V5.2 User Ports Configuration file must be uploaded to the EMS Software Manager and then downloaded to the specific TP-8410 Media Gateway board via **Download V5.2 Configuration Port File** action. You may choose whether the specified V5.2 User Port configuration file is applied as "additional" V5.2 ports configuration (i.e. incrementally added to the existing configuration) or as "entire" configuration (i.e. all previous configuration is removed).

➤ To download the V5.2 User Ports Configuration File:

1. Upload the configuration file to the EMS Software Manager:
 - a. From the **Tools** menu, select **Software Manager**. The Software Manager screen is displayed.
 
 - b. In the upper left corner, click . The add Files screen is displayed.
 - c. In **Auxiliary Files** tab, select V5.2 Configuration File type.
 - d. Click  and choose the prepared V5.2 User Ports configuration file (stored on your PC or on some network file server).
 - e. In the **File Description** field, type a meaningful description.
 - f. Click  to add the configuration file to the list.
 - g. Repeat steps c)-f) if you have several V5.2 User Port configuration files
 - h. Click **OK**. The files are uploaded to the EMS.
2. Ensure that all applicable V5.2 Interfaces are in the 'Offline' state
 - a. Access the V5.2 Interfaces List screen (as described in 'Configuring V5.2 Interfaces' on page 297).
 - b. Verify that all applicable V5.2 Interfaces are in the Offline state.
 - c. If some interfaces are not, right click on the corresponding entry and choose the **Offline** action.
3. Download the V5.2 User Ports Configuration File to the TP-8410 Media Gateway board:
 - a. Access the V5.2 Interfaces List screen (as described in 'Configuring V5.2 Interfaces' on page 297) and ensure that all applicable V5.2 Interfaces are in the Offline state. If some interfaces are not, right click on the corresponding entry and choose **Offline** action.
 - b. Click  to access the Gateway status screen.
 - c. Right-click on the specific TP-8410 Media Gateway board and choose **Maintenance -> Download V5.2 Configuration Ports File**.
 - d. Choose whether the downloaded file contains "additional" or "entire" V5.2 User Ports configuration.
 - e. Choose the V5.2 User Ports file (uploaded to the EMS in the previous step) and press **OK**.

4. Verify the V5.2 User Ports Configuration File download result:
 - a. When the configuration file is downloaded to the TP-8410 Media Gateway board, an operation status screen is displayed showing the summary of the applied V5.2 User Ports configuration.
 - b. Upon successful V5.2 User Ports configuration file download, the summary screen will include the following:
 - ◆ Number of lines added
 - ◆ Number of lines removed
 - ◆ Number of lines duplicate
 - ◆ Number of lines that don't exist
 - c. If the configuration file download fails, the summary screen will display the exact reason for the failure; for example:
 - ◆ Bad file version ID
 - ◆ File validation error

32.1.2.6 Bringing V5.2 Interfaces "In Service"

To complete the V5.2 configuration, bring all configured V5.2 Interfaces "In Service".

In order to do this, access the V5.2 Interfaces List screen (as described in 'Configuring V5.2 Interfaces' on page [297](#)). Right-click on the corresponding row and choose **In Service** action.

This page is intentionally left blank.

33 Configuring Security Settings

The Mediant 8000 requires IP network connectivity for its normal operation and therefore is subject to security attacks that may be launched by malicious users. To ensure secure operation of the Mediant 8000 take the following steps:

- Implement security features in the IP network to which the Mediant 8000 is connected (e.g. by limiting physical access to the network and using firewalls).
- Configure and maintain security features on the Mediant 8000 as described in this chapter.

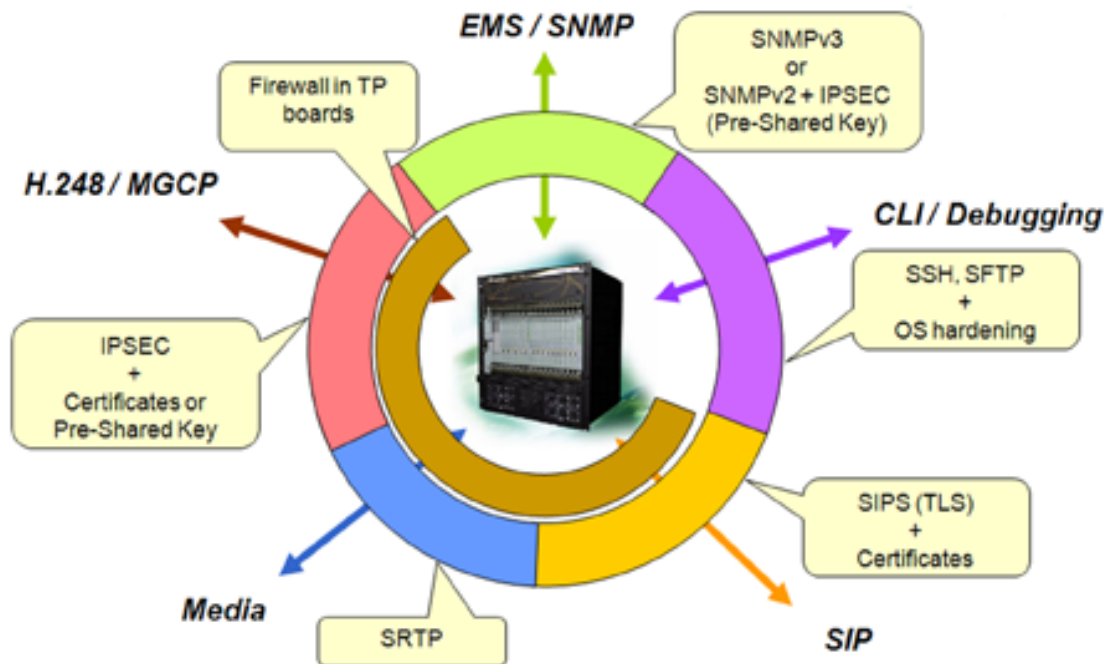
The Mediant 8000 provides the following security-related features:

- Security for OAM (management) interfaces:
 - Secure Operation Mode
 - Secure access to the SNMP interface (via SNMPv3 and/or SNMPv2+IPSEC)
 - Secure access to the CLI interface (via SSH and SFTP/SCP)
 - Disabled Remote Root Login
 - OS Hardening
 - OS Security Patches (on SC boards)
 - OS Auditing (on SC boards)
 - File Integrity Check
 - Firewall (on Media Gateway boards)
- Security for Call Control interfaces:
 - MGCP/MEGACO over IPSEC/IKE
 - SIPS (TLS) with X.509 Certificates
 - Firewall (on Media Gateway boards)
- Security for Media interfaces:
 - SRTP (with either ARIA or AES crypto suites)
 - Firewall (on Media Gateway boards)

In addition to the above list, subnet separation (as described in 'Configuring Network Topology' on page 182) may be used to separate between different types of traffic and to implement additional security at the network level (by preventing access of malicious users to specific network segments).

The figure below illustrates the most commonly used security features and interfaces/applications that they protect.

Figure 33-1: Security Features



Each security feature addresses a specific threat. For example, SNMPv3 protects the management interface and SRTP provides security for the media traffic. To enable proper Media Gateway operation in a hostile network environment, ensure to implement security features for all applicable Mediant 8000 components (boards), network segments (subnets) and applications.

33.1 Security Configuration Guidelines

The following guidelines are provided as a starting point for users who wish to implement basic security features on the Mediant 8000 Media Gateway. For a detailed description of each feature and for the additional security features, see the chapters below.

➤ **To implement basic security features on the Mediant 8000:**

1. Configure the Mediant 8000 to operate in a Secure Mode. See 'Secure Operation Mode' on page 306 for details.
2. Configure the Mediant 8000 to use secure version of management protocol – SNMPv3 or SNMPv2+IPSEC. Change default values of SNMP community strings (for SNMPv2) and passwords (for SNMPv3). Modify configuration of the EMS server and additional SNMP managers to match the new SNMP protocol configuration. See 'Configuring Connectivity with EMS Server' on page 153 for details.
3. Change passwords for all users on the Mediant 8000 CLI interface, including **root** and **ems** user, Remove all unused CLI users. See 'Administering Media Gateway's CLI Users on SC Boards' on page 361 for details.
4. Configure the Mediant 8000 to use a secure version of Call Control protocol. Alternatively, use a dedicated subnet for transmitting the call control traffic and implementing the appropriate security measurements and network level (e.g. by using firewalls). See 'Configuring IPSEC/IKE for Call Control and Signaling Interfaces (on TP boards)' on page 346 and 'SIP over SSL/TLS (SIPS)' on page 349 for details.
5. Configure the Mediant 8000 to use SRTP to secure Media traffic. Alternatively, use a dedicated subnet for transmitting the media traffic and implement appropriate security measurements and network level. See 'Media Security' on page 350 for details.

After the initial configuration of the Mediant 8000 security features, the following periodic maintenance tasks must be performed to ensure that the Mediant 8000 continues to operate in a secure manner. The frequency at which these tasks should be performed is determined by security policy on site.

➤ **To ensure that the Mediant 8000 continues to operate in a secure manner, perform the following periodic maintenance tasks:**

1. Periodically inspect Mediant 8000 trap notifications for security alarms and events. Take appropriate actions if needed.
2. Periodically change passwords for all users on the CLI interface (including **root** and **ems** user) and delete unused CLI users.
3. Periodically change SNMP community strings (for SNMPv2) and passwords (for SNMPv3).
4. Periodically change “pre-shared keys” used to secure call control and media traffic.
5. Periodically upgrade the Media Gateway software to receive the latest security fixes and OS patches.

33.2 Secure Operation Mode

The Secure Operation Mode must be enabled on the Mediant 8000 Media Gateway as a first step toward a secure configuration and prior to enabling additional security-related features.

When the Secure Operation mode is enabled, the following changes are applied to the Media Gateway:

- Insecure access to the CLI management interface (via Telnet) is disabled
- Insecure file transfer (via FTP) is disabled

The Secure Operation mode is enabled by default on the SC Rev.2 boards (using the Linux OS). For SC Rev.1 boards (using the Solaris OS), use the procedures described in the following sections to enable/disable Secure Operation mode.



Note: The Secure Mode is automatically enabled for SC Rev.2 boards (using the Linux OS) as part of the Mediant 8000 software installation.

When Secure Operation mode is enabled on SC Rev.1 boards (using the Solaris OS), the network sniffer utility **snoop** is removed from its standard location and archived in the **/Project/uninstall/snoop.gz** file. This archive file is used to restore the **snoop** utility to its default location when the Secure Operation Mode is disabled. Use the **rm /Project/uninstall/snoop.gz** command to delete the archive from the SC board altogether.

33.2.1 Enabling Secure Operation Mode



Note: The following procedures apply to SC Rev.1 boards (using the Solaris OS) only. Secure Mode is automatically enabled for SC Rev.2 boards (using the Linux OS).

The Media Gateway software must be stopped on both SC boards prior to changing the Secure Operation Mode configuration.

➤ **To enable Secure Operation Mode:**

1. Connect to the CLI interface on both SC boards. Use SSH protocol (and not Telnet) when connecting via the IP network. For more information, see Section 'The Command Line Interface (CLI)' on page [107](#)
2. Login as **root** user. For more information, see Section 'Logging in as a Root User' on page [115](#).
3. To stop Media Gateway software on both SC boards, on each SC board, at the prompt, type **tools sc dn** and press **Enter**. When prompted to confirm this command type **y** and press **Enter**.

```
client238::~~# tools sc dn
STOP SC SOFTWARE
```

```
Stop SC software? ([y]/n) : y
```

```
>>> Stop watchdog process...
>>> Wait for application to stop...
```

4. Perform basic configuration of the Media Gateway software on the SC board in Slot 1, as described in 'Performing Basic Configuration of the Mediant 8000 Software on the SC board to Operate as the Active Board' on page [147](#). At the **Enable Security** prompt, choose **1**.
5. Perform basic configuration of the Media Gateway software on SC board in Slot 2, as described in 'Performing Basic Configuration of the Mediant 8000 Software on the SC Board to Operate as the Standby Board' on page [150](#).
6. Reboot both SC boards.

33.2.2 Disabling Secure Operation Mode

This section describes how to disable the Secure Operaiton mode.



Note: The following procedures apply to SC Rev.1 boards (using the Solaris OS) only. Secure Mode is automatically enabled for SC Rev.2 (using the Linux OS) boards and cannot be disabled .

➤ To disable Secure Operation Mode:

- Repeat the same steps as described in 'Enabling Secure Operation Mode ' on page [307](#) above; however at the **Enable Security** prompt, choose **0** and press **Enter**.

33.3 Secure Access to the SNMP Management Interface

The SNMP management interface is used by EMS server and/or standards-compliant 3rd party SNMP managers to perform most of the Mediant 8000 management, configuration and status monitoring tasks. For detailed description, see 'SNMP Management Interface' on page [170](#).

The Mediant 8000 supports the following SNMP operational modes:

- **SNMPv2** – a simple default management mode widely deployed in many closed networks; has a relatively weak security model based on the plain-text read and write community strings and therefore is a security threat for systems connected to the public networks (e.g. Internet).
- **SNMPv2 + IPSEC** – a secure version of the SNMPv2 management mode; communication between the Media Gateway and the EMS server is secured via IPSEC/IKE protocol with a pre-shared key; any additional 3rd party SNMP manager must have valid IPSEC/IKE association to be able to access Media Gateway's SNMP interface.
- **SNMPv3** – the latest and secure version of the SNMP management protocol; use of IPSEC/IKE with SNMPv3 is not recommended, because SNMPv3 has its own authentication and encryption mechanisms.

For secure operation of the Mediant 8000 choose SNMPv2 + IPSEC or SNMPv3 management modes.

- See 'Configuring Connectivity between Media Gateway and EMS Server' on page [171](#) for detailed description on how to configure SNMP management mode and establish connectivity with EMS server.

- See 'Configuring Connectivity between the Media Gateway and Additional SNMP Managers' on page 174 for detailed description on how to configure connectivity with additional SNMP managers.
- See 'Configuring IPSEC/IKE for Management Interfaces (on SC boards)' on page 341 for a detailed description on how to configure the SNMPv2 + IPSEC management mode.

33.4 Secure Access to the CLI Interface

Secure access to the CLI management interface is achieved via the use of the Secure Shell (SSH) protocol. Associated file transfer protocols – Secure Copy (SCP) and Secure FTP (SFTP) – are used for transferring files to/from the Mediant 8000.

33.4.1 SSH Protocol

The Secure Shell (SSH) is a standard protocol that allows the establishment of a secure channel between a local and remote computer. It provides authentication, confidentiality and integrity of data exchanged between the two computers.

The Mediant 8000 uses SSH v2 to encrypt CLI management sessions. SSH connection is available even when Secure Operation mode is disabled and is a preferred connection type for the CLI management interface.

33.4.2 SCP and SFTP Protocols

Secure Copy (SCP) and Secure FTP (SFTP) are associated protocols that support files transfer over SSH connections. They are used to transfer backup files and debug data to/from the SC boards on the Mediant 8000 Media Gateway. For better performance and shorter file transfer times, use the SCP protocol instead of SFTP.

33.5 Disabled Remote Root Login

The Mediant 8000 does not allow use of **root** username when logging into the CLI interface via the IP network. This measurement reduces the chances of a successful brute force attack on **root** super-user account and is considered to be a common practice.

Users who require **root** permissions on the Mediant 8000's CLI interface, are still able to login as **root** user. However the login procedure is more complicated than for regular CLI users and leaves appropriate traces in system security log. see 'Logging in as a Root User' on page 115 for more details.

The Disabled Remote Root Login feature was not available in v3.2 or earlier of the Mediant 8000 software and for these versions is not enabled by default during the Online Software Upgrade. If you upgraded the Mediant 8000 from the version where the remote root login was not disabled, disable it manually as described below as soon as possible.

33.5.1 Enabling a Direct Remote Root Login

If due to exceptional circumstances, you need to enable remote root login to the specific SC boards, this can be done as follows:



Note: Enabled remote root login constitutes a severe security flaw. Therefore you should disable it immediately after completing the specific maintenance task.

➤ To enable a direct remote ROOT login:

1. Connect to CLI interface on the specific SC board. For more information, see Section 'The Command Line Interface (CLI)' on page 107.
2. Login as the **root** user. For more information, see Section 'Logging in as a Root User' on page 115.
3. At the prompt, type **tools user** and press **Enter**.
4. At the **Choose submenu** prompt, type **remote_root_login** and press **Enter**.

```
client238::/# tools user
```

```
CLI USERS MANAGEMENT
```

```
list          -- LIST: list CLI users
add           -- ADD: add user
del           -- DELETE: delete user

pwd           -- PASSWORD: change user password
copy          -- COPY: copy users & passwords from other SC

lock          -- LOCK: lock user
unlock        -- UNLOCK: unlock user
force         -- FORCE: force user to change password

remote_root_login -- REMOTE ROOT LOGIN: enable/disable remote root user login
Choose submenu : remote_root_login
```

5. At the **Enable/Disable Remote root Login** prompt, type **enable** and press **Enter**. Remote root login is enabled on the specific SC board.

```
REMOTE ROOT LOGIN
```

```
Enable/Disable Remote root Login ([disable]/enable) : enable
Remote root login was enabled.
```

33.5.2 Disabling a Direct Remote Root Login

This section describes how to disable the remote root login. You should perform this procedure in one of the following circumstances:

- If you have performed the Online Software Upgrade from the version where remote root login was enabled.



Note: Ensure that at least one CLI user is defined on both SC boards and provisioned with a known password. Otherwise, you will be unable to establish connection with the SC board's terminal over the IP network..

- If you have manually enabled the remote root login as described in the previous section.

➤ **To disable a direct remote ROOT login:**

- Repeat the steps described in 'Enabling a Direct Remote Root Login' on page 310; however at the **Enable/Disable Remote root Login** prompt, type **disable** and press **Enter**.

33.6 OS Hardening

The Mediant 8000 software automatically performs “hardening” of the Operating System on all its boards to minimize the risk of service disruption on any Mediant 8000 component by malicious user (hacker).

For SC boards, OS hardening is implemented according to the DoD IASE Security Technical Implementation Guidelines (STIGs) and includes the following:

- Unnecessary Solaris services and daemons are shut down.
- Permissions on OS configuration and binary files are adjusted to prevent their modification by malicious users.
- TCP/IP stack is tuned to prevent DoS attacks (including SYN and Smurf attacks).

For the Media Gateway (TP-6310 and TP-8410) and ES boards, OS hardening is achieved via the use of non-generic real-time OS and real-time design of the software that implements only services that are imperative for the board's operation.

33.7 OS Security Patches (on SC boards)

The Mediant 8000 software includes the latest relevant Operating System (OS) security patches released by 3rd party vendors (e.g. Linux or Sun Microsystems). These OS patches are automatically installed on the SC boards during the Mediant 8000 installation and/or Online Software Upgrade.

The OS security patches are updated at the following times:

- In each major Mediant 8000 software release (e.g. in Version 6.6 GA)
- In minor (maintenance) Mediant 8000 software releases – only if critical security patches are available or if the update is explicitly requested by customer

The OS security patches are considered to be part of the Mediant 8000 software and therefore are typically deployed via the regular software installation and/or upgrade procedures. Use of the matching versions of Mediant 8000 software and OS security patches, ensures that the Mediant 8000 software operates in a well-defined environment and eliminates the risk of incompatibility between the Mediant 8000 software and the underlying OS.

OS security patches may be upgraded via one of the following options:

- By upgrading the Mediant 8000 software to a latest version via the regular Online Software Upgrade procedure – this is the preferred option.
- By installing OS security patches from a latest Mediant 8000 Installation Package while maintaining the existing core Mediant 8000 software version.
- By installing OS patches from a standalone “OS security patch bundle” provided on customer request.

33.7.1 Installing OS Security Patches from a Latest Installation Package

This section describes how to install OS security patches from a latest Mediant 8000 Installation Package (e.g. 6.6.32) while preserving the existing core Mediant 8000 software version (e.g. 6.6.20).



Note: The procedure described in this chapter should be performed only as part of the Mediant 8000 software upgrade, as described in 'Pre-installing OS Patches' on page 817

➤ **To install OS security patches from a latest installation package:**

1. Determine which SC board currently operates as the Active and which as the Standby board, as described in 'Working with the SC Boards' on page 223.
2. Transfer the latest installation package to both SC boards as described in . 'Transferring the Mediant 8000 Installation Package to the SC Boards' on page 130. The package will be transferred to the home directory of the logged in CLI user (e.g. **acladmin**).
3. Connect to the CLI interface on the Standby SC board. For more information, see Section 'The Command Line Interface (CLI)' on page 107.
4. Login as **root** user. For more information, see Section 'Logging in as a Root User' on page 115.
5. Stop the Mediant 8000 software on the Standby SC board, by typing **tools sc dn** and pressing **Enter**. When prompted to confirm this command, type **y** and press **Enter**.

```
client238::~~# tools sc dn
STOP SC SOFTWARE
```

```
Stop SC software? ([y]/n) : y
```

```
>>> Stop watchdog process...
>>> Wait for application to stop...
```



Note: The Mediant 8000 software must be stopped on the Standby SC board during the OS patches installation. This however has no effect on the Mediant 8000 operation except for the fact that the SC board's redundancy is temporarily unavailable.

6. At the prompt, type **install ~acladmin/tg_6.6.32.install os_patch** and press **Enter**. Replace **acladmin** with the name of the CLI user that you used while transferring the Mediant 8000 package to the SC board. Replace

tg_6.6.32.install with the name of the latest Mediant 8000 installation package.
Don't forget to specify **os_patch** as the last command argument.

```
client241::~~# install ~acladmin/tg_6.6.32.install os_patch
```

```
Core Network Media Gateway
```

```
Version : 6.6.15
```

```
OS patches installation
```

```
WARNING: installation of OS patches may take up to 1 hour  
and may require reboot of the SC board.
```

```
To minimize the effect on Media Gateway service, install OS patches on  
the Standby SC board first (typically in Slot 2), then perform SC  
switchover and install OS patches on the remaining SC board.
```



Note: On SC boards with v5.6 or earlier software version installed, the **install** command may produce no output. In that case, use the following commands to start the Mediant 8000 software installation:

```
rm -f os_patch  
chmod u+x ~acladmin/tg_6.6.32.install  
~acladmin/tg_6.6.32.install os_patch
```

7. When you are prompted if you wish to start installation, type **y** and press **Enter**.
The OS patches installation begins.

```
Start installation? (y/n) : y  
Extracting /tmp/sc_software.tar installation archive... done  
Extracting OS patches... done  
Applying 118558-39 (1 of 2)... done  
Applying 140426-01 (2 of 2)... done (reboot required)
```

```
The following OS patches were successfully installed: 118558-39; 140426-01.
```

8. Wait patiently till the OS patches installation completes. For SC Rev.1 boards (using the Solaris OS) it may take up to 1 hour to install the latest OS patches. For SC Rev.2 boards (using the Linux OS), the OS patches installation typically takes less than 5 minutes.
9. After the OS patches installation successfully completes, you are prompted to reboot the SC board. At the prompt, type **y** and press **Enter**.

• SC board must be rebooted to complete *
• the OS patches installation !!! *
Reboot now? (y/n) [y]: y

10. The SC board reboots. It typically takes 2 minutes to complete the reboot. The Media Gateway software starts automatically after the SC board completes the reboot.
11. Perform SC activity switchover as described in 'Working with the SC Boards' on page 223.
12. Repeat steps 2-9 on the SC board that currently operates as Standby (initially operated as Active).
13. Perform SC activity switchover as described in 'Working with the SC Boards' on page 223 to restore the initial Mediant 8000 software configuration.

33.7.2 Installing the Latest OS Security Patches from the “OS Security Patch Bundle”

The “OS security patch bundle” is a special installation package that contains only the latest OS security patches (without the core Mediant 8000 software) and is provided on customer request.

Installation of the latest OS security patches from the “OS security patch bundle” is very similar to the procedure described in Installing OS Security Patches from a Latest Version Installation Package' above.

➤ **To install the latest OS Security Patches from the “OS Security Patch Bundle”:**

1. Complete steps 1-5 as described in the above procedure.
2. In step 6, at the prompt, specify **install ~acladmin/tg_os_patch_22_Apr_09.install** and press **Enter**. Replace **acladmin** with the name of the CLI user, that you used while transferring the “OS security patch bundle” to the SC board. Replace **tg_os_patch_22_Apr_09.install** with the name of the “OS security patch bundle”.

```
client241::~~# install ~acladmin/tg_os_patch_22_Apr_09.install
```

3. Complete steps 7-12 as described in the above procedure.

33.8 File System Integrity

A File System Integrity Check is implemented on SC boards and provides an additional security mechanism that helps to mitigate security risks such as hacker intrusion and malicious software installation. Since all Mediant 8000 software and configuration is stored on the SC boards and then distributed to the corresponding Mediant 8000 components (including Media Gateway and ES boards), implemented integrity measures essentially apply to the Mediant 8000 as a whole.

When the Media Gateway software is installed, a snapshot of the file system is created. This snapshot covers both the Media Gateway software and OS components, and includes both binary and configuration files.

Media Gateway software periodically scans file system and compares it against the snapshot. When unauthorized modifications are detected, a notification alarm is sent to the EMS and the integrity status of the SC board's file system is updated accordingly.

Each SC board performs the File System Integrity Check independently and reports the results accordingly.

33.8.1 Viewing the File System Integrity Status

The File System Integrity Status may be viewed via both the EMS GUI (basic status report) and dedicated CLI (advanced status report).

➤ To view the basic File System Integrity Status (via the EMS GUI):

1. Click  to access the Media Gateway status screen.
2. Select the desired SC board.
3. In the Configuration pane, click **SC Board Settings**; the SC Board Settings screen is displayed.
4. Review Parameters in the **Filesystem Integrity** tab as described in the 'Filesystem Integrity Status Parameters' table below.

Table 33-1: Filesystem Integrity Status Parameters

Parameter Name	Type	Provisioning Type	Description
File System Integrity Status	Enum, ok/failure	Read-only	Indicates File System Integrity Status.
Integrity Unauthorized Files	String	Read-only	When unauthorized modifications to the file system are detected, the exact names of the modified files are listed. This attribute has a limited length. For a complete list of modified files, use the command tools fs status as described below.

When unauthorized modifications to the file system are detected, the **File System Integrity Status** attribute of the corresponding SC board is changed to failure and the **Integrity Unauthorized Files** attribute is updated with the list of modified files. However, if the list of modified files is too long, it may not fit into the **Integrity Unauthorized Files** attribute. The following procedure enables you to view a complete list of modified files.

➤ **To view the advanced File System Integrity Status (via CLI):**

1. Connect to the CLI interface on the specific SC board. For more information, see Section 'The Command Line Interface (CLI)' on page 107.
2. Login as a CLI user with administrative privileges (e.g. **acladmin**). For more information, see Section 'Logging into the Command Line Interface' on page 115.
3. At the prompt type **tools fs status** and press **Enter**.

```
client238::~~# tools fs status
```

```
INTEGRITY CHECKING STATUS
```

```
Last Integrity Scan:
Thu Jan 11 15:09:34 GMT 2007
*** Detected Integrity Violation! ***
Affected Files:
```

```
/etc/hosts - CHANGED
/etc/hosts.old - ADDED
```

33.8.2 Scheduling File System Integrity Check

A File System Integrity check is performed on a daily basis. By default, the check is run at 2:00 AM; however, a user may modify this time to match the period when the amount of the traffic being served by the Media Gateway is low.

➤ To set the time of the File System Integrity Check:

1. In the EMS, click  to access the Media Gateway status screen.
2. In the Navigation pane, select **Security** and then in the configuration pane, click **Security Settings**; the Security Settings screen is displayed.
3. Modify the **File System Integrity Check Time** parameter according to the table below.

Table 33-2: Filesystem Integrity Configuration Parameters of the Media Gateway

Parameter Name	Type	Provisioning Type	Description
Integrity Check Time	String in HH:MM format	Instant	Time of the day when File System Integrity Check is performed daily. Format is HH:MM (24-hour clock). Default value is 2:00 (corresponds to 2:00 AM).

33.8.3 Restoring File System Integrity

When File System Integrity is violated, approach the corresponding SC board and restore the integrity via one of the following options:

- Unnecessary new files must be deleted.
- Necessary new files must be "acknowledged" as described below.
- Changed files may be restored from the backup or copied from the uncompromised SC board. Following this, they must be "acknowledged" as described below.
- Deleted files may be restored from the backup or copied from the uncompromised SC board. After completing either of these options, you must "acknowledge" the file deletion by providing the directory name to the **tools fs ack** command (see below).

When modified files are acknowledged, they are added to the File System snapshot. Acknowledged files are later removed from File System Integrity Check reports, unless further modifications are detected. When all compromised files are acknowledged, **File System Integrity Status** displays **OK**.

➤ To acknowledge changed files:

1. Connect to the CLI interface on the specific SC board. For more information, see Section 'The Command Line Interface (CLI)' on page 107.
2. Login as **root** user. For more information, see Section 'Logging in as a Root User' on page 115.
3. Review all compromised files. Remove malicious modifications from the files by restoring them from the backup or copying them from the uncompromised SC board. Delete all new and unneeded files.
4. For each file fixed in the previous step, at the prompt type **tools fs ack <filename>** and press **Enter**.

```
client238::~~# tools fs ack /etc/hosts
client238::~~# tools fs ack /etc/hosts.old
```

5. When all files are acknowledged, run File System Integrity Scan by typing **tools fs scan** and pressing **Enter**. Wait till the scan completes.

```
client238::~~# tools fs scan
```

6. If all problems are fixed, **File System Integrity Status** displays **OK** and the following report is produced.

```
INTEGRITY CHECKING STATUS
```

```
Last Integrity Scan:
Thu Jan 11 15:09:34 GMT 2007
*** No Integrity Violation Detected ***
```

33.9 OS Auditing on SC Boards

OS auditing is implemented on the SC boards and provides the capability to log the activity on a system at a granular level. The provided functionality complies with the Trusted Computer System Evaluation Criteria (TCSEC) at security level C2 and Common Criteria security requirements.

33.9.1 Auditing Goal

The primary goal of auditing is to record user actions to detect malicious intent. The problem is to determine which events generate plausible information, and which events generate negligible information that are so common that they clutter the audit trail.

The secondary goal of auditing is to avoid performance degradation. The more audit events recorded, the greater is the load on the system.

33.9.2 Auditing Trail File

When an event occurs, it is recorded in the Audit Trail File. The latter file contains all relevant audit data in a binary form. Some tools are required to examine the data in a human readable format. An administrator should periodically examine the Audit Trail File and analyze system behavior based on the recorded events.

The Solaris and Linux OS provide some basic report tools that may be used to examine the Audit Trail File. These report tools provide a good starting point for analyzing the auditing data; however for advanced auditing analysis and automatic intrusion detection and prevention, 3rd party Intrusion Detection Systems (IDS) should be used.

33.9.3 OS Auditing on the Mediant 8000 Media Gateway

When the Mediant 8000 Media Gateway software is installed on the SC boards, it automatically configures the OS auditing subsystem to record the most important security-related activity on the SC board. The list of recorded events complies with DoD IASE STIG and GR-815 security requirements.

Audit Trail Files are stored in the **/var/audit** or **/var/log/audit directory** (on the SC Rev.1 and SC Rev.2 boards ly). The size of a single audit trail file is limited to 1 MB. Multiple files are preserved to allow the storage of audit data for at least one week.



Note: These modifications should be performed with a great care to minimize the effect on the Media Gateway performance, and in general are not recommended.

When the auditing subsystem cannot properly record or store auditing events (e.g., due to a lack of space on the hard disk), a security alarm with an appropriate description is sent to the EMS server.

OS auditing is simultaneously performed on both active and standby SC boards. Each SC board contains its own audit trail data.

33.9.3.1 Analyzing the Audit Trail File on the Solaris OS

The following basic tools, provided by the Solaris OS may be used to analyze the audit trail files on SC Rev.1 boards.

To convert the binary audit trail data into human readable ASCII format, the **praudit** command is used. **Praudit** includes a few basic options that determine single or multi-line display and delimiters; however it provides no mechanism for choosing which events are displayed.

Choosing the events is performed by using the **auditreduce** command. This command takes binary audit trail(s) as its input and generates a new binary audit trail as the output.

For example, to find all of the login events for user Alice in October 2000:

```
client238::~~# auditreduce -a 20001001 -b +31d -u alice -c lo | praudit
```

See the man pages of **praudit** and **auditreduce** commands for more information.

33.9.3.2 Analyzing the Audit Trail File on the Linux OS

The following basic tools, provided by the Linux OS, may be used to analyze the audit trail files on SC Rev.2 boards.

Use the **aureport** command to produce various type of auditing data reports.

- **aureport—summary** – generates a broad overview of the current auditing statistics (events, logins, processes etc). To obtain detailed information about a specific event category, run individual reports for the event type.

```
client238::~# aureport--summary
Summary Report
```

```
Range of time in logs: 07/30/2009 02:40:01.533 - 08/11/2009 09:30:01.811
```

```
Selected time for report: 07/30/2009 02:40:01 - 08/11/2009 09:30:01.811
Number of changes in configuration: 3240
Number of changes to accounts, groups, or roles: 286
Number of logins: 248
Number of failed logins: 0
Number of authentications: 298
Number of failed authentications: 0
Number of users: 3
Number of terminals: 24
Number of host names: 6
Number of executables: 94
Number of files: 48349
Number of AVC's: 0
Number of MAC events: 1919
Number of failed syscalls: 766839
Number of anomaly events: 371
Number of responses to anomaly events: 0
Number of crypto events: 0
Number of keys: 0
Number of process IDs: 31774
Number of events: 1103347
```



Note: The generation of a complete audit summary report (as shown above) may take a few minutes. To speed up the report generation process, use **-ts** and **-te** options as described below to generate report for a specific period of time.

- **aureport--success** – generates statistics of successful events on the SC board; the report includes the same event categories as a summary report; to retrieve detailed information about a particular event, run the individual report with **success** option, for example: **aureport -f--success** to display all successful file-related events
- **aureport--failed** – generates statistics of failed events on the SC board; the report includes the same event categories as a summary report; to retrieve detailed information about a particular event, run the individual report with **failedsuccess** option
- **aureport--l** – generates a report of all login-related events;
- **aureport--p** – generates a report of all process-related events;
- **aureport--f** – generates a report of all file-related events;
- **aureport--u** – generates a report of all user-related events;

Use the **-ts** and **-te** (for start time and end time) options with any of the above commands to limit your reports to a certain time frame. Use the **-i** option with any of these commands to transform numeric entities to human-readable text.

For example, the following command creates a login report for the time between 8 am and 5:30 pm on the current day and converts numeric entries to text:

```
client238::~~# aureport -ts 8:00 -te 17:30 -l -i
Login Report
# date time auid host term exe success event
1. 08/11/2009 08:54:04 ems 10.13.2.19 /dev/pts/0 /usr/sbin/sshd yes
299898
2. 08/11/2009 09:37:17 root 10.7.2.37 /dev/pts/2 /usr/sbin/sshd yes
302103
```

Use the **ausearch** command to find a detailed log entry of individual events.

- **ausearch -a *audit_event_id*** – shows all audit trail records carrying a particular audit event ID. Each audit event message is logged along with a message ID consisting of a UNIX epoch time stamp plus a unique event ID separated by a colon. All events that are logged from one application's system call have the same event ID. As one application's system call may trigger several events to be logged, you are likely to retrieve more than one record from the log.
- **ausearch -ul *login_id*** – shows all audit trail records associated with a particular login user ID. It displays any records related to the user login ID specified provided that the user had been able to log in successfully.
- **ausearch -m *message_type*** – shows all audit trail records related to a particular message type. Examples of valid message types include PATH, SYSCALL, USER_LOGIN. Invoking **ausearch -m** without a message type displays a list of all message types.
- **ausearch -f *filename*** – shows all audit trail records containing a certain filename. Using the filename alone works well, however using relative paths does not.
- **ausearch -p *process_id*** – shows all audit trail records related to a certain process ID.

Use the **-ts** and **-te** (for start time and end time) options with any of the above commands to limit your reports to a certain time frame. Use the **-i** option with any of these commands to transform numeric entities to human-readable text.

For example, the following command searches for all audit events related to **/etc/audit/audit.conf** file that occurred within the last week:

```
client238::~~# ausearch -ts this-week -f /etc/audit/audit.conf -i
```

```
type=PATH msg=audit(08/09/2009 16:24:07.378:201348) : item=0  
name=/etc/audit/audit.rules inode=196865 dev=08:03 mode=file,640  
ouid=root ogid=root rdev=00:00
```

```
type=CWD msg=audit(08/09/2009 16:24:07.378:201348) : cwd=/  
type=SYSCALL msg=audit(08/09/2009 16:24:07.378:201348) : arch=i386  
syscall=chmod success=yes exit=0 a0=988a8f8 a1=1a0 a2=80515d4 a3=0  
items=1 ppid=16885 pid=16886 auid=root uid=root gid=root euid=root  
suid=root fsuid=root egid=root sgid=root fsgid=root tty=pts5 ses=1041  
comm=chmod exe=/bin/chmod key=(null)
```

```
type=PATH msg=audit(08/09/2009 16:24:35.019:202009) : item=0  
name=/etc/audit/audit.rules inode=196865 dev=08:03 mode=file,640  
ouid=root ogid=root rdev=00:00
```

```
type=CWD msg=audit(08/09/2009 16:24:35.019:202009) : cwd=/  
type=SYSCALL msg=audit(08/09/2009 16:24:35.019:202009) : arch=i386  
syscall=open success=yes exit=3 a0=9a36a00 a1=8241 a2=1b6 a3=8241 items=1  
ppid=16266 pid=16311 auid=root uid=root gid=root euid=root suid=root  
fsuid=root egid=root sgid=root fsgid=root tty=pts5 ses=1041 comm=perl  
exe=/usr/bin/perl key=(null)
```

For more information, see Section the man pages for the **aureport** and **ausearch** commands.

33.10 X.509 Public Key Infrastructure

X.509 is an ITU-T standard for Public Key Infrastructure (PKI). The X.509 standard was adapted to the Internet by the IETF PKIX working group (RFC 3280) and is currently the most widely used PKI standard that is utilized by many security applications, including SIP/TLS, HTTPS (SSL) and IPSEC/IKE.

The X.509 standard is typically used by applications that perform Public Key cryptography, also known as Asymmetric cryptography. The latter is a form of cryptography in which a user has a pair of cryptographic keys – a Public Key and a Private Key. The Private Key is kept secret, while the Public Key may be widely distributed. These keys are related mathematically; however, the Private Key can not be practically derived from the Public Key. A message encrypted with the Public Key can be decrypted only with the Private Key.

X.509 Public Key infrastructure uses Certificates to bind together a Public Key with an identity information, such as the name of the person or organization and their address. The Certificates are distributed between the participating parties and can be used to verify that the Public Key belongs to an individual.

In a typical PKI scheme, Certificates are issued by a Certificate Authority (CA) and provide an attestation by the certificate signer (CA) that the identity information and the public key belong together. CAs are organized in a structured hierarchical system that represents the trust relationships between them.

Each party has a list of Trusted Root Certificates – certificates of the CAs (or their roots) that are well-known and trusted by the party. When the certificate from the other party is received, its signing entity (CA) is compared with the Trusted Root Certificates list and if the match is found, the certificate is accepted.

In the Mediant 8000 Media Gateway, X.509 Certificates are used by the following applications:

- SIP/TLS – for secure SIP call control messaging.
- HTTPS (SSL) – for internal communication between the SC and the Media Gateway boards (e.g. for online provisioning of Auxiliary Files) and for secure access to the Media Gateway board's advanced status summary via WEB interface.
- IPSEC/IKE – for secure MGCP/MEGACO call control messaging; X.509 Certificates may be used as an alternative to pre-shared key authentication mode.

The Mediant 8000 Media Gateway uses the following files to implement X.509 Public Key Infrastructure:

- **Private Key File** – contains a private key that is used to perform decryption; it is the most sensitive part of security data and should never be disclosed to other entities.
- **Certificate File** – contains a digital signature that binds together Public Key with an identity information; Certificate may be issued by a CA (e.g. Veritas) or be self-signed (issued by the entity itself).
- **CA Certificate File** – certificate of the CA that issued Certificate for the Mediant 8000 Media Gateway; optional file that if present is used to validate the Certificate file.

- **Trusted Root Certificate File** – certificate of the Trusted Root; used to authorize certificates received from the remote parties, based on the identity of the CA that issued it; if the root certificate of this CA matches one of the Trusted Root Certificates, remote party is authorized.

The Mediant 8000 Media Gateway supports the following X.509 functionality:

- Generation of Private Key and Self-Signed Certificate
- Generation of Certificate Signing Request (CSR)
- On-line provisioning of Private Key and Certificate files
- Support for up to 3 Trusted Root Certificate files
- Expiration alarm for each provisioned Certificate file
- Check certificate revocation status via the OCSP protocol

33.10.1 Initial Configuration

Upon installation of the Media Gateway software, the Private Key and Self-Signed Certificate files are automatically generated, added to the Auxiliary Files repository and configured in the Media Gateway security settings. By default, all Media Gateway boards use these self-generated Private Key and Certificate files.

You can view the configuration data for these files in the **Security Settings** tab in the Media Gateway properties screen. You can later upgrade the self-signed certificate with a genuine certificate signed by a CA and you can also upgrade the private key.



Note: The Private Key and X.509 Certificate files are configured at Media Gateway level and are shared with all Media Gateway boards inside the Mediant 8000 chassis. This reduces the amount of the certification data required to provision fully occupied Media Gateway and simplifies the hardware replacement procedure. It also makes the addition of the new Media Gateway board fully transparent to the security administrator.

33.10.2 Self-Signed Certificate

A Self-Signed Certificate is the simplest form of an X.509 Certificate that is issued by the participant itself without the use of any Certificate Authority (CA). The Self-Signed Certificate consists of the Public Key of the party that is signed by the Private Key of the party itself. The Self-Signed Certificate is typically not appropriate for field deployments, since it does not utilize CA trust relationships and its authenticity cannot be reliably verified. The Self-Signed Certificate is typically used in lab environment or for a low-scale deployment where solution security may be sacrificed in favor of simplified configuration procedures.



Note: Use of the Self-Signed Certificates for field deployments is strongly discouraged. You should instead establish PKI infrastructure and use certificates signed by the genuine CAs. Refer to the sections described below for detailed instructions.

When Self-Signed Certificates are used by both parties who participate in the secure communication, the Self-Signed Certificate for each party should be used by the other party as a Trusted Root Certificate.

Media Gateway is pre-installed with a self-signed certificate upon installation. This certificate is primarily intended to enable internal communication between the SC board and the Media Gateway boards. However, some users may wish to periodically re-generate self-signed certificates to improve its security properties (by applying the new Public Key that is part of the certificate data). The instructions below describe how this operation can be performed.

➤ **To generate a new Self-Signed Certificate:**

1. Click  to access the Media Gateway status screen.
2. In the Navigation pane, select **Security** and in Configuration pane, click **Security Settings**; the Security Settings screen is displayed.

3. Click the Maintenance Actions icon  button in the top-right corner of the screen and select the **Generate X.509 Files** option; the Generate X.509 Files dialog is displayed.

Figure 33-2: Generating X.509 Files



4. Select the **Self-Signed Certificate** button.
5. Select a Private Key to be used for generating the Self-Signed Certificate.
6. In the **Self-Signed Certificate** field, enter a name of the new Self-Signed Certificate file.
7. Click **OK**. A new self-signed certificate file is generated and automatically added to the Auxiliary Files repository.
8. To activate the new self-signed certificate you must configure it in the **Media Gateway Security Settings** screen and apply the new configuration to the Media Gateway boards. For more information, see Section 'Activating the new X.509 Certificates on the Media Gateway' on page [331](#).

33.10.3 Generating a Certificate Signing Request (CSR)

Certificate Signing Request (CSR) is a message sent from an applicant to a Certificate Authority (CA) to apply for a digital identity certificate. The CSR contains information identifying the applicant and the Public Key. The Private Key is not included in the CSR; however, is used to digitally sign the entire request. The CSR may be accompanied by other credentials or proof of identity required by the Certificate Authority, and the Certificate Authority may contact the applicant for further information.

If the request is successful, the Certificate Authority will send back an identity certificate that has been digitally signed with the Private Key of the Certificate Authority. This certificate file, together with the certificate of the CA itself, must be added to the Media Gateway Auxiliary Files repository and configured in the Security Settings screen for the Media Gateway. You must also configure the Trusted Root Certificate file on the Media Gateway, depending on the identity of the CA who signed the certificate of the other participant (e.g. of the CA who issued the certificate for the Softswitch that communicates with the Media Gateway via SIP/TLS protocol).



Note: Never send the Private Key file to anybody. It contains the most sensitive security data and should never be disclosed. Use CSR instead as described below.

➤ To generate a Certificate Signing Request (CSR):

1. Click  to access the Media Gateway status screen.
2. In the Navigation pane, select **Security** and then in the configuration pane, click **Security Settings**; the Security Settings screen is displayed.

3. Click the Maintenance Actions icon in the top-right corner of the screen and select the **Generate X.509 Files** option. The **Generate X.509 Files** dialog is displayed.



The dialog box is titled "Generate X.509 Files" and has a close button (X) in the top right corner. It contains three radio buttons for selection: "CSR", "Self-Signed Certificate", and "Private Key".

- CSR:** The "Private Key" field is a dropdown menu showing "private.key". The "Subject" field is a text box containing "CSR".
- Self-Signed Certificate:** The "Private Key" field is a dropdown menu showing "private.key". The "Self-Signed Certificate" field is a text box containing "self_signed2.cert".
- Private Key:** The "Private Key" field is a text box containing "private2.key". The "Self-Signed Certificate" field is a text box containing "self_signed2.cert".

At the bottom right, there are "OK" and "Cancel" buttons.

4. Select the **CSR** button.
5. Select a Private Key to apply to the Certificate Signing Request.
6. In the **Subject** field, enter a brief description of the Certificate Signing Request.
7. Click **OK**. The **CSR** file is generated and the **Save As** dialog is displayed.
8. Enter the name of the CSR file and choose a folder on your computer where you wish to save it.
9. Send the CSR file to the Certificate Authority.

33.10.4 Adding Certificates to the Auxiliary Files Repository

After successfully generating the CSR and submitting it to the CA, you receive a digitally signed X.509 Certificate file from the CA. You should also have a certificate of the CA itself (for verification purposes) and a certificate of Trusted Root (depending on the PKI scheme that is implemented). All these files must be added to the Auxiliary Files repository prior to configuring them in the Media Gateway. For more information, see Section the section 'Auxiliary Files Repository' on page 422.

33.10.5 Activating the new X.509 Certificates on the Media Gateway

Once certificate files are added to the Auxiliary Files repository, take the following steps to activate the new X.509 configuration on the Media Gateway:

- Configure X.509 files in the Media Gateway Security Settings tab.
- Apply new X.509 configuration to the Media Gateway boards. See below.

➤ **To configure X.509 Security with the Media Gateway:**

1. Click  to access the Media Gateway status screen.
2. In the Navigation pane, select **Security** and then in the configuration pane, click **Security Settings**; the Security Settings screen is displayed.
3. In the **X.509 Certificates** tab, configure new X.509 files as described in the table 'Media Gateway Security Settings' below.

Table 33-3: Media Gateway Security Settings

Parameter Name	Type	Provisioning Type	Description
Private Key File	String	Instant	Private Key file
Certificate File	String	Instant	X.509 Certificate file. Contains Public Key and identity information, signed by the CA or by the entity itself.
CA Certificate File	String	Instant	X.509 Certificate of the CA that issued the Certificate File. This optional parameter is used to validate the Certificate file.
1 st Trusted Root Certificate File	String	Instant	X.509 Certificate of the 1 st Trusted Root. Certificates of the remote party are compared with the Trusted Roots repository and if the root certificate of the CA that signed remote party certificate matches one of the Trusted Roots, remote party certificate is accepted.

Parameter Name	Type	Provisioning Type	Description
2 nd Trusted Root Certificate File	String	Instant	X.509 Certificate of the 2 nd Trusted Root. Certificates of the remote party are compared with Trusted Roots repository and if the root certificate of the CA that signed remote party certificate matches one of the Trusted Roots, remote party certificate is accepted.
3 rd Trusted Root Certificate File	String	Instant	X.509 Certificate of the 3 rd Trusted Root. Certificates of the remote party are compared with Trusted Roots repository and if the root certificate of the CA that signed remote party certificate matches one of the Trusted Roots, remote party certificate is accepted.

When new X.509 certificates are configured for the Media Gateway they are not immediately applied to the Media Gateway board. This minimizes the effect of the wrong or expired certificate provisioning.

Two read-only parameters, available in the VoP Boards Status section of the X.509 configuration screen are used to indicate the status of the X.509 certificates on Media Gateway boards.

Table 33-4: X.509 Files Status Parameters of the Media Gateway

Parameter Name	Type	Provisioning Type	Description
VoP Boards Synchronized with the Media Gateway Configuration	String	Instant	A list of the Media Gateway boards that have X.509 configuration that matches configuration currently configured for the Media Gateway in the Security Settings tab. Normally all Media Gateway boards are listed in this list.

Parameter Name	Type	Provisioning Type	Description
VoP Boards Not Synchronized with the Media Gateway Configuration	String	Instant	A list of the Media Gateway boards that have X.509 configuration that is different from the configuration currently configured for the Media Gateway in the Security Settings tab. Normally this list is empty. It gets populated with all Media Gateway boards when X.509 configuration of the Media Gateway is changed. "Download certificates to VoP boards" action is used to apply new certificates to specific VoP boards and move them back from this list to the "VoP Boards Synchronized with the Media Gateway Configuration" list.

After you complete configuration of the new X.509 Files in the Media Gateway Security Settings tab, all Media Gateway boards are displayed in the **VoP Boards Not Synchronized with the Media Gateway Configuration** list. This indicates that the new configuration has not yet applied been to the Media Gateway board.

You may view the current X.509 configuration of each Media Gateway board in the Security Settings tab of the specific Media Gateway Board Properties screen.

Now you should activate the new X.509 configuration on Media Gateway boards. It is recommended to initially choose one Media Gateway board to activate the new X.509 configuration as a test activation. Once the new configuration has been validated, apply the new configuration to the other Media Gateway boards.

➤ **To apply the new X.509 configuration to Media Gateway boards:**

1. In the Security Settings screen, click the Maintenance Actions icon  in the top-right corner and select the **Download Certificates to VoP Boards** option; the Generate X.509 Files dialog is displayed.
 - Select one of the following options:
 - ♦ **All Boards** - apply new X.509 configuration to all Media Gateway boards
 - ♦ **Select Board** - apply new X.509 configuration to the specific Media Gateway board; if you select this option, choose the specific board from the drop-down list.

Figure 33-3: Activating X.509 Certificates



2. Click **OK**.

The new X.509 configuration (currently configured in the Media Gateway Security Settings tab) is applied to the specified board(s). The **VoP Boards Synchronized With Media Gateway Configuration** and **VoP Boards Not Synchronized With Media Gateway Configuration** lists are updated accordingly.



Note: The new X.509 configuration is applied to the Media Gateway board instantly without any effect on the board's service.

33.10.6 Configuring an X.509 Certificate Expiration Date Reminder

Each X.509 Certificate is issued for a specific period of time i.e validity period. The Mediant 8000 Media Gateway software automatically determines an expiration date for each configured X.509 certificate and triggers a Security Alarm to warn the user prior to the certificate expiration.

The Expiration date for each certificate is displayed in the Security Settings tab – both in the Media Gateway screen (for certificates configured for the entire Media Gateway) and in the Media Gateway Board screen (for certificates configured for the specific Media Gateway board, in case they differ from the Media Gateway configuration).

The Certificate Expiration alarm is issued twice. A few days before the expiration, an alarm with **warning** severity is issued. When you see this alarm, contact CA immediately for a new identity certificate. When the certificate actually expires, an alarm with **error** severity is issued. You may configure the amount of time between when these two alarms are triggered.

➤ To configure expiration date reminder for X.509 Certificate:

1. Click  to access the Media Gateway status screen.
2. In the Navigation pane, select **Security** and then in the configuration pane,; click **Security Settings**; the Security Settings screen is displayed.
3. In the X.509 Certificates tab, Configure the **Certificate Expiration Date Reminder Days** (for Certificate File) and the **Trusted Root Certificate Expiration Date Reminder Days** (for CA Certificate and Trusted Root Certificate Files) parameters.



Note: It is highly recommended to configure expiration date reminder alarms to alert users prior to the X.509 Certificate expiration. Set date reminder well in advance of the expiration date to ensure that new certificates are either generated in EMS or received from appropriate external bodies and properly configured.

33.10.7 Generating a New Private Key

Some users may wish to periodically re-generate the Private Key file to enhance security. When a new Private Key is generated, an accompanying Self-Signed Certificate is generated as well. This Self-Signed Certificate contains a matching Public Key. However, if you are implementing PKI infrastructure, you should generate a new CSR request, submit it to the Certificate Authority (CA) and receive from it a properly signed X.509 Certificate which matches the new Private Key.

➤ **To generate a new Private Key:**

1. Click  to access the Media Gateway status screen.
2. In the Navigation pane, select **Security** and then in the configuration pane, click **Security Settings**; the Security Settings screen is displayed.
3. Click the Maintenance Actions  in the top-right corner and select the **Generate X.509 Files** option. The **Generate X.509 Files** dialog is displayed.
4. Select **Private Key**.
5. In the Private Key field, enter a name of the new Private Key file.
6. In the Self-Signed Certificate field, enter a name of the new Self-Signed Certificate file.
7. Click **OK**. A new private key and self-signed certificate file are generated and automatically added to the Auxiliary Files repository.
8. If you use PKI infrastructure, you must issue a new CSR to the CA to receive a new signed X.509 Certificate that matches the new private key. For more information, see Section 'Generating a Certificate Signing Request (CSR)' on page 329.
9. To activate the new private key and certificate (self-signed or received from the CA), you must configure them in the Media Gateway Security Settings tab and apply the new configuration to the Media Gateway boards. For more information, see Section 'Activating the new X.509 Certificates on the Media Gateway' on page 331.

33.10.8 Checking Certificate Revocation Status

X.509 certificates are normally issued for a planned lifetime, which is defined through a validity start time and an explicit expiration date. However various circumstances may lead to a certificate becoming invalid prior to its expiration date. Such circumstances include change of name (for example, requiring to change the subject of a certificate), and compromise or suspected compromise of the CA's private key.

The Mediant 8000 uses the OCSP protocol (as defined in RFC 2560) to check the revocation status of X.509 certificates. To configure this functionality, use the following parameters located in the OCSP Settings tab of the Media Gateway Security Settings screen:

Table 33-5: OCSP Server Settings

Parameter Name	Type	Provisioning Type	Description
OCSP Mode	Enum Enable, Disable	Instant	Enables or disables the use of the OCSP protocol to verify X.509 certificate revocation status.
Default OCSP Response	Enum Reject, Allow	Instant	Defines Media Gateway behavior in the case where the OCSP responder is unreachable. Reject – reject certificate Allow – allow certificate use
Primary OCSP Server IP	IP Address	Instant	IP address of the primary OCSP server.
Secondary OCSP Server IP	IP Address	Instant	IP address of the secondary OCSP server.
OCSP Server Port	Integer 0-65535	Instant	TCP port of the OCSP server.

33.11 IPSEC and IKE

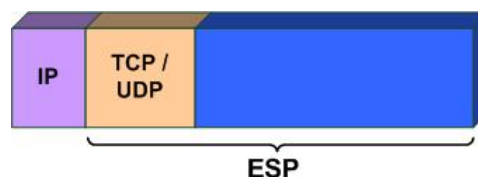
IPSEC and IKE protocols are part of IETF standards for a secured IP connection between two applications. Providing security services at the IP layer, IKE and IPSEC protocols are transparent to the IP applications.

IKE and IPSEC are used in conjunction to provide security for call control (e.g., MGCP and MEGACO) and management (e.g., SNMP) protocols, but not for media (i.e., RTP, RTCP and T.38).

The IKE protocol is responsible for obtaining the IPSEC encryption keys and encryption profile (known as IPSec Security Association (SA)).

IPSEC is responsible for securing the IP traffic. This is accomplished by using the Encapsulation Security Payload (ESP) protocol to encrypt the IP payload (illustrated in the figure below).

Figure 33-4: IPSec Encryption



IPSEC supports the following two modes of operation:

- Transport mode – used for host-to-host communication (e.g. for communication between the Media Gateway and the EMS server); encrypts the payload of the IP packet, but leaves IP headers intact.
- Tunnel mode – used to create Virtual Private Networks (VPNs) for network-to-network or host-to-network communication (e.g. for communication between the Media Gateway and the VPN gateway); the entire packet is encrypted and then encapsulated in a new IP packet with a new IP header.

The Mediant 8000 Media Gateway implements the following IPSEC/IKE specifications:

33.11.1 For Management Interfaces (on SC boards)

This section describes the Management Interfaces (on SC boards).

33.11.1.1 IKE Protocol

- Authentication: pre-shared key or X.509 certificate (*)
- IKE Phase 1 exchange mode: main
- IKE SA encryption algorithms: DES, 3DES and AES (*)
- IKE SA hash types: SHA1, SHA256 (*), SHA384 (*), SHA512 (*) and MD5
- Diffie-Helman groups: ModP768, ModP1024, ModP1536 (*), ModP2048 (*), ModP3072 (*), ModP4096 (*), ModP6144 (*) and ModP8192 (*)
- Dead-peer detection (as per RFC 3706) (*)

33.11.1.2 IPSEC Protocol

- Transport or tunnel mode
- Encapsulated Security Payload (ESP) only
- Support for Cipher Block Chaining (CBC)
- IPSEC SA encryption algorithms: DES, 3DES and AES (*)
- IPSEC SA hash types: SHA1, SHA256 (*), SHA384 (*), SHA512 (*) and MD5
- NAT Traversal (NAT-T) extension support (*)



Note: Features and algorithms marked with (*) are available on SC Rev.2 (Linux OS based) boards only.

33.11.2 For Call Control and Signaling Interfaces (on TP boards)

This section describes the Call Control and Signaling Interfaces (on TP boards).

33.11.2.1 IKE Protocol

- Authentication: pre-shared key or X.509 certificate
- IKE SA encryption algorithms: DES, 3DES and AES
- IKE SA hash types: SHA1 and MD5
- Diffie-Helman groups: ModP768 and ModP1024
- Dead-peer detection (as per RFC 3706)

33.11.2.2 IPSEC Protocol

- Transport or tunnel mode
- Encapsulated Security Payload (ESP) only
- IPSEC SA encryption algorithms: DES, 3DES and AES
- IPSEC SA hash types: SHA1 and MD5

33.11.3 Configuring IPSEC/IKE for Management Interfaces (on SC boards)

IPSEC/IKE protocols may be used to secure communication between the Media Gateway and SNMP managers, Syslog servers and NTP servers. The Transport mode IPSEC/IKE association between the Media Gateway and the EMS server is configured via the **tools ems** command (see Configuring Connectivity between the Media Gateway and the EMS Server on page 171). IPSEC/IKE associations between the Media Gateway and additional SNMP managers and/or tunnel mode IPSEC/IKE associations are configured as described below.

To configure IPSEC/IKE association for management interfaces, the following configuration entities (MOs) are used:

- SC IPSEC Rule – represents a single IPSEC/IKE association on SC boards (that handle all management traffic) ; up to 10 associations may be configured
- SC IKE Proposal – represents an IKE proposal (a set of encryption and authentication protocols) used for specific SC IPSEC Rule; up to 4 proposals may be configured for each rule

When IPSEC/IKE associations are configured for SNMP managers (EMS, NMS, OSS), the actual mode of operation is determined by the selected SNMP management mode.

Table 33-6: SNMP Management Modes

SNMP Management Mode	Actual mode of Operation
SNMPv2	IPSEC/IKE associations <i>may</i> be configured for specific SNMP managers. If such a configuration is performed, management traffic between the Media Gateway and <i>specific</i> SNMP manager is encrypted. Access to incoming SNMP port 161 on the Media Gateway is not protected. As a result, unsecured SNMP managers, provisioned with the correct public and private keys, may connect to it.
SNMPv2 + IPSEC	IPSEC/IKE associations <i>must</i> be configured for all SNMP managers who access the Media Gateway's MIB. IPSEC/IKE encryption is enforced on the incoming SNMP port 161, therefore unsecured SNMP managers can't connect to it. Unsecured SNMP managers (without proper IPSEC/IKE association configured) may be used to receive SNMP notifications (traps) from the Media Gateway.

SNMP Management Mode	Actual mode of Operation
SNMPv3	An IPSEC/IKE association <i>should not</i> be configured for SNMP managers. The SNMPv3 protocol has built-in security features, the result of which renders IPSEC/IKE abundant and irrelevant. If, for any reason, the IPSEC/IKE association is configured for specific SNMP manager, the SNMPv3 traffic will bypass the encryption (i.e. will not be encrypted via IPSEC/IKE).

➤ To add and configure SC IPSEC Rule:

1. Click  to access the Media Gateway status screen.
2. In the Navigation pane, select **Security SC IPSEC Rules**; the SC IPSEC Rules list is displayed.
3. Use the  or  buttons to add or remove entries.
4. Select a specific row and then in the configuration pane, click **SC IPSEC Rule Settings**; the SC IPSEC Rules Settings screen is displayed.
5. Configure the SC IPSEC Rule parameters according to the table below.

Table 33-7: SC IPSEC Rule Parameters (SC Boards)

Parameter Name	Type	Provisioning Type	Description
Name	String Up to 80 chars.	Instant	Textual name of the SC IPSEC Rule, used for easy identification.
Operation Mode	Enum Transport, Tunnel	Online	Defines IPSEC operation mode. Tunnel operation mode is supported on SC Rev.2 (Linux OS based) boards only.
Local IP Address	Enum Any, Global IP, Local IP	Online	Defines local IP address of the IPSEC SA.
Remote IP Address	String Up to 30 chars	Online	Defines the remote IP address of the IPSEC SA. Applicable for Transport mode only.
Remote Tunnel IP Address	String Up to 30 chars	Online	Defines the IP address of the remote IPSEC tunneling device. Applicable for Tunnel mode only.
Remote Subnet IP Address	String Up to 30 chars	Online	Defines the IP address of the remote subnet (behind the IPSEC tunneling device). Applicable for Tunnel mode only.

Parameter Name	Type	Provisioning Type	Description
Remote Subnet Prefix Length	Integer 0 – 128	Online	Defines the prefix length of the Remote Subnet IP Address. Applicable for the Tunnel mode only.
Local Port	Integer 0 – 65535	Online	Defines the local port of the IPSEC SA. Value 0 means 'any'.
Remote Port	Integer 0 – 65535	Online	Defines the remote port of the IPSEC SA. Value 0 means 'any'.
Protocol	Integer 0 – 255	Online	Defines the IP protocol of the IPSEC SA. Value 0 means 'any'. Commonly used values: 6 = TCP, 17 = UDP
Authentication Mode	Enum Preshared Key, Certificate	Online	Defines authentication mode. X.509 Certificate authentication mode is supported on SC Rev.2 (Linux OS based) boards only.
Preshared Key	String Up to 100 chars	Online	Defines the Pre-Shared Key in ASCII format. Applicable for Preshared Key authentication mode only. Once provisioned, the value is hidden from user via asterisks (*****) for security reasons.
IKE Lifetime (sec)	Integer 0 – 2147483647	Online	Defines the IKE SA Lifetime (in seconds).
IPSEC Lifetime (sec)	Integer 0 – 2147483647	Online	Defines the IPSEC SA Lifetime (in seconds).
DPD Delay (sec)	Integer 0 – 2147483647	Online	Activates Dead Peer Detection (DPD) and sets the time (in seconds) allowed between 2 proof of liveness requests. Value 0 disables DPD monitoring, but still negotiates DPD support. Supported on SC Rev.2 (Linux OS based) boards only.
DPD Retry (sec)	Integer 0 – 2147483647	Online	If DPD is activated, sets the the delay (in seconds) to wait for a proof of liveness before considering it as failed and sending another request. Supported on SC Rev.2 (Linux OS based) boards only.

Parameter Name	Type	Provisioning Type	Description
DPD Max Fail	Integer 0 – 2147483647	Online	If DPD is activated, sets the maximum number of proof of liveness to request (without reply) before considering the peer to be dead. Supported on SC Rev.2 (Linux OS based) boards only.
NAT Traversal	Enum Off, On, Force	Online	Enables use of the NAT-Traversal IPsec extension (NAT-T). NAT-T allows one or both peers to reside behind a NAT gateway (i.e., doing address- or port-translation). Presence of NAT gateways along the path is discovered during phase 1 handshake and if found, NAT-T is negotiated. When NAT-T is in charge, all ESP and AH packets of a given connection are encapsulated into UDP datagrams (port 4500, by default). On - NAT-T is used when a NAT gateway is detected between the peers. Off - NAT-T is not proposed/accepted. This is the default. Force - NAT-T is used regardless if a NAT is detected between the peers or not. Supported on SC Rev.2 (Linux OS based) boards only.

➤ **To add and configure SC IKE Proposal:**

1. Select the SC IPSEC Rule that you want to configure.
2. In the Navigation pane, select **SC IKE Proposals**; the SC IKE Proposals list is displayed.
3. Use the  or  buttons to add or remove entries.
4. Select a specific row and then in the configuration pane, click **SC IKE Proposal Settings**; the SC IKE Proposal Settings screen is displayed.
5. Configure the SC IKE Proposal parameters according to the table below.

Table 33-8: SC IKE Proposal Parameters

Parameter Name	Type	Provisioning Type	Description
Authentication	Enum MD5, SHA1, SHA256, SHA384, SHA512	Online	Defines the authentication algorithm for IPSEC and IKE SAs. SHA256, SHA384 and SHA512 authentication algorithms are supported on SC Rev.2 (Linux OS based) boards only.
Encryption	Enum DES, 3DES, AES	Online	Defines the encryption algorithm for IPSEC and IKE SAs. AES encryption algorithm is supported on SC Rev.2 (Linux OS based) boards only.
DH Group	Enum ModP768(1), ModP1024(2), ModP1536(5), ModP2048(14), ModP3072(15), ModP4096(16), ModP6144(17), ModP8192(18)	Online	Defines Diffie Hellman group. Only ModP768(1) and ModP1024(2) DH groups are supported on SC Rev.1 (Solaris OS based) boards.

➤ **To activate the new configuration:**

1. Select the SC IPSEC Rule that you configured above.
2. In the Actions bar, click **Unlock**

33.11.4 Configuring IPSEC/IKE for Call Control and Signaling Interfaces (on TP boards)

IPSEC/IKE protocols may be used to secure communication between Media Gateway and MGCP/MEGACO Call Agents and/or SIGTRAN signaling gateways.

To configure IPSEC/IKE association for call control and signaling interfaces, the following configuration entities (MOs) are used:

- TP IPSEC Profile – represents a set of IPSEC/IKE associations on TP board (that handle call control and signaling traffic); each profile may be attached to one or multiple TP boards
- TP IPSEC Rule – represents a single IPSEC/IKE association on TP board; up to 10 associations may be configured
- TP IKE Proposal – represents an IKE proposal (a set of encryption and authentication protocols) used by TP board; up to 4 proposals may be configured; contrary to SC boards' configuration, the same set of IKE proposals is used by all TP IPSEC Rules.

➤ To add and configure TP IPSEC Profile:

1. Click  to access the Media Gateway status screen.
2. In the Navigation pane, select **Security TP IPSEC Profiles**; the TP IPSEC Profiles list is displayed.
3. Use the  or  buttons to add or remove entries.
4. Select a specific row and then in the configuration pane, click **TP IPSEC Profile Settings**; the TP IPSEC Profile Settings screen is displayed.
5. Configure the TP IPSEC Profile parameters according to the table below.

Table 33-9: TP IPSEC Profile Parameters

Parameter Name	Type	Provisioning Type	Description
Profile Name	String Up to 80 chars	Instant	Textual name for the IPSEC Profile, enabling to identify it easily.

➤ To add and configure TP IPSEC Rule:

1. Select the TP IPSEC Profile that you wish to configure.
2. In the Navigation pane, select **TP IPSEC Rules**; the TP IPSEC Rules list is displayed.
3. Use the  or  buttons to add or remove entries.
4. Select a specific row and then in the configuration pane, click **TP IPSEC Rule Settings**; the TP IPSEC Rule Settings screen is displayed.
5. Configure the TP IPSEC Rule parameters according to the table below.

Table 33-10: TP IPSEC Rules Parameters (TP Boards)

Parameter Name	Type	Provisioning Type	Description
Name	String Up to 80 chars	Instant	Textual name for the IPSEC Rule, enabling to identify it easily.
Operation Mode	Enum Transport, Tunnel	Online	Defines IPSEC operation mode.
Remote IP Address	String Up to 30 chars	Online	Defines the remote IP address of the IPSEC SA. Applicable for Transport mode only.
Remote Tunnel IP Address	String Up to 30 chars	Online	Defines the IP address of the remote IPSEC tunneling device. Applicable for Tunnel mode only.
Remote Subnet IP Address	String Up to 30 chars	Online	Defines the IP address of the remote subnet (behind the IPSEC tunneling device). Applicable for Tunnel mode only.
Remote Subnet Prefix Length	Integer 0 – 128	Online	Defines the prefix length of the Remote Subnet IP Address. Applicable for Tunnel mode only.
Local Port	Integer 0 – 65535	Online	Defines the local port of the IPSEC SA. Value 0 means 'any'.
Remote Port	Integer 0 – 65535	Online	Defines the remote port of the IPSEC SA. Value 0 means 'any'.
Protocol	Integer 0 – 255	Online	Defines the IP protocol of the IPSEC SA. Value 0 means 'any'. Commonly used values: 6 = TCP, 17 = UDP
Authentication Mode	Enum Preshared Key, Certificate	Online	Defines authentication mode.
Preshared Key	String Up to 100 chars	Online	Defines the Pre-Shared Key in ASCII format. Applicable for Preshared Key authentication mode only. Once provisioned, the value is hidden from user via asterisks (*****) for security reasons.
IKE Lifetime (sec)	Integer 0 – 2147483647	Online	Defines the IKE SA Lifetime (in seconds).
IPSEC Lifetime (sec)	Integer 0 – 2147483647	Online	Defines the IPSEC SA Lifetime (in seconds).

Parameter Name	Type	Provisioning Type	Description
IPSEC Lifetime (kbytes)	Integer 0 – 2147483647	Online	Defines the IPSEC SA Lifetime (in kilobytes).
DPD Mode	Enum Disabled, Periodic Checks, On Demand Checks	Online	Activates Dead Peer Detection (DPD) as per RFC 3706.

➤ **To add and configure the TP IKE Proposal:**

1. Select the TP IPSEC Profile that you wish to configure.
2. In the Navigation pane, select **TP IKE Proposals**; the TP IKE Proposals list is displayed.
3. Use the  or  buttons to add or remove entries.
4. Select a specific row and then in the configuration pane, click **TP IKE Proposal Settings**; the IKE Proposal Settings screen is displayed.
5. Configure the TP IKE Proposal parameters according to the table below.

Table 33-11: TP IKE Proposal Parameters

Parameter Name	Type	Provisioning Type	Description
Authentication	Enum MD5, SHA1	Online	Defines the authentication algorithm for IPSEC and IKE SAs.
Encryption	Enum DES, 3DES, AES	Online	Defines the encryption algorithm for IPSEC and IKE SAs.
DH Group	Enum ModP768, ModP1024	Online	Defines the Diffie Hellman group.

➤ **To attach the TP IPSEC Profile to the TP board and activate the configuration:**

1. Click  to access the Media Gateway status screen.
2. Select the desired Media Gateway board.
3. In the Actions bar, click **Lock** to stop the service on the Media Gateway board.
4. In the Navigation pane, select **Security** and then in the configuration pane, click **Security Settings**; the Security Settings screen is displayed.

5. Configure the **IPSEC Profile** parameter to match the ID and name of the TP IPSEC Profile configured above.
6. In the Actions bar, click **Unlock** to restore the service on the Media Gateway board.

33.12 SIP over SSL/TLS (SIPS)

The Secure Socket Layer (SSL) / TLS (Transport Layer Security) protocol is used to provide confidentiality, integrity and authenticity between two communicating applications over TCP/IP.

The Mediant 8000 supports the use of the SSL/TLS protocol for encryption and authentication of SIP call control traffic.

Specifications of the SSL/TLS implementation in Mediant 8000:

- Supported transports: SSL 2.0, SSL 3.0, TLS 1.0
- Supported ciphers: DES, RC4 compatible
- Authentication: X.509 certificates

➤ **To enable SIP over SSL/TLS for a specific Media Gateway board:**

1. Click  to access the Media Gateway status screen.
2. Select the desired Media Gateway Board.
3. In the Navigation pane, select **SIP ► SIP General** and in the Configuration pane, click **SIP Protocol Settings**; The SIP Protocol Settings screen is displayed.
4. Set the **Transport Type** parameter to *TLS*.
In this mode, the Media Gateway board initiates a TLS connection only for the next network hop.
5. To enable TLS all the way to the destination (over multiple hops) set **Enable SIPS** parameter to *Enable* and **SIP Destination Port** parameter to *5061*.
6. If you wish the Media Gateway board to validate the certificate of the remote side, set the parameter **TLS Two-Way Authentication** to *Enable*.

33.13 Media Security

The Mediant 8000 Media Gateway supports two different types of Media Security:

- Packet Cable Security
- Secure RTP

33.13.1 Packet Cable Security

The Mediant 8000 supports media encryption via TGCP (Packet cable extension of the MGCP protocol). IP voice traffic for some or all channels is encrypted using predefined session keys. No key negotiation is performed for media security. Instead, key management is handled by higher-level protocols (TGCP).

Packet Cable Security specifications:

- AES (Rijndael) cipher algorithm, in CBC mode
- Key strength – 128 bit
- Encryption key supplied by TGCP

Packet Cable Security is enabled by default when TGCP call control is configured by setting **Call Control Compatibility Profile** to 32 (in the Media Gateway Controller configuration screen) and **DSP Load File Version** to 3 (in Media Gateway board Media Settings configuration screen).

33.13.2 Secure RTP

Secure RTP, a standard protocol defined by RFC 3711, provides confidentiality, message authentication and replay protection of the RTP & RTCP traffic. Key negotiation is not part of the SRTP. Instead, it is handled by a higher-level protocols (MGCP and MEGACO).

Secure RTP specifications:

- Encryption – AES 128 in Counter Mode or 128 or 192 ARIA (Korean standard) for Media Security
- Authentication – HMAC-SHA1
- Support of Key Derivation
- Key management is provided via MGCP and MEGACO



Note: See the version-specific Release Notes to check the availability of the SRTP application in a specific Media Gateway software release.

➤ **To enable Secure RTP:**

1. Click  to access the Media Gateway status screen.
2. Select the desired Media Gateway board.
3. In the Navigation pane, select **Security** and then in the configuration pane, click **Security Settings**; the Security Settings screen is displayed.
4. Set the **Enable Media Security** parameter to *Enable*. Configure additional SRTP parameters according to the table below.
5. In the Navigation pane, select **Media ▶ DSP Templates**; the DSP Templates list is displayed.
6. Use the  or  buttons to add or remove entries.
7. Select a specific row and then in the configuration pane, click **DSP Templates Settings**; the Templates Settings screen is displayed.
8. Set the **DSP Template Number** parameter to 0, 7 or 9.

Table 33-12: Media Gateway Board's Media Security (SRTP) Settings

Parameter Name	Type	Provisioning Type	Description
Enable Media Security	Enum Disable, Enable	Online	Enables encryption of RTP traffic as defined by Secure RTP protocol.
SRTP Authentication	Enum Disable, Enable	Instant	Defines whether to enable Authentication on a secured SRTP session.
Unencrypted SRTP Offer	Enum Disable, Enable	Instant	Defines whether to offer Unencrypted SRTP on a secured SRTP session.
Unencrypted SRTCP Offer	Enum Disable, Enable	Instant	Defines whether to offer Unencrypted SRTCP on a secured SRTP session.
MKI Enable/Size	Enum Disable, One Byte, Two Bytes, Three Bytes, Four Bytes	Instant	Defines the size of the parameter Master Key Identifier (MKI) in SRTP Tx packets.
Aria Media Security	Enum Disabled, Enabled	Online	Enables use of ARIA encryption protocol (Korean standard block cipher).

Parameter Name	Type	Provisioning Type	Description
SRTP offered Suites	Enum Disabled, Enabled	Online	Defines the offered SRTP crypto suites. ▪ [0] All = All available crypto suites (default) ▪ [1] AES_CM_128_HMAC_SHA1_80 = device uses AES-CM encryption with a 128-bit key and HMAC-SHA1 message authentication with a 80-bit tag. ▪ [2] AES_CM_128_HMAC_SHA1_32 = device uses AES-CM encryption with a 128-bit key and HMAC-SHA1 message authentication with a 32-bit tag. ▪ [4] ARIA_128_HMAC_SHA1_32 = device uses ARIA_128 encryption with a 128-bit key and HMAC-SHA1 message authentication with a 32-bit tag. ▪ [8] ARIA_192_HMAC_SHA1_32 = device uses ARIA_192 encryption with a 192-bit key and HMAC-SHA1 message authentication with a 32-bit tag.



Note: Use of media security i.e. AES and ARIA crypto suites reduces DSP channel capacity of the Gateway board.

33.14 Firewall Functionality on Media Gateway Boards

The Mediant 8000 provides Firewall functionality that helps to protect Media Gateway boards from unauthorized access. Media Gatewayboards may be configured to block incoming traffic from a specific IP address or from a specific network. Advanced functionality, such as being able to limit traffic based on individual packet size and bandwidth allocation, is provided.

Firewall definitions are not bound to a specific application and therefore may be used to protect the Media Gateway boards from all types of attacks and intrusion attempts – in the OAM (management), Call Control and Media subnets.

33.14.1 Firewall Rules

The Firewall Profile consists of a number of Firewall Rules. Each incoming Ethernet packet is checked against the defined rules. If a matching rule is found, an action is performed (a packet is dropped or accepted).

By default, each Firewall Profile contains the following rules:

- Default rules that allow communication with SC board and Redundant Media Gateway board (may not be modified by user)
- "Deny all" last rule



Note: In its default configuration, the Firewall Profile does not contain rules that allow a specific Media Gateway board to communicate with Media Gateway Controllers and other Media Gateways. Hence, such rules must be manually provisioned by the user, otherwise control/media traffic is blocked.

The Firewall configuration consists of two parts:

- Create and configure Firewall Profile
- Associate Firewall Profile with specific Media Gateway board



Note: A single Firewall Profile can be used for multiple Media Gateway boards. However, you can also define a separate Firewall Profiles for each Media Gateway board.

➤ To add and configure Firewall Profiles:

1. Click  to access the Media Gateway status screen.
2. In the Navigation pane, select **Security** ➤ **Firewall Profile**; the Firewall Profiles list is displayed.
3. Use the  or  buttons to add or remove entries (Firewall Profiles).

4. Select a specific Firewall Profile entry and in the Navigation pane, select **Firewall Rules**. The list of Firewall Rules, included in the specific Firewall Profile, is displayed. The list is populated with default values, which enable proper communication between the Media Gateway board and SC boards inside the chassis; however, block any communication with other Media Gateways or Softswitches. Additional entries should be added by the user to enable such communication.
5. Use the  or  buttons to add or remove entries (Firewall Rules).
6. Select a specific row and then in the configuration pane, click **Firewall Rule Settings**; the Firewall Rule Settings screen is displayed.
7. Configure the Firewall Rules according to the table 'Firewall Rule Parameters' below.

➤ **To associate the Firewall Profiles with a specific Media Gateway board:**

1. Click  to access the Media Gateway status screen.
2. Select the desired Media Gateway board.
3. In the Actions bar, click **Lock** to stop the service on the Media Gateway board.
4. In the Navigation pane, select **Security** and then in the configuration pane, click **Security Settings**; the Security Settings screen is displayed.
5. Configure the **Firewall Profile** parameter to match the ID and name of the Firewall Profile configured above.
6. In the Actions bar, click **UnLock** to restore the service on the Media Gateway board.

Table 33-13: Firewall Rule Parameters

Parameter Name	Type	Provisioning Type	Description
Rule Name	String Up to 20 chars.	Instant	Textual, user-defined name for the Firewall Rule.
Use Per Subnet	Enum AllSubnets, SpecificSubnet	Instant	Defines whether this rule applies to all subnets or a specific subnet.
Subnet	Integer 1 – 10	Instant	Defines the index of the subnet to which this rule applies. This parameter is relevant only if Use Per Subnet == Specific Subnet.

Parameter Name	Type	Provisioning Type	Description
Source IP	String Up to 60 chars.	Instant	Each Firewall Rule defines a simple mask applied on each incoming packet and firewall action (allow/block). Only packets that match pre-defined firewall rules are accepted by the TP board. This parameter defines the Source IP of the incoming IP packet. The parameters Source IP and NetMask provide the mechanism for filtering packets from a specific network host or network segment (subnet).
Net Mask	String Up to 20 chars.	Instant	Defines the Net Mask used to compare the Source IP with the incoming IP packet's source IP. For example: - Source IP = 10.7.10.1, Net Mask = 255.255.255.255 – matches specific IP address; - Source IP = 10.7.0.0, Net Mask = 255.255.0.0 – matches addresses in a specific subnet - Source IP = 0.0.0.0, Net Mask = 0.0.0.0 – matches all IP addresses
Start Port	Integer 0-65535	Instant	Defines the lower limit of the IP packet's port range. Default = 0.

Parameter Name	Type	Provisioning Type	Description
End Port	Integer 0-65535	Instant	Defines the upper limit of the IP packet's port range. Default = 65535.
Protocol String	Up to 10 chars.	Instant	Defines the incoming packet's IP protocol (as encoded in the IP header). Default value - 0 - implies any protocol.
Packet Size	Integer 0-65535	Instant	Defines the maximum packet size of incoming traffic. Default value - 0 - implies any size.
Byte Rate	Integer 0-2147483647	Instant	Defines the maximum byte rate of incoming traffic. Default value - 0 - implies any rate.
Byte Burst	Integer 0-2147483647	Instant	Defines the maximum byte burst of incoming traffic. Default value - 0 - implies any burst.
Action	Enum allow, block	Instant	Action to be applied for the packets that matches a specified rule - allow/block.
Source Port	Integer 0-65535	Instant	Defines the source UDP or TCP port (on the remote host) from where packets are sent to the device.

33.15 Network Services on the Mediant 8000

This chapter lists standard network services required for normal Mediant 8000 operation. Ensure that these services are allowed in the network to which the Mediant 8000 is connected and then configure external security equipment (e.g. Firewalls) accordingly.

Table 33-14: Network Services

Service Name	IP Address and Port	Description
SSH	Port 22 Global and private IP addresses of SC boards.	Used for accessing Mediant 8000 Command Line Interface (CLI) and transferring files to/from it.
SNMP	Port 161 Global IP address of SC boards	Used for management and fault monitoring tasks.
NTP	Port 123 Private IP addresses of SC boards.	Implements time and date synchronization.
VoIP protocols (SIP, MGCP, ME, GAC O, RTP etc)	IP addresses of Media Gateway boards	Used for carrying signaling and voice traffic.

33.16 OpenBoot PROM on SC Rev.1 Boards

This section describes the OpenBoot PROM on SC Rev.1 boards.



Note: This section is only applicable to SC Rev.1 boards using the Solaris OS.

OpenBoot PROM is a hardware-level user interface environment on SC boards that provides access to an extensive set of diagnostics commands, hardware configuration and fault isolation. This advanced interface is intended for Tech Support personnel only and its detailed description is beyond of scope of this document.

Access to the OpenBoot PROM environment may be limited by setting an EEPROM password. The EEPROM password should be changed periodically and should never be set to the same password as that of the **root** user.



WARNING

The EEPROM password should be used with caution!.

It may not be changed/reset from the OpenBoot PROM level. Therefore, if a user forgets the EEPROM password, and the SC board fails to successfully boot the Solaris OS, it is impossible to recover the SC board.

➤ To enable Open Boot PROM security:

1. Connect to the CLI interface on the specific SC board. For more information, see Section 'The Command Line Interface (CLI)' on page 107.
2. Login as **root** user. For more information, see Section 'Logging in as a Root User' on page 115.
3. At the prompt, type **eeeprom security-mode=command** and press **Enter**.
4. At the **Changing PROM password** prompt, type the password.
5. At the **New Password** prompt, type the new password and retype it at the **Retype new password** prompt.

```
client238::~~# eeeprom security-mode=command
Changing PROM password:
New password: *****
Retype new password: *****
```

Open Boot PROM security is enabled.

➤ **To set a new EEPROM password, at the prompt:**

1. Connect to the CLI interface on the specific SC board. For more information, see Section 'The Command Line Interface (CLI)' on page 107.
2. Login as **root** user. For more information, see Section 'Logging in as a Root User' on page 115.
3. At the prompt, type **eeeprom security-password=** and press **Enter**; do not forget the trailing equal sign).
4. At the **New Password** prompt, type the new password and retype it at the **Re-enter password** prompt.

```
client238::~~# eeeprom security-password=  
Changing PROM password:  
New password: password  
Retype new password: password
```

➤ **To disable Open Boot PROM security:**

1. Connect to the CLI interface on the specific SC board. For more information, see Section 'The Command Line Interface (CLI)' on page 107.
2. Login as **root** user. For more information, see Section 'Logging in as a Root User' on page 115.
3. At the prompt, type **eeeprom security-mode=none** and press **Enter**.

```
client238::~~# eeeprom security-mode=none
```

Open Boot PROM security is disabled.

33.17 CLI Login Banner

The Mediant 8000 supports a user-modifiable login banner, displayed to the user when logging into the Mediant 8000 Command Line Interface (CLI). This banner should be used to warn the user about accessing the equipment and provide all needed regulatory information, as defined in the site's security policy.

➤ **To modify the login banner:**

1. Connect to the CLI interface on the Active SC board. For more information, see Section 'The Command Line Interface (CLI)' on page 107.
2. Login as **root** user. For more information, see Section 'Logging in as a Root User' on page 115.
3. At the prompt, type **edit /etc/banner** and press **Enter**. The file opens in the default text editor.

```
client238::~~# edit /etc/banner
```

4. Modify the text of the banner and save the file.
5. To activate the modified banner, at the prompt, type **cp /etc/banner /etc/issue** and press **Enter**.

```
client238::~~# cp /etc/banner /etc/issue
```

6. Repeat steps 1-5 on the Standby SC board.



Note: Do not edit the **/etc/issue** file directly. The banner will be lost after the system is re-configured or Online Software Upgrade is performed.

33.18 Administering Command Line Interface (CLI) Users

This chapter provides detailed instructions on how to administer (add / delete / modify) users on the Mediant 8000 Command Line Interface. Ensure that you are familiar with the Mediant 8000 Command Line Interface (CLI) and its major features, as described in 'The Command Line Interface (CLI)' on page 107, prior to proceeding with this chapter

33.18.1 CLI Users Database and Operation Modes

Each CLI user must be defined in a CLI Users Database that contains the following information:

- User Name
- User Profile (user type, home directory, password change policy etc)

User Password The Mediant 8000 supports the following types of CLI Users Database:

- **Local CLI Users Database** – information is stored locally on both SC boards in the standard plain-text files (**/etc/passwd** and **/etc/shadow**). The local CLI User database is replicated from the Active SC board to the Standby SC board to ensure that the same CLI usernames and passwords are available when connecting to the CLI interface on both SC boards. See 'Synchronizing the CLI Users Database with the EMS Server' on page 367.
- **Local CLI Users Database Synchronized with the EMS server** – information is stored locally on SC boards, however is synchronized with the EMS user database. The same usernames and passwords are used both for logging into the EMS GUI and accessing the Mediant 8000 CLI interfaces. See 'Synchronizing the CLI Users Database with the EMS Server' on page 367.
- **Centralized CLI Users Database on RADIUS Server** – The CLI Users Database is maintained on an external RADIUS server. On-line protocol (RADIUS) is utilized by the Mediant 8000 to authenticate CLI users. The same protocol may be used by the EMS server to authenticate EMS users. See 'Centralized AAA Servers' on page 375.

Root and **ems** users are always defined in a Local CLI Users Database. This ensures that basic management and configuration tasks may be performed even when Media Gateway is completely isolated from any other network element.



Note: Even when the Mediant 8000 is configured to work with a centralized CLI Users database on the RADIUS server, **root** and **ems** users are defined in the local CLI Users database (on SC boards).

The Mediant 8000 is configured for **Local CLI Users Database Synchronized with EMS Server** operation mode by default.

➤ To view the current Mediant 8000 operational mode:

1. Click  to access the Media Gateway status screen.
2. In the Navigation pane, select **Security** and then in the configuration pane, click Security Settings; the Security Settings screen is displayed.
3. In the CLI Authentication tab, check the value of **Synchronize User Database With EMS** and **External Authentication Server** parameters.
4. In addition to above-described operation modes, the Mediant 8000 also supports password-less access to the CLI interface for specific users. See 'Password-less access to the CLI Interface' on page 390 for details.

33.18.2 Administering the ROOT User

The **root** user is typically defined in a local CLI Users Database located on both SC board. This architecture ensures availability of **root** account for emergency maintenance tasks even when Media Gateway has no connectivity with external IP equipment (e.g. RADIUS server).

The **root** user may not be deleted and its password will never expire.

The **root** user's password should be changed under the following circumstances:

- During the Mediant 8000 software installation or basic configuration.
- Periodically, when the Mediant 8000 is installed in a production environment.

33.18.2.1 Changing the ROOT User Password

The **root** user's password may be changed as part of Media Gateway software installation (see 'Installing Mediant 8000 Software on the SC Board to Operate as the Active Board' on page 134) or basic configuration (see 'Performing Basic Configuration of the Mediant 8000 to Operate as the Active Board' on page 147).

In addition, for enhanced security, it is recommended to change **root** password periodically via the following procedure:



Note: Changing the **root** password via the following procedure has no effect on the Media Gateway functionality.

➤ To change the ROOT user password:

1. Connect to the CLI interface on the Active SC board. For more information, see Section 'Command Line Interface' on page 107.
2. Login as **root** user. For more information, see Section 'Logging in as a Root User' on page 115.

3. At the prompt, type **tools user** and press **Enter**. The CLI USERS MANAGEMENT menu is displayed.

```
client238::~~# tools user
```

```
CLI USERS MANAGEMENT
```

```
list  -- LIST: list CLI users
add   -- ADD: add user
del   -- DELETE: delete user

pwd   -- PASSWORD: change user password
copy  -- COPY: copy users & passwords from other SC

lock  -- LOCK: lock user
unlock--UNLOCK: unlock user
force -- FORCE: force user to change password
```

4. At the **Choose submenu** prompt, type **pwd** and press **Enter**.

```
Choose submenu : pwd
```

```
CHANGE USER PASSWORD
```

5. At the **User Name** prompt, type **root** and press Enter.

```
User Name : root
```

6. At the **New Password** prompt, type the new password.

```
New Password:*****
```

7. At the **Re-enter new Password** prompt, type the new password again.

```
Re-enter new Password:*****
```

New password is configured on Active SC board and immediately replicated to the Standby SC board. Therefore there is no need to repeat steps 1-7 on the Standby SC.

8. In the EMS GUI, right-Click the specific Media Gateway in the MG Tree and choose **Details** option from the menu.
9. Enter the new password in the **Root password** field and click **OK** button.

33.18.2.2 Recovering the ROOT User Password

In the unlikely event that you forget the **root** password on a SC board, use the following procedure to reset **root** password to some a well-known default value.



Note :

- Physical access to the RS-232 console of the specific SC board is required to perform this maintenance task.
- The SC board seizes it's operation during the password reset operation. Therefore, if you need to reset the root password on both SC boards, perform the reset, one board at a time, so that the Media Gateway service is unaffected.

➤ **To reset the ROOT user password:**

1. Connect to the CLI interface on the specific SC board via RS-232 serial console. For more information, see Section 'Connecting to the CLI via an RS-232 Serial Console' on page 109.
2. Drop SC board to the OBP level (ok> prompt) by pressing the following 3-key sequence: **ENTER** ~ **Ctrl-B**. The keys must be pressed one after another. The interval between characters should be more than 0.5 seconds. An entire sequence must be entered in less than 5 seconds.
3. If you can not drop SC board to the OBP level (ok> prompt) via the above procedure, press the **ABORT** button on the SC board's front panel.
4. At the **ok>** prompt type, type **setenv oem-banner reset-password** and press **Enter**.

```
ok setenv oem-banner reset-password
oem-banner =          reset-password
ok
```

5. Reboot the SC board by entering boot command or by pressing the **RESET** button on the front panel.
6. Wait until the SC board completes the reboot (this may take up to 2 minutes).
7. Re-connect to the SC board's CLI interface and login as **root** user. Provide default password – **root**. Change **root** password to a new value as described in 'Changing ROOT Password' on page 362.

33.18.3 Administering the EMS User

The **ems** user is typically defined in a local CLI Users Database located on both the SC boards, similar to the **root** user. This architecture ensures that the EMS server may successfully connect to the Media Gateway even when the latter has no access to the centralized authentication server.

The **ems** user should not be deleted and its password will never expire. The default value of the **ems** user password on the Media Gateway matches the default value in the EMS server (to simplify initial system configuration). Nevertheless, you should change the password of the **ems** user prior to installing the Media Gateway in a production environment.

33.18.3.1 Changing the Password of the EMS User

The password of the **ems** user on the Media Gateway should be changed periodically for enhanced security.

➤ **To change the password of the EMS user:**

1. Connect to the CLI interface on the Active SC board. For more information, see Section "Command Line Interface" on page 107.
2. Login as **root** user. For more information, see Section 'Logging in as a Root User' on page 115.
3. At the prompt, type **tools user** and press **Enter**. The CLI USERS MANAGEMENT menu appears.

```
client238::~~# tools user
```

```
CLI USERS MANAGEMENT
```

```
list  -- LIST: list CLI users
add   -- ADD: add user
del   -- DELETE: delete user

pwd   -- PASSWORD: change user password
copy  -- COPY: copy users & passwords from other SC

lock  -- LOCK: lock user
unlock--UNLOCK: unlock user
force -- FORCE: force user to change password
```

4. At the **Choose submenu** prompt, type **pwd** and press **Enter**.

```
Choose submenu : pwd
```

```
CHANGE USER PASSWORD
```

5. At the **User Name** prompt, type **ems** and press **Enter**.

User Name : **ems**

6. At the **New Password** prompt, type the new password.

New Password:*****

7. At the **Re-enter new Password** prompt, type the new password again.

Re-enter new Password:*****

The new password is configured on the Active SC board and immediately replicated to the Standby SC board. Therefore there is no need to repeat steps 1-7 on the Standby SC.

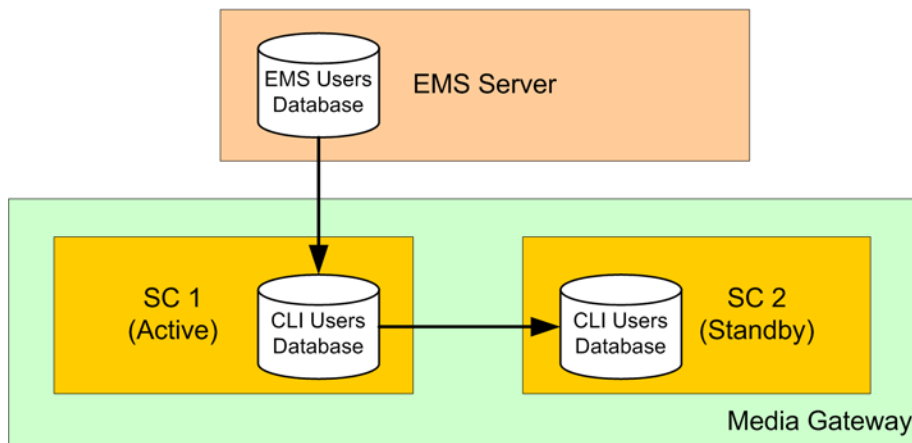
8. In the EMS GUI, right-Click the specific Media Gateway in the MG Tree and choose **Details** option from the menu.
9. Enter the new password in the **Ems Password** field and click **OK** button.

33.18.4 Synchronizing the CLI Users Database with the EMS Server

In the typical Media Gateway deployment scenario, the same users, passwords and access levels are used for all available Media Gateway management interfaces –the EMS GUI and the CLI.

To simplify user maintenance in such a scenario, the Media Gateway supports synchronization of the CLI Users Database with the EMS server. When this synchronization is activated, the Media Gateway will constantly synchronize its local CLI users database with the users database on the EMS server. Any change to the users database on the EMS server will be updated to all Media Gateways within a short period of time. All EMS server user profile attributes, including the access level and the password expiration policy are updated on both SC boards of all the Media Gateways connected to the EMS server. Use of the local CLI database ensures that the CLI users may access the Media Gateway even when there is no connectivity between the Media Gateway and the EMS server (e.g. in case of a network failure).

Figure 33-5: Synchronizing CLI Users Database with EMS Server



33.18.4.1 Synchronization Modes

When the CLI Users Database is synchronized with the EMS server, all user maintenance operations (user addition, removal and password change) must be performed via the interfaces provided on the EMS server. See the EMS User Manual for additional information. Only the passwords of **root** and **ems** users may be modified locally on the SC boards via **tools user** script as described in the previous sections.

■ Enable Block Mode

In this mode, CLI users whose passwords have expired are immediately denied access to the Media Gateway's CLI; in case of a network outage this means that some CLI users may be unable to access the CLI (if their passwords expire at the time of the outage).

■ Enable Seven Days

In this mode, CLI users whose passwords have expired are allowed access to the Media Gateway's CLI for an additional 7 days; this period is counted starting from the first user login after the password expiration; within these 7 days, users should access the EMS GUI and enter new passwords; users who do not renew their passwords within 7 days are denied access to the Media Gateway's CLI.

33.18.4.2 CLI User Synchronization with the EMS Server

CLI users synchronization may be enabled or disabled via the CLI interface on the Active SC board. Root privileges are required to modify the CLI users synchronization mode.

➤ **To enable CLI user Synchronization:**

1. Connect to the CLI interface on the Active SC board. For more information, see Section 'Command Line Interface' on page 107.
2. Login as **root** user. For more information, see Section 'Logging in as a Root User' on page 115.
3. At the prompt, type **tools user sync** and press **Enter**. The SYNCHRONIZE CLI USERS WITH EMS menu appears.

```
SYNCHRONIZE CLI USERS WITH EMS
```

```
enable_block-ENABLE BLOCK MODE:
Synchronize CLI and EMS users databases.
Block access to CLI for users with expired credentials.
enable_7days-ENABLE 7 DAYS MODE:
Synchronize CLI and EMS users databases.
Allow access to CLI for users with expired credentials
for additional 7 days.
disable-DISABLE
Do not synchronize CLI and EMS users databases.
CLI users should be managed via 'tools user' script.
```

4. At the **Choose submenu** prompt, choose the desired synchronization option and press **Enter**.

```
Choose submenu : enable_block
current mode is 'disable'
changing mode to enable_block
done
```

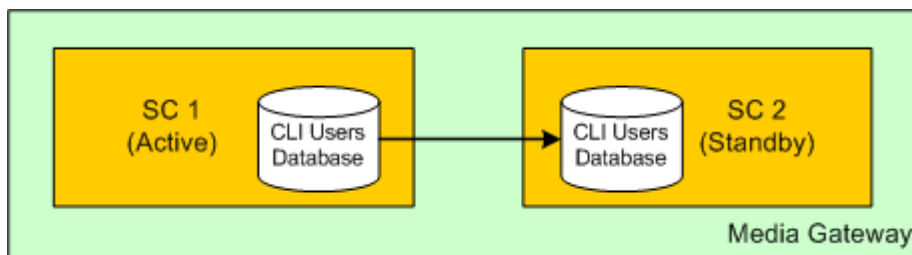
The synchronization mode is configured and immediately activated. If synchronization is enabled, the CLI users database will be synchronized with the EMS server within the next few minutes.

33.18.5 Administering the Local CLI User Database

In a simple Media Gateway configuration, the CLI users database is stored internally on each SC board and the **tools user** script is used to perform administration. The local CLI users database is constantly synchronized between the SC boards, therefore any change that is performed on the Active SC board is immediately replicated to the Standby SC board.

To configure the Media Gateway to use the Local CLI Users Database, run the **tools user sync** script and set synchronization mode to **disabled** (see chapter 'Synchronizing CLI Users Database with the EMS Server' on page 367 for details). Also ensure that external user authentication is disabled (see chapter 'Centralized RADIUS Servers' on page 384).

Figure 33-6: Local CLI Users Database on SC Boards



When the Media Gateway is configured to use the Local CLI Users Database, the security administrator should decide which users are allowed access to the Media Gateway CLI and to provision usernames and passwords via the **tools user** script as described below. It is strongly recommended to create a separate CLI account for each person who operates the Media Gateway and refrain from using shared accounts (i.e. accounts that are used by multiple users, such as the default **acladmin** account).

For enhanced security, passwords of CLI users must be periodically modified.



Note : The CLI Users Database is replicated from the active SC to the standby SC. Therefore always connect to the Active SC to perform user administration.

33.18.5.1 Creating a New CLI User

It is recommended to create a separate CLI user for each operator working with the Media Gateway.

➤ **To create a new CLI user:**

1. Connect to the CLI interface on the Active SC board. For more information, see Section 'Command Line Interface' on page 107.
2. Login as **root** user. For more information, see Section 'Logging in as a Root User' on page 115.
3. At the prompt, type **tools user** and press **Enter**. The CLI USERS MANAGEMENT menu appears.

```
client238::~~# tools user
```

```
CLI USERS MANAGEMENT
```

```
list  -- LIST: list CLI users
add   -- ADD: add user
del   -- DELETE: delete user

pwd   -- PASSWORD: change user password
copy  -- COPY: copy users & passwords from other SC

lock  -- LOCK: lock user
unlock--UNLOCK: unlock user
force -- FORCE: force user to change password
```

4. At the **Choose submenu** prompt, type **add** and press **Enter**.

```
ADD CLI USER
```

```
Choose submenu : add
```

5. At the **User Name** prompt, type the desired username and press **Enter**.

```
User Name : george
```

6. At the **User Privileges** prompt, type the desired user privileges level and press **Enter**.

```
User privileges ([a-administrator]/m-monitor) : a
```

7. At the **When password should expire** prompt, type the password expiration date (number of days). To configure password without an expiration date, type **0**.

When password should expire? ([0-never]/number of days) : **100**



Note: For improved security, it is strongly recommended to use an expiration date for all passwords.

8. At the **Prevent too often password changes** prompt, type the minimum interval between password changes (number of days). For not limiting the password change time interval, type **0**.

Prevent too often password changes? ([0-no]/number of days) : **1**



Note: For improved security, it is strongly recommended to limit password changes to not more than 1 change per day. This limitation affects only password change operations performed by users themselves. The administrative super-user (**root**) may modify the password of any user regardless of any time limitations.

9. At the **New Password** prompt, type the new password.

New Password:*****

10. At the **Re-enter new Password** prompt, type the new password again.

Re-enter new Password:*****

New CLI users are configured on Active SC board and immediately replicated to the Standby SC board. Therefore, there is no need to repeat steps 1-10 on the Standby SC.

33.18.5.2 Deleting a CLI User

CLI user accounts that are not in use should be deleted.

➤ **To delete CLI user:**

1. Connect to the CLI interface on the Active SC board. For more information, see Section 'Command Line Interface' on page 107.
2. Login as **root** user. For more information, see Section 'Logging in as a Root User' on page 115.
3. At the prompt, type **tools user** and press **Enter**. The CLI USERS MANAGEMENT menu appears.

```
client238::~~# tools user
```

```
CLI USERS MANAGEMENT
```

```
list  -- LIST: list CLI users
add   -- ADD: add user
del   -- DELETE: delete user

pwd   -- PASSWORD: change user password
copy  -- COPY: copy users & passwords from other SC

lock  -- LOCK: lock user
unlock--UNLOCK: unlock user
force -- FORCE: force user to change password
```

4. At the **Choose submenu** prompt, type **del** and press **Enter**.

```
Choose submenu : del
```

```
DELETE CLI USER
```

5. At the **User Name** prompt, type the desired username and press **Enter**. It is also possible to delete all CLI users by typing **all**.

```
User Name (all - delete all users): george
```

The CLI user is deleted from the Active SC board and this change is immediately replicated to the Standby SC board. Therefore, there is no need to repeat steps 1-6 on the Standby SC.

33.18.5.3 Changing Password of the CLI User

For security reasons, passwords of CLI users should be changed periodically. It is also important to change passwords of CLI users upon administrator reassignment.

CLI user passwords may be modified in one of the following ways:

- By CLI user– either upon password expiration (new password will be asked during the next login) or upon explicit user request (via **passwd** command)
- By security administrator – via **tools user** script, as described below.



Note: The CLI users database is always replicated from Active SC board to the Standby SC board. Therefore ensure that you change CLI user's password on Active SC board only.

➤ **To change the password of a CLI user:**

1. Connect to the CLI interface on the Active SC board. For more information, see Section 'Command Line Interface' on page 107.
2. Login as **root** user. For more information, see Section 'Logging in as a Root User' on page 115.
3. At the prompt, type **tools user** and press **Enter**. The CLI USERS MANAGEMENT menu is displayed.

```
client238::~~# tools user
```

```
CLI USERS MANAGEMENT
```

```
list  -- LIST: list CLI users
add   -- ADD: add user
del   -- DELETE: delete user

pwd   -- PASSWORD: change user password
copy  -- COPY: copy users & passwords from other SC

lock  -- LOCK: lock user
unlock--UNLOCK: unlock user
force -- FORCE: force user to change password
```

4. At the **Choose submenu** prompt, type **pwd** and press **Enter**. The CHANGE USER PASSWORD menu appears.

Choose submenu : **pwd**

CHANGE USER PASSWORD

5. At the **User Name** prompt, type the desired username and press **Enter**.
6. At the **When password should expire** prompt, type the password expiration date (number of days). To configure a password without an expiration date, type **0**.

When password should expire? ([0-never]/number of days) : **100**



Note: For improved security, it is strongly recommended to use an expiration date for all passwords.

7. At the **Prevent too often password changes** prompt, type the minimum interval between password changes (number of days). For not limiting the password change time interval, type **0**.

Prevent too often password changes? ([0-no]/number of days) : **1**



Note: For improved security, it is strongly recommended to limit password changes to not more than 1 change per day. This limitation affects only password change operations performed by users. The administrative super-user (**root**) may alter the password of any user regardless of any time limitations.

8. At the **New Password** prompt, type the new password.

New Password:*****

9. At the **Re-enter new Password** prompt, type the new password again.

Re-enter new Password:*****

The new password is configured on the Active SC board and immediately replicated to the Standby SC board. Therefore, there is no need to repeat steps 1-9 on the Standby SC.

33.18.6 Centralized AAA Servers

In large scale deployments, centralized Authentication, Authorization and Accounting (AAA) servers are used to control user access to different network equipment. AAA servers implement the following functionality:

- Authenticate user login to the specific equipment.
- Authorize certain tasks or commands that specific users may perform on specific equipment.
- Report which users are accounted for which tasks on the specific equipment.

Use of the AAA servers allows use of the same user credentials (usernames and passwords) across multiple network equipment. It also greatly simplifies user provisioning and may be used to enforce enhanced security policies, for example:

- Time-based login
- Enforce password complexity

Immediately revoke privileges from specific users The Mediant 8000 supports two types of centralized AAA servers:

- TACACS+ Servers
- RADIUS Servers

When the Mediant 8000 is configured to work with centralized AAA servers, all user maintenance and provisioning tasks should be performed on the AAA servers (using the corresponding configuration interfaces) and not via the **tools user** or **passwd** CLI commands.

33.18.6.1 Centralized TACACS+ Servers

Terminal Access Controller Access-Control System Plus (TACACS+) is a AAA protocol developed by Cisco and supported by most Cisco network equipment. TACACS+ servers provide all AAA services – authentication, authorization and accounting – thus greatly simplifying network administration and user management. Multiple TACACS+ servers may be deployed for high-available network setups.

The Mediant 8000 supports interworking with standard-compliant TACACS+ servers and implements all AAA services as defined by the protocol (see details below). Up to three TACACS+ servers may be defined for redundancy purposes. Local user cache is implemented for emergency access to the Mediant 8000 in case of network outage (for more information, see Section 'TACACS+ Protocol Overview' below).

33.18.6.1.1 TACACS+ Protocol Overview

The Mediant 8000 implements the latest version of the TACACS+ protocol as defined in IETF draft-grant-tacacs-02. All major protocol functionality, including message encryption, is supported.

Up to three TACACS+ servers may be configured for redundancy purposes. The Mediant 8000 falls back to the redundant TACACS+ server in case communication with the active TACACS+ server fails. Communication with the currently selected TACACS+ server continues until the next failure.

For each TACACS+ server, the following parameters may be configured by the user:

- IP address
- Port
- Secret Key

In addition, the **AAA Server Connection Timeout** parameter may be configured to determine how long the Media Gateway awaits the response from the currently active TACACS+ server, before falling back to the redundant server.

The Mediant 8000 implements the following TACACS+ services:

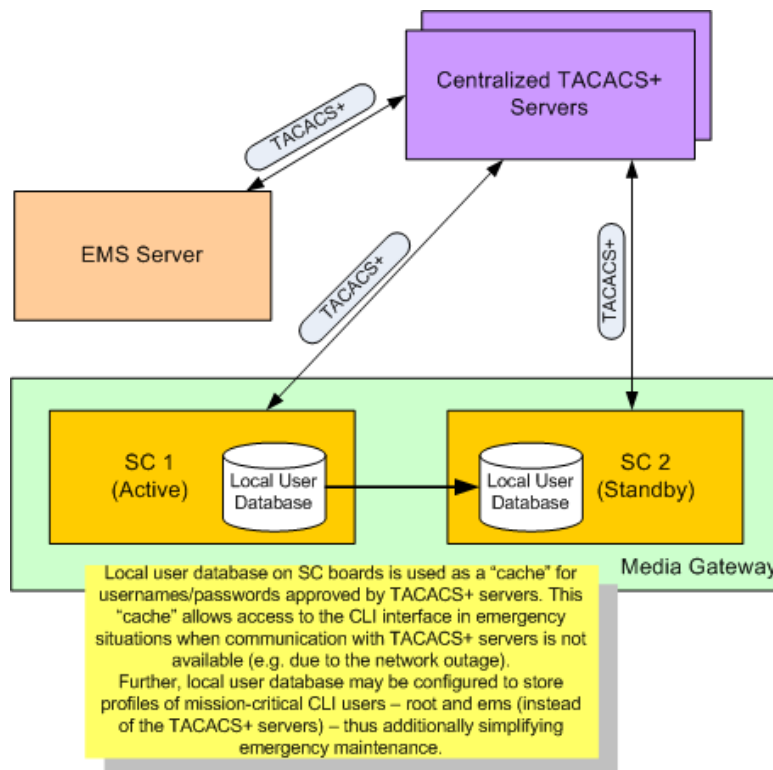
- Authentication – for user login via SSH, SCP, SFTP and RS-232 management interfaces and **su** command.
- Authorization – for all Media Gateway specific CLI commands (e.g. **show**, **tpCmd**, **tools**).
- Accounting – for all user activity on the Media Gateway CLI interface (i.e. both for Media Gateway specific commands – e.g. **show** – and for generic OS commands – e.g. **ls**).

Gateway implements a local cache of user profiles. This cache is used in emergency situations when communication with TACACS+ servers is not possible (e.g. in case of global network outage). In such scenarios, users who logged into the Mediant 8000 CLI interface recently (e.g. within the last 30 days) will be able to login using the credentials stored in the local user profile cache. The cache is automatically synchronized between active and standby SC boards.

Furthermore, **root** and **ems** users, who are critical for operation, may be configured in the local user database (and not on the TACACS+ servers) – thus additionally simplifying Mediant 8000 emergency maintenance.

The EMS management application also supports the interworking with TACACS+ servers. See the "LTRT-XXXX EMS User Manual" for detailed information.

Figure 33-7: Working with Centralized TACACS+ Servers



33.18.6.1.2 Working With TACACS+ Server : User Login

When the user logs into the Mediant 8000 CLI, Authentication and Authorization requests are sent towards the TACACS+ servers.

- **Authentication Request** includes username and password, encoded according to the "Inbound PAP Login" authentication scheme.
- **Authorization Request** includes the following AV-pairs:
 - **service** = "shell"
 - **cmd** = "" (empty)

Authentication and Authorization Responses, received from the TACACS+ server, determine whether the login is allowed or not. If the Authorization Response contains **priv-lvl** AV-pair, it will be used to determine the "privilege level" of the CLI user (administrator/monitor) according to the table below. Otherwise the CLI administrator privilege level will be granted.

Priv-lvl Value	CLI Privilege Level
0	Monitor
1 – 14	Administrator
15	For root username - super-user (the only supported option); For others - administrator

Upon successful Authentication and Authorization Responses, user credentials are "cached" in the local user database on SC boards. This "cache" allows access to the CLI interface in emergency cases when communication with TACACS+ servers is impossible (e.g. due to the network outage). Local "cache" entries have limited lifetime (configurable via **AAA Cache Password Expiration** parameter) – after which they are invalidated.

33.18.6.1.3 Working With TACACS+ Server : Command Execution

When the user enters a command in the Mediant 8000 CLI interface, Authorization and Accounting requests are sent towards the TACACS+ server.

Authorization Request is sent for all Media Gateway specific CLI commands (e.g. **show** or **tpCmd**); however not for generic OS commands (e.g. **ls**). Authorization Response, received from the TACACS+ server, determines whether specific command execution is allowed or not.

Authorization Request includes the following AV-pairs:

- **service** = "shell"
- **cmd** = <command> (e.g. show)
- **cmd-arg** = <arguments>" (e.g. moBoard#6)

Multiple **cmd-arg** elements may be included according to the number of command arguments provided by the user. To simplify the processing of Authorization Requests by the TACACS+ server, commands entered by the user are automatically expanded. For example, if command "**sh br#8**" is entered, the corresponding expanded command "**show moBoard#8**" is sent instead.

Accounting Requests are sent for all activity performed on the Media Gateway's CLI interface (i.e. both for Media Gateway's specific commands – e.g. **show** – and for generic OS commands – e.g. **ls**). Two Accounting Requests are generated – one before the command execution and one immediately after.

An **Accounting Request** sent before the command execution, includes the following AV-pairs:

- **start_time** = <start time> (in seconds since 1/1/1970)
- **cmd** = <command> (e.g. show)

- **cmd-arg** = <arguments>" (e.g. moBoard#6)

Accounting Request sent after the command completion, includes the following AV-pairs:

- **stop_time** = <stop time> (in seconds since 1/1/1970)
- **elapsed_time** = <elapsed time> (in seconds)
- **cmd** = <command> (e.g. show)
- **cmd-arg** = <arguments>" (e.g. moBoard#6)

33.18.6.1.4 Working With TACACS+ Server : ROOT and EMS Users

For typical configurations, the Mediant 8000 should be configured to perform authentication of **root** and **ems** users using the local user database (instead of via the TACACS+ servers). This architecture ensures that common maintenance tasks performed by the EMS server (e.g. Online Software Upgrade) do not depend on the TACACS+ servers' availability and will continue to work even in case of a temporary network outage. It also allows provisioning of different passwords for these task-critical users on different Media Gateways – thus enhancing overall network security.

Users who nevertheless wish to store user profiles for **root** and **ems** users on TACACS+ server, may do so by configuring the parameter **Skip AAA Validation For Special Users** to *Disabled* as described in the following sections.

33.18.6.1.5 Configuring Media Gateway to Work With TACACS+ Servers

➤ To configure the Mediant 8000 to work with centralized TACACS+ servers:

1. Connect to the Mediant 8000 CLI interface (on active SC board) and login as **root** user.
2. Disable synchronization of local CLI user database with EMS server via **tools user sync disable** command.
3. Delete all CLI users, except **root** and **ems** from the local user database on SC boards, via the **tools user del all** command.
4. In the EMS, click  to access the Media Gateway status screen.
5. In the Navigation pane, select **Security** and then in the configuration pane, select **Security Settings**; the Security Settings screen is displayed.
6. In the Security Settings screen, select the **CLI Authentication** tab.
7. At the bottom of the screen, use the  or  buttons to add or remove TACACS+ servers. Configure TACACS+ server settings according to the "AAA Server Settings" table below. After completing the configuration, unlock table entries by right-clicking on the row and choosing **Unlock**.
8. Set **External Authentication Server** to TACACS.
9. Configure TACACS+ settings according to the "TACACS+ Settings" table below.

Table 33-15: Centralized AAA Server Settings

Parameter Name	Type	Provisioning Type	Description
External Authentication Server	Enum None, RADIUS, TACACS	Instant	Defines whether or not centralized AAA servers are used for CLI users' authentication, authorization and accounting. ▪ None – local user database (on SC boards) is used for CLI user authentication ▪ RADIUS – centralized RADIUS servers are used for CLI user authentication ▪ TACACS – centralized TACACS+ servers are used for CLI user authentication, authorization and accounting

Table 33-16: AAA Server Settings

Parameter Name	Type	Provisioning Type	Description
Server Name	String Up to 80	Instant	Defines a textual name for the AAA server, enabling users to identify it easily.
Server IP	String Up to 20	Instant	Defines the IP address of the AAA server.
Server Port	Integer 0 – 65535	Instant	Defines the port of the AAA server. For standard TACACS+ servers, port 49 is typically used.
Server Password	String Up to 80	Instant	Defines secret key used to encrypt communication with specific AAA server. Empty value disables encryption.

Table 33-17: TACACS+ Settings

Parameter Name	Type	Provisioning Type	Description
Skip AAA Validation For Special Users	Enum Disable, Enable	Instant	Defines whether authentication for task-critical (root and ems) users is performed using the local user database or via the centralized authentication server. ▪ Disable – root and ems users are authenticated via the centralized TACACS+ server (like any other CLI user) ▪ Enable – root and ems users are authenticated using the local user database on SC boards.
AAA Server Connection Timeout	Integer 0 – 60	Instant	Defines the maximum time (in seconds) that the Media Gateway awaits response from the currently active TACACS+ server prior to falling back to the redundant server. Note, that the actual "failed server detection" time is typically much lower – e.g. failure in TCP/IP connection establishment typically takes less than 1 second.
AAA Active Server	Integer 1 – 3	Instant	Indicates the currently active TACACS+ server. May be also used to force the Media GatewayMedia Gateway to work with the specific TACACS+ server (assuming that the server is available).
AAA Cache Password Expiration	Integer 0 – 90	Instant	Defines the expiration time for "cached" entries in the local user database. For example, when set to 30, after a successful login to the Mediant 8000 the CLI username and password are "cached" for 1 month. In case of network outage, within this period, a specific user will be able to login into the Gateway CLI using the same credentials. Value 0 disables the local cache feature. Note, however, that in this case access to the Gateway CLI will

Parameter Name	Type	Provisioning Type	Description
			be impossible in certain emergency scenarios (e.g. in case of network outage).

33.18.6.1.6 Sample TACACS+ Server Configuration

Use the following sample TACACS+ server configuration file as a reference when deploying the Mediant 8000 in your network environment. The file is compatible with version F4.0.4.19 of TACACS+ daemon released by Shrubbery Networks Inc. that may be downloaded from 'http://www.shrubbery.net/tac_plus.'

```
# tac_plus.cfg
#
# Sample TACACS+ server configuration for Mediant 5000/8000
#

key = 1234567890
# user "root"
#   super-user
user = root {
    default service = permit
    pap = cleartext "root"
    service = exec {
        priv-lvl = 15
    }
}

# user "ems"
#   CLI administrator privilege level
#   permit all commands
user = ems {
    default service = permit
    pap = cleartext "pass_1234"
    service = exec {
        priv-lvl = 1
    }
}

# user "john"
#   CLI administrator privilege level
#   permit all commands, except "tpCmd" and "tools bk"
user = john {
    default service = permit
    pap = cleartext "pass_1234"
    service = exec {
        priv-lvl = 1
    }
    cmd = tpCmd {
        deny .*
    }
    cmd = tools {
        deny bk
        permit .*
    }
}

# user "fred"
#   CLI monitor privilege level
#   allow only "show" command
user = fred {
    pap = cleartext "pass_1234"
    service = exec {
```

```
priv-lvl = 0
}
cmd = show {
  permit .*
}
}
```

33.18.6.2 Centralized RADIUS Servers

Remote Authentication Dial In User Service (RADIUS) is a standard AAA protocol defined by IETF and widely deployed in many networks for centralized user authentication. Contrary to the TACACS+, the RADIUS protocol does not support separate requests for authentication and authorization services – instead a single Access Request is used to combine both services (refer to RFC 2865 for details). The Accounting service is implemented via a separate Accounting Request (refer to RFC 2866 for details).

The Mediant 8000 supports interworking with standard-compliant RADIUS servers and implements authentication and authorization service for user login as defined by the protocol (see details below). Up to three RADIUS servers may be defined for redundancy purposes. Local user cache is implemented for emergency access to the Mediant 8000 in case of network outage (for more information, see for more information, see Section 'TACACS+ Protocol Overview' below).

33.18.6.2.1 RADIUS Protocol Overview

The Mediant 8000 implements the authentication and authorization parts of the RADIUS protocol as defined in RFC 2865. Authorization is implemented using Audiocodes vendor-specific attributes (VSAs) or, alternatively, using CISCO VSAs.

Up to three RADIUS servers may be configured for redundancy purposes. The Mediant 8000 falls back to the redundant RADIUS server in case communication with the active RADIUS server fails. Communication with the currently selected RADIUS server continues until the next failure.

For each RADIUS server, the following parameters may be configured by the user:

- IP address
- Port
- Secret Key

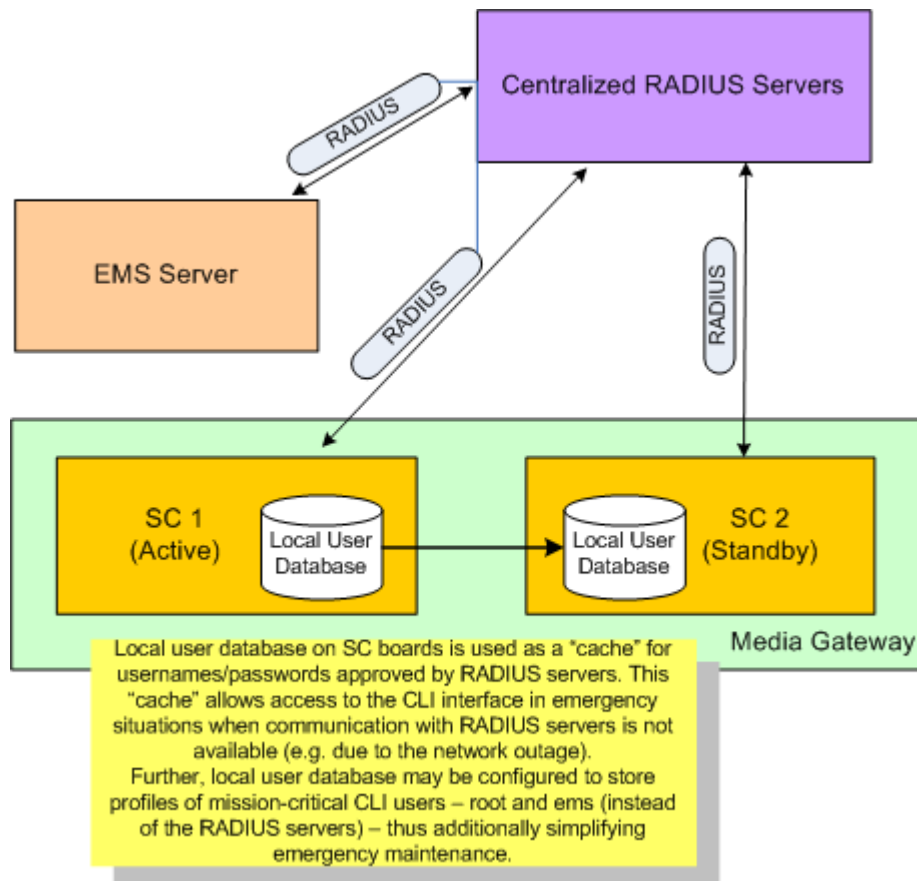
In addition, RADIUS Retransmit Timeout and RADIUS Number Of Retries parameters may be configured to determine how long the Media Gateway awaits the response from the currently active RADIUS server, before falling back to the redundant server.

Gateway implements a local cache of user profiles. This cache is used in emergency situations when communication with RADIUS servers is not possible (e.g. in case of a global network outage). In such scenarios, users who recently logged into the Gateway CLI interface (e.g. within the last 30 days) will be able to login using the credentials stored in the local user profile cache. The cache is automatically synchronized between active and standby SC boards.

Furthermore, root and ems users, who are critical for operation, may be configured in the local user database (and not on the RADIUS servers) – thus additionally simplifying Mediant 8000 emergency maintenance.

EMS management application also supports user authentication using centralized RADIUS servers. Its implementation lacks the above limitation and does not require new user pre-provisioning. See the "LTRT-XXXX EMS User Manual" for detailed information.

Figure 33-8: Centralized User Authentication via RADIUS Protocol



33.18.6.2.2 Working With RADIUS Server : User Login

When user logs into the Mediant 8000 CLI, **Access-Request** message containing username and password is sent to the RADIUS servers. In response, one of the following messages may be received:

- **Access-Accept** – indicates that user is allowed to log in; if the response contains Reply-Message attribute, it is displayed to the user.
- **Access-Reject** – indicates that user is not allowed to log in; if the response contains Reply-Message attribute, it's displayed to the user.
- **Access-Accept** message may contain one of the following Vendor-Specific Attributes (VSAs) that are used to determine the "privilege level" of the CLI user (administrator/monitor):
 - AudioCodes VSA
 - ◆ Vendor ID: 5003
 - ◆ Vendor Type: 35
 - ◆ Values: 0 = no access, 1-99 = monitor level; 100-255 = administrator level
 - CISCO VSA
 - ◆ Vendor ID: 9
 - ◆ Vendor Type: 1
 - ◆ Values: "shell:priv_lvl=x", where x is: 0=monitor level, 1-15=administrator level

33.18.6.2.3 Configuring the Media Gateway to Work With RADIUS Servers

This section describes how to configure the Media Gateway to Work With RADIUS servers.

➤ **To configure Mediant 8000 to work with centralized RADIUS servers:**

1. Connect to the Mediant 8000 CLI interface (on active SC board) and login as **root** user.
2. Disable synchronization of local CLI user database with EMS server via **tools user sync disable** command.
3. Delete all CLI users except **root** and **ems** from local user database on SC boards via **tools user del all** command.
4. Click  to access the Media Gateway status screen.
5. In the Navigation pane, select **Security** and then in the configuration pane, select **Security Settings**; the Security Settings screen is displayed.
6. In the Security Settings screen, select the **CLI Authentication** tab.
7. At the bottom of the screen, use the  or  buttons to add or remove RADIUS servers. Configure RADIUS server settings according to the "AAA Server Settings" table above. After completing the configuration, unlock table entries by right-clicking on the row and choosing **Unlock**.
8. Set **External Authentication Server** to **RADIUS**.

9. Configure RADIUS servers' settings according to the "RADIUS Servers' Settings" table below.

Table 33-18: RADIUS Settings

Parameter Name	Type	Provisioning Type	Description
Skip AAA Validation For Special Users	Enum Disable, Enable	Instant	Defines whether authentication for task-critical (root and ems) users is performed using the local user database or via the centralized authentication server. ▪ Disable – root and ems users are authenticated via the centralized RADIUS server (like any other CLI user) ▪ Enable – root and ems users are authenticated using the local user database on SC boards.
RADIUS Auth Retransmit Timeout (sec)	Integer 1-100	Instant	Defines the timeout (in seconds) between RADIUS requests retransmissions.
RADIUS Auth Number Of Retries	Integer 1-100	Instant	Defines the number of retransmission attempts for each RADIUS server.
AAA Active Server	Integer 1 – 3	Instant	Indicates the currently active RADIUS server. May be also used to force the Media Gateway to work with the specific RADIUS server (assuming that the server is available).
AAA Cache Password Expiration	Integer 0 – 90	Instant	Defines the expiration time for "cached" entries in the local user database. For example, when set to 30, after a successful login to the Mediant 8000, the CLI username and password are "cached" for one month. In case of network outage, within this period, a specific user will be able to login into the Gateway CLI using the same credentials. Value 0 disables the local cache feature. Note, however, that in this case, access to the Gateway CLI will be impossible in certain emergency scenarios (e.g. in case of network outage).

33.18.6.2.4 Sample RADIUS Server Configuration

Use the following sample RADIUS server configuration file as a reference when deploying the Mediant 8000 in your network environment. The file is compatible with FreeRADIUS server that may be downloaded from '<http://www.freeradius.org>'.

```
#
# clients.conf - clients configuration file
#
client 10.7.9.231 {
secret = 1234567890
shortname = M8K_SC1
}

client 10.7.9.232 {
secret = 1234567890
shortname = M8K_SC2
}

#
# dictionary - AudioCodes VSA dictionary
#
VENDOR AudioCodes 5003
ATTRIBUTE ACL-Auth-Level 35 integer AudioCodes
VALUE ACL-Auth-Level ACL-Auth-UserLevel 50
VALUE ACL-Auth-Level ACL-Auth-AdminLevel 100

#
# users - local users configuration file
#
john Auth-Type := Local, User-Password == "qwerty"
Service-Type = Login-User,
ACL-Auth-Level = ACL-Auth-AdminLevel

larry Auth-Type := Local, User-Password == "123456"
Service-Type = Login-User,
ACL-Auth-Level = ACL-Auth-UserLevel
```


33.18.7 CLI Interface Access Control

SSH and Telnet services on SC boards are used to access the Media Gateway Command Line Interface (CLI). In the default configuration, these services are accessible from any IP address and user authentication is performed via username and password (see Section CLI User Administration) for details.

For enhanced security, you may restrict access to the SSH and Telnet services on SC boards by specifying an explicit list of IP addresses that are allowed to access the CLI interface.

➤ **To enable access control on the CLI interface:**

1. Click  to access the Media Gateway status screen.
2. In the Navigation pane, select **Security** and then in the configuration pane, click **Security Settings**; the Security Settings screen is displayed.
3. In the **CLI Access Control** section, configure the CLI Interface Access Control parameters according to the table below.

Table 33-19: CLI Interface Access Control Parameters

Parameter Name	Type	Provisioning Type	Description
CLI Access Control	Enum Disable, Enable	Instant	Limit access to CLI interface on SC boards. When enabled, SSH, SFTP, SCP, Telnet and FTP services on SC boards are granted only to IP's explicitly specified by user. Note that CLI access is always granted to SNMP managers (EMS, NMS, OSS and APS).
CLI Access IP 1	IP Address	Instant	Defines the first IP address that is allowed access to the SC board's CLI interface.
CLI Access IP 2	IP Address	Instant	Defines the second IP address that is allowed access to the SC board's CLI interface.
CLI Access IP 3	IP Address	Instant	Defines the third IP address that is allowed access to the SC board's CLI interface.
CLI Access IP 4	IP Address	Instant	Defines the fourth IP address that is allowed access to the SC board's CLI interface.
CLI Access IP 5	IP Address	Instant	Defines the fifth IP address that is allowed access to the SC board's CLI interface.

33.18.8 Password-less Access to the CLI Interface

The Mediant 8000 may be configured to perform CLI user authentication based on the RSA or DSA private/public key pair. When such authentication is enabled, users are granted access to the Mediant 8000 CLI without the need to interactively enter a password.



Note: Password-less access is only supported when you connect to the CLI interface via the SSH protocol.

In order to enable RSA or DSA private/public key based authentication, take the following steps:

- Generate a RSA or DSA private/public key pair for the SSH client.
- Transfer the generated public key to the Mediant 8000 and authorize its use for a specific CLI user.
- Verify that the password-less login works, by starting the SSH client software and using the generated private key for authentication.

RSA keys are generally considered to be stronger than DSA keys. Therefore if your SSH client application supports both authentication mechanisms, it is recommended to generate RSA keys.

RSA or DSA private/public key authentication may be configured to be the only valid authentication scheme for a specific CLI user. However, this configuration may not be applied to **root** and **ems** users who are utilized by the EMS server.

33.18.8.1 Generating a Private/Public Key Pair

An RSA or DSA private/public key pair must be generated on the SSH client. The exact procedures for key generation may differ, depending on the SSH client software used – therefore if the below procedures do not work, refer to your SSH client documentation.

➤ **If you use standard Linux/UNIX command-line SSH client software:**

1. Log in to your client machine with the same credentials (username / password) that you will be using for starting the SSH client.
2. To generate an RSA key, type **ssh-keygen -t rsa** at the prompt.

```
$ ssh-keygen -t rsa
Generating public/private rsa key pair.
```

3. Accept the default location for the file by pressing Enter when prompted for the file name.

Enter file in which to save the key (/home/user/.ssh/id_rsa):

4. The generated private/public key pair may be protected by a passphrase for enhanced security. However use of the passphrase makes SSH login interactive (user will be asked for a passphrase instead of the username/password).
For enhanced security, enter the passphrase at the prompt. For an empty passphrase, press **Enter**.

Enter passphrase (empty for no passphrase):
Enter same passphrase again:

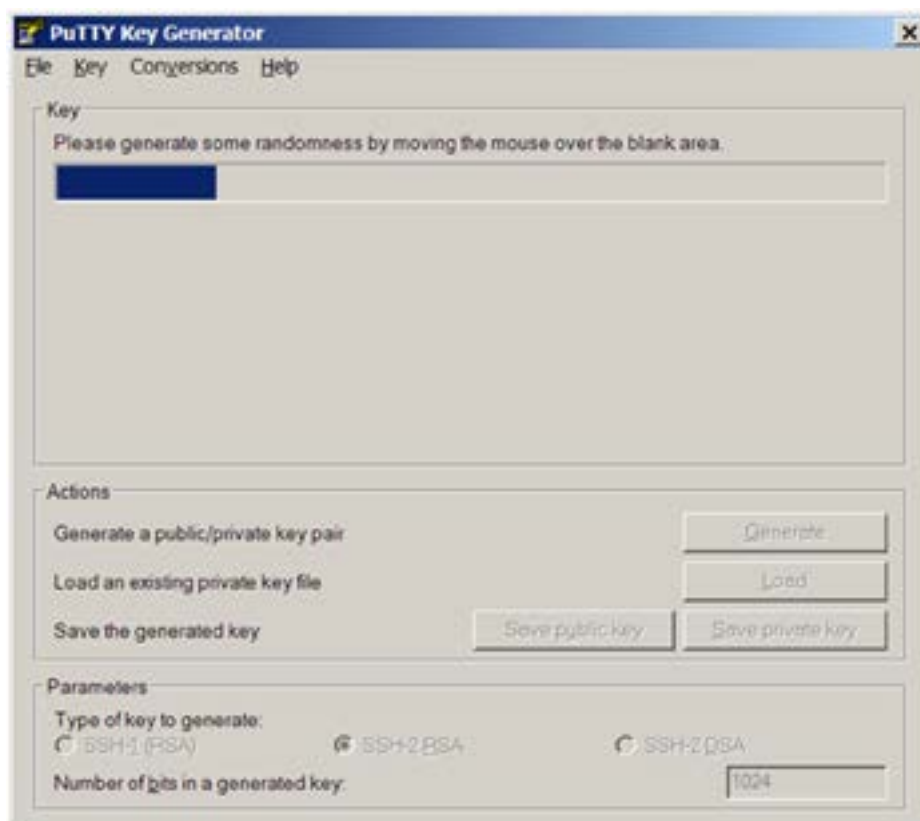
5. Finally, **ssh-keygen** will confirm the completion and creation of the private/public key files.

Your identification has been saved in /home/user/.ssh/id_rsa.
Your public key has been saved in /home/user/.ssh/id_rsa.pub.
The key fingerprint is:
41:0a:51:fo:23:ea:ac:38:e4:f8:80:9a:d3:3b:a0:87 user@ssh-client

➤ If you use PuTTY client software (for Windows PC), take the following steps:

1. Locate and run the **Puttygen.exe** (Putty Key Generator) binary.
2. Select **SSH-2 RSA** key type, press **Generate** button and move the mouse over the blank area (as prompted) to generate some randomness on the keys.

Figure 33-9: PuTTY Key Generator



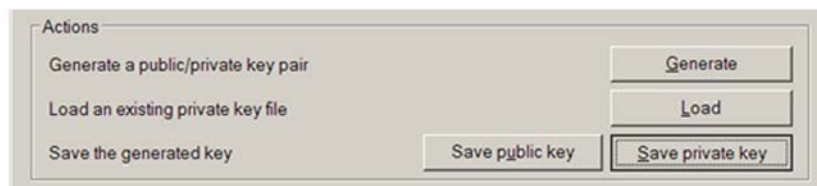
3. When the key generation has completed, copy all text of the public-key in the box and paste it into a text file – this is the public key file. Transfer this file to the Mediant 8000, where it should be authorized.

Figure 33-10: PuTTY Key Generator-Public Key



4. Click the **Save Private Key** button to save the private key file that should be used by the PuTTY client to authenticate itself.

Figure 33-11: PuTTY Key Generator-Generate Action



33.18.8.1.1 Transferring and Authorizing the Public Key to the Mediant 8000

The RSA or DSA public key, generated in the previous step, must be transferred to the Mediant 8000 and authorized for the specific CLI user. Authorization implies that the SSH client that uses the private key will be granted credentials and access permission of the specific CLI user.

To transfer the generated public key file to the Active SC board via SFTP/SCP/FTP, use any standard-compliant SFTP/SCP/FTP client software. Connect to the Global IP address and when prompted for a username/password, enter the CLI user credentials (e.g. **acladmin/pass_1234**).



Note: In the secure operation mode, FTP access to the Mediant 8000 is disabled. Use SFTP/SCP instead.

➤ To authorize the use of the transferred public key for password-less SSH authentication:

1. Connect to the CLI interface on the Active SC board. For more information, refer to 'Command Line Interface' on page 107.
2. Login as the CLI user upon which the password-less SSH login will be authorized. Alternatively you may also login as **root** user; however, you will later be prompted to enter the CLI user name.

3. At the prompt, type **tools ssh_key** and press **Enter**. The SSH Key Management menu is displayed.

```
SSH KEY MANAGEMENT

list      -- LIST: list authorized keys
add       -- ADD: authorize new key
del       -- DELETE: delete key authorization
```

4. At the **Choose submenu** prompt type **add** and press **Enter**.

```
Choose submenu : add

ADD AUTHORIZED SSH KEY
```

5. Enter the name of the public key file that you transferred to the Active SC board and press **Enter**.

```
Enter public key filename ([id_rsa.pub]) : id_rsa.pub
```

6. The public key will be parsed and keys from it will be added to the authorized keys list. You will be informed on the progress of the operation.

```
Parsing public key file id_rsa.pub
Adding RSA public key "rsa-key-20081127"
done
```



Note: Authorized SSH keys, provisioned on the Active SC board, may also be used for connecting to the CLI interface on the Standby SC boards. The Mediant 8000 software automatically replicates all required information between the Active and the Standby SC boards. Therefore there is no need to manually authorize SSH keys on the Standby SC board.

33.18.8.1.2 Starting the SSH client and Using a Generated Private Key for Authentication

Now you may verify that the password-less login works, by starting the SSH client and using the generated private key for authentication. The exact procedures for starting the SSH client may differ, depending on the SSH client software being used – therefore if the below procedures do not work, refer to your SSH client documentation.

➤ **If you use standard Linux/UNIX command-line SSH client software:**

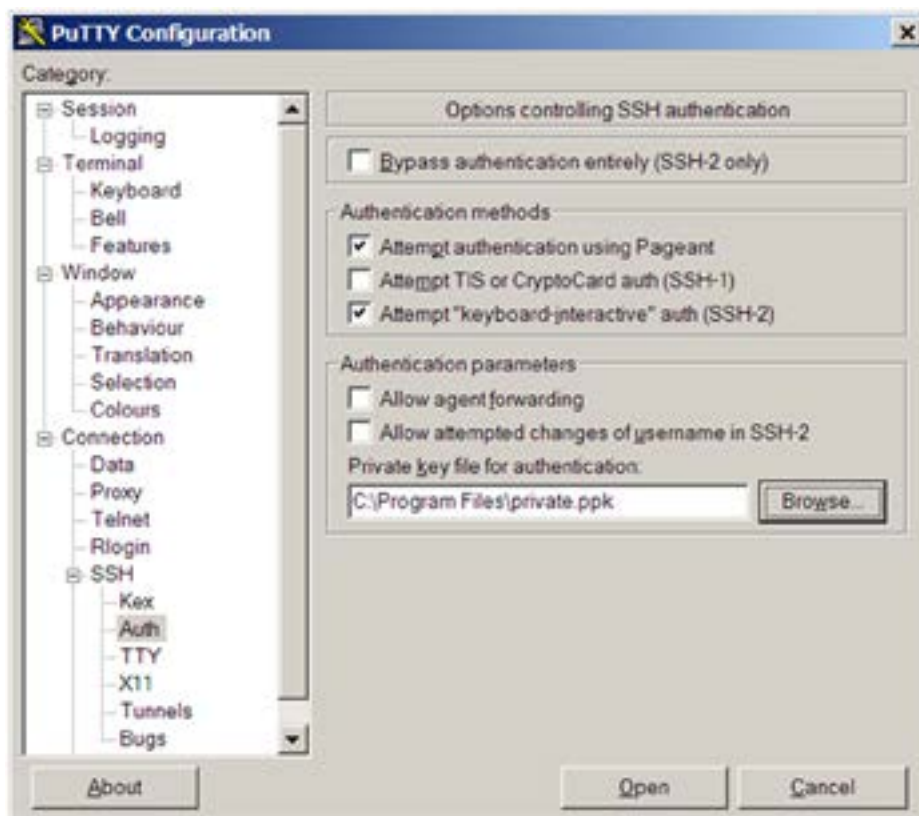
1. Log in to your client machine with the same credentials (username/password) that you used while generating the private/public key pair (in Step 1).
2. Start the SSH client and specify the CLI username and the Active SC's IP address as command-line parameters:

```
$ ssh acldadmin@10.7.13.91
```

➤ **If you use PuTTY client software (for Windows PC):**

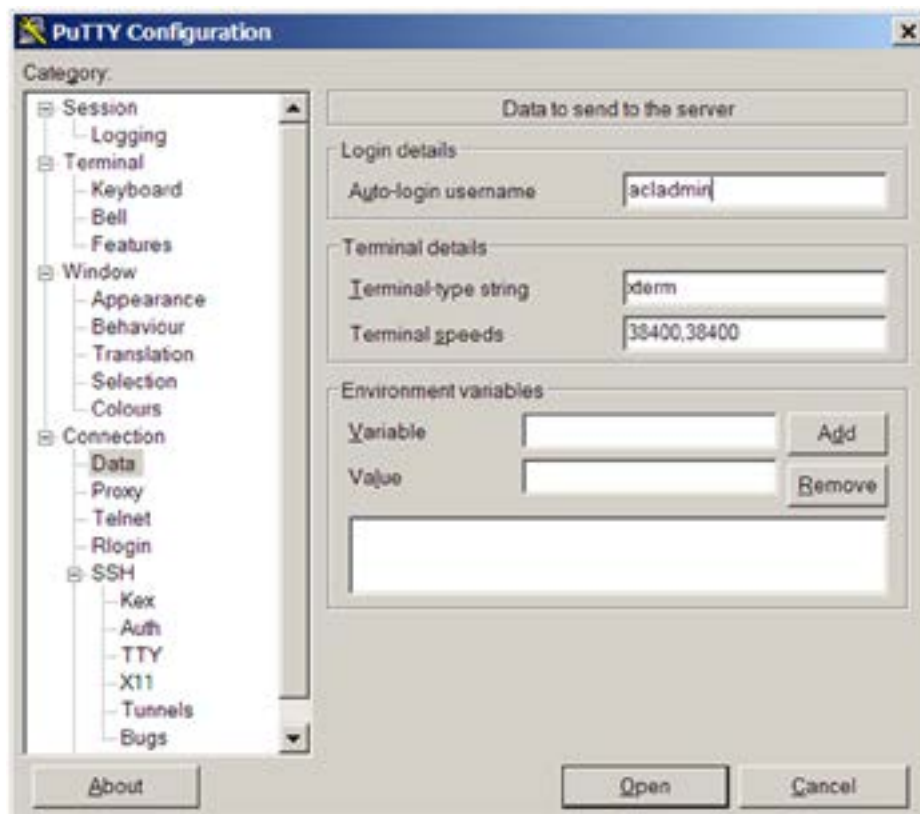
1. Locate and run the **PuTTY.exe** (Putty client) binary.
2. In **Connection -> SSH -> Auth**, choose the saved private key for authentication.

Figure 33-12: PuTTY Client-SSH Authentication



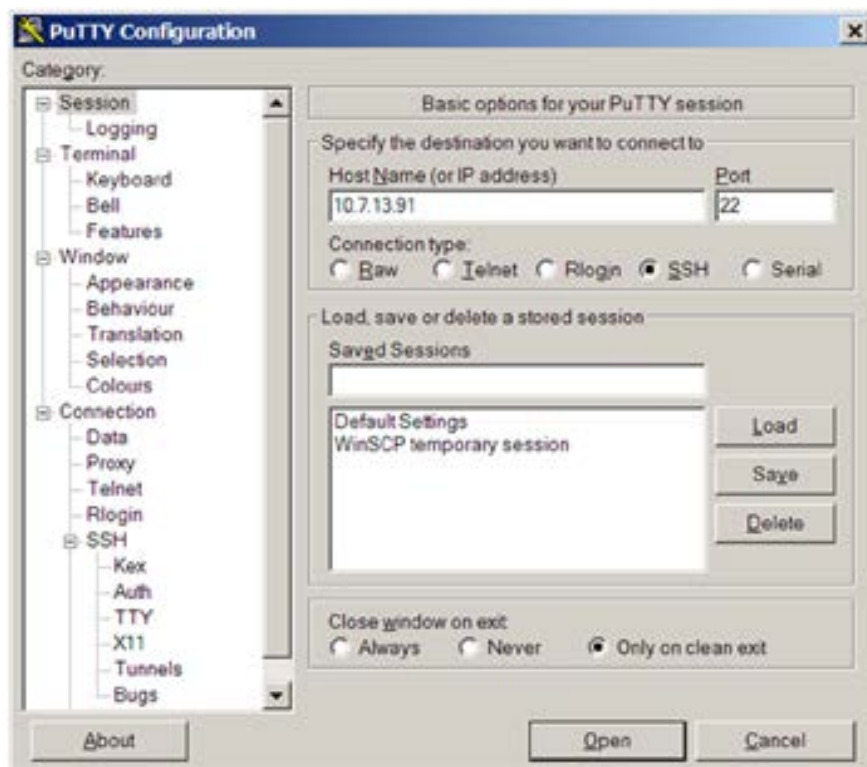
3. In **Connection -> Data**, specify the CLI user name for auto-login.

Figure 33-13: PuTTY Configuration-Auto-login



4. In **Session**, enter Global IP address, choose **SSH** connection type and click the **Open** button.

Figure 33-14: PuTTY Configuration-Host Name



33.18.8.1.3 Configuring Private/public key Authentication as the only Valid Authentication Scheme

RSA or DSA private/public key authentication may be configured to be the only valid authentication scheme for a specific CLI user. This may be done by disabling the password for a specific CLI user. Note, however, that there are some limitations to this approach:

- Passwords may not be disabled for **root** and **ems** users who are utilized by the EMS server.
- Passwords may be disabled only when the Synchronization of CLI and EMS users option is turned off.

➤ To disable the password for a specific CLI user:

1. Connect to the CLI interface on the Active SC board. For more information, refer to 'Command Line Interface' on page 107.
2. Login as **root** user. For more information, refer to 'Logging in as a Root User' on page 115.
3. At the prompt, type **tools user** and press **Enter**. The CLI USER MANAGEMENT menu is displayed.

CLI USERS MANAGEMENT	
list	-- LIST: list CLI users
add	-- ADD: add user
del	-- DELETE: delete user
pwd	-- PASSWORD: change user password
copy	-- COPY: copy users & passwords from other SC
lock	-- LOCK: lock user
unlock	-- UNLOCK: unlock user
force	-- FORCE: force user to change password
disable	-- DISABLE: disable user (delete password and unlock)
remote_root_login	-- REMOTE ROOT LOGIN: enable/disable remote root user login
sync	-- SYNC: synchronize users with EMS

4. At the **Choose submenu** prompt, type **disable** and press **Enter**.

Choose submenu : disable
DISABLE CLI USER

5. At the **User Name** prompt, enter the name of the user who you wish to disable, and press **Enter**.

User Name : acldadmin

The password is deleted for the specified user and its account is unlocked (thus allowing its use if SSH private/public key based authentication is successful).

33.18.8.1.4 Managing SSH Public Keys Authorization

Use the **tools ssh-key** command to manage SSH public key authorizations. The following options are provided:

- **list** – list authorized public keys; when run by CLI user – lists authorized keys for specific user; when run by **root** – lists authorized keys for all CLI users.
- **add** – authorize a new SSH public key.
- **del** – delete existing authorization; public key identifier (as shown by list command) must be passed as a parameter.

33.19 Intrusion Detection Events

When a malicious user tries to gain access to the CLI Interface on SC boards, several security-related events occur (e.g. the user may attempt to enter an incorrect username and/or password). These events are recorded by the operating system in the **/var/adm/messages** log file and are reported by the Mediant 8000 software to the EMS and additional SNMP managers as Intrusion Detection Events. Each Intrusion Detection Event contains the following data:

- detailed event description (e.g. "REPEATED LOGIN FAILURES ON /dev/pts/2 FROM 10.7.13.104")
- event severity
- intrusion time
- description of the SC board where intrusion was detected

In certain environments, an Intrusion Detection Event may be issued for normal activity – e.g. there may be some automated network scanner that periodically tries to access the Media Gateway with incorrect credentials and thus triggers an Intrusion Detection Event. For such environments, it is possible to prevent the reporting of the specific events by modifying the Intrusion Detection Filter parameter. The latter is a plain text filter applied to all line entries in the **/var/adm/messages** log file to determine whether each entry must be reported as an Intrusion Detection Event.

The Intrusion Detection Filter has the following format:

keywordA;keywordB1&&keywordB2;keywordC

The following rules apply:

- A keyword starting with ! implies that the string must not contain this keyword
- **&&** implies logical AND; for example **apple&&!green** matches strings that contains the word apple and not the word green.
- Spaces are supported

33.20 Configuration Freeze and Configuration Change Event

In a typical deployment, the Media Gateway is configured by authorized personnel as part of initial site setup and only routine maintenance tasks such as locking or unlocking specific trunks or performing VoP board switchover are performed later on. For such environments, it may be desirable to “freeze” the Media Gateway configuration to prevent its change by mistake.

When Media Gateway configuration is “frozen”, any attempt to alter it (e.g. change the value of a configuration parameter) will fail with a corresponding error message. Regular maintenance tasks (e.g. lock and unlock) are supported in a “frozen” state.

A “Frozen” Media Gateway includes the following indication at the top of the status screen in the EMS:



➤ To freeze Media Gateway configuration:

1. Click  to access the Media Gateway status screen.
2. In the Navigation pane, select **Security** and then in the configuration pane, click **Security Settings**; the Security Settings screen is displayed.
3. Set the parameter **Configuration Freeze Flag** to *Frozen*.

An alternative approach to freezing Media Gateway configuration is to use a Configuration Change Event. When the latter is enabled, the Media Gateway issues an event, visible in the EMS Alarms Browser upon each configuration change. This event contains a full description of the change.

➤ To enable Configuration Change Event:

1. Click  to access the Media Gateway status screen.
2. In the Navigation pane, select **Security** and then in the configuration pane, click **Security Settings**; the Security Settings screen is displayed.
3. Set the parameter **Configuration Change Event Mode** to *Enable*.

This page is left intentionally blank

34 Performance Measurements

Performance Measurements (PMs) may be used to analyze functionality and determine abnormal behavior of the Mediant 8000 Media Gateway or other network components. Choose PMs that are applicable to your specific network environment and compare collected data with PMs gathered on other equipment (e.g., Softswitch or other Media Gateways).

The following chapters provide basic information on performance measurements operation. For additional information, see the 'Performance Measurements' section in *Element Management System User's Manual*, Document #: LTRT-910xx.

Mediant 8000 Media Gateway supports two types of Performance Measurements:

- Real-Time PMs
- Historic PMs

34.1 PM Profiles

PM Profiles can be generated to enable performance monitoring to be performed according to specific sets of performance monitoring criteria. For example, you can generate a profile to collect various Voice Call statistics. Once the profile is generated, it can be applied to the Media Gateway and then polling can be activated on this entity.

34.2 Real-Time PMs

Real-time PMs are polled at a high rate (typically every 5 seconds) and are used to display current values of most critical system parameters (e.g. CPU utilization or Trunk Usage). The value of Real-Time PM are calculated at the time of the polling and may be different at the consequent poll (due to the highly volatile nature of most parameters). Use real-time PMs to acquire a current "snapshot" of the Media Gateway's state.

34.3 Historic PMs

Historic PMs are polled at a much lower rate (typically every 15 minutes) and are used to display the average, minimum and maximum value of certain system parameters over the polling interval (15 minutes). Use historic PMs to monitor system state over an extended period of time and perform long-term system analysis.

34.4 PM Threshold Alarms

The Mediant 8000 is capable of generating PM Threshold Alarms when values of specific History PMs exceed user-defined thresholds. The alarms are reported to the EMS and other SNMP managers and may be customized to match specific customer needs. The alarm is cleared when the PMs value drops below the user-defined Low Threshold value.

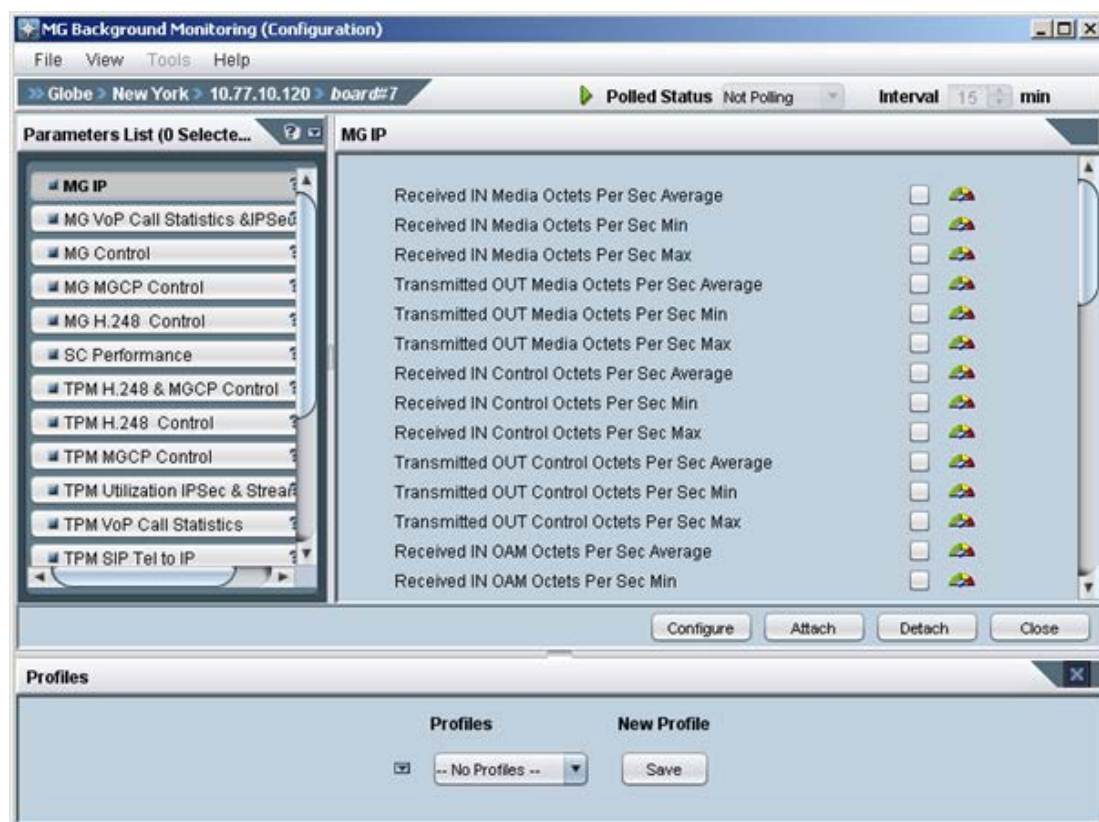
34.5 Performance Monitoring Profiles

This section describes how to configure Performance Monitoring Profiles for a Media Gateway entity. The Profile includes a list of selected parameters arranged according to the relevant configuration frame (see screen below). Once you have generated a profile, you can attach it to the Gateway entity and activate polling. For example, you can collect various statistics for the SC CPU, Memory and Disk utilization. When polling is activated via this screen, only History statistics are collected.

➤ To generate Performance Monitoring Profiles:

1. Click  to access the Media Gateway status screen.
2. Select the relevant Media Gateway entity for which you wish to generate a PM Profile. For example, select the Media Gateway board and in the toolbar, click **Performance**.
3. In the Performance Pane, select **PM Configuration**; the MG Background Monitoring screen is displayed.

Figure 34-1: MG Background Monitoring



Each parameter is measured using either **Gauges** or **Counters**. Gauges are indicated by  and Counters are indicated by . For each PM query, if you selected the Graph view then you cannot select parameters measured by both Gauges and Counters.

4. Do one of the following:
 - Select an existing PM Profile from the Profiles drop-down list. Proceed to step 7.
 - Select the performance measurements that you wish to collect. Proceed to step 4.
5. In the Parameters List, select the parameters group that you wish to display performance measurements (e.g., MG CPU Performance).
All parameters for the selected Parameter Group are displayed in the right pane.
6. In the Parameters List, right-click the Parameter group and check all parameters for the group or individually check the desired parameters from the selected Parameter Group.
7. In the Profiles pane, click the **Save** button. In the New Profile dialog, enter a name for your new PM profile and click **OK**.
8. Click the **Attach** button to attach the specific PM Profile to the Media Gateway. The "Question" dialog is displayed.

Figure 34-2: Do You Wish to Start Polling



9. Select **Yes** to start parameter's polling; the information dialog is displayed.

Figure 34-3: Polling Started



10. Verify that Polled Status changes to **Polled**.



Note: History performance measurements are collected for all entities in the Media Gateway. For example, if you choose the parameter **Trunk Utilization Avg**, it will be collected for all trunks on all Media Gateway boards.



11. When you have completed performance monitoring, click the  Stop Polling button to stop parameter's polling and close the "Real-Time Performance Measurement Display" window.



Notes:

- You may optionally detach the profile.
- To restart polling for an attached profile, click the  **Start Polling** button .

34.6 Real-Time Performance Measurements

Real-Time PMs provide high-frequency polling of various system parameters, such as CPU utilization or Trunk usage.

➤ **To view Real-Time Performance Measurements:**

1. Click  to access the Media Gateway status screen.
2. Select the relevant Media Gateway entity for which you wish to display Real Time PMs. For example, select the Media Gateway board, then in the Toolbar, click **Performance**.
3. In the Performance pane, select **Real Time PM**.
4. The "Select Screen" window is displayed.

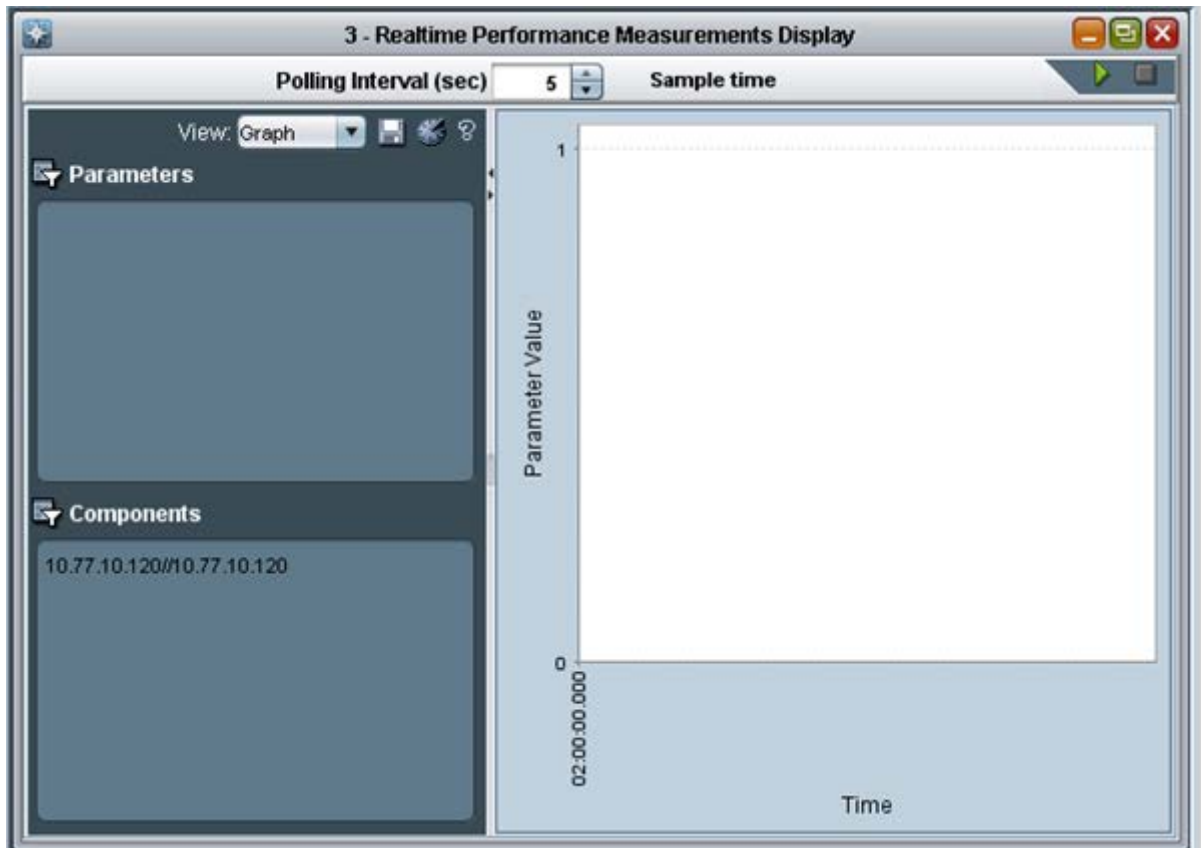
Figure 34-4: Select Screen



Select the screen where you wish to display new data. If you choose a new screen, enter the custom screen name.

The Real-Time Performance Measurement Display window is displayed. Note, if you selected more than one entry in an MO's list, all of the selected entries are displayed in the Components pane.

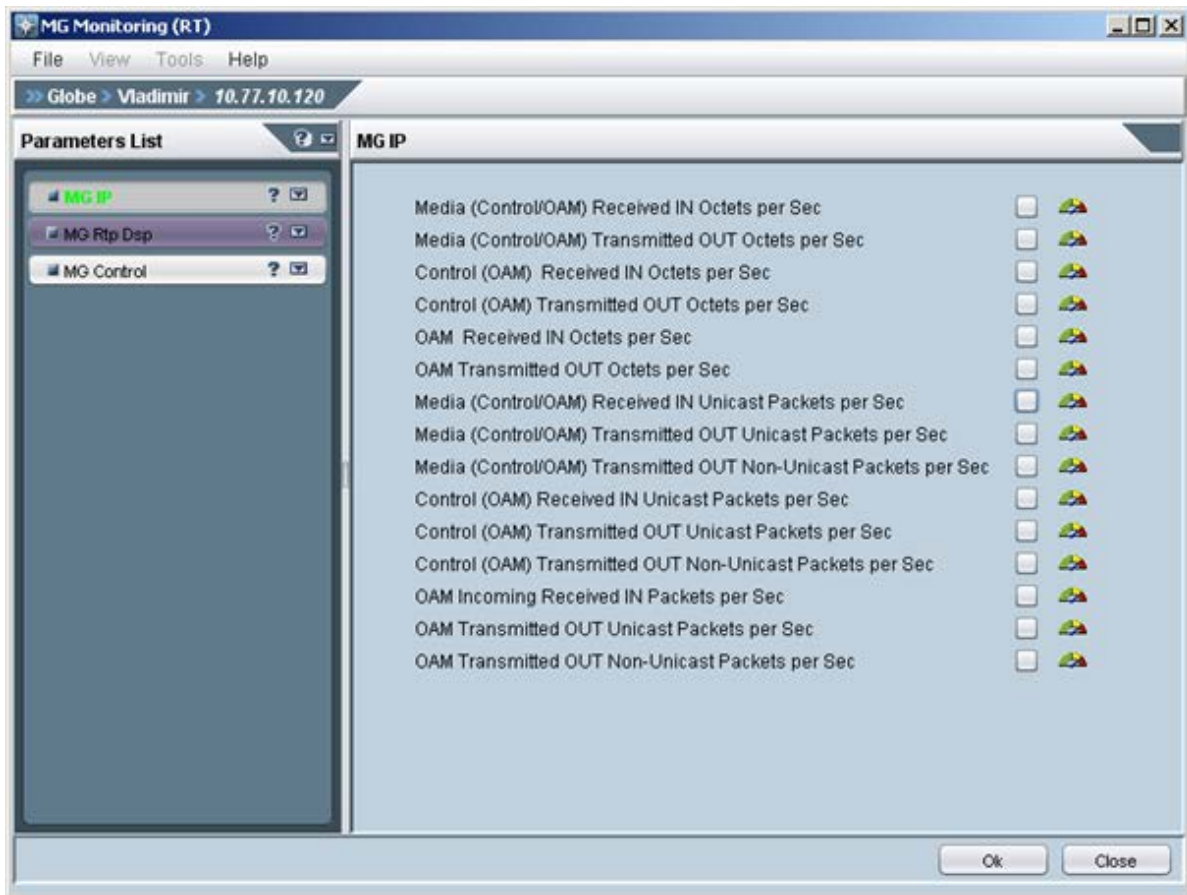
Figure 34-5: Real-Time Performance Measurement Display Window



5. Choose the type of view (Graph or Table).

6. Click the  **Parameters** button. The MG Monitoring (RT) window is displayed.

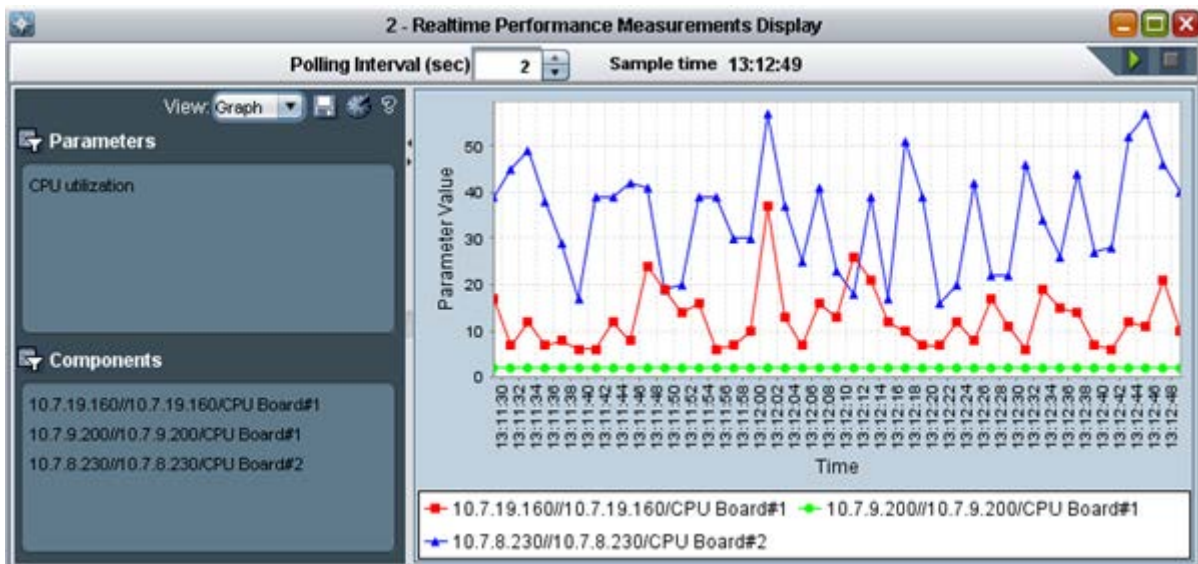
Figure 34-6: MG Monitoring Window



Each parameter is measured using either **Gauges** or **Counters**. Gauges are indicated by  and Counters are indicated by . For each PM query, if you selected the Graph view then you cannot select parameters measured by both Gauges and Counters.

7. Select the parameters group for which you wish to display performance measurements (e.g., MG IP).
All parameters for the selected Parameter Group are displayed.
8. Check the desired parameters from the Parameter Group. You may select up to 5 parameters in the same entity (select a total of 10 parameters) or compare parameters over different entities (e.g. over different trunks or boards).
9. Click **OK** button to return to the Real-Time Performance Measurement Display window.
10. In the Real-Time Performance Measurement Display window, choose polling interval and click the **Start Polling** button  to start polling.

A real-time graph or table is displayed.



You can pause polling by clicking the  **Pause Polling** button.



You can resume polling by clicking the the **Start Polling** button.

A color legend is displayed below the graph for all parameters and  entities. You can choose to save the graph as an image by clicking the **Save** button in the left pane. Historical data of the selected components and parameters can be viewed by clicking the **History** button  and then defining the **History View**. To view the Online Help, press the Help button .

In addition, you can apply Parameters or Components filters by clicking the **filter** button .



11. When you have completed performance monitoring, click the **Stop Polling** button to stop parameter's polling and close the Real-Time Performance Measurement Display window.

34.7 History Performance Measurements

History PMs are polled at much longer intervals than Real-Time PMs (15 minutes by default). They are typically collected over long time periods. You may view and analyze collected History PMs data.

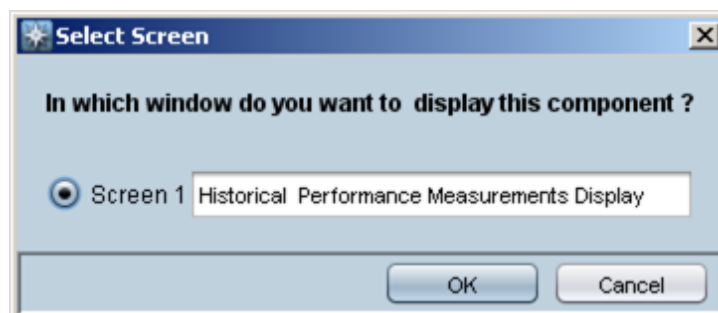


Note: Before collecting History Performance measurements, you must define a PM profile. For more information, see 'Performance Monitoring Profiles' on page 402.

➤ **To view collected History Performance Measurements:**

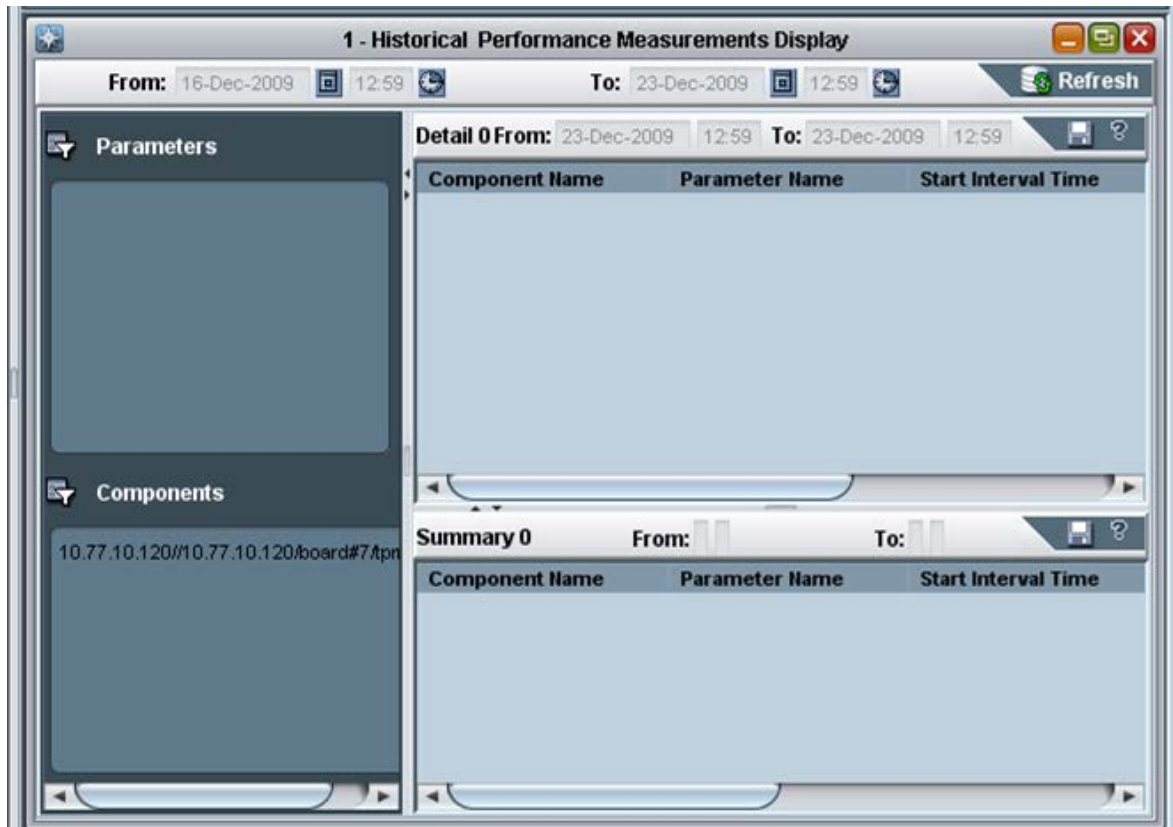
1. Click  to access the Media Gateway status screen.
2. Select the relevant MO entity for which you wish to display Historical PMs. For example, select the Media Gateway board, then in the Toolbar, click **Performance**.
3. In the Performance pane, select **History PM**.
4. The "Select Screen" window is displayed.
Select the screen where you wish to display history performance measurements data.

Figure 34-7: History PMs Select Screen



The History Performance Measurements Display window is displayed. Note, when you select more than one entry in an MO's list, all of the selected entries are displayed in the Components pane.

Figure 34-8: History Performance Measurements Display



5. Click the  button and select the components and parameters to be displayed.

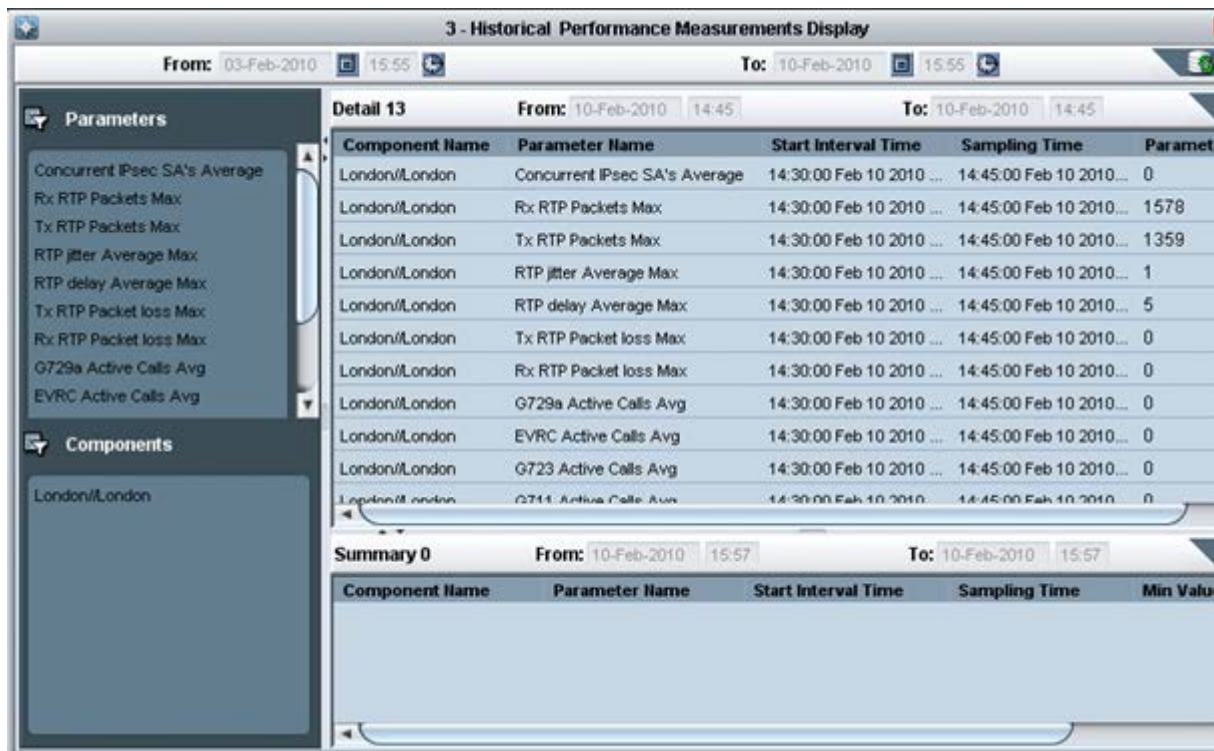


Note: You can select up to 15 parameters to be displayed.

6. Select the Time Interval for the history PMs data to be displayed and click **Refresh**.

Historical performance measurements display is comprised of two tables. The upper table displays detailed data and the table below displays the summarized data.

Figure 34-9: History Performance Measurements Display-Results Screen



Each time a sample is taken from the Media Gateway, it is stored in the details table. After every 24 hours of sampled data, the detailed data is summarized and the summary table is updated.

Detailed data is stored for a period of 7 days (in intervals of 15 minutes).
Historical data is stored for 30 days (in intervals of 24 hours).

34.8 Performance Measurement Threshold Alarms

For each History PM, the user may customize a threshold value. When the PM value exceeds the high threshold, a PM Threshold Alarm is generated and reported to the EMS and other SNMP managers. When the PM value drops below the low threshold value, the corresponding alarm is cleared.

Use PM Threshold alarms to monitor mission-critical performance measurement and receive immediate indication when a specific problem (indicated by a change in corresponding PM value) occurs.

➤ To configure PM Threshold Alarms:

1. Click  to access the Media Gateway status screen.
2. In the toolbar, click **Performance**.
3. In the Performance pane, select **Threshold Alarms**; the Threshold Alarms list is displayed.
4. Use the  or  buttons to add or remove entries.
5. When a new entry is added, the Threshold Alarm Parameters screen is displayed.
6. In the Threshold Alarm Parameters screen, select the specific History PM and configure its Threshold Alarm properties according to the table below.

7. Unlock the Threshold Alarm to activate it.

Figure 34-10: Threshold Alarms Parameters Screen

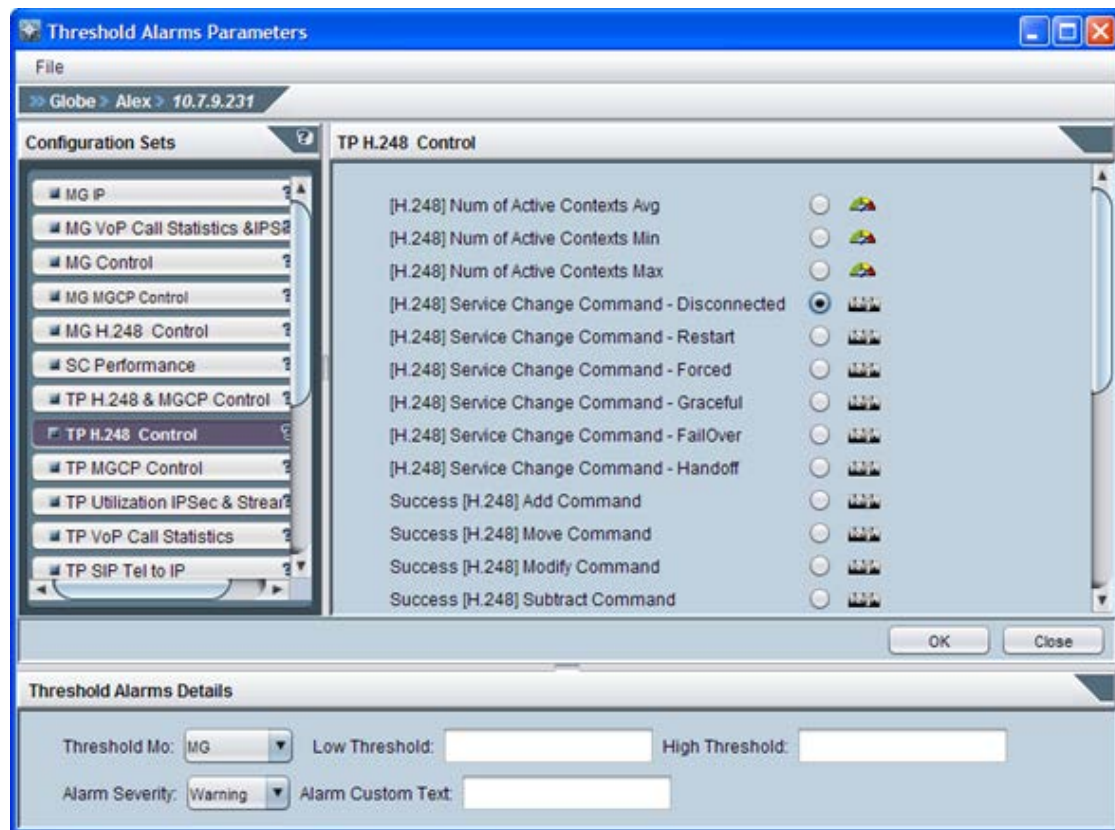


Table 34-1: PM Threshold Alarm Settings

Parameter Name	Type	Provisioning Type	Description
Threshold MO	Enum.	Online	Defines the MO to which the threshold is applied. MG – threshold is applied to all PM instances (e.g. in case of a History PM parameter on Media GatewayMedia Gateway boards, threshold is applied to all boards) Board#x – threshold is applied to PM instances on a specific Media Gateway board only.
High Threshold	Counter64	Online	Defines the high threshold value. When the PM value exceeds the high threshold, the corresponding Threshold Alarm is raised.

Parameter Name	Type	Provisioning Type	Description
Low Threshold	Counter64	Online	Defines the low threshold value. When the PM value drops below the low threshold, the corresponding Threshold Alarm is cleared.
Alarm Severity	Enum Warning, Minor, Major, Critical	Online	Defines the severity of Threshold Alarm.
Alarm Custom Text	String Up to 80 chars	Online	Defines a custom text included in Threshold Alarm (in Additional Info1 field).

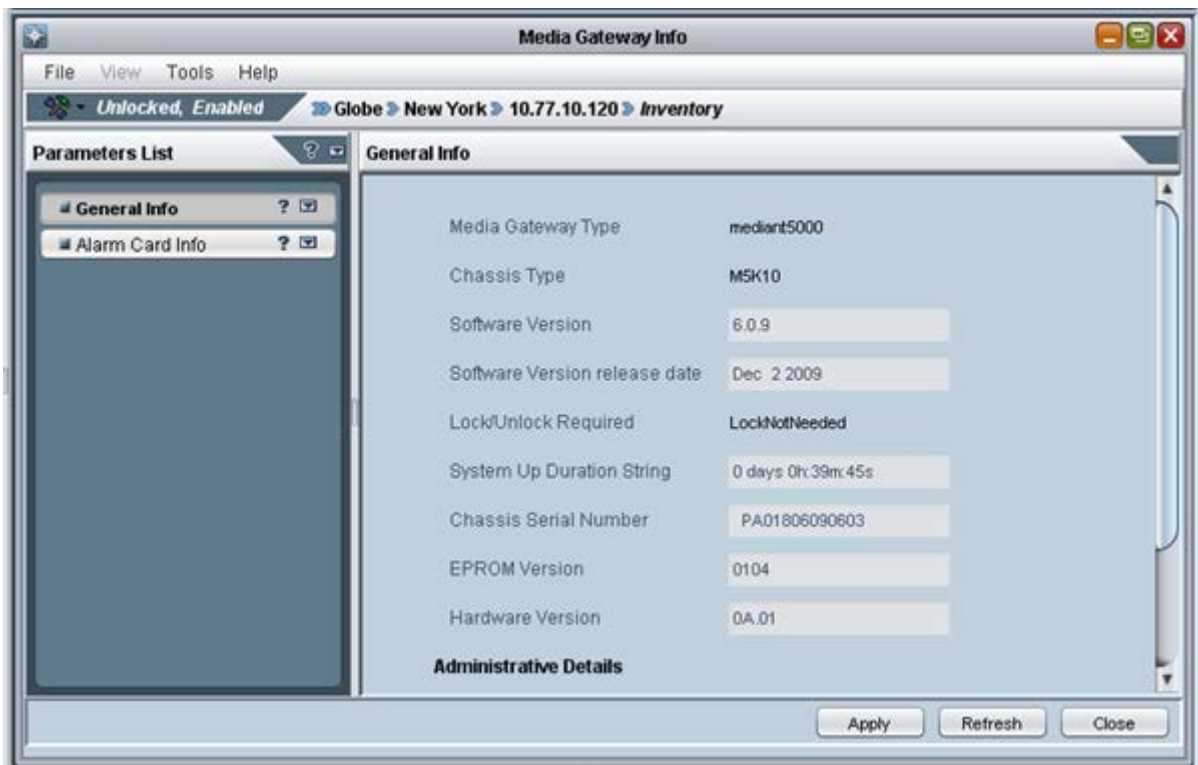
35 Media Gateway Inventory

The Media Gateway Inventory screen contains a summary of all of the hardware components of the Media Gateway and their relevant data including serial numbers, hardware and EEPROM versions and board IP addresses.

➤ To view Media Gateway Inventory:

1. Click  to access the Media Gateway status screen.
2. In the Navigation pane, select **Inventory** and in Configuration pane, click **Media Gateway Info**; the Media Gateway Info screen is displayed.

Figure 35-1: Mediant 8000 Inventory



This page is intentionally left blank.

36 Media Gateway Boards' Configuration Backdoor

Media Gateway Boards are normally configured via the management objects (MOs) in the Mediant 8000 Media Gateway's configuration database. The configuration is performed via the dedicated EMS GUI configuration screens (described in the corresponding sections of this manual) or via the CLI interface.

In an unlikely event that you need to configure a parameter for the Media Gateway board that does not exist in the Mediant 8000 Media Gateway configuration database, you can use the Media Gateway Board's Configuration Backdoor for provisioning such parameters.

Prior to configuring the Media Gateway Board's Configuration Backdoor you must receive the following information from AudioCodes Tech Support:

- The parameter's *ini* file name
- The parameter's *ini* file value
- The parameter's *ini* file value for the redundant board
- The update mode
- The redundancy mode

➤ **To configure Media Gateway Board's Configuration Backdoor, take these 6 steps:**

1. Click the  button to access the Media Gateway status screen.
2. In the Navigation pane, select **Troubleshooting** and then in the configuration pane, click **Troubleshooting Settings**; the Troubleshooting Settings screen is displayed.
3. Select the **Configuration Backdoor** tab. The list of VoP Board Configuration backdoors is displayed.
4. Use the  or  buttons to add or remove entries.
5. Configure the VoP Board Configuration Backdoor parameters according to the 'Configuration-Backdoor Parameters' table below.
6. Right click on the specific entry and choose **Unlock** to activate the backdoor configuration.

Table 36-1: Configuration-Backdoor Parameters

Parameter Name	Type	Provisioning Type	Description
Boards IDs	String Up to 40 chars.	Online	Defines the Media Gateway boards to which this backdoor parameter is applied. Syntax: - Number value 1 to 20 – the number of board's slot, e.g., "5" for slot 5. - Multiple number values (delimited by comma or space), e.g., "5,6,7" for slots 5, 6 and 7. - Value range (delimited by dash), e.g., "5-7" for slots 5, 6 and 7. - Mix of value range and numbers, e.g., "5,6-8,10" for slots 5, 5, 7, 8 and 10. - Value "all" – to define the value for all boards
Trunks IDs	String Up to 40 chars.	Online	Defines Trunks to which this backdoor parameter is applied. Syntax: - Number value 1 to 84 – the number of trunk - Multiple Number values (delimited by comma or space), e.g., "4,5,6" - Value range (delimited by dash), e.g., "4-5" - Mix of value range and numbers, e.g., "4,8-12,16" - Value "all" – to define the value for all trunks - Value "none" – configuration applies to the board itself and not to its trunks
Parameter name	String Up to 80 chars.	Online	Defines the backdoor parameter name as written in the <i>ini</i> file. If the Trunk ID is specified (i.e., it is not all/none) – a Trunk ID is appended to the parameter name.

Parameter Name	Type	Provisioning Type	Description
Parameter value	String Up to 80 chars.	Instant	Defines the backdoor parameter value as written in the <i>ini</i> file. If the parameter value must be surrounded by quotation marks in the <i>ini</i> file, the Parameter value should be set to the string that contains the quotation marks.
Parameter value of redundant	String Up to 80 chars.	Instant	Defines the backdoor parameter value for the redundant Media Gateway board When empty (by default), the same value is used for both regular and redundant Media Gateway boards.
Update mode	Enum Instant, TPRreset	Online	Defines how the backdoor parameter is applied. Instant – the backdoor parameter value is instantly applied to all relevant Media Gateway boards, as soon as the Configuration Backdoor is unlocked TPRreset – backdoor requires the Media Gateway board to be reset (lock/unlock). The reset is not automatically enforced and should be manually performed by the user at the appropriate time. Affected board list and Affected board list with different values are updated accordingly (see below).
Redundancy Support	Enum Warm, Hot	Online	Defines how the backdoor parameter affects the Media Gateway boards' redundancy mechanism. Warm – if the backdoor configuration is applied to the normal Media Gateway board and not to the redundant Media Gateway board, warm switchover is enforced. Hot – the backdoor configuration is fully supported by the redundancy mechanism and therefore even if the parameter's value differs among the boards, Hot Switchover may be performed.

The Media Gateway Board's Configuration Backdoor status is represented by the standard **Operational State** and **Administrative State** attributes. In addition, the following attributes are used:

- **Affected board list** – lists all of the Media Gateway boards to which the Configuration Backdoor is applied
- **Affected board list with different values** – lists all of the Media Gateway that must be reset (locked/unlocked) to apply the Configuration Backdoor parameter value.

36.1 Supported Actions

The following actions are available on the Media Gateway Board's Configuration Backdoor:

- **Add** – add a Backdoor Configuration parameter.
- **Remove** – remove Backdoor Configuration parameter (backdoor must be locked prior to using the **remove** action).
The BackdoorConfiguration is **automatically** deleted when all of the Media Gateway boards to which it applies are deleted. When the Backdoor parameter affects more than one board, a deleted board is removed from the **Board IDs** attribute's range (except when the value range is defined as "all").
- **Lock** – prepare the BackdoorConfiguration for removal. Locking the Backdoor Configuration is allowed only when all of the relevant Media Gateway boards are locked.
- **Unlock** – activate the ConfigurationBackdoor. The backdoor parameter is applied to the relevant Media Gateway boards according to the Update mode attribute.

36.2 Usage Tips

- No validation is performed on the names and values of the Media Gateway Board's parameters configured via the Configuration Backdoor. Make sure that you provision the backdoor information *precisely* as instructed by Tech Support.
- Configuration Backdoor is automatically removed during Online Software Upgrade if the new version contains the configuration parameter. The Backdoor parameter value is merged into the Media Gateway configuration database.

37 Using Auxiliary Files

Auxiliary Files are needed for different aspects of Media Gateway operation. For example, Call Progress Tones, Voice Prompts etc. Typically, they must be modified to match specific customer requirements.

Auxiliary Files are created using the DConvert utility, which is provided on the Mediant 8000 software installation package CD (The *Utilities\DConvert* directory). The CD also contains sample auxiliary files (The *AuxiliaryFiles* directory) that can be used as a reference for building customer-specific auxiliary files.

Table 37-1: Supported Auxiliary Files

Auxiliary File Type	Description	Can be modified by the user?
CMP (firmware)	The Media Gateway board's software package	No
Call Progress Tones (CPT)	Defines different Call Progress Tones and User-Defined Tones to be detected/generated by the Media Gateway board	Yes
Pre-Recorded Tones (PRT)	Provides more flexible tone generation capability than the CPT mechanisms (which have limitations, such as limited number of predefined tones or limited number of frequency integrations in a single tone)	Yes
Voice Prompts	User-recorded voice prompts	Yes
CAS File	The CAS protocol state machine that allows protocol customization and adaptation	Yes
VXML for IPmedia	Voice XML file (for the IPmedia application)	Yes
VXML for SIP	Voice XML file (for the SIP application)	Yes
External Coders	Defines coders that are supported by the Media Gateway board	Yes
User Information	Defines user information (for the SIP application)	Yes
X.509 Private Key	X.509 Private Key	Yes
X.509 Certificate	X.509 Public Certificate	Yes
X.509 Trusted Root Certificate	X.509 Public Certificate of Trusted Root entity (CA)	Yes
Dial Plan	Dial Plan file	Yes
Alarm Propagation Rules	Defines alarm severity propagation rules	Yes
V5.2 Ports Configuration	V5.2 User Ports Configuration file	Yes

37.1 Auxiliary Files Repository

Auxiliary Files are stored on both SC boards and are constantly replicated between them. Some "default" auxiliary files (CMP files) are added during the Media Gateway installation and may not be modified by the user.

Adding an Auxiliary file consists of the following steps:

1. Adding an Auxiliary file to the **auxiliary files repository** on the Media Gateway.
2. Associating an Auxiliary file with a specific Media Gateway board or application.

➤ **To add an Auxiliary File to the auxiliary files repository:**

1. Upload the auxiliary file to the EMS Software Manager:
 - a. From the **Tools** menu, select **Software Manager**; the Software Manager screen is displayed.
 - b. In the upper left corner, click ; the Add Files screen is displayed.
 - c. In  **Auxiliary** or **Auxiliary M5K/M8K** tab, for each of the file types you require, click and navigate to the desired file.
 - d. Click **OK**. The file name is displayed in the **File Name** field.
 - e. In the **File Description** field, type a meaningful description.
 - f. Do the same for any additional file type you require.
 - g. Click **OK**; the files are uploaded to the EMS.

37.2 Call Progress Tones (CPT) Files

Call Progress Tones (CPT) files contain definition of the Call Progress and User-Defined Tones to be detected/generated by the Media Gateway board.

CPT file may contain definitions of the following tones:

- Call Progress Tones
- User-Defined Tones

The **Call Progress Tones** are mostly used for Telephony In-Band Signaling applications (e.g., Ring Back tone). Each tone can be configured as one of the following types:

- Continuous
- Cadence (up to 4 cadences)
- Burst

A tone can also be configured for Amplitude Modulated (AM) (only 8 of the Call Progress Tones can be AM tones). The Call Progress Tones frequency range is 300 Hz to 1890 Hz.

The **User-Defined Tones** are general-purpose tones to be defined by the user. They can be set only as 'Continuous' and their frequency range is 300 Hz to 3800 Hz.

The maximum number of tones that can be configured for the User Defined and Call Progress Tones together is 32. The maximum number of frequencies that may be configured in the User Defined and Call Progress Tones together is 64 (each tone may be composed of more than one frequency).

Call Progress Tones (CPT) files must be uploaded to the Media Gateway boards in **binary format**. You should edit the "source" tones file in any text editor (as described in 'Modifying the "Source" Call Progress Tones (CPT) File' on page 423) and convert it to the binary format using the **DConvert utility** (as described in 'Converting the Call Progress Tones File to Binary Format' on page 429).



Note: Only **binary** CPT files may be uploaded to the Media Gateway boards.

➤ **To associate a Call Progress Tones (CPT) file with a Media Gateway board:**

1. Click  to access the Media Gateway status screen.
2. Select the desired Media Gateway board.
3. In the Navigation pane, select **Inventory** and then in the configuration pane, click **Inventory Settings**; the Inventory Settings screen is displayed.
4. Select the **Setup Files** tab.
5. In the Setup Files tab, configure **Call Progress Setup File** parameter to match the desired CPT file.

37.2.1 Modifying the "Source" Call Progress Tones (CPT) File

This section describes syntax of the text-based "source" Call Progress Tones file. This file must be converted to the binary format via the **DConvert utility** prior to uploading it to the Media Gateway.

37.2.1.1 The Call Progress Tones Section Format

In the "source" Call Progress Tones file, the Call Progress Tones section starts with the following string:

[NUMBER OF CALL PROGRESS TONES] - contains the following key only:

- **Number of Call Progress Tones** - defines the number of Call Progress Tones to be defined in the file.

[CALL PROGRESS TONE #X] - contains the Xth tone definition (starting from 0 and not exceeding the number of Call Progress Tones -1 defined in the first section) using the following keys:

- **Tone Type** - Call Progress Tone-Type

Basic Tone Type Indices (The number is the tone-type code)

1. Dial Tone
2. Ringback Tone
3. Busy Tone
4. Congestion Tone
5. N/A
6. Warning Tone
7. Reorder Tone

8. Confirmation Tone

9. Call Waiting Tone

- **Tone Modulation Type** – The tone can be either Amplitude Modulated (1) or regular (0).
- **Tone Form** – The format of the tone can be one of the following indices:
 - Continuous
 - Cadence
 - Burst
- **Low Freq [Hz]** – The frequency in Hertz of the lower tone component for a dual frequency tone, or the frequency of the tone for a single tone. This parameter is relevant only in case the tone is not Amplitude Modulated.
- **High Freq [Hz]** – The frequency in Hertz of the higher tone component for of a dual frequency tone, or zero (0) for a single tone. This parameter is relevant only in case the tone is not modulated.
- **Low Freq Level [-dBm]** – The generation level 0 dBm to -31 dBm. This parameter is relevant only when the tone is not Amplitude Modulated.
- **High Freq Level [-dBm]** – The generation level. 0 to -31 dBm. The value is zero (0) for a single tone. This parameter is relevant only when the tone is not Amplitude Modulated.
- **First Signal On Time [10 msec]** – The “Signal On” period (in 10 msec units) for the first cadence ON-OFF cycle, for cadence tone. When a tone is configured to be continuous, this parameter defines the tone On event detection time. When a tone is configured to be burst tone, it defines the tone’s duration.
- **First Signal Off Time [10 msec]** – The “Signal Off” period (in 10 msec units) for the first cadence ON-OFF cycle, for cadence tone. In case of burst tone, this parameter defines the off time required after burst tone ended until the tone detection is reported. For a continuous tone, this parameter is ignored.
- **Second Signal On Time [10 msec]** – The “Signal On” period (in 10 msec units) for the second cadence ON-OFF cycle. This may be omitted if there is no second cadence.
- **Second Signal Off Time [10 msec]** – The “Signal Off” period (in 10 msec units) for the second cadence ON-OFF cycle. This may be omitted if there is no second cadence.
- **Third Signal On Time [10 msec]** – The “Signal On” period (in 10 msec units) for the third cadence ON-OFF cycle. This may be omitted if there is no third cadence.
- **Third Signal Off Time [10 msec]** – The “Signal Off” period (in 10 msec units) for the third cadence ON-OFF cycle. This may be omitted if there is no third cadence.
- **Fourth Signal On Time [10 msec]** – The “Signal On” period (in 10 msec units) for the fourth cadence ON-OFF cycle. This may be omitted if there is no fourth cadence.
- **Fourth Signal Off Time [10 msec]** – The “Signal Off” period (in 10 msec units) for the fourth cadence ON-OFF cycle. This may be omitted if there is no fourth cadence.

- **Carrier Freq [Hz]** – The Carrier signal frequency when the tone is Amplitude Modulated.
- **Modulation Freq [Hz]** – The Modulated signal frequency when the tone is Amplitude Modulated (valid range from 1 Hz to 128 Hz).
- **Signal Level [-dBm]** – The tone level when the tone is Amplitude Modulated.
- **AM Factor [steps of 0.02]** – The amplitude modulation factor. Valid values: 1 to 50. Recommended values: 10 to 25.
- **Default Duration [msec]** - The default duration (in 1 msec units) of the generated tone.



Notes:

- When defining the same frequencies for both a continuous tone and a cadence tone, the Signal On Time parameter of the continuous tone should have a value that is greater than the Signal On Time parameter of the cadence tone. Otherwise, the continuous tone is detected instead of the cadence tone.
- The tone frequency should differ by at least 40 Hz from one tone to other defined tones.

37.2.1.2 The User-Defined Tones Section Format

In the "source" Call Progress Tones file, the User-Defined Tones section starts from the following string:

[NUMBER OF USER DEFINED TONES] - contains the following key only:

- **Number of User Defined Tones** - defines the number of User Defined Tones to be defined in the file.

[USER DEFINED TONE #X] - contains the Xth tone definition (starting from 0 and not exceeding the number of User Defined Tones -1 defined in the first section) using the following keys:

- **Tone Type** - Call Progress ToneType

Basic Tone Type Indices (The number is the tone-type code)

1. Dial Tone
2. Ringback Tone
3. Busy Tone
4. Congestion Tone
5. N/A
6. Warning Tone
7. Reorder Tone
8. Confirmation Tone
9. Call Waiting Tone

- **Low Freq [Hz]** – The frequency in Hertz of the lower tone component for a dual frequency tone, or the frequency of the tone for a single tone.
- **High Freq [Hz]** – The frequency in Hertz of the higher tone component for of a dual frequency tone, or zero (0) for a single tone.

- **Low Freq Level [-dBm]** – The generation level 0 dBm to -31 dBm.
- **High Freq Level [-dBm]** – The generation level. 0 to -31 dBm. The value is zero (0) for a single tone.
- **Default Duration [msec]** - The default duration (in 1 msec units) of the generated tone.

37.2.1.3 Default Configuration

The following table describes the default Call Progress Tones configuration of the Media Gateway boards:

Table 37-2: Default Call Progress Tones

[NUMBER OF CALL PROGRESS TONES]	
Number of Call Progress Tones=9	
#Dial tone [CALL PROGRESS TONE #0]	Tone Type=1 Tone Form = 1 (Continuous) Low Freq [Hz]=350 High Freq [Hz]=440 Low Freq Level [-dBm]=13 (-13dBm) High Freq Level [-dBm]=13 First Signal On Time [10msec]=300
#Dial tone [CALL PROGRESS TONE #1]	Tone Type=1 Tone Form = 1 (Continuous) Low Freq [Hz]=440 High Freq [Hz]=0 Low Freq Level [-dBm]=10 (-10dBm) High Freq Level [-dBm]=0 First Signal On Time [10msec]=300
#Ringback [CALL PROGRESS TONE #2]	Tone Type=2 Tone Form = 2 (Cadence) Low Freq [Hz]=440 High Freq [Hz]=480 Low Freq Level [-dBm]=19 (-19dBm) High Freq Level [-dBm]=19 First Signal On Time [10msec]=200 First Signal Off Time [10msec]=400
#Ringback [CALL PROGRESS TONE #3]	Tone Type=2 Tone Form = 2 (Cadence) Low Freq [Hz]=440 High Freq [Hz]=0

[NUMBER OF CALL PROGRESS TONES]**Number of Call Progress Tones=9**

	Low Freq Level [-dBm]=16 (-16dBm) High Freq Level [-dBm]=0 First Signal On Time [10msec]=100 First Signal Off Time [10msec]=300
#Busy [CALL PROGRESS TONE #4]	Tone Type=3 Tone Form = 2 (Cadence) Low Freq [Hz]=480 High Freq [Hz]=620 Low Freq Level [-dBm]=24 (-24dBm) High Freq Level [-dBm]=24 First Signal On Time [10msec]=50 First Signal Off Time [10msec]=50
#Busy [CALL PROGRESS TONE #5]	Tone Type=3 Tone Form = 2 (Cadence) Low Freq [Hz]=440 High Freq [Hz]=0 Low Freq Level [-dBm]=20 (-20dBm) High Freq Level [-dBm]=0 First Signal On Time [10msec]=50 First Signal Off Time [10msec]=50
#Reorder tone [CALL PROGRESS TONE #6]	Tone Type=7 Tone Form = 2 (Cadence) Low Freq [Hz]=480 High Freq [Hz]=620 Low Freq Level [-dBm]=24 (-24dBm) High Freq Level [-dBm]=24 First Signal On Time [10msec]=25 First Signal Off Time [10msec]=25
#Confirmation tone [CALL PROGRESS TONE #7]	Tone Type=8 Tone Form = 2 (Cadence) Low Freq [Hz]=350 High Freq [Hz]=440 Low Freq Level [-dBm]=20 (-20dBm) High Freq Level [-dBm]=20 First Signal On Time [10msec]=10 First Signal Off Time [10msec]=10

[NUMBER OF CALL PROGRESS TONES]

Number of Call Progress Tones=9

#Call Waiting Tone [CALL PROGRESS TONE #8]	Tone Type=9 Tone Form = 2 (Cadence) Low Freq [Hz]=440 High Freq [Hz]=0 Low Freq Level [-dBm]=20 (-20dBm) High Freq Level [-dBm]=0 First Signal On Time [10msec]=30 First Signal Off Time [10msec]=900

37.2.1.4 Editing the "Source" Call Progress Tones File

Use the default call progress tones file provided on the Media Gateway software installation CD as a reference.

Modify the section according to your specific needs. For example, to change the dial tone to 440 Hz only, replace the *#Dial tone* section with the following text:

```
#Dial tone
[CALL PROGRESS TONE #1]
Tone Type=1
Tone Form = 1
Low Freq [Hz]=440
High Freq [Hz]=0
Low Freq Level [-dBm]=10 (-10dBm)
High Freq Level [-dBm]=0
First Signal On Time [10msec]=300; the dial tone is detected after 3 sec
If the Call Progress Tones file contains multiple definitions of the same tone type:
```

- The first definition is used for generation of specific tone
- All definitions are used for detecting the specific tone

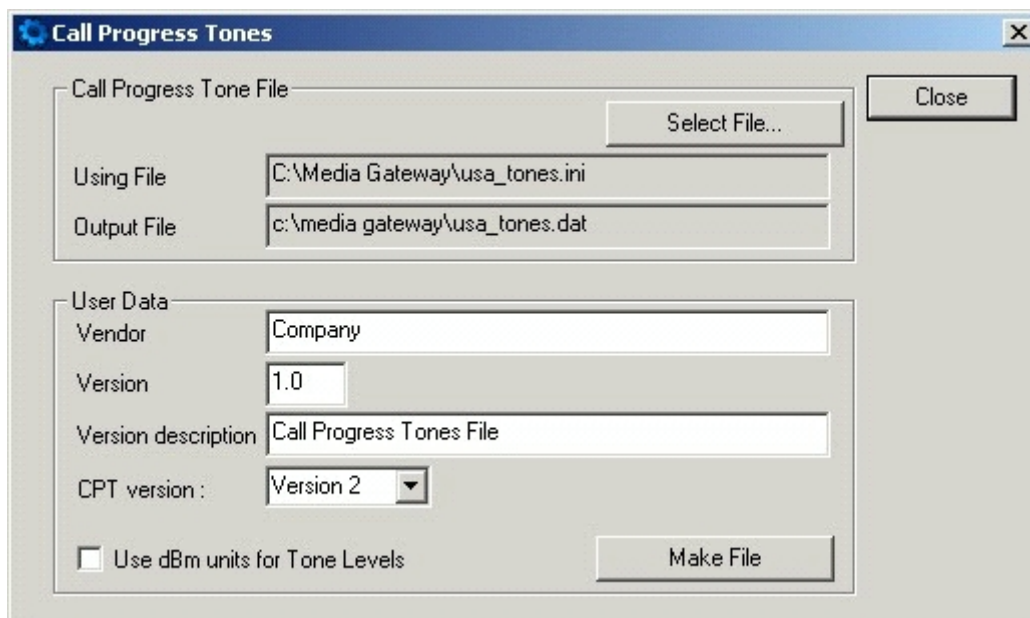
37.2.2 Converting the Call Progress Tones File to Binary Format

After editing the "source" Call Progress Tones file, you must convert it to the binary format using the **DConvert utility** provided on the Media Gateway Software Installation CD.

➤ To convert a "source" CPT file to a binary format:

1. Execute *DConvert.exe* and click the **Process Call Progress Tones file(s)** button; the Call Progress Tones dialog is displayed.

Figure 37-1: Call Progress Tones Screen



2. Click the **Select File** . button and navigate to the location of the "source" CPT *ini* file that you want to convert.
3. Select the desired file and click **Open**. The name and path of both the CPT *ini* file and the *dat* file appear in the **Using File** field and **Output File** field respectively. (The file names and paths are identical except for the file extension.)
4. Fill in the **Vendor**, **Version** and **Version Description** fields.
 - **Vendor** field - 256 characters maximum
 - **Version** field - must be made up an integer, followed by a period '.', then followed by another integer (e.g., 1.2, 23.4, 5.22)
 - **Description** field - 256 characters maximum
5. The default value of the CPT version drop-down list is **Version 3** – leave it unchanged.
6. Click a checkmark in **Use dBm units for tone levels** checkbox to use -dBm units for setting the Call Progress Tone and User Defined Tone Levels.
7. Click the **Make File** button. The binary *dat* file is generated and placed in the same directory as shown in the **Output File** field. A message box informing you that the operation was successful indicates that the process is completed.

37.3 Pre-Recorded Tones (PRT) Files

The Call Progress Tones (CPT) files have several limitations, such as the limited number of predefined tones, or limited number of frequency integrations in one tone. To solve this situation and provide a more flexible tone generation capability, Pre-Recorded Tones (PRT) files can be used.

The Pre-Recorded Tones (PRT) file consists of one or more *PCM (WAV)* file with the following characteristics:

Table 37-3: Pre-Recorded Tones (PRT) file Characteristics

Characteristic	Description
Coder	G.711 A-law, G.711 μ -law or Linear PCM
Rate	8 kHz
Resolution	8-bit
Channels	mono

The PRT files are played repeatedly (in auto-rewind mode). This allows recording only part of the tone, while still playing it for the full duration. For example, if a tone has a cadence of 2 seconds on and 4 seconds off, the recorded file should contain only the 6 seconds of the cadence. The PRT module repeatedly plays this cadence for the configured duration. Similarly, a continuous tone can be played by repeating only a part of it.

Pre-Recorded Tones (PRT) files must be created using **DConvert utility** (as described in 'Creating a Pre-Recorder Tones File' on page 431).

➤ To associate a Pre-Recorded Tones (PRT) file with a Media Gateway board:

1. Click  to access the Media Gateway status screen.
2. Select the desired Media Gateway Gateway board.
3. In the Navigation pane, select **Inventory** and then in the configuration pane, click **Inventory Settings**; the Inventory Settings screen is displayed.
4. In the **Setup Files** tab, configure the **Prerecorded Tones File** parameter to match the desired PRT file.

**Notes:**

- The maximum number of prerecorded tones that can be stored in one *dat* file is 40.
- The maximum PRT file size for TP-6310 board is 1 MB.
- If the same tone type is defined as **PRT** and **CPT** Tone, the tone is played using the PRT module.

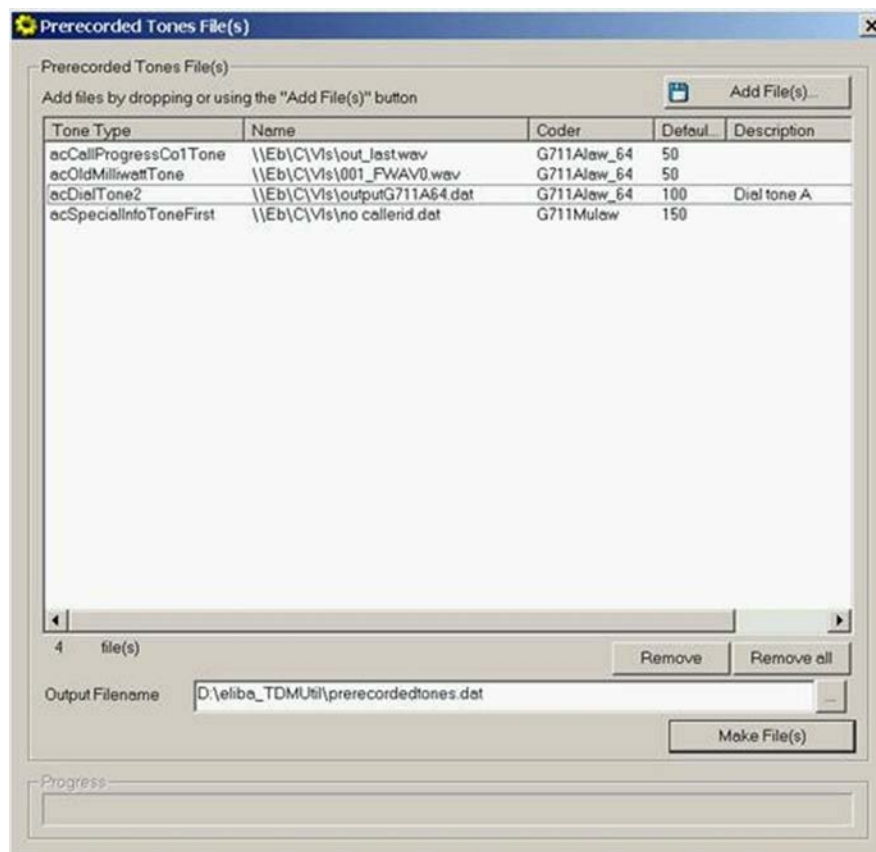
37.3.1 Creating a Pre-Recorder Tones File

Pre-recorded PCM (WAV) files must be converted to the binary format using the **DConvert utility** provided on the Media Gateway Software Installation CD.

➤ **To create Pre-Recorded Tones file:**

1. Execute **DConvert.exe** and click the **Process Prerecorded Tones file(s)** button; the Prerecorded Tones file(s) window is displayed.
2. Select the raw Prerecorded Tones files (created in Step 1) utilizing one of these actions:
 - a. Click the **Add Files** button in the upper right corner; the Add Files window is displayed.
Navigate to the appropriate file.
Select it and click the **Add>>** button. (To close the Add Files window, click the  Exit button. Press the **Esc** key to cancel changes.) You are returned to the Prerecorded Tones file(s) window.

Figure 37-2: Prerecorded Tones File(s) Screen with wav Files



- b. From any location on the PC, select the appropriate files and drag-drop them into the Prerecorded Tones File(s) Screen.
3. To define a tone type, coder and default duration for each file, select the file (or group of files to be set the same) and double click or right Click it; the File Data window is displayed.

Figure 37-3: File Data Dialog Box



4. From the **Type** drop-down list, select a Ring parameter type.
5. From the **Coder** drop-down list, select a coder type (G.711 A-law_64, G.711 μ -law, or Linear PCM).
6. In the **Description** field, enter a description (optional).
7. In the **Default** field, enter the duration in msec.
8. Click the  Exit button. (Press the **Esc** key to cancel changes.) You are returned to the Prerecorded Tones file(s) window.

9. The default **Output** file name is *prerecordedtones.dat*. You can modify it. Or, Use the  Browse button to select a different Output file. Navigate to the desired file and select it. The selected file name and its path appear in the **Output** field.
10. Click **Make File(s)** button. The Progress bar at the bottom of the window is activated. The *.dat* file is generated and placed in the same directory as shown in the **Output File** field. A message box informing you that the operation was successful indicates that the process is completed.

37.4 Voice Prompts Files

The Voice Prompts file contains definitions of the Voice Prompts played by the Media Gateway board upon MGC request. Individual Voice Prompts can be recorded in proprietary *RAW* or *PCM (WAV)* format. They must be assembled into the Voice Prompts File using the **DConvert utility** (as described in 'Creating a Voice Prompts File' on page 433).

To associate Voice Prompts file with Media Gateway board, see 'Auxiliary Files Repository' on page 422.

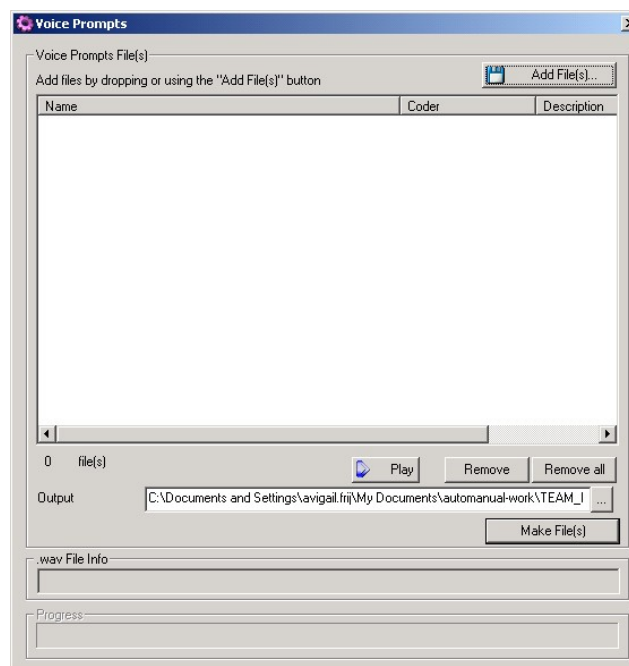
37.4.1 Creating a Voice Prompts File

This section describes how to create a Voice Prompts File.

➤ **To create a Voice Prompts file:**

1. Execute *DConvert.exe* and click the **Process Voice Prompts file(s)** button; the Voice Prompts window is displayed.

Figure 37-4: Voice Prompts Screen



2. Select the raw Voice Prompt files (created in Step 1) step either by one of these actions:

- a. Click the **Add Files** button in the upper right corner. The Add Files window appears. (See the figure, "Select Files Window" below.)

Navigate to the appropriate file.

Select it and click the **Add>>** button. To close the Add Files window, click

the  Exit button. (Press the **Esc** key to cancel changes.)

Figure 37-5: Select Files Window

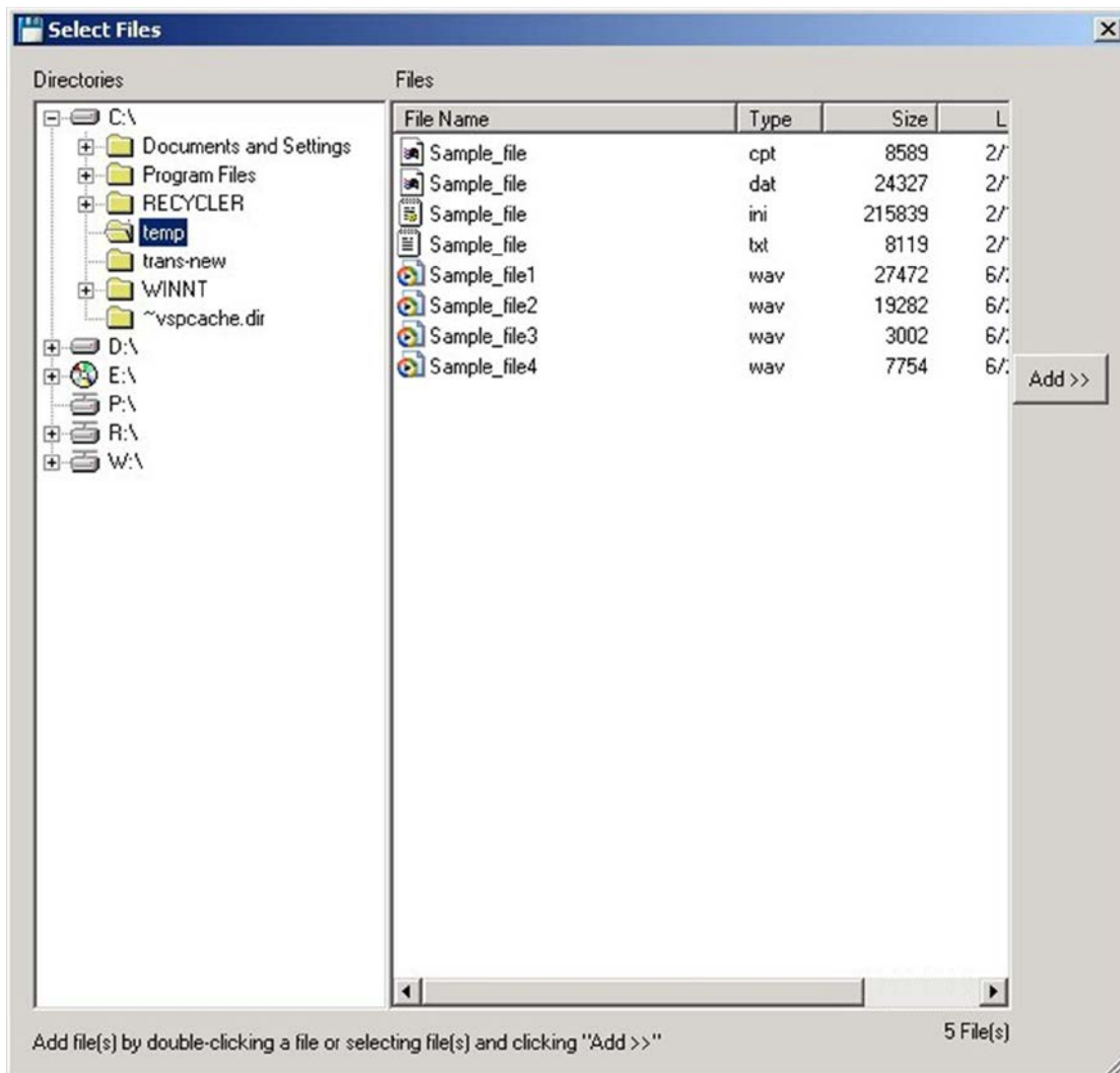
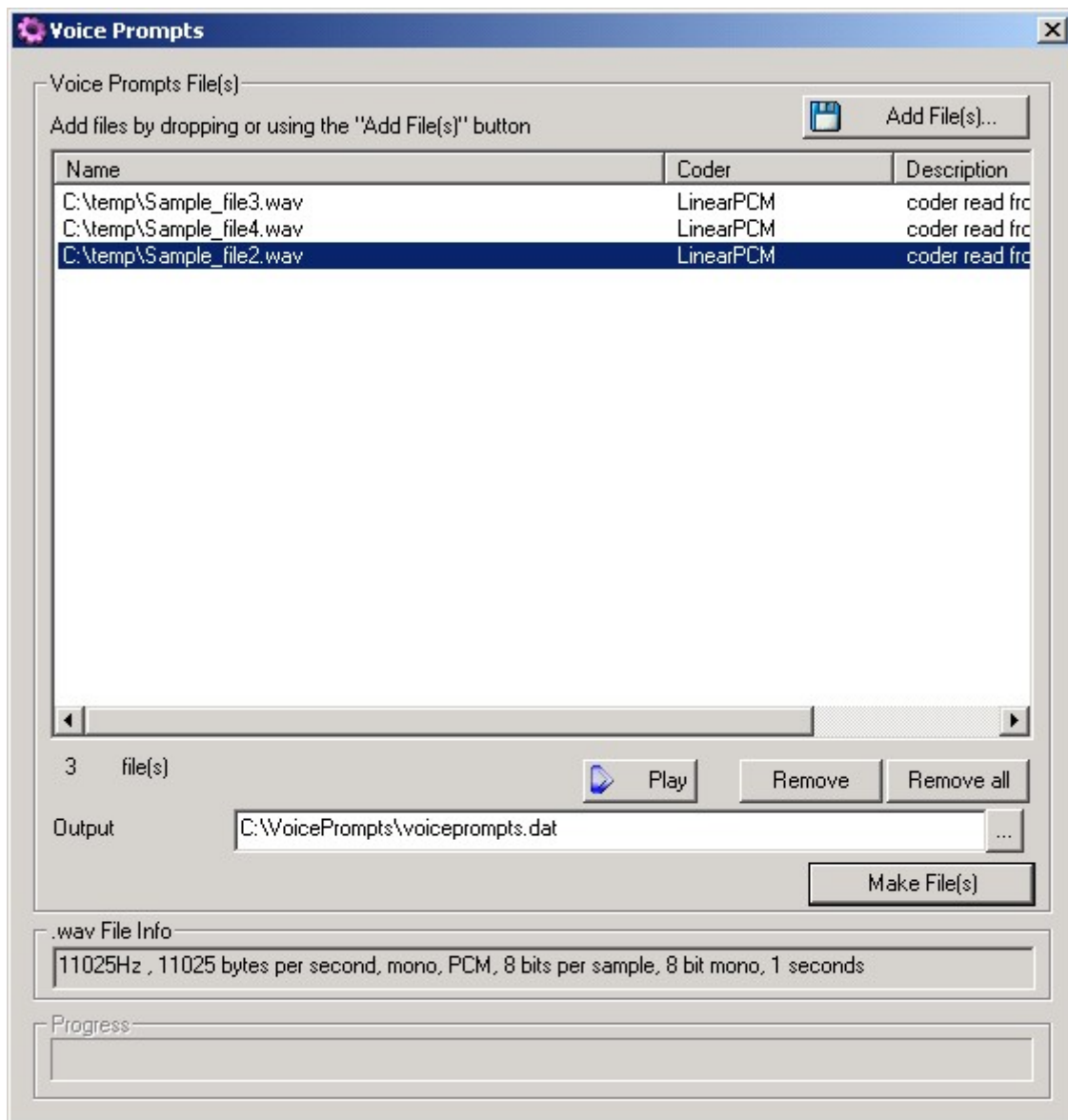


Figure 37-6: Voice Prompts Window with wav Files



- b. From any location on the PC, select the appropriate files and drag-drop them into the Voice Prompts window.
3. Arrange the files as desired by dragging and dropping them from one location in the list to another location.



Note: The sequence of files in the "Add Files..." window defines the Voice Prompt ID.

4. Use the **Play** button to preview the sound of the wav file. Use the **Remove** and **Remove all** buttons to remove files in the list as needed.
5. Select a coder for each file by first selecting the file (or files) and then double-clicking or right-clicking on it. The File Data window appears.

Figure 37-7: File Data Window



6. From the **Coder** drop-down list, select a coder type.
7. In the **Description** field, enter a description (optional).



Note: For wav files, a coder is automatically selected from the wav file header.

8. Close the File Data dialog by clicking on the  Exit button. (Press the **Esc** key to cancel changes.). You are returned to the Voice Prompts window.
9. The default **Output** file name is *voiceprompts.dat*. You can modify it.
Or,
Use the  Browse button to select a different Output file. Navigate to the desired file and select it. The selected file name and its path appear in the **Output** field.
10. Click the **Make File(s)** button to generate the Voice Prompts file. The Progress bar at the bottom of the window is activated. The *.dat* file is generated and placed in the same directory as shown in the **Output File** field. A message box informing you that the operation was successful indicates that the process is completed.

37.5 CAS Files

CAS files contain the state machine that fully defines the entire CAS protocol message exchange. It consists of States, pre-defined Actions/Events and pre-defined functions, and allows the fully customization of the CAS protocol implementation.

CAS files must be uploaded to the Media Gateway boards in *binary format*. You can edit the "source" CAS file in any text editor (as described 'CAS File Syntax' on page 437) and convert it to the binary format using the **DConvert utility** (as described in Converting CAS File to Binary Format).

➤ **To associate a CAS file with a Media Gateway board:**

1. Click  to access the Media Gateway status screen.
2. In the Navigation pane, select **PSTN ► CAS Files Setup** and in the Configuration pane, click **CAS Files Settings**; the CAS Files Settings screen is displayed.
3. Configure **CAS File X Name** parameters to match the desired CAS file.
4. Click Gateway to access the Media Gateway status screen.
5. Select the desired Media Gateway board.
6. In the Navigation pane, select **PSTN** and in the Configuration pane, click **PSTN Settings**; The PSTN Settings screen is displayed.
7. In the **CAS/ISDN Settings** tab, configure **No. of CAS Config Files** parameter to match the number of CAS files.
8. In the Navigation pane, select **PSTN ► DS1 Trunks**; The DS1 Trunks list is displayed.
9. Select the desired trunk and in the Configuration pane, select Trunk Setting; The Trunk Settings screen is displayed.
10. In the **CAS** tab, configure **CAS File Index** parameter to match the index of the specific CAS file configured at the Media Gateway level.

37.5.1 CAS File Syntax

This section describes syntax of the text-based "source" CAS file. Two files must be created by the user:

- Specific protocol/script text file (*xxx.txt*)
- Numeric values file (*xxx.h*)

Both of these files must be converted to binary format via **DConvert utility** prior to uploading them to the Media Gateway.

The **CASSetup.h** file, provided on the Media Gateway Software Installation CD, includes all of the pre-defined tools needed to build a new "source" CAS protocol file or modify an existing one.

37.5.1.1 INIT Variables

Numeric values in **UserProt_defines_xxx.h**, are defined by the user. For example, INIT_RC_IDLE_CAS defines the ABCD bits expected to be received in the IDLE state, INIT_DTMF_DIAL defines the On-time and Off-time for the DTMF digits generated towards the PSTN. See the detailed list in **CASSetup.h** and in the sample protocol text file.

37.5.1.2 Actions

Actions (i.e., protocol table events) - Protocol table events activated either by the DSP (e.g., EV_CAS_01) or by the user (e.g., EV_PLACE_CALL, EV_TIMER_EXPIRED1). The full list of the possible pre-defined events can be found in the **CASSetup.h** file.

37.5.1.3 Functions

Functions - Define a certain procedure that can be activated in any state or in the transition from one state to another. The available functions include, for example, SET_TIMER (timer number, timeout in ms.) and SEND_CAS (AB value, CD value). A full list of the possible pre-defined functions can be found in the **CASSetup.h** file.

37.5.1.4 States

States - Each Protocol table consists of several states that it switches between during the call setup and tear-down process. Every state definition begins with the prefix ST_ followed by the state name and colons. The body of the state is composed of up to four unconditional performed functions and list of actions that can trigger this state.

The table below is from an E&M wink start "source" protocol file and is shown here as an example.

Table 37-4: Example - ST_DIAL state in CAS File

Action	Function	Parameters			Next State
		#1	#2	#3	
FUNCTION0	SET_TIMER	2	Extra Delay Before Dial	None	DO
EV_TIMER_EXPIRED2	SEND_DEST_NUM	None	None	None	NO_STATE
EV_DIAL_ENDED	SET_TIMER	4	No Answer Time	None	ST_DIAL_ENDED

When the state machine reaches the dial state, it sets timer number 2 and then waits for one of the two possible actions to be triggered: either timer 2 expiration or end of dial event. When timer 2 expires, the protocol table executes the SEND_DEST_NUM function and remains in the same state (NEXT_STATE=NO_STATE). When the dial event ends, the protocol table sets timer 4 and moves to ST_DIAL_ENDED written in the NEXT_STATE field.

Although users can define their own states, there are two states defined in the **CASSetup.h** file and must appear in every protocol table created.

The two pre-defined states are ST_INIT and ST_IDLE.

■ **ST_INIT** - When channels initialization is selected, the table enters the INIT state. This state contains functions that initialize the following global parameters:

- **RC_IDLE_CAS** - Defines the ABCD bits expected to be received in the IDLE state in the specific protocol.
- **TX_IDLE_CAS** - Defines the ABCD bits transmitted on IDLE state in the specific protocol.
- **DIAL_PLAN** - The incoming call detection event is processed by declaring end of digit reception in the following ways (both for ADDRESS/destination number and ANI/source number):
 - ◆ Receiving '#' digit (in MF or DTMF)
 - ◆ The number of digits collected reaches its maximum value as defined in the DIAL_PLAN Parameter #1 and #2 for destination and ANI numbers respectively
 - ◆ A pre-defined time-out value defined in the DIAL_PLAN Parameter #3 elapses



Note: This method is not used when working with MFC/R2 protocols. MFC/R2 uses expected number of digits defined in *ProtUser_defines_xxx.h*.

- **DTMF_DIAL** - Defines the On-time and Off-time for the DTMF digits generated towards the PSTN.
- **COMMA_PAUSE_TIME** - Defines the delay between each digit when a comma is used as part of the dialed number string.
- **DTMF_DETECTION** - Defines the minimum/maximum On-time for DTMF digit dialing detection.
- **PULSE_DIAL_TIME** - Not supported by current stack version. Defines the Break and Make time for pulse dialing.
- **PULSE_DIAL** - Not supported by the current stack version. Defines the Break and Make ABCD bits for pulse dialing.
- **DEBOUNCE** - Defines the interval time of CAS to be considered as a hit.
- **COLLECT_ANI** - Enables or Disables reception of ANI in a specific protocol.
- **DIGIT_TYPE** - Defines the dialing method used (DTMF, MF). On MFC/R2 protocols this parameter is not applicable (digits are assumed to be R2)

digits).

- **NUM_OF_EVENT_IN_STATE** - Inserted for detection on TOTAL_NUMBER_OF_EVENTS_IN_STATE (**CASSetup.h**).
- **INIT_MGCP_REPORT** - Enables the event for MGCP. These tables are specifics and relevant for MGCP only. Do not use it otherwise.
- **INIT_GLOBAL_TIMERS** - Initiates specific timers, is used with Parameter#1 for metering pulse timer duration.
- **INIT_VERSION** - Defines the version number. The version number is related to the release version number.
- **INIT_SIZE_OF_TABLE_PARAM** - Users must insert the definition of TOTAL_NUMBER_OF_EVENTS_IN_STATE from the **CASSetup.h**.
- **ST_IDLE** - When no active call is established or in the process of being established, the table resides in Idle state, allowing it to start the process of incoming or outgoing calls. When the call is cleared, the state machine table returns to its idle state.

37.5.1.5 Reserved Words

For reserved words, such as DO, NO_STATE, refer to the **CASSetup.h** file.

37.5.1.6 State's Line Structure

Each text line in the body of each state is composed of six columns:

- Action/Event
- Function
- Parameter #1
- Parameter #2
- Parameter #3
- Next State

37.5.1.6.1 Action/Event

Action/Event is the name of the table's events that are the possible triggers for the entire protocol state machine. They can be selected from the list of events in the **CASSetup.h** file (e.g., EV_DISCONNECT_INCOMING).

At the beginning of the state, there can be up to four special unconditional Action/Events called FUNCTION. These events are functions that are unconditionally performed when the table reaches the state. These actions are labeled FUNCTION0 to FUNCTION3.

The following is the list of available protocols table actions (events to the state machine):

- **User Command Oriented:**
 - **EV_PLACE_CALL** - When initiating a new outgoing call
 - **EV_ANSWER** - When answering an incoming call
 - **EV_DISCONNECT_OUTGOING** - When disconnecting outgoing call.
 - **EV_DISCONNECT_INCOMING** - When disconnecting incoming call.

- **EV_RELEASE_CALL** - When releasing a call
 - **EV_USER_BLOCK_COMND** - When using blocking/unblocking a channel.
 - **EV_MAKE_METERING_PULSE** - When starting the metering pulse while using the SET_PULSE_TIMER function to start the timer to get the Off event (refer to the EV_METERING_TIMER_PULSE_OFF below.).
 - **EV_METERING_TIMER_PULSE_OFF** - event after timer (SET_PULSE_TIMER function) expires.
 - **EV_MAKE_FLASH_HOOK** - When a flash hook is triggered.
- **CAS Change Oriented:**
- **EV_CAS_1_1** - a new CAS A,B bits are received (A=1, B=1, was stable for the bouncing period).
 - **EV_CAS_1_0** - a new CAS A,B bits are received (A=1, B=0, was stable for the bouncing period).
 - **EV_CAS_0_1** - a new CAS A,B bits are received (A=0, B=1, was stable for the bouncing period).
 - **EV_CAS_0_0** - a new CAS A,B bits are received (A=0, B=0, was stable for the bouncing period).
- **Timer Oriented:**
- **EV_TIMER_EXPIRED1** - timer 1 that was previously set by table has expired.
 - **EV_TIMER_EXPIRED2** - timer 2 that was previously set by table has expired.
 - **EV_TIMER_EXPIRED3** - timer 3 that was previously set by table has expired.
 - **EV_TIMER_EXPIRED4** - timer 4 that was previously set by table has expired.
 - **EV_TIMER_EXPIRED5** - timer 5 that was previously set by table has expired.
 - **EV_TIMER_EXPIRED6** - timer 6 that was previously set by table has expired.
 - **EV_TIMER_EXPIRED7** - timer 7 that was previously set by table has expired.
 - **EV_TIMER_EXPIRED8** - timer 8 that was previously set by table has expired.
- **Counter Oriented:**
- **EV_COUNTER1_EXPIRED** - counter 1 value has reached 0.
 - **EV_COUNTER2_EXPIRED** - counter 2 value has reached 0.
- **IBS oriented:**
- **EV_RB_TONE_STARTED** - Ring back tone as defined in the call progress ini file (type and index) is detected.
 - **EV_RB_TONE_STOPPED** - Ring back tone as defined in the call progress ini file (type and index) is stopped after it has been previously detected.
 - **EV_DIAL_TONE_DETECTED** - Dial tone as defined in the call progress ini file (type and index) is detected.

- **EV_DIAL_TONE_STOPPED** - Dial tone as defined in the call progress **ini** file (type and index) was stopped after it has been previously detected.
- **MF Oriented (MFCR2 protocol related):**
 - **EV_MFRn_1** - MF digit 1 is detected.
 - **EV_MFRn_2** - MF digit 2 is detected.
 - **EV_MFRn_3** - MF digit 3 is detected.
 - **EV_MFRn_4** - MF digit 4 is detected.
 - **EV_MFRn_5** - MF digit 5 is detected.
 - **EV_MFRn_6** - MF digit 6 is detected.
 - **EV_MFRn_7** - MF digit 7 is detected.
 - **EV_MFRn_8** - MF digit 8 is detected.
 - **EV_MFRn_9** - MF digit 9 is detected.
 - **EV_MFRn_10** - MF digit 10 is detected.
 - **EV_MFRn_11** - MF digit 11 is detected.
 - **EV_MFRn_12** - MF digit 12 is detected.
 - **EV_MFRn_13** - MF digit 13 is detected.
 - **EV_MFRn_14** - MF digit 14 is detected.
 - **EV_MFRn_15** - MF digit 15 is detected.
 - **EV_MFRn_1_STOPPED** - MF digit 1 previously detected, is now stopped.
 - **EV_MFRn_2_STOPPED** - MF digit 2 previously detected, is now stopped.
 - **EV_MFRn_3_STOPPED** - MF digit 3 previously detected, is now stopped.
 - **EV_MFRn_4_STOPPED** - MF digit 4 previously detected, is now stopped.
 - **EV_MFRn_5_STOPPED** - MF digit 5 previously detected, is now stopped.
 - **EV_MFRn_6_STOPPED** - MF digit 6 previously detected, is now stopped.
 - **EV_MFRn_7_STOPPED** - MF digit 7 previously detected, is now stopped.
 - **EV_MFRn_8_STOPPED** - MF digit 8 previously detected, is now stopped.
 - **EV_MFRn_9_STOPPED** - MF digit 9 previously detected, is now stopped.
 - **EV_MFRn_10_STOPPED** - MF digit 10 previously detected, is now stopped.
 - **EV_MFRn_11_STOPPED** - MF digit 11 previously detected, is now stopped.
 - **EV_MFRn_12_STOPPED** - MF digit 12 previously detected, is now stopped.
 - **EV_MFRn_13_STOPPED** - MF digit 13 previously detected, is now stopped.
 - **EV_MFRn_14_STOPPED** - MF digit 14 previously detected, is now stopped.
 - **EV_MFRn_15_STOPPED** - MF digit 15 previously detected, is now stopped.
 - **EV_END_OF_MF_DIGIT** - When dialing MF and no more dialed number digits are available. (They already have been sent. For example, the far side requests the next ANI digit, but all digits already have been sent). This event

usually appears in MFR2 tables.

- **EV_NO_ANI** - When dialing MF and no ANI was specified by the outgoing user. (MFCR2 protocols specifications should define what to do when no ANI digits are available. Usually I-12 is sent).



Note: MF digit is MF R1 or R2-FWD or R2-BWD according to the context, protocol type and call direction.

- **EV_ACCEPT** - When using accepting a call (used only in MFC/R2) with CALLED_IDLE as its reason parameter.
- **EV_REJECT_BUSY** - When rejecting a call with CALLED_BUSY as its reason parameter.
- **EV_REJECT_CONGESTION** - When rejecting a call with CALLED_CONGESTION reason.
- **EV_REJECT_UNALLOCATED** - When rejecting a call with CALLED_UNALLOCATED reason.
- **EV_REJECT_RESERVE1** - When rejecting a call with CALLED_RESERVE1 reason.
- **EV_REJECT_RESERVE2** - When rejecting a call with CALLED_RESERVE2 reason.

■ **Miscellaneous:**

- **EV_DIALED_NUM_DETECTED** - (Incoming call) dialed destination number is collected after START_COLLECT was previously activated and the condition for incoming_call_detected event is satisfied (see ST_INIT for conditions details).
- **EV_DIAL_ENDED** - Dialing initiated by table SEND_DEST_NUM is completed (last digit has been sent).
- **EV_ANI_NUM_DETECTED** - This action is used to inform the script file of a successful reception of the ANI digits string, or when timeout of digit waiting occurs. This is reported at the incoming call detected event, when the ANI flag is YES.
- **EV_FIRST_DIGIT** - Reception of first digit out of the incoming digit string. Used in the FXO protocols, where informing the script of receiving of the first digit, enables the script to use the SEND_PROG_TON function to stop the dial tone.

37.5.1.6.2 Function

The function column holds the name of the function to be activated when the action specified in the action/events field occurs. Select the functions from the list of eight functions defined in *CasSetup.h*. (e.g., START_COLLECT). When NONE is specified in this column, no function is executed.

37.5.1.6.3 Parameters

Parameter #1, #2 and #3 columns are used as the function's parameters. The list of global parameters can be found in *CasSetup.h*. If a parameter is not essential, the parameter is marked **None**.

The following are the available user-functions and their parameters:

- **SET_TIMER (timer number, timeout)** - Set timers that are managed per B-channel, and their expiration triggers the state machine table. Each protocol table/state machine can use up to 8 timers per B-channel/call, (timeout in msec).
- **SEND_CAS (AB value, CD value)** - ABCD bits are sent as line signaling for the specific channel when the call is setup.
- **SEND_EVENT (event type, cause)** - The specific event type is sent to the host/user.
- **SEND_DEST_NUM** - Enbloc dialing: Enbloc dialing: refers to the digits string. Three types are available: (1) DestPhoneNum (2) InterExchangePrefixNum (3) SourcePhoneNum.
- **DEL_TIMER (timer number)** - Delete specific or all timers (0 for all) for the B-channel.
- **START_COLLECT** - Initiates the collection of address information i.e., the dialed (destination) number for incoming calls where appropriate according to the protocol. At the time between START_COLLECT and STOP_COLLECT, no digit is reported to the user (EV_DIGIT is blocked) and the destination number is reported in the EV_INCOMING_CALL_DETECTED event.
- **STOP_COLLECT** - See START_COLLECT.
- **SET_COUNTER (counter number, counter value or NONE)** - Set counters that are managed per B-channel and their expiration triggers the state machine. The counter initialization value should be a non-negative number. To delete all timers, perform this function with 0 in the counter number field.
- **DEC_COUNTER (counter number)** - Decreases counter value by 1. When the counter value reaches 0, EV_COUNTERx_EXPIRES is sent to the table (The x represent the counter number).
- **SEND_MF (MF type, MF digit or index or NONE, MF sending time)** - This function is used only with MFC/R2 protocols.

The Channel Parameter structure contains three parameters regarding sending digits.

- **AddressVector and ANIDigitVector** - These parameters are initialized when a call is placed. When the code reaches the dialing section, it sends MF digit according to the MF type specified in the MF type cell (the types are defined in *CASSetup.h* file):
 - **ADDRESS** - Sends the digit from the address vector (destination number) according to the index requested. (Refer to the Index definition).
 - **ANI** - Sends the digit from the ANI vector (source number) according to the index requested.
 - **SPECIFIC** - Sends the MF digit specified in the Parameter #2 rubric.
 - **SOURCE_CATEGORY** - Sends the pre-defined source category MF digit. The source category digit is set as the SourceNumberingType parameter when a call is placed. The second and third parameters have no use when

using this type.

- **TRANSFER_CAPABILITY** - Send the pre-defined line category MF digit. The line category digit is set as the TransferCapability parameter when a call is placed. The second and third parameters have no use when using this type.
- **Index** - Specifies the Offset of the next digit to be sent from the vector (ADDRESS or ANI types described above):
 - **Index 1** - Used to send the next digit in the vector.
 - **Index -n** - Used to send the last **n** digit. Underflow can occur if **n** is greater than the number of digits sent so far.
 - **Index 0** - Used to send the last sent digit.
 - **Index SEND_FIRST_DIGIT** - Used to start sending the digits vector from the beginning.
 - • (Refer to **CASSetup.h**.)
- **MF Send Time** - This send time parameter specifies the maximum transmission time of the MF.
 - **STOP_SEND_MF** - Stops sending the current MF.
 - **SEND_PROG_TON** - Operation, Tone or NONE.
 - ◆ Two operations are available.
 - ◆ Sends the Call Progress Tone specified in the Parameter #2 rubric (The second parameter can be taken from **CASSetup.h**).
 - ◆ Stops sending the last parameter.
 - **CHANGE_COLLECT_TYPE** (Collect Type) - Used only in MFCR2 protocol by the incoming user to indicate his waiting for the reception of the MF digit of the requested type. The type can be one of the following:
 - **ADDRESS** - The user is waiting for the reception of address digits.
 - **ANI** - The user is waiting for the reception of ANI digits.
 - **SOURCE_CATEGORY** - The user is waiting for the reception of the source category.
 - **TRANSFER_CAPABILITY** - The user is waiting for the reception of the source transfer capability (line category).

37.5.1.6.4 Next State

The Next State column contains the next state the table moves to after executing the function for that action/event line. When the user selects to stay in the same state, insert NO_STATE or use the current state.

The difference between NO_STATE and the current state name in this field. If the user selects to stay in the same current state, the unconditional actions (FUNCTION0) at the beginning of the state are performed. In contrast, NO_STATE skips these functions and waits for another action to come.

Reserved word "DO" must be written in the next state field if the unconditional actions (FUNCTION0) at the beginning of the state are used.

37.5.1.6.5 Action/Event

Action/Event is the name of the table's events that are the possible triggers for the entire protocol state machine. They can be selected from the list of events in the *CASSetup.h* file (e.g., *EV_DISCONNECT_INCOMING*).

At the beginning of the state, there can be up to four special unconditional Action/Events called FUNCTION. These events are functions that are unconditionally performed when the table reaches the state. These actions are labeled FUNCTION0 to FUNCTION3.

The following is the list of available protocols table actions (events to the state machine):

■ **User Command Oriented:**

- **EV_PLACE_CALL** - When initiating a new outgoing call
- **EV_ANSWER** - When answering an incoming call
- **EV_DISCONNECT_OUTGOING** - When disconnecting outgoing call.
- **EV_DISCONNECT_INCOMING** - When disconnecting incoming call.
- **EV_RELEASE_CALL** - When releasing a call
- **EV_USER_BLOCK_COMND** - When using blocking/unblocking a channel.
- **EV_MAKE_METERING_PULSE** - When starting the metering pulse while using the *SET_PULSE_TIMER* function to start the timer to get the Off event (refer to the *EV_METERING_TIMER_PULSE_OFF* below.).
- **EV_METERING_TIMER_PULSE_OFF** - event after timer (*SET_PULSE_TIMER* function) expires.
- **EV_MAKE_FLASH_HOOK** - When a flash hook is triggered.

■ **CAS Change Oriented:**

- **EV_CAS_1_1** - a new CAS A,B bits are received (A=1, B=1, was stable for the bouncing period).
- **EV_CAS_1_0** - a new CAS A,B bits are received (A=1, B=0, was stable for the bouncing period).
- **EV_CAS_0_1** - a new CAS A,B bits are received (A=0, B=1, was stable for the bouncing period).
- **EV_CAS_0_0** - a new CAS A,B bits are received (A=0, B=0, was stable for the bouncing period).

■ **Timer Oriented:**

- **EV_TIMER_EXPIRED1** - timer 1 that was previously set by table has expired.
- **EV_TIMER_EXPIRED2** - timer 2 that was previously set by table has expired.
- **EV_TIMER_EXPIRED3** - timer 3 that was previously set by table has expired.
- **EV_TIMER_EXPIRED4** - timer 4 that was previously set by table has expired.
- **EV_TIMER_EXPIRED5** - timer 5 that was previously set by table has expired.
- **EV_TIMER_EXPIRED6** - timer 6 that was previously set by table has

expired.

- **EV_TIMER_EXPIRED7** - timer 7 that was previously set by table has expired.
- **EV_TIMER_EXPIRED8** - timer 8 that was previously set by table has expired.

■ **Counter Oriented:**

- **EV_COUNTER1_EXPIRED** - counter 1 value has reached 0.
- **EV_COUNTER2_EXPIRED** - counter 2 value has reached 0.

■ **IBS oriented:**

- **EV_RB_TONE_STARTED** - Ring back tone as defined in the call progress *ini* file (type and index) is detected.
- **EV_RB_TONE_STOPPED** - Ring back tone as defined in the call progress *ini* file (type and index) is stopped after it has been previously detected.
- **EV_DIAL_TONE_DETECTED** - Dial tone as defined in the call progress *ini* file (type and index) is detected.
- **EV_DIAL_TONE_STOPPED** - Dial tone as defined in the call progress *ini* file (type and index) was stopped after it has been previously detected.

■ **MF Oriented (MFCR2 protocol related):**

- **EV_MFRn_1** - MF digit 1 is detected.
- **EV_MFRn_2** - MF digit 2 is detected.
- **EV_MFRn_3** - MF digit 3 is detected.
- **EV_MFRn_4** - MF digit 4 is detected.
- **EV_MFRn_5** - MF digit 5 is detected.
- **EV_MFRn_6** - MF digit 6 is detected.
- **EV_MFRn_7** - MF digit 7 is detected.
- **EV_MFRn_8** - MF digit 8 is detected.
- **EV_MFRn_9** - MF digit 9 is detected.
- **EV_MFRn_10** - MF digit 10 is detected.
- **EV_MFRn_11** - MF digit 11 is detected.
- **EV_MFRn_12** - MF digit 12 is detected.
- **EV_MFRn_13** - MF digit 13 is detected.
- **EV_MFRn_14** - MF digit 14 is detected.
- **EV_MFRn_15** - MF digit 15 is detected.
- **EV_MFRn_1_STOPPED** - MF digit 1 previously detected, is now stopped.
- **EV_MFRn_2_STOPPED** - MF digit 2 previously detected, is now stopped.
- **EV_MFRn_3_STOPPED** - MF digit 3 previously detected, is now stopped.
- **EV_MFRn_4_STOPPED** - MF digit 4 previously detected, is now stopped.
- **EV_MFRn_5_STOPPED** - MF digit 5 previously detected, is now stopped.
- **EV_MFRn_6_STOPPED** - MF digit 6 previously detected, is now stopped.
- **EV_MFRn_7_STOPPED** - MF digit 7 previously detected, is now stopped.
- **EV_MFRn_8_STOPPED** - MF digit 8 previously detected, is now stopped.

- **EV_MFRn_9_STOPPED** - MF digit 9 previously detected, is now stopped.
- **EV_MFRn_10_STOPPED** - MF digit 10 previously detected, is now stopped.
- **EV_MFRn_11_STOPPED** - MF digit 11 previously detected, is now stopped.
- **EV_MFRn_12_STOPPED** - MF digit 12 previously detected, is now stopped.
- **EV_MFRn_13_STOPPED** - MF digit 13 previously detected, is now stopped.
- **EV_MFRn_14_STOPPED** - MF digit 14 previously detected, is now stopped.
- **EV_MFRn_15_STOPPED** - MF digit 15 previously detected, is now stopped.
- **EV_END_OF_MF_DIGIT** - When dialing MF and no more dialed number digits are available. (They already have been sent. For example, the far side requests the next ANI digit, but all digits already have been sent). This event usually appears in MFR2 tables.
- **EV_NO_ANI** - When dialing MF and no ANI was specified by the outgoing user. (MFCR2 protocols specifications should define what to do when no ANI digits are available. Usually I-12 is sent).



Note: MF digit is MF R1 or R2-FWD or R2-BWD according to the context, protocol type and call direction.

- **EV_ACCEPT** - When using accepting a call (used only in MFC/R2) with CALLED_IDLE as its reason parameter.
- **EV_REJECT_BUSY** - When rejecting a call with CALLED_BUSY as its reason parameter.
- **EV_REJECT_CONGESTION** - When rejecting a call with CALLED_CONGESTION reason.
- **EV_REJECT_UNALLOCATED** - When rejecting a call with CALLED_UNALLOCATED reason.
- **EV_REJECT_RESERVE1** - When rejecting a call with CALLED_RESERVE1 reason.
- **EV_REJECT_RESERVE2** - When rejecting a call with CALLED_RESERVE2 reason.

■ **Miscellaneous:**

- **EV_DIALED_NUM_DETECTED** - (Incoming call) dialed destination number is collected after START_COLLECT was previously activated and the condition for incoming_call_detected event is satisfied (see ST_INIT for conditions details).
- **EV_DIAL_ENDED** - Dialing initiated by table SEND_DEST_NUM is completed (last digit has been sent).

- **EV_ANI_NUM_DETECTED** - This action is used to inform the script file of a successful reception of the ANI digits string, or when timeout of digit waiting occurs. This is reported at the incoming call detected event, when the ANI flag is YES.
- **EV_FIRST_DIGIT** - Reception of first digit out of the incoming digit string. Used in the FXO protocols, where informing the script of receiving of the first digit, enables the script to use the SEND_PROG_TON function to stop the dial tone.

37.5.1.6.6 Function

The function column holds the name of the function to be activated when the action specified in the action/events field occurs. Select the functions from the list of eight functions defined in *CasSetup.h*. (e.g., START_COLLECT). When NONE is specified in this column, no function is executed.

37.5.1.6.7 Parameters

Parameter #1, #2 and #3 columns are used as the function's parameters. The list of global parameters can be found in *CasSetup.h*. If a parameter is not essential, the parameter is marked **None**.

The following are the available user-functions and their parameters:

- **SET_TIMER (timer number, timeout)** - Set timers that are managed per B-channel, and their expiration triggers the state machine table. Each protocol table/state machine can use up to 8 timers per B-channel/call, (timeout in msec).
- **SEND_CAS (AB value, CD value)** - ABCD bits are sent as line signaling for the specific channel when the call is setup.
- **SEND_EVENT (event type, cause)** - The specific event type is sent to the host/user.
- **SEND_DEST_NUM** - Enbloc dialing: Enbloc dialing: refers to the digits string. Three types are available: (1) DestPhoneNum (2) InterExchangePrefixNum (3) SourcePhoneNum.
- **DEL_TIMER (timer number)** - Delete specific or all timers (0 for all) for the B-channel.
- **START_COLLECT** - Initiates the collection of address information i.e., the dialed (destination) number for incoming calls where appropriate according to the protocol. At the time between START_COLLECT and STOP_COLLECT, no digit is reported to the user (EV_DIGIT is blocked) and the destination number is reported in the EV_INCOMING_CALL_DETECTED event.
- **STOP_COLLECT** - See START_COLLECT.
- **SET_COUNTER (counter number, counter value or NONE)** - Set counters that are managed per B-channel and their expiration triggers the state machine. The counter initialization value should be a non-negative number. To delete all timers, perform this function with 0 in the counter number field.
- **DEC_COUNTER (counter number)** - Decreases counter value by 1. When the counter value reaches 0, EV_COUNTERx_EXPIRES is sent to the table (The x represent the counter number).
- **SEND_MF (MF type, MF digit or index or NONE, MF sending time)** - This

function is used only with MFC/R2 protocols.

The Channel Parameter structure contains three parameters regarding sending digits.

- **AddressVector and ANIDigitVector** - These parameters are initialized when a call is placed. When the code reaches the dialing section, it sends MF digit according to the MF type specified in the MF type cell (the types are defined in **CASSetup.h** file):
 - **ADDRESS** - Sends the digit from the address vector (destination number) according to the index requested. (Refer to the Index definition).
 - **ANI** - Sends the digit from the ANI vector (source number) according to the index requested.
 - **SPECIFIC** - Sends the MF digit specified in the Parameter #2 rubric.
 - **SOURCE_CATEGORY** - Sends the pre-defined source category MF digit. The source category digit is set as the SourceNumberingType parameter when a call is placed. The second and third parameters have no use when using this type.
 - **TRANSFER_CAPABILITY** - Send the pre-defined line category MF digit. The line category digit is set as the TransferCapability parameter when a call is placed. The second and third parameters have no use when using this type.
- **Index** - Specifies the Offset of the next digit to be sent from the vector (ADDRESS or ANI types described above):
 - **Index 1** - Used to send the next digit in the vector.
 - **Index -n** - Used to send the last **n** digit. Underflow can occur if **n** is greater than the number of digits sent so far.
 - **Index 0** - Used to send the last sent digit.
 - **Index SEND_FIRST_DIGIT** - Used to start sending the digits vector from the beginning.
 - • (Refer to **CASSetup.h**.)
- **MF Send Time** - This send time parameter specifies the maximum transmission time of the MF.
 - **STOP_SEND_MF** - Stops sending the current MF.
 - **SEND_PROG_TON** - Operation, Tone or NONE.
Two operations are available.
 - ◆ Sends the Call Progress Tone specified in the Parameter #2 rubric (The second parameter can be taken from **CASSetup.h**).
 - ◆ Stops sending the last parameter.
 - **CHANGE_COLLECT_TYPE** (Collect Type) - Used only in MFCR2 protocol by the incoming user to indicate his waiting for the reception of the MF digit of the requested type. The type can be one of the following:
 - **ADDRESS** - The user is waiting for the reception of address digits.
 - **ANI** - The user is waiting for the reception of ANI digits.
 - **SOURCE_CATEGORY** - The user is waiting for the reception of the source category.

- **TRANSFER_CAPABILITY** - The user is waiting for the reception of the source transfer capability (line category).

37.5.1.6.8 Next State

The Next State column contains the next state the table moves to after executing the function for that action/event line. When the user selects to stay in the same state, insert NO_STATE or use the current state.

The difference between NO_STATE and the current state name in this field. If the user selects to stay in the same current state, the unconditional actions (FUNCTION0) at the beginning of the state are performed. In contrast, NO_STATE skips these functions and waits for another action to come.

Reserved word "DO" must be written in the next state field if the unconditional actions (FUNCTION0) at the beginning of the state are used.

37.5.2 Converting CAS File to Binary Format

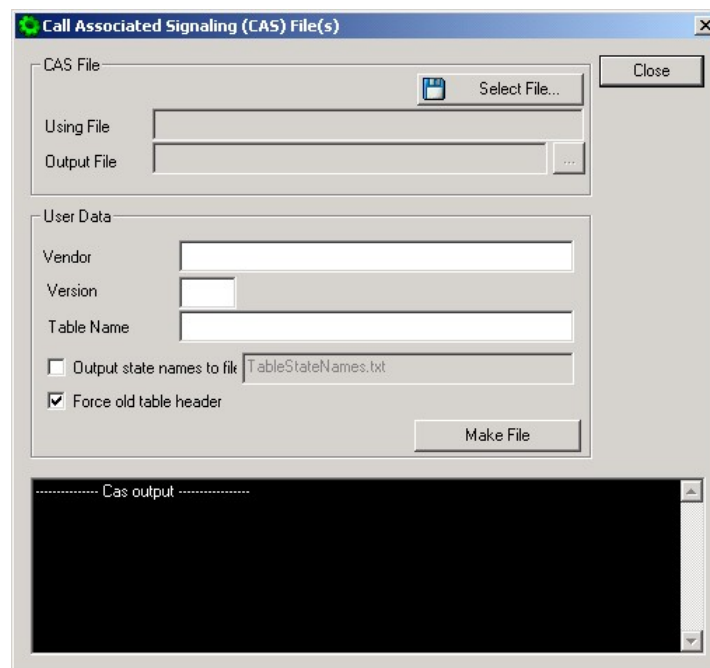
After editing the "source" CAS file you must convert it to the binary format using the *DConvert utility* provided on the Media Gateway Software Installation CD.

➤ To convert a "source" CAS file to a binary format:

1. Copy the "source" CAS files (both xxx.txt and xxx.h file) to the same directory in which *DConvert.exe* is located and make sure that the two following files, **CASSetup.h** and **CPP.exe**, are also located in this same directory.
2. Copy the files generated in the previous step (or at least the xxx.h file) to the same directory in which *DConvert.exe* is located and make sure that the two following files, **CASSetup.h** and **CPP.exe**, are also located in this same directory.

3. Execute **DConvert.exe** and click the **Process CAS Tables** button. The Call Associated Signaling (CAS) Window appears.

Figure 37-8: Call Associated Signaling (CAS) Screen



4. Click the **Select File** button. A Browse window appears.
5. Navigate to the desired location and select the file to be converted. (This automatically designates the output file as the same name and path, but with the *dat* extension. The Table Name is also automatically designated.)
6. Fill in the **Vendor** and **Version** fields.
 - **Vendor** Field - 32 characters maximum
 - **Version** Field - must be made up an integer, followed by a period ".", then followed by another integer (e.g., 1.2, 23.4, 5.22)
7. Modify the **Table Name** if desired.
8. For troubleshooting purposes, you can click a check into the **Output state names to file** checkbox. This activates the file name field in which the default file name, **TableState Names.txt** appears. You can modify the file name if desired. The file is located in the same directory as the **Using file** and **Output file** designated above.
9. If the file to be converted uses the **new table header**, un-check the **Force old table header** checkbox.
10. Click the **Make File** button. The *dat* file is generated and placed in the same directory as shown in the **Output File** field. A message box informing you that the operation was successful indicates that the process is completed.

On the bottom of the Call Assisted Signaling (CAS) Files(s) window, the Cas output log box displays the log generated by the process. It can be copied as needed. The information in it is **NOT** retained after the window is closed.

37.6 External Coders Files

The External Coders file defines which coders are to be supported by the Media Gateway board. It is limited to the supported coders according to the loaded DSP template. Other coders can not be added.

External Coders files must be uploaded to the Media Gateway boards *in binary format*. You can edit the "source" coders file in any text editor (as described in 'Modifying the "Source" External Coders File' on page 453) and convert it to the binary format using the **DConvert utility** (as described in 'Converting External Coders File to Binary Format' on page 454).

To associate an External Coders file with a Media Gateway board, see 'Auxiliary Files Repository' on page 422.

37.6.1 Modifying the "Source" External Coders File

This section describes syntax of the text-based "source" External Coders file. This file must be converted to the binary format via the **DConvert utility** prior to uploading it to the Media Gateway.

The following is an example of a "source" External Coders **file**.

[Internal name]	[Coder name]	[Txpayload]	[RxPayload]	[Ptime]
PCMA	PCMA	8	8	20
PCMU	PCMU	0	0	20
G726-16	G726-16	35	35	20
G726-24	G726-24	36	36	20
G726-32	G726-32	2	2	20
G726-40	G726-40	38	38	20
X-G727-16	X-G727-16	39	39	20
X-G727-24-16	X-G727-24-16	40	40	20
X-G727-24	X-G727-24	41	41	20
X-G727-32-16	X-G727-32-16	42	42	20
X-G727-32-24	X-G727-32-24	43	43	20
X-G727-32	X-G727-32	44	44	20
X-G727-40-16	X-G727-40-16	45	45	20
X-G727-40-24	X-G727-40-24	46	46	20
X-G727-40-32	X-G727-40-32	47	47	20
G723HIGH	G723	4	4	30
G723LOW	G723	80	80	30
G729	G729	18	18	20
G728	G728	15	15	20
GSM	GSM	3	3	20
X-CCD	X-CCD	56	56	20
iLBC13	iLBC	100	100	30
iLBC15	iLBC	101	101	20
BV16	BV16	102	102	20
EVRC_C	EVRC	103	103	20
telephone-event	telephone-event	96	96	20
RED	RED	104	104	20
CN	CN	13	13	20

The first field is a text representation of the internal coder name. The second field is free text, and contains the name that is to be used in the SDP. The two payload fields define the default payload for this coder. The PTIME field defines the default to be used for this coder. The maximal value is the basic packet size (i.e., 20) multiplied by 6.

37.6.1.1 New Coders Introduced with the Table

- **EVRC0** – This is actually the corrected name (according to RFC 3558) of a existing coder. (It was formerly called EVRC.)
- **BV16** – Supported for BCT only.
- **iLBC** – Supported for BCT only.

37.6.1.2 Coders Support Level

The application defines the following support levels for coders:

- **None** - A coder with support level "None" is not supported. An error is generated if an attempt is made to use the coder.
- **Full** - A coder with support level "Full" is valid for all type of calls.
- **BCT** - A coder with support level "BCT" (a new feature) is valid ONLY for BCT calls. The coders, **iLBC** and **BV16** belong to this feature. Other coders that appear in the file, but are not supported in the current DSP template, also receive this support level.

The support level is defined internally by the board.

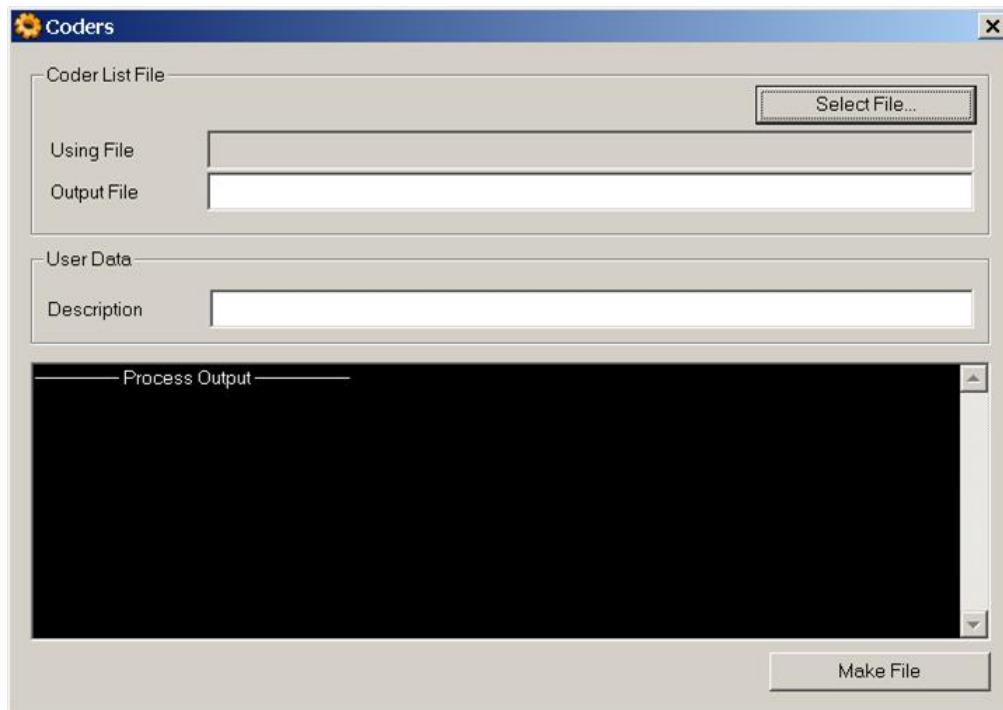
37.6.2 Converting External Coders File to Binary Format

After editing the "source" External Coders file, you must convert it to the binary format using the **DConvert utility** provided on the Media Gateway Software Installation CD.

➤ To convert a "source" External Coders file to a binary format:

1. Execute *DConvert.exe* and click the **Process Coders Description** button; the Coders Window is displayed.

Figure 37-9: Coders Window



2. Click the **Make File** button. A Browse window appears.
3. Navigate to the desired location and select the file to be converted. (This automatically designates the output file as the same name and path, but with the *.dat* extension). The output file name may be altered.
4. Fill in the **Description** field. This step is optional. The maximum description length is 64 chars.
5. Click the **Make File** button. The *.dat* file is generated and placed in the same directory as shown in the **Output File** field. A message box informing you that the operation was successful indicates that the process has been completed.
6. On the bottom of the Coders window, the Coders output log box displays the log generated by the process. It may be copied as needed.


Note :

- This information is **NOT** retained after the window has been closed.
- The process verifies the input file for validity. Invalid data causes an error and aborts the process. The log box contains further relevant information.

37.7 Dial Plan Prefix Tags for IP-to-Tel Routing

This feature enables the VoIP board to support the use of string labels (or "tags") in the external Dial Plan file for tagging incoming IP-to-Tel calls. The special "tag" is added as a prefix to the called party number, and then the "IP to Telephone/Inbound Routing Table" uses this "tag" instead of the original prefix. Manipulation is then performed after routing in the "Destination Phone Number Manipulation Table for IP to Tel calls", which strips the "tag" characters before sending the call to the endpoint.

This feature resolves the limitation of entries in the "IP to Telephone/Inbound Routing Table" for scenarios in which many different routing rules are required. For example, a city may have many different area codes, some for local calls and others for long distance calls (e.g. 425-202-xxxx for local calls; however 425-200-xxxx for long distance calls).

For using tags, the dial plan file is defined as follows:

- Number of dial plan (text)
 - Dial string prefix (ranges can be defined in brackets)
 - User-defined routing tag (text)
1. Configure the dial plan routing tags:
 - a. Open a text file using a text editor.
 - b. Define an external Dial Plan file similar to the example configuration below:
In this example configuration, multiple prefixes exist for local and long distance calls, where the following two routing tags are used:
 - ◆ "LOCL" - for local calls
 - ◆ "LONG" - for long distance calls

```
[ PLAN1 ]
42520[3-5], 0, LOCL
425207, 0, LOCL
42529, 0, LOCL
425200, 0, LONG
425100, 0, LONG
```

When an incoming IP call to destination prefix 425203 (for example) is received, the device adds the prefix tag "LOCL" (as specified in the Dial Plan file), resulting in the number "LOCL425203".

Specify a separate plan number for each Dial Plan you wish to configure i.e. PLAN1, PLAN2 etc.

2. Assign the tag prefixes to trunk groups:

Once you have configured the dial plan file, you need to assign the tag prefixes to the trunk groups. In this example, you assign one tag to the trunk group "Local" for local calls, and another to the trunk group "Long" for long distance calls.

- a. Click  to access the Media Gateway status screen.
 - b. Select the specific Media Gateway board.
 - c. In the Navigation pane, select **SIP ► GW/IP to IP ► Routing ► IP to Tel/Inbound**; the SIP IP to Tel Routing List is displayed.
 - d. Use the  to add an entry.
 - e. Select the new row and then in the Configuration pane, select **SIP Routing IP to Tel Settings**; the **SIP Routing IP to Tel Settings** screen is displayed.
 - f. In the "Dest Phone Prefix" field, set the value 'LOCL' and the "Trunk Group ID" to '1'. This rule is assigned to local Trunk Group '1'.
 - g. Repeat steps 4 and 5 and then in the "Dest Phone Prefix" field, set the value 'LONG' and the "Trunk Group ID" to '2'. This rule is assigned to a long distance Trunk Group '2'.
3. Configure phone number manipulation for local and long distance calls:
In this example, you set two manipulation rules, one for local calls and another for long distance calls.
- a. In the Navigation pane, select **SIP ► GW/IP to IP ► Manipulation ► Dest Number IP to Tel**; the Manipulation Dest IP to Tel list is displayed.
 - b. Use the  to add an entry.
 - c. Select the new row and then in the Configuration pane, select **SIP Manipulations Dest IP to Tel**; the **SIP Manipulations Dest IP to Tel** screen is displayed.
 - d. In the "Destination Prefix" field, set to 'LOCL'.
 - e. In the "Num Of Stripped Digits Left" field, set to '4'.
 - f. Repeat steps 2-3 and then in the "Destination Prefix" field, set to 'LONG' and in the "Num Of Stripped Digits Left" field, set to '4'.
4. Apply the dial plan to a Tel Profile for a specific board:
- a. In the Navigation pane, select **SIP ► GW/IP to IP ► Trunk Groups ► Tel Profile**; the Profiles Tel List is displayed.
 - b. Use the  to add an entry.
 - c. Select the new row and then in the Configuration pane, click **SIP Profiles Tel Settings**; the **SIP Profiles Tel Settings** screen is displayed.
 - d. In the Dial Plan index drop-down list, choose the desired Dial Plan number.

This page is intentionally left blank.

38 Configuring the PSTN Subsystem

The Mediant 8000 provides the following functionality that is used for connecting it to the Public Switch Telephony Network (PSTN) and is described in this chapter below.

- Physical PSTN interfaces:
 - STM-1/OC-3
 - T3 Interfaces
 - E1/T1 Trunks
- Channel Status screen
- PSTN Clock Synchronization
- SS7 Subsystem (for M2UA and M3UA applications)
- ISDN Subsystem (for IUA and DUA applications)

38.1 Configuring Media Gateway Board's PSTN Settings

The basic PSTN subsystem configuration is performed for each Media Gateway board as described below.

➤ To configure Media Gateway Board's PSTN Settings:

1. Click  to access the Media Gateway status screen.
2. Select the specific Media Gateway board.
3. In the Navigation pane, select **PSTN** and then in the configuration pane, click **PSTN Settings**; the PSTN Settings screen is displayed.
4. Configure Media Gateway board's PSTN parameters according to the table 'Media Gateway board's PSTN Parameters' below.

Table 38-1: Media Gateway Board's PSTN Parameters

Parameter Name	Type	Provisioning Type	Description
Trunks In Board	Integer 0 – 84	Read-Only	Indicates the number of E1/T1 trunks available in the Media Gateway board.
None Mode Clk Source	Enum Internal, PSTN, ATM	Online	Defines the PSTN clock source for 'Stand Alone Board Clock Mode'. See 'Standalone Sync Clock Mode' on page 516 for detailed information.
PCM Law	Enum None, A-Law, Reserved, Mu-Law	Online	Defines the PCM Law algorithm (as per CCITT G.711). Mu-Law PCM is used in North America and Japan, and A-Law is used in most other countries.

Parameter Name	Type	Provisioning Type	Description
Idle ABCD Pattern	Integer 0 – 15	Online	Defines the ABCD (CAS) pattern to be applied on the signaling bus before it is changed by the user or the PSTN protocol. This is only relevant when using PSTN interface with CAS protocols.
MGC Disconnect	Enum No Action, Trunk Disable, Reset Board	Online	Defines the Media Gateway board's behavior upon losing connectivity with an H.248 Call Agent. - No Action – keep routing traffic - Disable Trunks – stop routing traffic; however, RTP remains active - Reset Board – stop all

38.2 Configuring STM-1/OC-3 Interfaces

Two redundant optical STM-1/OC-3 interfaces, featuring automated protection switching (APS) are provided on each TP-6310 Media Gateway board for connecting to the SDH/SONET fiber networks. These interfaces are available on 6310/RTM modules, located on the back of the Mediant 8000 chassis, behind corresponding TP-6310 Media Gateway boards. For additional details, see TP-6310 Media Gateway and '6310/RTM - Rear Transition Module' on page 49.

The Media Gateway software uses the term **PSTN Fiber Group** to describe this pair of STM-1/OC-3 interfaces. Configuration and fault monitoring of STM-1/OC-3 interfaces is performed as follows.

➤ To view status of the PSTN Fiber Group on specific Media Gateway board:

1. Click  to access the Media Gateway status screen.
2. Double-click the specific Media Gateway board.

3. The 6310 Status screen is displayed. This screen lists the physical interfaces provided by the Gateway board.

Figure 38-1: TP-6310 Board Status Screen

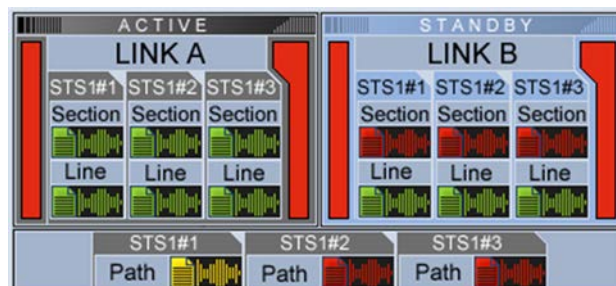


4. Double-click the line that corresponds to the **PSTN Fiber Group**; the PSTN Fiber Group status screen is displayed. This screen displays the status of the PSTN Fiber Group and all its physical and logical components.

Figure 38-2: STM-1 PSTN Fiber Group Status Screen



Figure 38-3: OC-3 PSTN Fiber Group Status Screen



➤ **To configure the PSTN Fiber Group on a specific Media Gateway board:**

1. Access the TP-6310 Board Interfaces screen as described above.
2. In the TP-6310 Board Interfaces screen, select the PSTN Fiber Group Interface and then in the configuration pane, click **Fiber Group Settings**; the Fiber Group Settings screen is displayed.
3. Modify parameters as described in the table 'PSTN Fiber Group Properties' below. Note that most of the PSTN Fiber Group parameters are of Offline provisioning type; therefore you must lock the corresponding Media Gateway board to modify them.

4. Activate the new configuration by unlocking the corresponding Media Gateway board (if it was locked before).

Table 38-2: PSTN Fiber Group Properties

Parameter Name	Type	Provisioning Type	Description
Fiber Group Name	String Up to 20 chars	Instant	Defines name of the PSTN Fiber Group allowing user to easily identify it.
Interface Type	Enum Unknown, STM1, OC3	Offline	Defines type of the Fiber Group Interface.
Protection Mode	Enum Unprotected, Protected	Offline	Defines the APS protection mode of the Fiber Group.
Active Link	Integer 1-2	Read-Only	Indicates which of the Fiber Group links (A or B) is currently active.
Revertive Mode	Enum Non-Revertive, Revertive	Offline	Defines revertive or non-revertive behavior of the APS protection mode. In revertive mode, when failed Link A returns to service, activity is automatically switched back to it. In non-revertive mode the activity remains on Link B.
Wait-To-Restore Delay (WTR)	Integer 5-13	Offline	Defines delay time-out (in seconds) for Wait-To-Restore feature.
APS Dir Mode	Unidirectional, Bidirectional	Offline	Defines whether unidirectional or bidirectional APS mode is used.
KLM Numbering Scheme	Enum ETSI, GR253, Timeslots	Offline	Defines the scheme for VC/VT numbering inside STM-1/OC-3. Once a scheme is selected, there is mapping of 3 numbers (K,L,M) identifying VC/VT inside the STM-1/OC-3 to an E1/T1 trunk number.
Mapping Type	Enum AsyncVT15ofDS1, AsyncTU12ofE1, STS1ofDS3	Offline	Defines the SDH/SONET mapping type (TU/VT/STS1 signal label + payload mapping type). ▪ AsyncVT15ofDS1 – T1/VT1.5 mapper for SONET ▪ AsyncTU12ofE1 – E1/TU12 mapper for SDH ▪ STS1ofDS3 – T3/STS1 mapper for SONET (channelized T3)

38.3 Configuring T3 Interfaces

Three T3 interfaces are provided on each TP-6310 Media Gateway board for connecting to the PSTN network. These interfaces are available on the 6310/RTM modules, located on the back of the Mediant 8000 chassis, behind the corresponding TP-6310 Media Gateway boards. For additional details, see Section 'TP-6310 Media Gateway Board' on page 45 and '6310/RTM - Rear Transition Module' on page 49.

Configuration and fault monitoring of T3 interfaces is performed as follows.

➤ To view status of the T3 interfaces on a specific Media Gateway board:

1. Click  to access the Media Gateway status screen.
2. Select the specific Media Gateway board.
3. In the Navigation pane, select **PSTN ► DS3**; the DS3 Status screen is displayed.

Figure 38-4: DS3 Status Screen



#	Name	Clock Source	Admin State	Oper State	Severity
1	none	slave	Locked	Disabled	clear
2	none	slave	Locked	Disabled	clear
3	none	slave	Locked	Disabled	clear

4. To view the detailed list and status of T1 trunks, corresponding to the specific T3 interface, double-click the line that corresponds to the specific T3 interface. The E1/T1 Trunks status screen, containing relevant trunks, is displayed. For more information, see Section 'Configuring the E1/T1 Trunks'.

➤ To configure a T3 Interface on specific Media Gateway board:

1. Access the DS3 Status screen, as described above.
2. In the DS3 Status screen, select a T3 interface and then in the configuration pane, click **DS3 Settings**; the DS3 Settings screen is displayed.
3. Modify parameters as described in the table 'T3 Interface Properties' below.

Table 38-3: T3 Interface Properties

Parameter Name	Type	Provisioning Type	Description
DS3 Name	String Up to 20 chars.	Instant	Defines textual name for the DS3 Interface enabling user to easily identify it.
DS3 Clock Source	Enum Slave, Master, LocalPLL	Instant	Defines the clock source for the specific DS3 interface. See Section 'Timing Module Line Sync Clock Mode' on page 522 for details.
DS3 Framing Method	Enum M23, C-bitParity	Instant	Defines the framing method for DS3 interface.
DS3 Line Build Out	Enum 672mv, 744mv, 816mv, 888mv, 960mv, 1008mv	Instant	Defines the build-out voltage (in mili-volts) for DS3 interface.

38.3.1 Channelized T3

In “channelized T3” configuration, T3 interfaces are carried inside the OC-3 (SONET) optical links. Up to three T3 trunks can be channelized. To configure channelized T3 trunks, configure the Fiber Group as follows:

- **Fiber Group Interface Type** = OC3
- **Fiber Group Mapping Type** = STS1ofDS3

See Table 'PSTN Fiber Group Properties' for details.

In contrast to the regular T3 coaxial interfaces, “channelized T3” configuration benefits from the APS protection provided by the OC-3 (SONET) optical links.

In a “channelized T3” configuration, both the OC-3 PSTN Fiber Group Status Screen (as shown in 'Figure : OC-3 PSTN Fiber Group Status Screen) and the DS3 Status Screen (as shown in 'Figure DS-3 Status Screen) are accessible.

Configuration is also supported for both the PSTN Fiber Group and the T3 Interface, as described in the previous sections.

38.4 Configuring the E1/T1 Trunks

The term **Trunk** is commonly used to define a connection between switches within the PSTN exchange. A Trunk contains a specific number of channels that may carry voice or signaling messages (depending on the PSTN protocols being used).

E1/T1 trunks are provided by both the TP-6310 and TP-8410 Media Gateway boards.

For TP-8410 Media Gateway boards, physical E1/T1 trunk connectors are available on the 8410/RTM module, located at the back of the Mediant 8000 chassis. For additional details, see 'TP-8410 Media Gateway Board' on page [52](#).

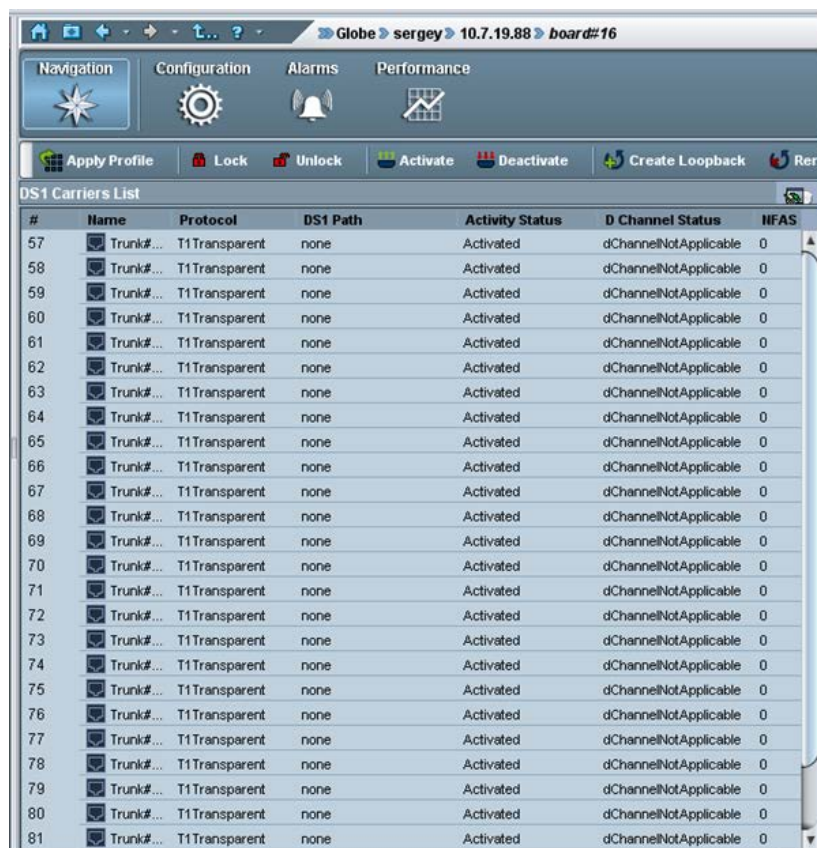
For TP-6310 Media Gateway's, E1/T1 trunks are “confined” inside the STM-1/OC3 optical links or T3 interfaces.

38.4.1 Status in the EMS

The Status of the Trunk is represented by standard **Operational State** and **Administrative State** attributes.

- When the Trunk is functioning properly, its **Operational State** is set to *Enabled* and the trunk is colored *green* in the EMS.
- When the Trunk is not functioning properly (not synchronized with the remote side), its **Operational State** is set to *Disabled* and the trunk is colored *red* in the EMS.
- When the Trunk is locked, its **Administrative State** is set to *Locked* and the trunk is colored *grey* in the EMS.

Figure 38-5: E1/T1 Trunks Status Screen



#	Name	Protocol	DS1 Path	Activity Status	D Channel Status	NFAS
57	Trunk#...	T1Transparent	none	Activated	dChannelNotApplicable	0
58	Trunk#...	T1Transparent	none	Activated	dChannelNotApplicable	0
59	Trunk#...	T1Transparent	none	Activated	dChannelNotApplicable	0
60	Trunk#...	T1Transparent	none	Activated	dChannelNotApplicable	0
61	Trunk#...	T1Transparent	none	Activated	dChannelNotApplicable	0
62	Trunk#...	T1Transparent	none	Activated	dChannelNotApplicable	0
63	Trunk#...	T1Transparent	none	Activated	dChannelNotApplicable	0
64	Trunk#...	T1Transparent	none	Activated	dChannelNotApplicable	0
65	Trunk#...	T1Transparent	none	Activated	dChannelNotApplicable	0
66	Trunk#...	T1Transparent	none	Activated	dChannelNotApplicable	0
67	Trunk#...	T1Transparent	none	Activated	dChannelNotApplicable	0
68	Trunk#...	T1Transparent	none	Activated	dChannelNotApplicable	0
69	Trunk#...	T1Transparent	none	Activated	dChannelNotApplicable	0
70	Trunk#...	T1Transparent	none	Activated	dChannelNotApplicable	0
71	Trunk#...	T1Transparent	none	Activated	dChannelNotApplicable	0
72	Trunk#...	T1Transparent	none	Activated	dChannelNotApplicable	0
73	Trunk#...	T1Transparent	none	Activated	dChannelNotApplicable	0
74	Trunk#...	T1Transparent	none	Activated	dChannelNotApplicable	0
75	Trunk#...	T1Transparent	none	Activated	dChannelNotApplicable	0
76	Trunk#...	T1Transparent	none	Activated	dChannelNotApplicable	0
77	Trunk#...	T1Transparent	none	Activated	dChannelNotApplicable	0
78	Trunk#...	T1Transparent	none	Activated	dChannelNotApplicable	0
79	Trunk#...	T1Transparent	none	Activated	dChannelNotApplicable	0
80	Trunk#...	T1Transparent	none	Activated	dChannelNotApplicable	0
81	Trunk#...	T1Transparent	none	Activated	dChannelNotApplicable	0

➤ To view the status of the E1/T1 trunks on specific Media Gateway board:

1. Click  to access the Media Gateway status screen.
2. Select the specific Media Gateway board.
3. In the Navigation pane, select **PSTN ▶ DS1 Trunks**; the DS1 Trunks list is displayed.

38.4.1.1 Supported Actions

The following actions can be performed on the E1/T1 Trunk and are available in EMS when you right-click the specific trunk in the E1/T1 Trunks Status screen:

- **Lock** – take the trunk out-of-service and allow modification of its configuration (and specifically of Online configuration parameters); the synchronization with the remote PSTN side will be lost and corresponding voice and signaling traffic will be dropped; locked trunks will remain out-of-service even if the Media Gateway board is restarted (as a result of lock/unlock maintenance actions or board failure); use the Unlock action to restore service on locked trunks
- **Unlock** – return the trunk in-service.

- **Deactivate** – take the trunk out-of-service by raising AIS alarm; the synchronization with the remote PSTN side will be lost, but you will not be able to modify the Online configuration parameters of the trunk; use this action to temporarily stop service on the specific trunk when the Lock action is unavailable (e.g. when SS7 link is defined on the trunk); note however that service on the deactivated trunk will be restored when the Media Gateway board restarts (as a result of lock/unlock maintenance actions or board failure)
- **Activate** – restore service on the deactivated trunk.
- **D-Channel Switchover** – switch over from a primary enabled NFAS trunk to its backup enabled NFAS trunk. Both trunks should be unlocked, enabled and in the same NFAS Group.

38.4.1.2 Trunks Configuration

To connect the Mediant 8000 to the PSTN network, connect the proper PSTN cables to the TP-6310 or TP-8410 Media Gateway boards, as described in 'Connecting to the PSTN Network' on page 122. Change the configuration of the E1/T1 trunks to match the configuration on the remote PSTN side and unlock all the E1/T1 trunks that are actually connected.

➤ **To configure E1/T1 trunks on specific Media Gateway board:**

1. Access the DS1 Trunks List screen, as described above.
2. Select a DS1 Trunk and then in the configuration pane, click **Trunk Settings**; the Trunk Settings screen is displayed.
3. Modify parameters as described in the table 'Trunk Properties' below.



Note: Pay special attention to the **Framing Method Type** attribute in Trunk's configuration – it must match the **Protocol Type** attribute.

4. Click **Apply** to complete the configuration.
5. Unlock all trunks that are actually connected to the remote PSTN equipment, by selecting the corresponding trunks in the DS1 Trunks List screen and choosing **Unlock** in the Actions menu.
6. Verify that the trunk is successfully synchronized with the remote side and is ready for service by checking that its **Operational State** is *Enabled* (trunk will be colored **Green** in the EMS GUI).



Note: To minimize the amount of irrelevant traps and notifications, keep the disconnected and/or unsynchronized trunks locked.

Table 38-4: Trunk Properties

Parameter Name	Type	Provisioning Type	Description
Trunk Name	String Up to 20 chars.	Instant	Textual, user-defined name assigned to a trunk, enabling user to easily identify it.
Protocol Type	Enum None, E1 Euro ISDN, T1 CAS, T1 Raw CAS, T1 Transparent, E1 Transparent 31, E1 Transparent 30, E1 MFC R2, E1 CAS R2, E1 Raw CAS, T1 NI2 ISDN, T1 4ESS ISDN, T1 5ESS 9 ISDN, T1 5ESS 10 ISDN, T1 DMS100 ISDN, J1 Transparent, T1 NTT ISDN, E1 Austel ISDN, E1 Hkt ISDN, E1 Kor ISDN, T1 Hkt ISDN, E1 QSIG, E1 TNZ22, T1 QSIG, V5.2 AN, V5.2 LE, T1 IUA, E1 IUA, E1 French VN6 ISDN, E1 French VN3 ISDN, T1 Euro ISDN, T1 DMS100 Meridian ISDN, T1 NI1 ISDN, E1 DUA, E1 Q.931 Packets, T1 Q.931 Packets, E1 NI2 ISDN, E1 CAS R1.5, V5	Offline	Defines the PSTN protocol to be used for this trunk.

Parameter Name	Type	Provisioning Type	Description
Framing Method Type	Enum Extended Super Frame, Super Frame, E1 Framing DDF, E1 Framing MFF CRC4, E1 Framing MFF CRC4 Ext, T1 Framing F4, T1 Framing F12, T1 Framing ESF, T1 Framing ESF CRC6, T1 Framing F72, T1 Framing ESF CRC6 JT	Online	Defines the trunk's framing method, that should match the chosen Protocol Type.
Trace Level Type	Enum		
Line Build-Out Loss	Enum 0 db, 7.5 db, 15 db, 22.5 db	Instant	Defines line build-out loss to be used for this trunk.
Line Code	Enum B8ZS, AMI, HDB3	Instant	Use this parameter to select the line code type to be used for this trunk. B8ZS - use B8ZS line code (for T1 trunks only). AMI - use AMI line code. HDB3 - use HDB3 line code (for E1 trunks only). B8ZS or AMI is used for T1 spans; HDB3 or AMI is used for E1 spans.

38.5 Viewing Trunk Channels Status

The Trunk Channels status screen displays the status of all voice and signaling channels of all E1/T1 trunks of a specific Media Gateway board. It may be used to visualize the current E1/T1 trunks usage and signaling channels configuration.

➤ To view the Trunk Channel status screen:

1. Click  to access the Media Gateway screen.
2. Select the specific Media Gateway board.
3. In the Navigation pane, select **PSTN > Trunks Channels**; the Trunks Channels status screen is displayed.

Figure 38-6: Trunk Channels Status Screen

Trunks Channels Table																		
#	name	Alarm Name	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	 Trunk#1	Active																
2	 Trunk#2	Active																
3	 Trunk#3	Active																
4	 Trunk#4	Active																
5	 Trunk#5	Active																
6	 Trunk#6	Active																
7	 Trunk#7	LOS_LOF																
8	 Trunk#8	LOS_LOF																
9	 Trunk#9	LOS_LOF																
10	 Trunk#...	LOS_LOF																
11	 Trunk#...	Active																
12	 Trunk#...	Active																
13	 Trunk#...	Active																
14	 Trunk#...	Active																
15	 Trunk#...	Active																

Each row in the Trunk Channels Status screen consists of the following elements:

- Trunk number
- Icon that represents the operational status of each trunk
- Trunk name
- Trunk's PSTN alarm (if any)
- Icons that represent the PSTN configuration and status of the trunk's channels

The Trunk status icon, located to the left of the trunk name, is color-coded according to the trunk's operational state, administrative state and severity. This is a standard way that all objects (MOs) displayed in the EMS are color-coded. See 'Faults and Alarms Monitoring' on page 167 for detailed color-coding description.

The Trunk's PSTN alarm field displays the name of the PSTN alarm currently raised on the trunk (if such alarm exists). The field is color-coded as follows:

Table 38-5: Trunk PSTN Alarm

PSTN Alarm	Color
Disabled	Grey
Active	Green
RAI	Yellow
AIS	Blue
D-Channel Alarm	Orange
LOS/LOF	Red

Each trunk channel is represented by an icon that is color-coded according to the channel status and configuration as follows:

Table 38-6: Trunk Channel Status

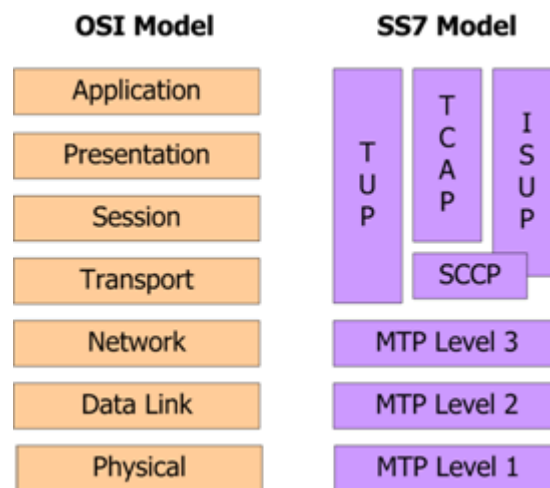
Channel Color	Channel Status
	Active
	Inactive
	Non-Voice
	SS7
	ISDN Signaling
	CAS Blocked

38.6 Configuring the SS7 Subsystem

Signaling System #7 (SS7) is a global standard for telecommunications defined by the ITU-T. The SS7 standard defines the procedures and protocols by which network elements in the public switched telephone network (PSTN) exchange information over a digital signaling network to effect wireless and wireline call setup, routing and control.

The hardware and software functions of the SS7 protocol are divided into functional abstractions called "levels". These levels are mapped to the OSI 7-layer model.

Figure 38-7: OSI Reference Model and SS7 Protocol Stack



SS7 messages are exchanged between network elements over bidirectional channels called **signaling data links**. Signaling occurs out-of band on dedicated channels rather than in-band on voice channels.

Each **signaling point (node)** in the SS7 network is uniquely identified by a numeric **point code**. Point codes are carried in signaling messages exchanged between signaling points to identify the source and destination of each message.

Each signaling point uses a routing table to select the appropriate signaling path for each message. The collection of signaling links between two adjacent nodes is known as **linkset**. The MTP3 automatically load shares between links within a linkset and re-routes traffic to a working link within the same linkset on a detection of failure.

MTP3 is also able to load share between two linksets that serve the same destination (through the use of intermediate nodes), the link sets here being contained within a **routeset**.

38.6.1 SIGTRAN (or UAL)

SIGTRAN (or UAL) is a set of protocols defined by IETF used to transport PSTN signaling messages over IP networks. The communication is performed between Signaling Gateway (SG) and Media Gateway Controller (MGC). The following UAL protocols specifically apply to SS7 networks:

- **M2UA** – used for backhauling of SS7 MTP2 user signaling messages
- **M3UA** – used for transport of SS7 MTP3 user signaling messages (such as ISUP and SCCP messages) between SG and MGC

38.6.2 Supported SS7 Architectures

The SS7 subsystem may be configured to support different SS7 network architectures. This flexibility allows Mediant 8000 to successfully interop with different 3rd party equipment and signaling networks.

Supported SS7 architecture types are:

- SS7 M2UA (SG Side) Architecture
- SS7 MTP3/M3UA Architecture
- SS7 M2TN Tunneling Architecture

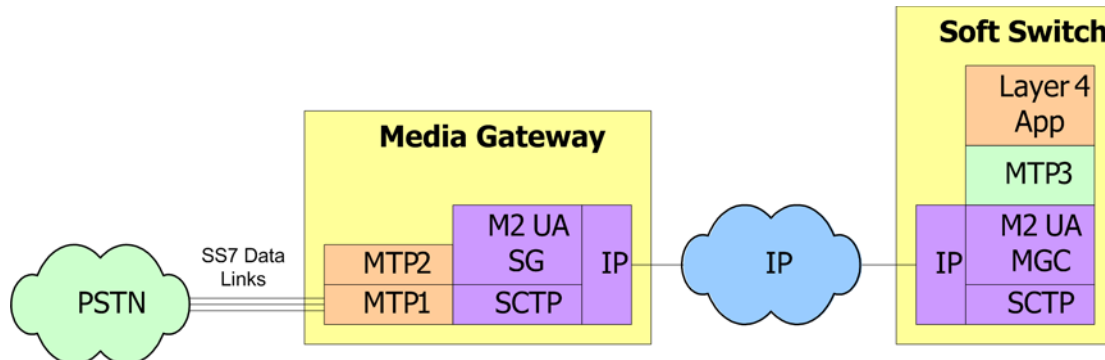


Note: Multiple SS7 and ISDN applications may be configured simultaneously on the same Media Gateway board (e.g. M2UA and IUA); however, when a redundant MTP3 application is configured (see Configuring the MTP3/M3UA Application), no other applications are supported.

38.6.2.1 SS7 M2UA (SG Side) Architecture

The Mediant 8000 is physically connected to the SS7 network. MTP2 traffic is backhauled to the SoftSwitch (or MGC) via IP network (M2UA).

Figure 38-8: SS7 M2UA (SG side) Architecture



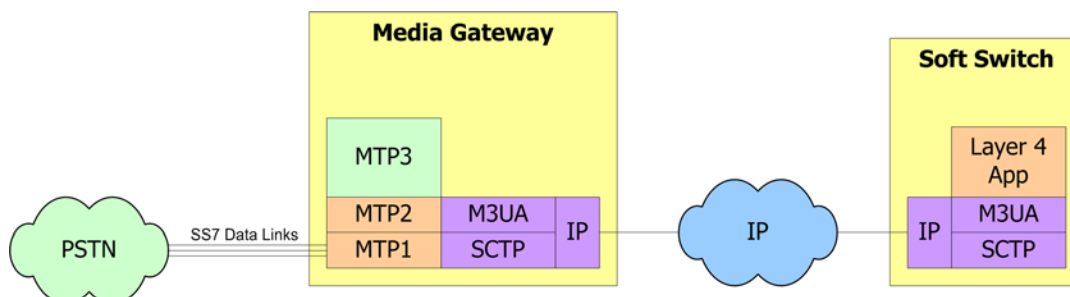
The Mediant 8000 has the following M2UA capabilities:

- Up to 64 SS7 Data Links per Media Gateway board
- Up to 84 UAL Interfaces per Media Gateway board
- Up to 3 UAL Groups per Media Gateway board

38.6.2.2 SS7 MTP3/M3UA Architecture

The Mediant 8000 is physically connected to the SS7 network. It processes MTP3 payload and sends upper application layers to the SoftSwitch (or MGC) via IP network (M3UA). In this architecture, contrary to the M2UA architecture, all SS7 network routing is accomplished by the Media Gateway.

Figure 38-9: SS7 MTP3/M3UA Architecture



The Mediant 8000 contains the following MTP3/M3UA capabilities:

- Up to 64 SS7 Data Links per Media Gateway board
- Up to 2 SS7 Nodes per Media Gateway board
- Up to 32 SS7 Linksets per SS7 Node
- Up to 30 SS7 Routesets per SS7 Node
- Up to 8 SS7 Linkset Links per SS7 Linkset

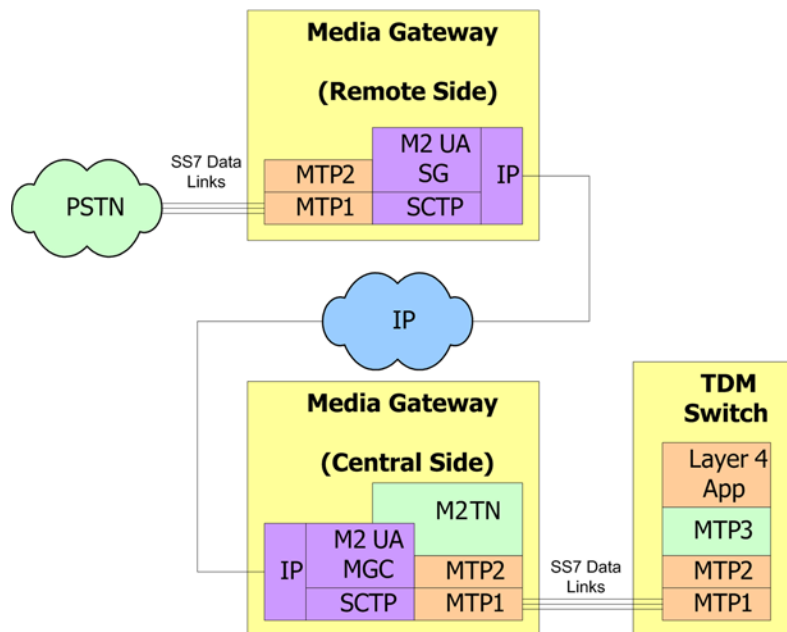
- Up to 4 SS7 Routes per SS7 Routeset
- Up to 16 UAL Groups per Media Gateway board (only 3 local SCTP ports are supported, however multiple UAL Groups may be defined on the same SCTP port)
- Up to 16 Routing Contexts per SS7 Node
- Multiple Media Gateway boards may be attached to the same MTP3 Group to improve redundancy of SS7 subsystem (For more information, see Section 'Configuring the MTP3/M3UA Application' on page 485).

38.6.2.3 SS7 M2TN Tunneling Architecture

M2TN tunneling is used for transferring **MTP2 signaling link** over IP network while both sides of the link are pure TDM sources, which are unaware of the IP tandem that is used in between them.

The solution is composed of two Media Gateway boards: one at the "remote" PSTN side and another one at the "central" SS7 TDM switch.

Figure 38-10: SS7 M2TN Tunneling Architecture



The Media Gateway at the "remote" PSTN side is configured as follows:

- MTP2 towards the PSTN network
- M2UA SG side towards the IP network (no proprietary extensions are needed)

The Media Gateway at the "central" SS7 TDM switch side is configured as follows:

- MTP2 towards the PSTN network
- M2UA MGC side towards the IP network

- AudioCodes proprietary M2TN application:
 - Transmits traffic from MTP2 to M2UA and vice versa
 - Controls the maintenance behavior of both sides according to the network and internal events

SCTP is used for increased reliability of data transmission over the IP network.

38.6.3 Configuring the M2UA (SG Side) Application

The following entities are relevant to the M2UA (SG side) application:

- **SS7 Data Link** – represents **MTP2 signaling link** connected to the PSTN network
- **UAL Groups** – represents **SCTP association** between the Media Gateway and the Softswitch
- **UAL Interface** – represents single **M2UA link** transferred over the SCTP association
- **MTP2Profile** – defines **MTP2 signaling link** timers and configuration

➤ To configure the M2UA (SG side) application:

1. Create and configure an SS7 Data Link for each signaling link connected to the PSTN network:
 - a. Click  to access the Media Gateway status screen.
 - b. Select the desired Media Gateway board.
 - c. In the Navigation pane, select **PSTN ► SS7 ► SS7 Data Links**; the SS7 Data Links list is displayed.
 - d. Use the  or  buttons to add or remove entries.
 - e. Select a specific row and then in the configuration pane, click **SS7 Data Link Settings**; the SS7 Data Link Settings screen is displayed.
 - f. Configure SS7 Data Link properties according to the tables, 'SS7 Data Link Properties - Data Link General Info Tab' below and 'SS7 Data Link Properties - Data Link MTP Tab' on page 479.
Make sure to configure **Layer2Type** as **MTP2** and **Layer3Type** as *M2UA*.
2. Create and configure an UAL Group for each **SCTP association** that is to be established with the SoftSwitch:
 - a. Click  to access the Media Gateway status screen.
 - b. Select the desired Media Gateway board.
 - c. In the Navigation pane, select **PSTN ► Sigtran ► UAL Groups**; the UAL Group list is displayed.
 - d. Use the  or  buttons to add or remove entries.
 - e. Select a specific row and then in the configuration pane, click **UAL Group Settings**; the UAL Group Settings screen is displayed.

- f. Configure the UAL Group properties according to the table 'UAL Group Properties' on page 480.

Make sure to configure **Protocol Type** as *M2UA* and **Functionality** as *SG*.

- 3. Create and configure a UAL Interface for each SS7 Data Link configured in step 1:

- a. Click  to access the Media Gateway Status screen.
- b. In the Status screen, select the desired Media Gateway board.
- c. In the Navigation pane, select **PSTN ► Sigtran ► UAL Interfaces**; the UAL Interfaces list is displayed.
- d. Use the  or  buttons to add or remove entries.
- e. Select a specific row and then in the configuration pane, click **UAL Interface Settings**; the UAL Interface Settings screen is displayed.
- f. Configure the UAL Interface properties according to the table 'UAL Interface Properties' on page 481.

Make sure to attach it to the UAL Group and SS7DataLink defined in the previous steps.

- 4. Bring all of the configured entities into service.

- a. Click  to access the Media Gateway Status screen.
- b. Select the specific Media Gateway board.
- c. If the Media Gateway board is not already unlocked, unlock it by clicking **Unlock** in the Actions bar. Wait until the board completes the restart and its **Operational State** is changed to *Enabled* (board will be color-coded *Green* in the EMS).
- d. In the Navigation Pane, select **PSTN ► Sigtran ► UAL Groups**.
- e. Unlock all of the UAL Groups configured in Step 2 by clicking **Unlock** in the Actions bar (you may skip this step if you did not previously unlock the Media Gateway board i.e. UAL Groups are automatically unlocked as part of the Media Gateway Board's Unlock action).
- f. In the Navigation Pane, select **PSTN ► Sigtran ► UAL Interfaces**.
- g. Unlock all of the UAL Interfaces defined in Step 3 by clicking **Unlock** in the Actions bar. The corresponding SS7 Data Links and E1/T1 Trunks are automatically unlocked as part of the UAL Interface Unlock action.
- h. Perform the corresponding configuration on the Signaling Gateway and/or Softswitch to which the Mediant 8000 is connected. Bring all configured entities in service.
- i. On the Mediant 8000, verify that the **Operational State** of all configured entities (i.e. UAL Group, UAL Interface, SS7 Data Link and E1/T1 Trunk) is *Enabled*.

Table 38-7: SS7 Data Link Properties - Data Link General Info Tab

Parameter Name	Type	Provisioning Type	Description
SS7 Link Name	String Up to 20 chars.	Offline_create	The textual, user-defined name assigned to the SS7 Data Link, enabling it to be identified intuitively and easily.
Layer 2 Type	Enum Mtp2, M2ua, Saal	Offline_create	Defines the Layer 2 entity as implemented by SS7 Data Link. - For the M2UA (SG side) and MTP3/M3UA applications, define the Layer 2 type as MTP2. - For the M2UA (MGC side) application, define the Layer 2 type as M2UA. - For the broadband SS7 (UMTS) application, define the Layer 2 type as SAAL.
Layer 2 Variant	Enum Itu, Ansi	Online	Defines the national variant of the Layer 2 protocol used by SS7 Data Link. The value must match the configuration on the remote PSTN side.
Layer 3 Type	Enum M2ua, Mtp3, M2tn	Offline_create	Defines the Layer 3 entity from/to which the SS7 Data Link transfers the data. - For the M2UA (SG side) application, define the Layer 3 type as M2UA - For MTP3/M3UA, M2UA (MGC side) and broadband SS7 (UMTS) applications, define the Layer 3 type as MTP3. - For the M2TN tunneling application, define the Layer 3 type as M2TN
Trace Level	Integer 0-1	Instant	The trace-level indication for the SS7 Link Layer protocols.

Table 38-8: SS7 Data Link Properties - Data Link MTP Tab

Parameter Name	Type	Provisioning Type	Description
Trunk ID	Integer 0-84	Online	Relevant for Layer2Type=MTP2 only. Defines the ID of the trunk used for carrying the SS7 signaling messages.
Time Slot Number	Integer 0-31	Online	Relevant for Layer2Type=MTP2 only. Defines the ID of the timeslot used for carrying the SS7 signaling messages.
MTP2 Profile ID	Integer 0-3	Online	Relevant for Layer2Type=MTP2 only. Defines the ID of the MTP2Profile that contains timers and basic MTP2 layer configuration for specific SS7 Data Link. Multiple SS7 Data Links may use the same MTP2 Profile.
Congestion Low Mark	Integer 0-255	Online	Relevant for Layer2Type=MTP2 only. Defines the low threshold of the congestion mark on the SS7 Data Link. When the transmit queue of a congested link contains less than the 'Low Mark' messages, a congestion condition no longer exists.
Congestion High Mark	Integer 0-255	Online	Relevant for Layer2Type=MTP2 only. Defines the high threshold of the congestion mark on the SS7 Data Link. When a link contains more than the 'High Mark' messages on the transmit queue, the link is congested.

Table 38-9: UAL Group Properties

Parameter Name	Type	Provisioning Type	Description
UAL Group Name	String Up to 20 chars.	Online	The textual, user-defined name assigned to the UAL Group, enabling it to be identified intuitively and easily.
Functionality	Enum Sg, Mgc	Online	Defines the Signaling Gateway (SG) or Media Gateway Controller (MGC) functionality of the UAL Group. - For the M2UA (SG side) application, define the functionality as SG. - For the M2UA (MGC side) application, define the functionality as MGC. - For the MTP3/M3UA and broadband SS7 (UMTS) applications, define the functionality according to the remote side configuration (typically the remote side is configured as an MGC and therefore UAL Group is configured as SG.)
UAL Type	Enum Iua, M2ua, M3ua, M2tn, Dua	Online	Defines the application type of UAL Group. For the M2UA (SG and MGC side) application, define the UAL Type as M2UA. - For MTP3/M3UA application, define the UAL Type as M3UA - For M2TN tunneling application define it as M2TN - For the IUA application, define the UAL Type as IUA " For the DUA application, define the UAL Type as DUA
Traffic Mode	Enum Override, Loadshare, Broadcast	Online	Defines the UAL Group SCTP traffic mode. Only Override mode is currently supported.
Recovery Timer (Tr)	Integer 0-10000000	Online	Defines the SCTP Recovery Timer (Tr).
Ack Timer (Tack)	Integer 0-10000000	Online	Defines the SCTP Acknowledge Timer (Tack).
Heartbeat Timer (Tbeat)	Integer 0-10000000	Online	Defines the SCTP Heartbeat Timer (Tbeat).

Parameter Name	Type	Provisioning Type	Description
Behavior Type	Enum Default(0), FixedRoutingContext(512)	Online	Defines the internal SCTP protocol implementation. - For standard RFC-compliant implementation, define the Behavior Type as Default - For Draft2-compliant implementation, define the Behavior Type as FixedRoutingContext.
SCTP Port number	Integer 0-65535	Online	Defines the local IP port used by the SCTP associations. Each UAL Group on the Media Gateway Board must have a unique local SCTP port. SCTP port 2905 is reserved for the M3UA application. Use port 2904 or any other port for the M2UA or M2TN application.
M3UA Variant	Enum Itu, Ansi, China	Online	Relevant for UALType=M3UA only. Defines the national M3UA variant. It must match configuration on the remote IP side.

Table 38-10: UAL Interface Properties

Parameter Name	Type	Provisioning Type	Description
UAL Interface Name	String Up to 20 chars.	Online	The textual, user-defined name for the UAL Interface, enabling it to be identified intuitively and easily.
UAL Group ID	Integer 1-16	Online	Defines the UAL Group to which this UAL Interface belongs.
Interface Number	Integer 0-2147483647	Online	Defines the Interface Number (Interface ID) of the M2UA signaling link represented by the UAL Interface.
Select SS7 Data Link ID (M2UA)	Integer 0-32	Online	Relevant for the M2UA (SG and MGC side) application only. Defines the ID of the MTP2 SS7 Data Link with which this UAL Interface is associated.
Select Trunk (IUA/DUA)	Integer 0-63	Online	Relevant for the IUA and DUA application only. Defines the ID of the Trunk with which this UAL Interface is associated.

Parameter Name	Type	Provisioning Type	Description
Select SS7 Node ID (M3UA)	Integer 0-4	Online	Relevant for the MTP3/M3UA application only. Defines the ID of the SS7 Node with which this UAL Interface is associated.

38.6.3.1 M2UA (SG Side) Operational Status

The Operational status of the M2UA (SG side) application may be determined by inspecting the Operational Status of the following entities:

- Trunk – indicates status of the MTP1 link layer
- SS7 Data Link – indicates status of the MTP2 link layer

38.6.3.2 Online Provisioning

The configuration of the M2UA (SG side) application may be modified online.

See 'Configuring the M2UA (SG Side) Application' on page 476 for the full list of entities that must be configured and specific parameters' description and provisioning policies.

LOCK/UNLOCK operations may be performed on both M2UA SS7 DataLinks and UAL Interfaces. The Administrative state of both entities is always synchronized.

Some of the SS7 Data Link parameters are of the **Offline_create** provisioning type. To modify them, either lock the Media Gateway board or delete the SS7 Data Link and define a new one.

The M2UA entities in the UALInterface and SS7DataLink tables are linked one to another. When you delete a UAL Interface entity, the entity in the SS7DataLink table is deleted as well and vice-versa.

38.6.3.3 Redundant Configuration

The M2UA (SG side) application is partially supported by the Media Gateway board redundancy mechanism.

To achieve redundancy of the M2UA (SG side) application, distribute signaling links of each routeset across at least 2 different Media Gateway boards and configure the latter for Hot redundancy. If the Media Gateway board fails, the redundant board will become active and SCTP associations will be dropped. Consequently, the M2UA links will go out of service.

It is SoftSwitch's responsibility to identify this failover, re-establish SCTP associations, re-activate ASPs and re-establish the M2UA interfaces. When all of the above events occur, M2UA signaling links will return to service.

Nevertheless active calls should not be affected by the above-mentioned scenario, because the SS7 linkset will remain in service, since it is also comprised of the other links (on other boards) that remain in service.

38.6.3.4 Advanced Configuration

Additional parameters and timers of MTP2 **signaling links** may be configured via MTP2 Profile. The default MTP2 Profile contains all default settings as specified in the ITU standard. In a typical configuration, all SS7 Data Links are attached to the same MTP2 Profile.

You can create additional MTP2 Profiles and attach them to specific SS7 Data Links. Or, alternatively, you can modify the existing MTP2 Profile configuration.

Table 38-11: MTP2 Profile Properties

Parameter Name	Type	Provisioning Type	Description
MTP2 Profile Name	String Up to 20 chars.	Online	Defines the name of the MTP2 Profile, enabling user to easily identify it.
SS7 MTP-2 Link Rate	Enum D56kbps(56), A64kbps(64)	Online	Defines the MTP2 Link Rate.
Error Correction Method	Enum Basic(0), PCRC(1)	Online	Defines the error correction method – Basic or Preventive Cyclic Retransmission. Refer to ITU-T Q.703 for details.
SUERM Threshold (T)	Integer 0 – 255	Online	Defines the Signal Unit Error Rate Monitor (SUERM) Threshold (T) – the number of consecutive signal units received in error that will cause an error rate high indication. Refer to ITU-T Q.703 for details.
Lowest SU Error Rate (D)	Integer 0 – 256	Online	Defines the D, where the lowest signal unit error rate - which is 1/D (signal unit errors/signal unit) - will ultimately cause an error rate high indication. Refer to ITU-T Q.703 for details.
# Octets Received (N)	Integer 0 – 256	Online	Defines the number of octets received while in octet counting mode. Refer to ITU-T Q.703 for details.
Norm ER Threshold (Tin)	Integer 0 – 20	Online	Defines the Normal ER Threshold (Tin) - that a specific proving period is aborted. Refer to ITU-T Q.703 for details.
Emergency ER Threshold (Tie)	Integer 0 – 10	Online	Defines the Emergency Threshold (Tie) - that a specific proving period is aborted. Refer to ITU-T Q.703 for details.

Parameter Name	Type	Provisioning Type	Description
# Aborts Before OOS (M)	Integer 0 – 10	Online	Defines the number of aborted proving attempts before sending an out-of-service indication to Layer 3. Refer to ITU-T Q.703 for details. Note that the proving attempts is part of the process of establishing a connection between two points in an SS7 network.
Alignment Ready Timer (T1)	Integer 0 – 100000	Online	Defines the Alignment Ready timer (T1). Refer to ITU-T Q.703 for details.
Not Aligned Timer (T2)	Integer 0 – 200000	Online	Defines the Not Aligned timer (T2). Refer to ITU-T Q.703 for details.
Aligned Timer (T3)	Integer 0 – 20000	Online	Defines the Aligned timer (T3). Refer to ITU-T Q.703 for details.
Normal Proving Period (T4n)	Integer 0 – 15000	Online	Defines the Normal Proving Period (T4n). Refer to ITU-T Q.703 for details.
Emergency Proving Period (T4e)	Integer 0 – 5000	Online	Defines the Emergency Proving Period (T4e). Refer to ITU-T Q.703 for details.
Sending SIB Timer (T5)	Integer 0 – 2400	Online	Defines the Sending SIB Timer (T5). Refer to ITU-T Q.703 for details.
Remote Congestion Timer (T6)	Integer 0 – 10000	Online	Defines the Remote Congestion Timer (T6). Refer to ITU-T Q.703 for details.
Excess Ack Delay Timer (T7)	Integer 0 – 5000	Online	Defines the Excess Ack Delay Timer (T7). Refer to ITU-T Q.703 for details.
LSSU Length	Integer 1 – 2	Online	Defines the LSSU length in bytes. Refer to ITU-T Q.703 for details.
PCR N2	Integer 0 – 512	Online	Defines Preventive Cyclic Retransmission - the number of message signal unit octets available for retransmission. Refer to ITU-T Q703 for details.

38.6.4 Configuring the MTP3/M3UA Application

The following entities are relevant to the MTP3/M3UA application:

- **SS7 Data Link** – represents the MTP2 **signaling link** connected to the PSTN network
- **MTP3Group** – represents the complete MTP3 configuration applied to specific Media Gateway board
- **SS7Node** – represents the **signaling node** in the SS7 network
- **SS7Linkset** – represents a collection of **signaling links** between the Media Gateway board and the **adjacent** signaling node
- **SS7Routeset** – represents a collection of **routes** (essentially **linksets**) that constitute a routing path between the Media Gateway board and the **destination** signaling node
- **SS7LinksetLink** – represents properties of a specific **signaling link** as part of the specific **linkset**
- **SS7Route** – represents properties of a specific **linkset** as part of the specific **routeset**
- **UAL Group** – represents the **SCTP association** between the Media Gateway and the Softswitch
- **M3UA Routing Group and Context** – defines **routing rules** for M3UA messages based on their source point code and service indicator. For example, you may define that all M3UA messages from OPC 0xA will be routed to ASP 1, while messages from OPC 0xB will be routed to ASP 2.
- **MTP2Profile** – defines the **MTP2 signaling link** timers and configuration
- **SS7NodeTimers** – defines the **signaling node** timers
- **SS7LinksetTimers** – defines the **linkset** timers

This simplest configuration contains minimum redundancy capabilities. For full redundancy configuration capabilities, see **Redundant Configuration on page 499**.

➤ To configure the MTP3/M3UA application:

1. Create and configure an SS7 Data Link for each **signaling link** connected to the PSTN network:
 - a. Click  to access the Media Gateway status screen.
 - b. Select the desired Media Gateway board.
 - c. In the Navigation pane, select **PSTN ► SS7 ► SS7 Data Links**; the SS7 Data Links list is displayed.
 - d. Use the  or  buttons to add or remove entries.
 - e. Select a specific row and then in the configuration pane, click **SS7 Data Link Settings**; the SS7 Data Link Settings screen is displayed.
 - f. Configure SS7 Data Link properties according to the tables 'SS7 Data Link Properties - Data Link General Info Tab' and 'SS7 Data Link Properties - Data Link MTP Tab'.

Make sure to configure **Layer2Type** as **MTP2** and **Layer3Type** as **MTP3**.

2. Create a new MTP3 Group and configure it:
 - a. Click  to access the Media Gateway status screen.
 - b. In the Navigation pane, select PSTN ► SS7 MTP3; the MTP3 Groups list is displayed.
 - c. Use the  or  buttons to add or remove entries.
 - d. Select a specific row and then in the configuration pane, click **MTP3 Group Settings**; the MTP3 Group Settings screen is displayed.
 - e. Configure MTP3 Group properties according to the table 'MTP3 Group Properties'.
3. Stop the service on the Media Gateway board:
 - a. Click  to access the Media Gateway status screen.
 - b. Select the desired Media Gateway board.
 - c. Stop the service on the Media Gateway board by clicking **Lock** in the Actions bar.
4. Attach the Media Gateway board to the MTP3 Group.
 - a. In the Navigation Pane, select **PSTN** and then in the configuration pane, click **PSTN Settings**; the PSTN Settings screen is displayed.
 - b. In the **SS7 Settings** tab, configure **MTP3 Group** parameter to match the the specific MTP3 Group as configured in the step 2. See 'Media Gateway Board's MTP3/M3UA Properties'.
5. Create a new SS7 Node and configure it.
 - a. Click  to access the Media Gateway status screen.
 - b. In the Navigation pane, select **PSTN ► SS7 MTP3**; the MTP3 Groups list is displayed.
 - c. Select the MTP3 Group created in step 2.
 - d. In the Navigation pane, select **SS7 Nodes**; the SS7 Nodes list is displayed.
 - e. Use the  or  buttons to add or remove entries.
 - f. Select a specific row and then in the configuration pane, click **SS7 Node Settings**; the SS7 Node Settings screen is displayed.
 - g. Configure the SS7 Node properties according to the table 'SS7 Node Properties'.
6. Restore service on the Media Gateway board.
 - a. Click  to access the Media Gateway status screen.
 - b. Select the desired Media Gateway board.
 - c. Restore service on the Media Gateway board by clicking **Unlock** in the Actions bar.
 - d. Wait till the Media Gateway board completes restart and its **Operational State** becomes *Enabled* (board will be color-coded Green in the EMS).

7. Create and configure an SS7 Linkset for each **adjacent SS7 signaling node**.
 - a. In the Navigation pane, select the SS7 Node configured in step 5.
 - b. In the Navigation pane, select **SS7 Linksets**; the SS7 Linksets list is displayed.
 - c. Use the  or  buttons to add or remove entries.
 - d. Select a specific row and then in the configuration pane, click **SS7 Linkset Settings**; the SS7 Linkset Settings screen is displayed.
 - e. Configure the SS7 Linkset properties according to the table 'MT3/M3UA - SS7 Linkset Properties'. Make sure to provision the point code of **adjacent SS7 signaling node** as Destination Point Code (DPC).
8. Create and configure an SS7 LinksetLink for each SS7 Data Link configured in step 1. Each **signaling link** should be attached to the specific SS7 Linkset (that is associated with **adjacent SS7 signaling node**).



Note: Each SS7 Data Link can be attached to one SS7 Linkset only.

- a. In the Navigation pane, select the SS7 Linkset configured in step 7.
 - b. In the Navigation pane, select the SS7 Linkset Links; the SS7 Linkset Links list is displayed.
 - c. Use the  or  buttons to add or remove entries.
 - d. Select a specific row and then in the configuration pane, click **SS7 Linkset Link Settings**; the SS7 Linkset Link Settings screen is displayed.
 - e. Configure SS7 Linkset Link properties according to the table 'MTP3/M3UA - SS7 Linkset Link Properties'. Make sure to attach it to the **SS7 Data Link** configured in step 1.
9. Create and configure an SS7 Routeset for each **destination SS7 signaling node**.
 - a. In the navigation pane, select the SS7 Node configured in step 5.
 - b. In the Navigation pane, select **SS7 Routesets**; the SS7 Routesets list is displayed.
 - c. Use the  or  buttons to add or remove entries.
 - d. Select a specific row and then in the configuration pane, click **SS7 Routeset Settings**; the SS7 Routeset Settings screen is displayed.
 - e. Configure the SS7 Routeset properties according to the table 'MTP3/M3UA - SS7 Routeset Properties'. Make sure to provision the point code of **destination SS7 signaling node** as Destination Point Code (DPC).

10. Determine all possible routing paths to the **destination SS7 signaling node** and configure SS7 Routes for each alternative **adjacent SS7 signaling node** that may be used for reaching the destination.



Note: Each SS7 Linkset can be attached to more than one SS7 Routeset.

- a. In the Navigation pane, select the SS7 Routeset configured in step 9.
 - b. In the Navigation pane, select **SS7 Routes**; the SS7 Routes list is displayed.
 - c. Select a specific row and then in the configuration pane, click **SS7 Route Settings**; the SS7 Route Settings screen is displayed.
 - d. Configure the SS7 Route properties according to the table 'MTP3/M3UA - SS7 Route Properties'. Make sure to attach it to the SS7 Linkset configured in step 7.
11. Create and configure an M3UA Routing Group and Context that defines **routing rules** for M3UA messages based on their source point codes and service indicators.
 - a. Click  to access the Media Gateway Status screen.
 - b. Select the desired Media Gateway board.
 - c. In the Navigation pane, select **PSTN ► SS7 ► M3UA Routing Groups**; the M3UA Routing Group list is displayed.
 - d. Use the  or  buttons to add or remove entries.
 - e. Select a specific row and in the Navigation pane select M3UA Routing Contexts; the M3UA Routing Contexts list is displayed.
 - f. Use the  or  buttons to add or remove entries.
 - g. Select a specific row and then in the configuration pane, click **M3UA Routing Context Settings**; the M3UA Routing Context Settings screen is displayed.
 - h. Configure the M3UA Routing Context properties according to the table 'M3UA Routing Context Properties'.
 12. Create and configure the UAL Group for each **SCTP association** that is established with the SoftSwitch.
 - a. Click  to access the Media Gateway Status screen.
 - b. Select the desired Media Gateway board.
 - c. In the Navigation pane, select **PSTN ► Sigtran ► UAL Groups**; the UAL Group list is displayed.
 - d. Use the  or  buttons to add or remove entries.
 - e. Select a specific row and then in the configuration pane, click **UAL Group Settings**; the UAL Group Settings screen is displayed.

- f. Configure the UAL Group properties according to the table 'UAL Group Properties'. Make sure to configure **Protocol Type** as **M3UA** and attach the **SS7 Node** configured in step 1 and M3UA Routing Group configured in step 11.

13. Bring all of the configured entities into service.

- a. Click  to access the Media Gateway Status screen.
- b. In the Navigation pane, select **PSTN** and then select the SS7 Node configured in step 5.
- c. In the Actions bar, click **Recursive Unlock**.

This operation affects all MTP3-related MOs that were configured in the previous steps:

- ◆ SS7 DataLink
- ◆ SS7 Node
- ◆ SS7 Linkset
- ◆ SS7 Routeset

SS7 LinksetLink SS7 Route One of the following event occur:

- ◆ If the Media Gateway board is locked, the action causes these MOs to be unlocked as soon as Media Gateway board is unlocked.
- ◆ If the Media Gateway board is unlocked, the action immediately unlocks all of the MOs.



Note:

- The **Recursive Unlock** operation may fail if the configuration of some of the MTP3 entities is inconsistent. If this occurs, correct the configuration and repeat the operation.
- Instead of performing the **Recursive Unlock** operation on the SS7 Node, you may also perform a regular Unlock operation on all relevant MOs according to the SS7 MOs' hierarchy, i.e. : SS7 Data Links, SS7 Linksets, SS7 Routesets, UAL Groups.

- d. In the Navigation pane, select the corresponding Media Gateway board.
 - e. If the Media Gateway board is not already unlocked, in the Actions bar, click **Unlock**. Wait until the board completes the restart and its **Operational State** changes to *Enabled* (board will be color-coded *Green* in the EMS).
 - f. In the Navigation Pane, select **PSTN ► Sigtran ► UAL Groups**.
 - g. Unlock all of the UAL Groups configured in Step 12 by clicking **Unlock** in the Actions bar. This step may be skipped if you unlocked the Media Gateway board beforehand, as UAL Groups are automatically unlocked as part of the Media Gateway Board's unlock action.
14. Perform the corresponding configuration on the Signaling Gateway and/or Softswitch to which the Mediant 8000 is connected. Bring all configured entities in service.

15. On the Mediant 8000, verify that the **Operational State** of all configured entities (i.e. SS7 Node, SS7 Linkset, SS7 Routeset, SS7 Data Link, UAL Group and E1/T1 Trunk) is *Enabled*.

Table 38-12: MTP3 Group Properties

Parameter Name	Type	Provisioning Type	Description
Mtp3 Group Name	String Up to 20 chars.	Instant	The textual, user-defined name for the SS7 MTP3 Group, enabling it to be identified intuitively and easily.
Redundancy Mode	Enum none, dualCpu	Online	Defines the Redundancy mode. For a simple configuration, where only one Media Gateway board is associated with the MTP3 Group, define the Redundancy Mode as <i>none</i>. In this configuration, the MTP3/M3UA application does not survive the Media Gateway boards' switchover (All MTP3 entities go out of service.) ▪ For a redundant MTP3 configuration, where two Media Gateway boards are associated with the same MTP3 Group and signaling node is distributed across both boards, define the Redundancy Mode as <i>dualCpu</i>. In this configuration the MTP3/M3UA application is preserved during Media Gateway boards' switchover/switchback.

Table 38-13: SS7 Node Properties

Parameter Name	Type	Provisioning Type	Description
SS7 Node Name	String Up to 20 chars.	Offline_create	The textual, user-defined name for the SS7 Node, enabling it to be identified intuitively and easily.
Network Type	Enum Narrowband, Broadband	Offline	Defines the SS7 network type. - For the MTP3/M3UA application, define the Network Type as narrowband - For the Broadband SS7 (UMTS) configuration, define the Network Type as broadband. For narrowband SS7 Node only, the MTP2 signaling links are supported. For broadband SS7 Node only, the SAAL signaling links are supported.
Variant	Enum Itu, Ansi, China	Offline	Defines the international or national MTP3 variant.
Originating PC	String Up to 20 chars.	Offline	Defines the signaling point code of the SS7 Node. It can be specified in numeric (e.g., 15) or X-Y-Z (e.g., 0-1-1) formats. The ANSI point code uses 24-bits. It consists of three octets – network, cluster and member. An octet is an 8-bit byte which can contain any value between 0 and 255. The ITU point code uses 14 bits. It is a pure binary number that may be stated in terms of zone (3 bits), area/network (8 bits) and signaling point identification (3 bits) numbers. The China point code uses 24-bits and is incompatible with both ANSI and ITU networks.
Network Indicator	Enum International, InternationalSpare, National, NationalSpare	Offline	Defines the network indicator.
Routing Functionality	Enum Sp, Stp	Offline	Defines the routing functionality of the SS7 Node – Signaling Point (SP) or Signal Transfer Point (STP).

Parameter Name	Type	Provisioning Type	Description
MSU Window	Integer 0-255	Offline	Defines the number of Message Signal Units (MSUs) on a congested routeset between 2 congestion indications.
SS7 Node Timers ID	Integer 1-3	Offline	Defines the ID of the SS7 Node Timers profile that contains timers and basic MTP3 layer configuration for specific SS7 Node. Multiple SS7 Nodes can use the same SS7 Node Timers profile.
ISUP Layer 4 App	Enum None, Ual	Offline	Defines the Layer 4 application to which the ISUP messages are transferred. For example: to transfer an ISUP payload to the MGC via M3UA link, define this parameter as UAL. If the payload-specific Layer 4 App equals none, the payload is discarded.
SCCP Layer 4 App	Enum None, Ual	Offline	Defines the Layer 4 application to which the SCCP messages are transferred.
BISUP Layer 4 App	Enum None, Ual	Offline	Defines the Layer 4 application to which the BISUP messages are transferred.
ALCAP Layer 4 App	Enum None, Ual, Alcap	Offline	Defines the Layer 4 application to which the ALCAP messages are transferred. - None – ALCAP payload is discarded - UAL – ALCAP payload is forwarded to the remote entity via UAL - ALCAP – ALCAP payload is locally processed on the Media Gateway board

Table 38-14: SS7 Linkset Properties

Parameter Name	Type	Provisioning Type	Description
SS7 Link Set Name	String Up to 20 chars.	Offline_create	The extual, User-defined name for the SS7 Linkset, enabling it to be identified intuitively and easily.
Destination PC	String Up to 20 chars.	Online	Defines the point code of the adjacent signaling node that this linkset connects with. Can be specified in numeric (e.g., 15) or X-Y-Z (e.g., 0-1-1) formats. The ANSI point code uses 24-bits. It consists of three octets – network, cluster and member. An octet is a 8-bit byte which can contain any value between 0 and 255. The ITU point code uses 14 bits. It is a pure binary number that may be stated in terms of zone (3 bits), area/network (8 bits) and signaling point identification (3 bits) numbers. The China point code uses 24-bits and is incompatible with both ANSI and ITU networks.
Linkset Timers ID	Integer 1-3	Offline_create	Defines the ID of the SS7 Linkset Timers profile that contains timers and basic MTP3 layer configuration for a specific SS7 Node. Multiple SS7 Linksets can use the same SS7 Linkset Timers profile.
Link Mask	Integer 0-255	Online	Defines the SS7 Linkset mask, to select a signaling link on the basis of the MTP3 SLS/SLC field.
Alternate Link Mask	Integer 0-255	Online	Defines the alternate SS7 Linkset mask to select an alternate signaling link set on the basis of the field MTP3 SLS/SLC. Note: This calculates an inner link index which may not be the same as the actual chosen link. It is recommended to set the value of this field to: 255 - link mask.

Table 38-15: SS7 Routeset Properties

Parameter Name	Type	Provisioning Type	Description
SS7 Route Set Name	String Up to 20 chars.	Offline_create	The textual, User-defined name for the SS7 Routeset, enabling it to be identified intuitively and easily.
Destination PC	String Up to 20 chars.	Offline_create	Defines the point code of the destination signaling node with which this routeset connects. It can be specified in numeric (e.g., 15) or X-Y-Z (e.g., 0-1-1) formats. The ANSI point code uses 24-bits. It consists of three octets – network, cluster and member. An octet is a 8-bit byte which can contain any value between 0 and 255. The ITU point code uses 14 bits. It is a pure binary number that may be stated in terms of zone (3 bits), area/network (8 bits) and signaling point identification (3 bits) numbers. The China point code uses 24-bits and is incompatible with both ANSI and ITU networks.
Route Mask	Integer 0-255	Online	Defines the mask used to select the SS7 Route / Linkset on the basis of the field SLS/SLC.

Table 38-16: SS7 Linkset Link Properties

Parameter Name	Type	Provisioning Type	Description
Board ID	Integer 0-19	Offline_create	Defines the ID (slot number) of the Media Gateway board where the SS7 Data Link is defined.
SS7 Link ID	Integer 0-32	Offline_create	Defines the ID of the SS7 Data Link.
MTP3 SLS/SLC	Integer 0-15	Offline_create	Defines the SLS/SLC number for this SS7 signaling link, for MTP3 outgoing link selection.

Table 38-17: SS7 Route Properties

Parameter Name	Type	Provisioning Type	Description
SS7 Link Set ID	Integer 0-16	Offline_create	Defines the ID of the SS7 Linkset.
Link Set Priority	Integer 0-255	Offline_create	Defines the priority of the route within the routeset.

Table 38-18: XE "M3UA Routing Context Properties" M3UA Routing Group Properties

Parameter Name	Type	Provisioning Type	Description
Routing Group Name	String Up to 40 chars	Instant	Defines the name of M3UA Routing Group enabling user to easily identify it.
Half-Board ID	Enum TPM1, TPM2	Online	Only relevant for TP-1610 boards. Defines the ID of the Media Gateway board's CPU module in which the Routing Group is defined. Must match the Half-Board ID of the attached UAL Group.
Referenced By	String Up to 255 chars.	Read-Only	Indicates UAL Groups associated with this M3UA Routing Group.

Table 38-19: M3UA Routing Context Properties

Parameter Name	Type	Provisioning Type	Description
SS7 Node ID	Integer 0-4	Online	Defines the ID of the SS7 Node with which this M3UA Routing Context is associated.
Alias Point Code ID	Integer 0 – 2	Online	If set to 0 (default), an M3UA Routing Context is associated with the SS7 Node itself. If set to a positive value, defines the ID of the SS7 Alias Point code with which this M3UA Routing Context is associated.

Parameter Name	Type	Provisioning Type	Description
OPC 1	String Up to 20 chars.	Online	Defines the 1st filter Originating Point Code. MTP3 messages that originate at a specific point code will be associated with this M3UA Routing Context. An empty value means that the filter is deactivated. Can be specified in numeric (e.g. 15) or X-Y-Z (e.g. 0-1-1) formats. ANSI point code uses 24-bits. It consists of three octets - network, cluster and member octet. An octet is a 8-bit byte which can contain any value between 0 and 255. ITU point code uses 14 bits. It is a pure binary number that can be stated in terms of zone (3 bits), area/network (8 bits) and signaling point identification (3 bits) numbers. China point code uses 24-bits and is incompatible with both ANSI and ITU networks.
OPC 2	String Up to 20 chars.	Online	Defines 2nd filter Originating Point Code. MTP3 messages that originate at specific point code will be associated with this M3UA Routing Context. An empty value means that the filter is deactivated.
OPC 3	String Up to 20 chars.	Online	Defines 3rd filter Originating Point Code. MTP3 messages that originate at a specific point code will be associated with this M3UA Routing Context. An empty value means that the filter is deactivated.
OPC 4	String Up to 20 chars.	Online	Defines 4th filter Originating Point Code. MTP3 messages that originate at a specific point code will be associated with this M3UA Routing Context. An empty value means that the filter is deactivated.
Service Indicator 1	Enum none,0-15	Online	Defines the 1st filter Service Indicator. MTP3 messages that match a specific SI will be associated with this M3UA Routing Context. The value 'none' means that the filter is deactivated.

Parameter Name	Type	Provisioning Type	Description
Service Indicator2	Enum none,0-15	Online	Defines the 2 nd filter Service Indicator. MTP3 messages that match a specific SI will be associated with this M3UA Routing Context. The value 'none' means that the filter is deactivated.
Service Indicator 3	Enum none,0-15	Online	Defines the 3 rd filter Service Indicator. MTP3 messages that match a specific SI will be associated with this M3UA Routing Context. The value 'none' means that the filter is deactivated.
Service Indicator 4	Enum none,0-15	Online	Defines the 4 th filter Service Indicator. MTP3 messages that match a specific SI will be associated with this M3UA Routing Context. The value 'none' means that the filter is deactivated.

Table 38-20: Media Gateway Board's MTP3/M3UA Properties

Parameter Name	Type	Provisioning Type	Description
MTP3 Group	Integer 0 – 15	Online	Defines index of the SS7 MTP3 Group that this Media Gateway board belongs to. When set to 0 - no MTP3 application is defined.
SS7 M3UA Traffic Behavior	Enum None, Deactivate, SIPO	Online	Defines the M3UA behavior when the SS7 links are up, but there is no association to the soft switch. none – no special behaviour deactivate – deactivate (busy) links SIPO – put links in Local Processor Outage (LPO) state

38.6.4.1 MTP3/M3UA Operational Status

The Operational Status of the MTP3/M3UA application may be determined by inspecting the Operational Status of the following entities:

- Trunk – indicates status of the MTP1 link layer
- SS7 Data Link – indicates status of the MTP2 link layer
- SS7 Linkset – indicates status of the SS7 Linkset
- SS7 Routeset – indicates status of the SS7 Routeset
- SS7 Node – indicates status of the SS7 Node

38.6.4.2 Online Provisioning

The configuration of the MTP3/M3UA application can be modified online.

See the 'Configuring the MTP3/M3UA Application' on page 20 for the full list of entities that must be configured and the specific parameter descriptions and provisioning policies.

The LOCK/UNLOCK operations are not supported on the MTP3 Group and SS7 Node. Perform the operation on the Media Gateway board. In particular, when you define a new SS7 Node, you must lock/unlock the Media Gateway board to bring the SS7 Node into service (unlock it).

Due to hierarchical and cross-reference dependencies between MTP3 application entities (SS7 Node, SS7 Routeset, SS7 Linkset and SS7 Data Link), specific maintenance operations must be performed in the following order:

- Unlock of SS7 Linkset and Routeset is not allowed when a SS7 Node is locked.
- Unlock of SS7 Linkset is not allowed when no SS7 Data Links are attached to it (via use of SS7 LinksetLink MOs) and vice versa.

To simplify the online configuration, lock/unlock operations are not supported on “virtual connector” MOs, namely SS7 Linkset Link and SS7 Route. Use lock/unlock actions on SS7 Data Link and SS7 Linksets instead.

Since the MTP3/M3UA application involves many configuration entities, ensure that while performing the online configuration, you unlock all newly defined entities to bring the application to service. Consider use of “Recursive Unlock” action on the SS7 Node instead of performing “Unlock” action on the SS7 Node, SS7 Routeset, SS7 Linkset and SS7 Data Link. Note, however, that the use of an “Unlock” action on specific MO provides better control of the configuration and a more simple way of correcting configuration errors.

Some of the configuration parameters (e.g. in SS7 Data Link and SS7 Linkset entities) have the **Offline_create** provisioning type. To modify them, either lock the Media Gateway board or delete the entity (e.g. SS7 Data Link or SS7 Linkset) and define a new entity.

38.6.4.3 Redundant Configuration

The MTP3/M3UA application in its simplest form (as described above) is not fully supported by the Media Gateway redundancy mechanism. Even if the Media Gateway board is configured for Hot redundancy, the MTP3/M3UA application is not fully recovered on a redundant Media Gateway board after the Media Gateway board switchover/switchback takes place. The MTP3 entities go out of service and then it takes some time (typically up to a minute) before the service is restored. All SS7 signaling is dropped and calls may be closed by the MGC/Softswitch (depending on their configuration).

In addition, the SCTP associations are dropped during the Media Gateway board switchover and MGC should be responsible for re-establishing the SCTP associations.

To overcome this limitation, the Redundant MTP3 Group configuration was developed.

The **Redundant MTP3 Group** configuration enables Hot redundancy for the MTP3/M3UA application. In this configuration, a **Signaling node** is distributed across multiple Media Gateway boards. The **Signaling links** can be defined on any of the Media Gateway boards that belong to the **Redundant MTP3 Group**.



Note: Up to two Media Gateway boards can be attached to the same **Redundant MTP3 Group**.

When a specific Media Gateway board fails, the **signaling node** remains in service via the other Media Gateway board that belongs to the same **Redundant MTP3 Group**.

MTP2 signaling links are restored on the redundant Media Gateway board after the Media Gateway boards' switchover/switchback takes place – thereby the status of the whole MTP3 subsystem is preserved.

To configure the **Redundant MTP3 Group**, apply the following changes to the configuration described in 'Configuring the MTP3/M3UA Application' on page 485 (It is recommended to define and bring-up a partial simple MTP3/M3UA configuration prior to defining the full redundant MTP3 configuration):

➤ To configure the Redundant MTP3 Group:

1. Stop service on both Media Gateway boards (both the one that is currently associated with specific MTP3 Group and the one to be associated with it).
 - a. Click  to access the Media Gateway status screen.
 - b. Select the Media Gateway board that is currently associated with the MTP3 Group.
 - c. Stop service on the Media Gateway board by clicking **Lock** in the Actions bar.

2. Configure an MTP3 group to be the redundant MTP3 group.
 - a. Click  to access the Media Gateway status screen.
 - b. In the Navigation pane, select **PSTN** and then select the specific MTP3 Group.
 - c. In the Configuration pane, click **MTP3 Group Settings**; The MTP3 Group Settings screen is displayed.
 - d. Set the **Redundancy Mode** to *dualCPU*.
3. Associate an additional Media Gateway board with the specific MTP3 group.
 - a. Click the  button to access the Media Gateway status screen.
 - b. Select the additional Media Gateway board.
 - c. In the Actions bar, click **Lock** to stop the service on the additional Media Gateway board.
 - d. In the Navigation pane, select **PSTN** and then in the configuration pane, click **PSTN Settings**; The Media Gateway board's PSTN Settings screen is displayed.
 - e. In the SS7 Settings tab, configure **MTP3 Group** parameter to match the the specific MTP3 Group.
4. For each Media Gateway board that is associated with the **Redundant MTP3 Group**, define an "internal point code".
 - a. Click the  button to access the Media Gateway status screen.
 - b. In the Navigation pane, select **PSTN** and then select the corresponding SS7 Node.
 - c. In the Navigation pane, select **SS7 Node Redundancy**. The SS7 Node Redundancy list is displayed.
 - d. The SS7 Node Redundancy list is automatically populated with the entries for each Media Gateway board associated with the redundant MTP3 Group. Therefore there is no need to add or remove entries from it.
 - e. Select a specific row and then in the configuration pane, click **SS7 Node Redundancy Settings**; The SS7 Node Redundancy Settings screen is displayed.
 - f. Configure the **Internal OPC** parameter to be a unique, unused point code value. Refer to the table below.



Note: **Internal OPC** is used for internal communication between Media Gateway boards that belong to the same MTP3 Group. However, it is important to make sure that Internal OPC does not duplicate any real **point code** used in your SS7 network.

5. Restore service on both Media Gateway boards.
 - a. Click  to access the Media Gateway status screen.
 - b. Select the first Media Gateway board associated with the MTP3 Group.
 - c. Restore the service on the Media Gateway board by clicking **Unlock** in the Actions bar.
 - d. Repeat the steps for the second Media Gateway board associated with the MTP3 Group.
 - e. Wait till both Media Gateway boards complete restart and their Operational State becomes Enabled (boards will be color-coded Green in the EMS)
6. Create and configure an SS7 Data Link for each **signaling link** connected to the newly associated Media Gateway board.
 - a. Click  to access the Media Gateway status screen.
 - b. Select the newly associated Media Gateway board.
 - c. In the Navigation pane, select **PSTN ► SS7 ► SS7 Links**; The SS7 Links list is displayed.
 - d. Use the  or  buttons to add or remove entries.
 - e. Select a specific row and then in the configuration pane, click **SS7 Data Link Settings**; The SS7 Data Link Settings screen is displayed.
 - f. Configure SS7 Data Link properties according to the tables 'M2UA - SS7 Data Link Properties - Data Link General Info Tab' and 'M2UA - SS7 Data Link Properties - Data Link MTP Tab'. Make sure to configure **Layer2Type** as *MTP2* and **Layer3Type** as *MTP3*.
7. Each **signaling link** must be attached to the SS7 Linkset (that is associated with **adjacent SS7 signaling node**). Create and configure a SS7 LinksetLink for each newly added SS7 Data Link.
 - a. Click  to access the Media Gateway status screen.
 - b. In the Navigation pane, select **PSTN** and then select the appropriate SS7 Linkset.
 - c. In the Navigation pane, select **SS7 Linkset Links**. The SS7 Linkset Links list is displayed.
 - d. Use the  or  buttons to add or remove entries.
 - e. Select a specific row and then in the configuration pane, click **SS7 Linkset Link Settings**; The SS7 Linkset Link Settings screen is displayed.
 - f. Configure SS7 Linkset Link properties according to the table 'MTP3/M3UA - SS7 Linkset Link Properties'. Make sure to attach it to the SS7 Data Link configured in the previous step.
8. Create and configure the UAL Group for each SCTP association that is established between the newly associated Media Gateway board and the SoftSwitch.
 - a. Click  to access the Media Gateway Status screen.
 - b. Select the desired Media Gateway board.

- c. In the Navigation pane, select **PSTN ► Sigtran ► UAL Groups**; The UAL Group list is displayed.
 - d. Use the  or  buttons to add or remove entries.
 - e. Select a specific row and then in the configuration pane, click **UAL Group Settings**; The UAL Group Settings screen is displayed.
 - f. Configure the UAL Group properties according to the table 'UAL Group Properties'. Make sure to configure **Protocol Type** as *M3UA* and attach the corresponding **SS7 Node** and **M3UA Routing Group**.
9. Bring all of the configured entities into service.
- a. Click  to access the Media Gateway Status screen.
 - b. In the Navigation pane, select **PSTN** and then select the corresponding SS7 Node.
 - c. In the Actions bar, click **Recursive Unlock**.



Note: Instead of performing the **Recursive Unlock** operation on SS7 Node, you may also perform a regular **Unlock** operation on all the newly added SS7 Data Links.

10. In the Navigation pane, select the the newly associated Media Gateway board.
 - a. If the Media Gateway board is not already unlocked, in the Actions bar, click **Unlock**. Wait until the board completes the restart and its **Operational State** changes to *Enabled* (board will be color-coded *Green* in the EMS).
 - b. In the Navigation Pane, select **PSTN ► Sigtran ► UAL Groups**.
 - c. Unlock all of the UAL Groups configured in Step 8 by clicking **Unlock** in the Actions bar. This step may be skipped if you previously unlocked the Media Gateway board, as UAL Groups are automatically unlocked as part of the Media Gateway Board's Unlock action.
11. Perform the corresponding configuration on the Signaling Gateway and/or Softswitch to which the Mediant 8000 is connected. Bring all configured entities in service.
12. On the Mediant 8000, verify that the **Operational State** of all configured entities (i.e. SS7 Node, SS7 Linkset, SS7 Routeset, SS7 Data Link, UAL Group and E1/T1 Trunk) is *Enabled*.

Table 38-21: SS7 Node Redundancy Properties

Parameter Name	Type	Provisioning Type	Description
SS7 Node Redundancy name	String Up to 40 chars.	Instant	The SS7 Node Redundancy name.
Internal OPC	String Up to 20 chars.	Online	The Redundancy point code used for communication between the Media Gateway boards that belong to the same MTP3 Group. The Internal OPC must be unique for each Media Gateway board that belongs to the same MTP3 Group. It is important to make sure that Internal OPC does not duplicate any real point code used in your SS7 network.
ALCAP OPC	String Up to 20 chars.	Online	Relevant for broadband SS7 (UMTS) configuration only. The point code of the Media Gateway board that processes the ALCAP payload.

38.6.4.4 Advanced Configuration

Additional parameters and timers of MTP2/MTP3 signaling layers may be configured via MTP2 Profile, SS7 Node Timers and SS7 Linkset Timers.

By default, a single instance of each profile entity is created and all MTP2/MTP3 entities are attached to it.

You can create additional MTP2/MTP3 Profiles and attach them to specific SS7 entities. Or, alternatively, modify the existing MTP2/MTP3 profile configurations.

38.6.4.5 STP Functionality (Alias Point Code)

The Mediant 8000 normally operates as a SP (Signaling Point) entity in the SS7 network. However, for some deployments, STP (Signaling Transfer Point) functionality may be required.

To implement STP functionality, up to two additional “alias” point codes may be added to the “primary” point code of the SS7 Node (as defined via the **Originating PC** parameter, see table “SS7 Node Properties” for details) . SS7 messages that arrive at the specific Media Gateway board, and have an “alias” point code set as their destination, will be relayed to the SoftSwitch via the M3UA protocol, similar to the messages destined to the SS7 Node’s “primary” point code. M3UA Routing Contexts may be used to define different routing rules for “alias” and “primary” point codes.

➤ **To configure Alias Point Codes:**

1. Configure the MTP3/M3UA application, as described in 'Configuring the MTP3/M3UA Application' on page 485.
2. Click  to access the Media Gateway Status screen.
3. In the Navigation pane, select **PSTN** and then select the corresponding SS7.
4. In the Navigation pane, select **SS7 Alias Point Code**; the SS7 Alias Point Code status screen is displayed.
5. Use the  or  buttons to add or remove entries.
6. Select a specific row and then in the configuration pane, click **SS7 Alias Point Code Settings**; the SS7 Alias Point Code Settings screen is displayed.
7. Configure the "alias" point code value. Use the same syntax as for **Originating PC** parameter in SS7 Node.
8. For each defined Alias Point Code, create and configure an M3UA Routing Context that defines **routing rules** for M3UA messages based on their source point codes and service indicators. Use the same procedure as described in 'Configuring the MTP3/M3UA Application' on page 485.
9. Activate the new configuration by restarting the corresponding Media Gateway board via **Lock** and consequent **Unlock** maintenance actions (for redundant configurations, you must lock **both** Media Gateway boards that are associated with the specific MTP3 Group).

38.6.5 Configuring the M2TN Application

The following entities are relevant to the M2TN (SG side) application:

- SS7 Data Link – represents the **MTP2 signaling link** connected to the PSTN network.
- UAL Group – represents the **SCTP association** between the Media Gateway boards.
- UAL Interface – represents the single **M2UA link** transferred between the Media Gateway boards via the IP network.
- MTP2Profile – defines the **MTP2 signaling link** timers and configuration.

To configure a Media Gateway on the Remote PSTN side, see Section 'Configuring the M2UA (SG Side) Application' on page 476. Define one UAL Group for SCTP association between Media Gateway boards.

➤ **To configure Media Gateway on the Central TDM switch side:**

1. Create and configure **tunneling** SS7 Data Links for each **signaling link** connected to the central TDM switch.
 - a. Click  to access the Media Gateway status screen.
 - b. Select the desired Media Gateway board.
 - c. In the Navigation pane, select **PSTN** ➤ **SS7** ➤ **SS7 Data Links**; the SS7 Data Links list is displayed.

- d. Use the  or  buttons to add or remove entries.
 - e. Select a specific row and then in the configuration pane, click **SS7 Data Link Settings**; the SS7 Data Link Settings screen is displayed.
 - f. Configure the SS7 Data Link properties according to the table, 'SS7 Data Link Properties - Data Link General Info Tab' on page 478. Make sure to configure the **Layer2Type** as *M2UA* and the **Layer3Type** as *M2TN*.
2. Create and configure a **MTP2** SS7 Data Link for each **signaling link** connected to the central TDM switch:
 - a. In the SS7 Data Links list, select a specific row and then in the configuration pane, click **SS7 Data Link Settings**; the SS7 Data Link Settings screen is displayed.
 - b. Configure the SS7 Data Link properties according to the table "M2UA - SS7 Data Link Properties - Data Link General Info Tab" on page 478. Make sure to configure the **Layer2Type** as *MTP2* and the **Layer3Type** as *M2TN*.
 - c. Associate the **MTP2** link with the tunneling link created in step 1 by configuring the **Tunneling MGC Link ID** parameter in Data Link Tunneling tab to match the **tunneling link ID**.
 3. Create and configure the UAL Group for the **SCTP association** between the Media Gateway boards.
 - a. Click  to access the Media Gateway status screen
 - b. Select the desired Media Gateway board.
 - c. In the Navigation pane, select **PSTN ► Sigtran ► UAL Groups**; the UAL Groups list is displayed.
 - d. Use the  or  buttons to add or remove entries.
 - e. Select a specific row and then in the configuration pane, click **UAL Group Setting**; the UAL Group Settings screen is displayed.
 - f. Configure the UAL Group properties according to the table 'MT3/M3UA - MTP3 Group Properties' on page 490. Make sure to configure the **UAL Type** as *M2UA* and the **Functionality** as *MGC*.
 4. Create and configure the UAL Interface for each **tunneling** SS7 DataLink configured at step 1.
 - a. Click  to access the Media Gateway status screen.
 - b. Select the desired Media Gateway board.
 - c. In the Navigation pane, select **PSTN ► Sigtran ► UAL Interfaces**; the UAL Interfaces list is displayed.
 - d. Use the  or  buttons to add or remove entries.
 - e. Select a specific row and then in the configuration pane, click **UAL Interface Settings**; the UAL Interface Settings screen is displayed.
 - f. Configure the UAL Interface properties according to the table, 'UAL Interface Properties' on page 481. Make sure to attach it to the **UAL Group** and **tunneling SS7 Data Link** defined in the previous steps.

5. Bring all of the configured entities into service.
 - a. Click  to access the Media Gateway status screen.
 - b. Select the specific Media Gateway board.
 - c. If the Media Gateway board is not already unlocked, in the Toolbar, click **Unlock**. Wait until the Media Gateway board completes the restart and its **Operational State** is changed to *Enabled* (board will be color-coded *Green* in the EMS).
 - d. Unlock all Trunks associated with the **MTP2** SS7 Data Links, configured in step 2 (if they are not already unlocked).
 - e. Unlock all UALGroups, configured in step 3 (if they are not already unlocked).
 - f. Unlock all UAL Interfaces, configured in step 4 (if they are not already unlocked). A warning will be displayed advising you that the online configuration of the M2TN links is not supported and that you should LOCK/UNLOCK the Media Gateway board once again. Lock and unlock the Media Gateway board as advised.
 - g. Verify that the **Operational State** of all of the configured entities is *Enabled*. This occurs only when the Media Gateway boards on both sides of the tunnel are enabled and their configurations fully match.

38.6.5.1 Online Provisioning

The configuration of the M2TN application can not be modified online. Lock the Media Gateway board prior to making any modification and unlock it to activate the new configuration. The double LOCK/UNLOCK procedure may be required (as described in the in the previous section).

38.6.5.2 Redundant Configuration

The M2TN application has the same redundancy support as M2UA (SG side) application. For more information, see Section 'Redundant Configuration' on page 482.

38.6.5.3 Advanced Configuration

Additional parameters and timers of MTP2 **signaling links** can be configured via the MTP2 Profile. The default MTP2 Profile contains all of the default settings specified in the ITU standard. In a typical configuration, all SS7 Data Links are attached to the same MTP2 Profile.

Additional MTP2 Profiles can be created and attached to specific SS7 Data Links. Or alternatively, the existing MTP2 Profile configuration can be modified.

38.7 Configuring the CAS/ISDN Subsystem

CAS (Common Associated Signaling) is a telecommunication signaling protocol used to interconnect PBXs or other legacy PSTN equipment. When using CAS, routing information is encoded and transmitted in the same channel as the payload itself.

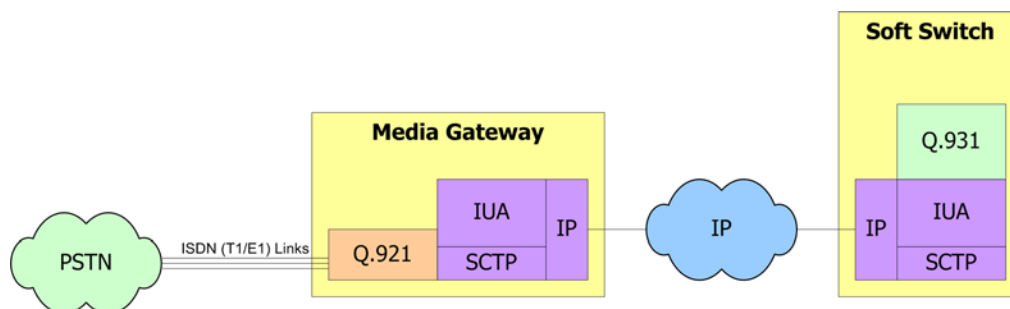
The Mediant 8000 supports “CAS interworking function” where signaling messages arriving from the CAS trunk are relayed to the Softswitch (e.g. via the MEGACO or SIP protocols), and vice versa.

ISDN (Integrated **S**ervices **D**igital **N**etwork) is an international communications standard for sending voice and data over digital telephone lines or land-line telephone wires. When using ISDN, voice and data are carried by bearer channels (*B channels*) occupying a bandwidth of 64 kb/s. A data channel (*D channel*) handles signaling at 16 kb/s or 64 kb/s, depending on the service type.

The Mediant 8000 supports “ISDN interworking function” where signaling messages coming from the ISDN trunk are relayed to the Softswitch (e.g. via the SIP protocols), and vice versa.

Additionally, the Mediant 8000 supports the relay of ISDN signaling messages using the SIGTRAN IUA (ISDN User Adaptation Layer) protocol. A signaling message coming to the Mediant 8000 from the ISDN connection goes through the data link layer and the Q.931 protocol data unit and is relayed to the SoftSwitch using IUA over SCTP.

Figure 38-11: ISDN Relay via IUA



DPNSS (**D**igital **P**rivate **N**etwork **S**ignaling **S**ystem) is a network protocol used on digital trunk lines for connecting two PABXs. It was originally defined by British Telecom. The Mediant 8000 supports the relay of DPNSS signaling using SIGTRAN DUA (DPNSS User Adaptation Layer) protocol.

The Mediant 8000 has the following IUA/DUA capabilities:

- Up to 84 UAL Interfaces per Media Gateway Board
- Up to 3 UAL Groups per Media Gateway Board

38.7.1 Configuring the CAS/ISDN Application

The configuration of the CAS/ISDN application is spread across the Media Gateway board and corresponding E1/T1 Trunks. In addition, the IUA/DUA application may be configured as described in the following chapter.

➤ To configure the Media Gateway board's CAS/ISDN settings:

1. Click  to access the Media Gateway status screen.
2. Select the specific Media Gateway board.
3. In the Navigation pane, select **PSTN** and then in the configuration pane, click **PSTN Settings**; the PSTN Settings screen is displayed.
4. In the **CAS/ISDN Settings** tab, configure parameters according to the table 'Media Gateway board's CAS/ISDN Parameters' below.

Table 38-22: Media Gateway board's CAS/ISDN Parameters

Parameter Name	Type	Provisioning Type	Description
Q.931 Relay Mode	Enum None, Activate LAPD Messaging, Q931 Relay To Host, Layer 3 Is IUA	Online	▪ Defines whether Q.931 relay mode is activated or not. ▪ Q.931 relay is a new way to establish or tear down a call in a Media Gateway Host/channel architecture. It is suitable for Users who need to handle a complete Q.931 protocol at the HOST level. Normally, ISDN call operation is controlled by PSTN library commands or events. In Q.931 relay mode, Users can get or send a packet with Q.931 message information to a specific trunk (LAPD interface). Q.931 data is 'relayed' directly between the link and Host. Notice that PRI D-channel Maintenance is still controlled by the on-board ISDN stack.
No. of CAS Config Files	Integer 0 – 1	Online	Defines the number of CAS protocol configuration files. When the CAS protocol is not to be used, set this parameter to 0.
Trunking To Analog Functionality Mapping Profile	Enum Disabled, MelCAS	Online	Defines the Trunking to Analog Functionality Profile.

Parameter Name	Type	Provisioning Type	Description
DPNSS Number Of Virtual Channels	Integer 0 – 30	Instant	Defines the number of virtual channels for DPNSS protocol.

➤ To configure E1/T1 Trunk's CAS/ISDN settings:

1. Click  to access the Media Gateway status screen.
2. Select the specific Media Gateway board.
3. In the Navigation pane, select **PSTN > DS1 Trunks**; the E1/T1 Trunks list is displayed.
4. Select a DS1 Trunk and then in the configuration pane, click **Trunk Settings**; the Trunk Settings screen is displayed
5. In the **ISDN/DPNSS** and **CAS** tabs, configure parameters according to the tables below.

Table 38-23: E1/T1 Trunk's ISDN/DPNSS Parameters

Parameter Name	Type	Provisioning Type	Description
D-Channel Configuration	Enum Primary, Backup, NFAS, Not ISDN Trunk	Online	Defines D-channel configuration. This setting is only applicable to ISDN PRI protocols that support the NFAS and/or D-channel backup procedures.
Termination Side	Enum User Side, Network Side	Online	▪ Defines the termination side of the ISDN trunk. ▪ Configure the parameter as User Side when the PSTN or PBX side is configured as Network Side, and vice-versa.

Parameter Name	Type	Provisioning Type	Description
ISDN Q931 Layer Response Behavior	Unsigned 0 – 4294967295	Online	▪ Defines ISDN Q.931 state machine behaviour via a bitmap that contains the following bits: ▪ NO STATUS ON UNKNOWN IE ▪ NO STATUS ON INV OP IE ▪ ACCEPT UNKNOWN FAC IE ▪ SEND USER CONNECT ACK ▪ EXPLICIT INTERFACE ID ▪ ALWAYS EXPLICIT ▪ ACCEPT MU LAW ▪ EXPLICIT PRES SCREENENG ▪ STATUS INCOMPATIBLE STATE ▪ STATUS ERROR CAUSE ▪ ACCEPT A LAW ▪ RESTART INDICATION ▪ FORCED RESTART ▪ NS_ACCEPT_ANY_CAUSE
ISDN Outgoing Calls Behavior	Unsigned 0 – 4294967295	Online	Defines ISDN Q.931 state machine behaviour for outgoing calls via a bitmap that contains the following bits: ▪ USER SENDING COMPLETE ▪ USE MU LAW ▪ DIAL WITH KEYPAD ▪ STORE CHAN ID IN SETUP ▪ USE A LAW ▪ NUMBERING PLAN FOR T1 ▪ ACCEPTS ANY IA5 CHARACTER ▪ DLCI REVERSED OPTION
ISDN Incoming Calls Behavior	Unsigned 04294967295	Online	Defines ISDN Q.931 state machine behaviour for incoming calls via a bitmap that contains the following bits: ▪ DATA CONN RS ▪ VOICE CONN RS ▪ CHAN ID IN FIRST RS ▪ USER SETUP ACK ▪ CHAN ID IN CALL PROC ▪ PROGR IND IN SETUP ACK ▪ NI-2 SECOND REDIRECT NUMBER

Parameter Name	Type	Provisioning Type	Description
ISDN General CC Behavior	Integer 0 – 2147483647	Online	Defines ISDN Q.931 call control state machine behaviour via a bitmap that contains the following bits: - REVERSE CHAN ALLOC ALGO - CHAN ID 16 ALLOWED - USE T1 PRI - USE E1 PRI - START WITH B CHAN OOS - CHAN ALLOC LOWEST - CHAN ALLOC HIGHEST
DPNSS Behavior	Integer 0 – 2147483647	Online	Defines ISDN Q.931 state machine behaviour via a bitmap that contains the following bits: - DPNSS STOP SABMR AFTER NL & NT1 - DPNSS FULL STARTUP SUCCESS - DPNSS DLC OOS AFTER NL AND NT1 - DPNSS DLC OOS WHEN L3 Q FULL - DPNSS DASS2 PROTOCOL - DPNSS SIMULTANEOUS STARTUP
NFAS Interface ID	Integer 0 – 255	Online	Defines the NFAS Interface ID.
NFAS Group Number	Integer 0 – 9	Online	- Defines the NFAS Group number. - Value 0 indicates that Trunk is not NFAS.

Table 38-24: E1/T1 Trunk's CAS Parameters

Parameter Name	Type	Provisioning Type	Description
CAS File Index	Integer 0 – 7	Online	Defines the index of the CAS state-machine file to be used on specific trunk. CAS files must be pre-configured in Media Gateway ▶ PSTN ▶ Configuration ▶ CAS Setup Files .
CAS Delimiter Padding	Enum Number Sign, Asterisk	Online	Defines the digits string delimiter padding usage per trunk. Number Sign – default address string padding: '*XXX#' (where XXX is the digit string that begins with '*' and ends with '#', when using padding). Asterisk – special use of asterisks delimiters: '*XXX*YYY*' (where XXX is the address, YYY is the source phone number and * is the only delimiter padding).
Dial Plan Name	String Up to 11 chars	Instant	Defines which Dial Plan (from a Dial Plan file) to use for a specific trunk.

38.7.2 Configuring the IUA/DUA Application

The following entities are relevant to the IUA/DUA application:

- **Trunk** – represents a **ISDN/DPNSS link** connected to the PSTN network.
- **UAL Group** – represents **SCTP association** between Media Gateway and the SoftSwitch.
- **UAL Interface** – represents a single **IUA/DUA link** transferred over the SCTP association.

➤ To configure the IUA/DUA application:

1. Configure the Media Gateway board's Trunk type as IUA/DUA and update its ISDN/DPNSS parameters.
 - a. Click  to access the Media Gateway status screen.
 - b. Select the desired Media Gateway board.
 - c. In the Navigation pane, select **PSTN ▶ DS1 Trunks**; the DS1 Trunks list is displayed.
 - d. In the DS1 Trunks List, select a DS1 trunk and then in the configuration pane, click **Trunk Settings**; the Trunk Settings screen is displayed.
 - e. Change the **Protocol Type** parameter as follows:
 - ◆ For IUA application configure Trunk's **Protocol Type** as *T1IUA* or *E1IUA*.
 - ◆ For DUA application configure Trunk's **Protocol Type** as *E1DUA*.
 - f. In the **ISDN/DPNSS** tab, configure ISDN/DPNSS trunk parameters as described in the table 'ISDN/DPNSS Trunk Parameters of the Trunk' described in 'Configuring the CAS/ISDN Application' on page 508.
2. Create and configure a UAL Group for each **SCTP association** that is to be established with the SoftSwitch:
 - a. Click  to access the Media Gateway status screen.
 - b. Select the desired Media Gateway board.
 - c. In the Navigation pane, select **PSTN ▶ Sigtran ▶ UAL Groups**; the UAL Group list is displayed.
 - d. Use the  or  buttons to add or remove entries.
 - e. Select a specific row and then in the configuration pane, click **UAL Group Settings**; the UAL Group Settings screen is displayed.
 - f. Configure **UAL Type** parameter as follows (for more information, see Section table 'UAL Group Properties' on page 480):
 - ◆ For the IUA application, configure **UAL Type** as *IUA*.
 - ◆ For the DUA application, configure **UAL Type** as *DUA*.
 - ◆ Configure **Functionality** as *SG*.

3. Create and configure a UAL Interface for each Trunk configured in step 1:
 - a. Click  to access the Media Gateway status screen.
 - b. Select the desired Media Gateway board.
 - c. In the Navigation pane, select **PSTN ► Sigtran ► UAL Interfaces**; the UAL Interfaces list is displayed.
 - d. Use the  or  buttons to add or remove entries.
 - e. Select a specific row and then in the configuration pane, click **UAL Interface Settings**; the UAL Interface Settings screen is displayed.
 - f. Configure UAL Interface properties according to the table 'UAL Interface Properties' on page 481.
Make sure to attach it to the **UAL Group** and **Trunk** configured in the previous steps.
4. For the DUA application only, configure Media Gateway board's DPNSS parameters.
 - a. Click  to access the Media Gateway status screen.
 - b. Select the desired Media Gateway board.
 - c. In the Navigation pane, select **PSTN ► DS1 Trunks**; the DS1 Trunks list is displayed.
 - d. In the DS1 Trunks List, select a DS1 trunk and then in the configuration pane, click **Trunk Settings**; the Trunk Settings screen is displayed.
 - e. In the **ISDN/DPNSS** tab, configure ISDN/DPNSS trunk parameters as described in the table, ISDN/DPNSS Trunk Parameters of the Trunk.
5. Bring all of the configured entities into service.
 - a. Click  to access the Media Gateway status screen.
 - b. Select the specific Media Gateway board.
 - c. If the Media Gateway board is not already unlocked, unlock it. Wait till the board completes restart and its Operational State becomes Enabled (board will be color-coded Green in the EMS).
 - d. Unlock all Trunk, configured in step 1 (if they are not already unlocked).
 - e. Unlock all UAL Groups, configured in step 2 (if they are not already unlocked)
 - f. Unlock all UAL Interfaces, configured in step 3 (if they are not already unlocked).
 - g. Perform the corresponding configuration on the Signaling Gateway and/or Softswitch to which the Mediant 8000 is connected. Bring all configured entities in service.
 - h. On Mediant 8000, verify that the **Operational State** of all configured entities (i.e. UAL Group, UAL Interface and E1/T1 Trunk) is *Enabled*.

38.7.3 Online Provisioning

The configuration of the IUA/DUA application may be modified online.

See 'Configuring the IUA/DUA Application' on page 513 for the full list of entities that must be configured and the specific parameters' description and provisioning policies.

38.7.4 ISDN Operational Status

The Operational status of the IUA/DUA application may be determined by inspecting the Operational Status of the following entities:

- Trunk – indicates status of the ISDN physical link layer
- UAL Interface – for a IUA application, indicates the status of the D-channel; for a DUA application, mirrors the status of the Trunk.

38.7.5 Redundant Configuration

The IUA/DUA application is partially supported by the Media Gateway board redundancy mechanism. If the Media Gateway board is configured for Hot redundancy, the IUA/DUA application goes out of service and SCTP associations are dropped. It is the SoftSwitch's responsibility to identify this failover, re-establish SCTP associations, re-activate ASPs and re-establish the IUA interfaces. If all the above-mentioned events are completed prior to the expiration of the Q.931 T-309 timer, established calls will be preserved upon Media Gateway switchover.



Note: The SCTP associations are dropped during the Media Gateway board switchover and it is the SoftSwitch's responsibility to re-establish them.

38.8 Configuring TDM Clock Synchronization

In a traditional TDM service network, such as PSTN, both ends of the TDM connection must be synchronized. If they are not synchronized, voice frames are either dropped (to prevent a buffer overflow condition) or inserted (to prevent an underflow condition). In both cases connection quality and reliability is affected.

The Mediant 8000 Media Gateway supports different Clock Synchronization modes. The following clock synchronization modes are available:

- **Standalone Board Sync mode**— each Media Gateway board synchronizes itself by the clock received on one of the PSTN interfaces (OC-3/STM-1 optical links T3 trunks or E1/T1 trunks) connected to it; there is no global clock synchronization between different Media Gateway boards. For more information, refer to 'Stand Alone Board Clock Mode' on page [516](#)
- **Timing Module BITS Sync mode** – all Media Gateway boards are synchronized with dual BITS (Building Integrated Timing Source) trunk clock sources connected to dual SA-1/RTMs; for more information, refer to 'Timing Module BITS Sync Clock Mode' on page [519](#).
- **Timing Module Line Sync mode** – all Media Gateway boards are synchronized by up to four “reference” OC-3/STM-1 links or T3 trunks connected to the specific Media Gateway boards; for more information, refer to 'Timing Module Line Sync Clock Mode' on page [522](#).

The following sections describe each of the available clock synchronization modes in details. Detailed instructions are provided on connecting to the external hardware and configuring the Media Gateway software.

38.8.1 Stand Alone Board Clock Mode

In Standalone Sync clock mode, each board synchronizes its own clock. The clock may be derived from the following sources:

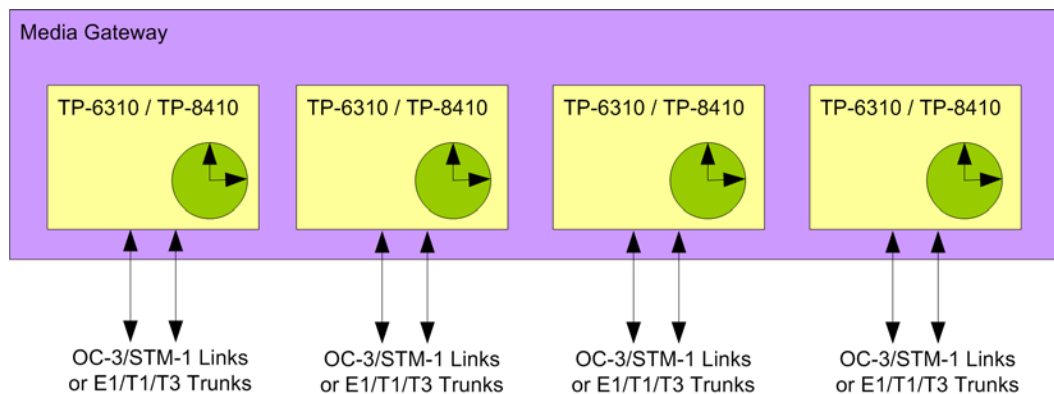
- PSTN interface (OC-3/STM-1 optical links, or E1/T1/T3 trunks)
- Internal board's clock reference

There is no global clock synchronization across different Media Gateway boards.



Note: Standalone Board Sync clock mode is primarily intended for initial Media Gateway setup in the lab environment. For field deployments, it is strongly recommended to use one of the available synchronized modes instead (e.g. Timing Module BITS Sync mode. For more information, see Section 'Timing Module BITS Sync Clock Mode' on page [519](#).

Figure 38-12: Stand-Alone Clock Synchronization Mode



In Standalone Board Sync clock mode, the clock is derived from the high-level communication layer protocol of the PSTN interface (OC-3, STM-1, T1 on T3 for TP-6310 or E1/T1 on TP-8410) or from the internal board's clock reference.

38.8.1.1 Connecting the Media Gateway to the External Equipment

In the Standalone Board Sync clock mode, the clock is derived from the PSTN interface (OC-3, STM-1, E1, T1 or T3) connected to the Media Gateway board or from the internal board's clock reference. If you wish to derive the clock from the PSTN interface, you must simply connect the PSTN interface links/trunks to the Media Gateway boards. If you wish to use internal board's clock reference, there is no need to connect the Media Gateway to any external equipment.

38.8.1.2 Configuring the Media Gateway Software

This section describes how to configure the Standalone Board Sync Clock Mode.

➤ To configure the Standalone Board Sync Clock Mode:

1. Click  to access the Media Gateway status screen.
2. In the Navigation pane, select **PSTN** and then in the configuration pane, click **Clock Settings**; the Clock Settings screen is displayed.
3. Configure **Timing Mode** parameter as *StandaloneBoardSync*.
4. In the **Standalone Board Mode Settings** tab, configure the **None Mode Clk Source** parameters as follows:
 - **internal** – the board synchronizes according to the internal clock reference
 - **pstn** – the board takes the clock from the PSTN interface; for OC-3/STM-1 links the clock is taken from the high-level communication layer protocol of the PSTN interface; for T3/E1/T1 trunks the clock is taken from one of the available T3/E1/T1 trunks; selection of the T3/E1/T1 trunk is performed according to **Clock Reference Candidate** and **Clock Reference Priority** parameters setting trunk with **Clock Reference Candidate** set to *enabled* and the highest "Clock Reference Priority" selected.

The above-described settings are applied to all boards; however, it is possible to override the Clock Reference settings for a specific board as follows:

- Click  to access the Media Gateway status screen.
- Select the desired Media Gateway board.
- In the Navigation pane, select **PSTN** and then in the configuration pane, click **PSTN Settings**; the PSTN Settings screen is displayed.
- Set the **None Mode Clk Source** parameter as described above.

For T3/E1/T1 clock reference sources, you must also configure Clock Reference trunks and their priorities as described below:

➤ **To configure Clock Reference T3/E1/T1/trunks and their priorities:**

1. Open Media Gateway board's PSTN Settings configuration screen as described above.
2. Select the Standalone Board Mode Settings tab. The list of all Media Gateway boards and their current clock sources is displayed.
3. Right-click the entry in the list that represents specific Media Gateway board and from the drop-down menu, select **Trunks Clock Reference**; the Clock Priorities screen is displayed.
4. In the Clock Priorities screen, right-click the T3/E1/T1 trunk to be used as a clock reference and perform the following actions:
 - **Lock row** – to stop service on the specific trunk.
 - **Enable Reference With Trunk Priority** or **Enable Reference With Trunk Priority** – to select specific trunk as **Clock Reference Candidate** and update it's **Clock Reference Priority**.
 - **Unlock row** – to return the trunk into service.

38.8.2 Timing Module BITS Sync Clock Mode

In Timing Module BITS Sync clock mode, all Media Gateway boards are synchronized by two BITS Generators (Building Integrated Timing Source) trunks. These trunks are synchronized with the Media Gateway boards via two SA-1/RTMs, each with a designated timing module. Two SA-1/RTMs are required to ensure seamless clock operation in case of failure of one of the SA-1/RTMs modules.



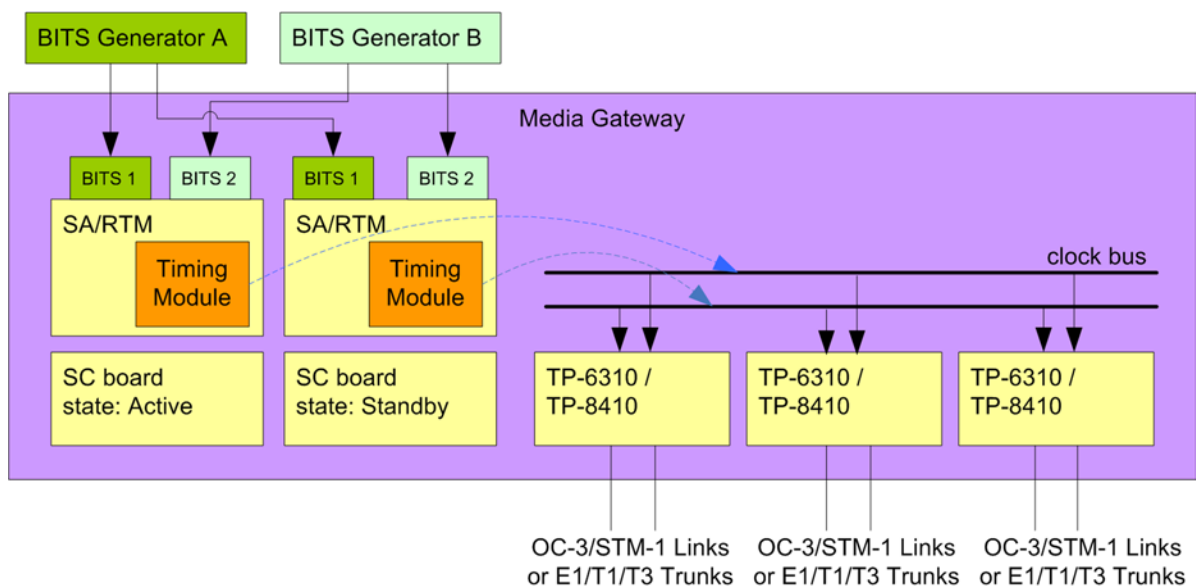
Note: To activate the Timing Module BITS Sync clock mode, you must order SA-1/RTMs (SA/RTM with a resident Timing Module). To order the Media Gateway with this module, see the AudioCodes price list.

When one of the reference clock sources (BITS Generator) fails, the Timing Module automatically switches to another source and continues using it as a reference clock for the whole Media Gateway.

Automatic failover of the BITS Generator clock source can be disabled by configuring the Selector Mode parameter to Manual (see table below). In the manual mode, the Timing Module will always use the clock source with a higher priority, even when this source fails. The manual mode is primarily intended for the lab usage and is not recommended for field deployments.

When all clock reference source links/trunks fail, the Timing Module functions as the holdover clock source for up to 24 hours. The clock provided by the Timing Module complies with STRATUM 3 (4.6ppm) requirements (for more information, see Section 'SA/RTM Synchronization and Alarm Rear Transition Module' on page 69).

Figure 38-13: Timing Module BITS Sync Clock Mode



When both BITS trunks fail, the Timing Module continues to function as the clock ("clock holdover") for up to 24 hours. The clock provided by the Timing Module complies with STRATUM 3 (4.6ppm) requirements.

When clock source (BITS trunk) with a higher priority returns in service after the failure, the Timing Module may either revert to the higher-priority clock source or continue using the lower-priority clock source. The behavior is controlled via the **Auto Clock Reference Mode** parameter.

38.8.2.1 Connecting Media Gateway to the External Equipment

Connect the BITS trunks from two BITS generators to corresponding entries on SA-1/RTM. Two trunks from the BITS Generator A should be connected to the BITS 1 RJ-48c connector on both SA-1/RTM modules. Two trunks from the BITS Generator B should be connected to the BITS 2 RJ-48c connector on both SA-1/RTM modules. For more information, see Section the figure above.

38.8.2.2 Configuring Media Gateway Software

➤ To configure Timing Module BITS Sync Clock Mode configurations:

1. Click the  button to access the Media Gateway status screen.
2. In the Navigation pane, select **PSTN** and then in the configuration pane, click **Clock Settings**; the Clock Settings screen is displayed.
3. Configure the **Timing Mode** parameter to *TimingModuleBITSSync*.
4. Configure **General Timing Module Settings** parameters as described in the below table 'General Timing Module Settings Parameters' below.

Table 38-25: General Timing Module Settings Parameters

Parameter Name	Type	Provisioning Type	Description
Source Mode	Enum Manual, Automatic	Instant	Defines the operational mode of the clock reference selection algorithm. Automatic – selection between clock sources (BITS 1 and 2) is performed automatically; when one source fails, another source is automatically used. Manual – selection is performed according to the user-defined External Reference Clock Priority; the source with the highest priority is used; even when the selected clock source fails. In this case, Media Gateway does not switch to another source.

Parameter Name	Type	Provisioning Type	Description
Auto Clock Reference Mode	Enum Non Revertive, Revertive	Instant	Defines system behavior when clock source with higher priority returns to service after the failure. Revertive – Media Gateway will switch to this source. Non Revertive – continue using the current source until the latter fails. Note that when the clock reference mode is set to Auto Revertive and the higher priority clock source is unstable, the system will switch the clock source each time the higher priority clock fails and returns in service .
Reference Validation Time	Integer	Instant	Defines the validation time (in seconds) for reference clock.

5. In the **TM External IF Settings** tab, configure parameters as described in the table 'TM External IF Settings Parameters' below.

Table 38-26: TM External IF Settings Parameters

Parameter Name	Type	Provisioning Type	Description
External Reference Type	Enum E1, DS1, T12, none	Online	Defines the external line reference (BITS) transmission format.
T1 Line Coding	Enum B8ZS, AMI	Online	Defines line coding for the T1 clock synchronization interfaces: ▪ B8ZS – B8ZS line code ▪ AMI – AMI line code
T1 Framing	Enum ESF, SF	Online	Defines the framing method for the T1 clock synchronization interfaces: ▪ ESF-Extended Super Frame ▪ SF-Super Frame
Tx Pulse Shape	Enum db0, db7p5, db15, db22p5	Instant	Defines the quality of the transmission signal on the clock synchronization interfaces.

Parameter Name	Type	Provisioning Type	Description
Transmit Control	Enum SystemClock, DerivedLine, AIS, Disable	Instant	Defines the transmission pattern on the clock synchronization interfaces.
External Ref 1 Clock Priority	Enum Not Used, Low, High	Instant	Defines the priority of the 1 st external reference clock (connected to the BITS 1). Priority Not Used means that the specific reference clock is not used.
External Ref 2 Clock Priority	Enum Not Used, Low, High	Instant	Defines the priority of the 2 nd external reference clock (connected to the BITS 2). Priority Not Used means that the specific reference clock is not used.

38.8.3 Timing Module Line Sync Clock Mode

In Timing Module Line Sync clock mode, all Media Gateway boards are synchronized by “reference” to OC-3/STM-1 links or E1/T1/T3 trunks connected to the specific Media Gateway boards. Up to four clock reference” source fiber links or trunks may be defined in the Mediant 8000 Media Gateway and one clock reference source can be defined per board. Each of these links are assigned with a user-defined priority.

The clock is distributed across all Media Gateway boards via SA/RTM with a designated Timing Module. Two SA/RTMs are required to ensure seamless clock operation in case of failure of one of the SA/RTM modules.

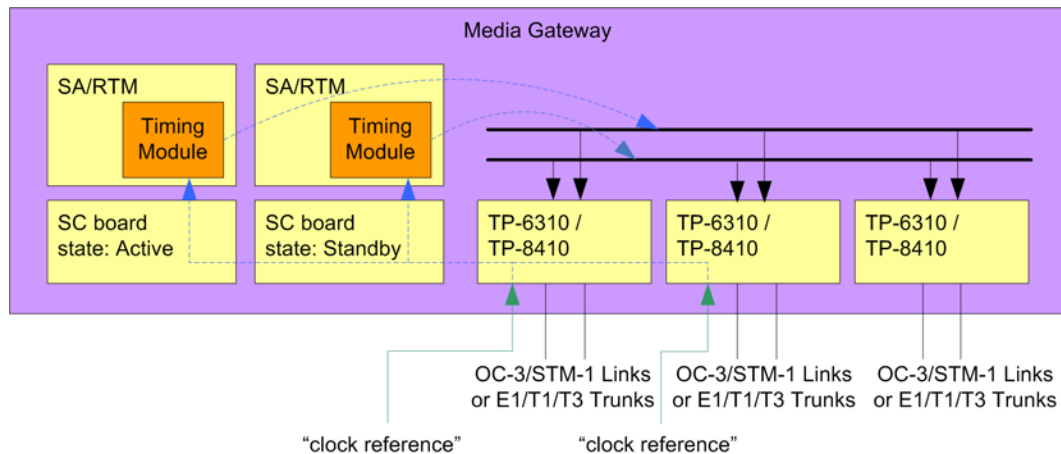


Note: To activate the Timing Module Line Sync clock mode, you must order SA-1/RTMs (SA/RTM with a resident Timing Module). To order the Media Gateway with this module, refer to the AudioCodes price list.

When one of the clock reference source links/trunks fails, the Timing Module automatically switches to another source and continues using it as a reference clock source for the whole Media Gateway. The user may prevent the use of the specific reference source by locking the corresponding line in the TM Line Sync Settings tab (see below).

When all clock reference source links/trunks fail, the Timing Module functions as the holdover clock source for up to 24 hours. The clock provided by the Timing Module complies with STRATUM 3 (4.6ppm) requirements (for more information, see Section 'SA Synchronization and Alarm RTM' on page 69).

Figure 38-14: Timing Module Line Sync Clock Mode



When a clock source (OC-3/STM-1 link or E1/T1/T3 trunk) with a higher priority returns in service after the failure, the Timing Module may either revert to the higher-priority clock source or continue using the lower-priority clock source. The behavior is controlled via the **Auto Clock Reference Mode** parameter.

When the Media Gateway board fails, the redundant Media Gateway board performs switchover and takes control over the OC-3/STM-1 links or T1/E1/T3 trunks that were connected to the failed board. When the Timing module fails, the redundant Timing module performs switchover and takes control over the OC-3/STM-1 links or T1/E1/T3 trunks that were connected to the failed Timing module.

The Timing Module will switch to the next available clock reference source during the switchover; however if the **Auto Clock Reference Mode** parameter is set to *Auto Revertive*, it switches back to the previous "reference source" as soon as switchover is complete.

38.8.3.1 Connecting the Media Gateway to the External Equipment

Connect OC-3/STM-1 links or E1/T1/T3 trunks to use as a clock reference source and activate them (unlock corresponding entities). Use active Media Gateway boards only and connect each clock reference source to a separate board.

View the **Operational State** of corresponding entity (trunk or link) at any time to verify that the clock reference source connection is *enabled*.

38.8.3.2 Configuring Media Gateway Software

➤ To configure Timing Module Line Sync Clock Mode:

1. Click  to access the Media Gateway status screen.
2. In the Navigation pane, select **PSTN** and then in the Configuration pane, click **Clock Settings**; the Clock Settings screen is displayed.
3. Configure the **Timing Mode** parameter to *TimingModuleLineSync*.
4. Configure **General Timing Module Settings** parameters as described in the table 'General Timing Module Settings' above.
5. Select the TM Line Sync Settings tab; A clock reference sources table is displayed. Each row in the table corresponds to one of the four supported clock reference sources and contains both configuration and status parameters.
6. Configure parameter for all physically connected clock reference sources as described in the table 'TM Line Sync Settings Parameters' below.
7. Right-click the clock reference source entry to Unlock it and thereby activate the entry in the Media Gateway configuration.

Table 38-27: TM Line Sync Settings Parameters

Parameter Name	Type	Provisioning Type	Description
Board Index	Integer	Online	Slot number of the Media Gateway board where "reference source" is connected to.
Reference Index in Board	Integer	Online	Index of the clock reference source STM-1/OC-3 link or DS1 trunk inside the board. For STM-1/OC-3 leave it at its default value 1. For E1/T1/E3, the number of the E1/T1 trunk that contains the "reference clock".
Priority	Integer	Instant	User-defined priority of the "reference source". When Timing Module chooses new synchronization source, it chooses the available source with the highest priority.

38.8.3.2.1 Configuring the DS3 Interface

For T3 configurations, the Timing Module on the SA-1/RTM rear card controls clock settings of the individual DS1 trunks only. Timing of the DS3 Interface (high-level communication protocol on the PSTN Interface) should be configured similar to the Standalone Board Sync mode.

➤ To configure timing of the DS3 interface:

1. Click  to access the Media Gateway status screen.
2. Select the desired Media Gateway board.
3. In the Navigation pane, select **PSTN ► DS3**; the DS3 Interfaces List is displayed.
4. Select a specific row and then in the configuration pane, click **DS3 Settings**; the DS3 Setting screen is displayed.
5. Configure the **DS3 Clock Source** parameter as follows:
 - **master** – the clock is taken from the internal board's clock reference.
 - **slave** – the clock is taken from the DS3 protocol layer of the PSTN interface.

This page is intentionally left blank.

39 Configuring the Media Settings

Media Settings define different aspects of the media packetization performed by the Mediant 8000 when transferring the calls over the IP network.

➤ **To configure the Media Settings:**

1. Click  to access the Media Gateway status screen.
2. Select the desired Media Gateway board.
3. In the Navigation pane, select Media and then in the configuration pane, click Media Settings; the Media Settings screen is displayed.
4. Configure Media parameters as described below.

Table 39-1: Media Gateway Board's Voice Settings

Parameter Name	Type	Provisioning Type	Description
Voice Volume	Integer -32 – 31	Instant	Defines the Voice Gain Control (volume).
PCM Input Gain	Integer -31 – 31	Instant	Defines the PCM input gain.
RFC2833 Receive Payload Type	Integer 96-127	Instant	Defines the RFC 2833 Receive Relay RTP Payload type.
RFC2833 Transmit Payload Type	Integer 96-127	Instant	Defines the RFC 2833 Transmit Relay RTP Payload type.
Voice Stream Upload Method	Enum Post, Put	Online	Defines the voice stream upload method.
Voice Streaming	Enum Disabled, Enabled	Online	Enables voice streaming over NFS protocol. NFS allows for a richer set of functionalities, including skip forward, skip backward, pause and continue operations. Applicable mainly to the Media Server application.
Voice Volume	Integer -32 – 31	Instant	Defines the Voice gain control (in decibels). This parameter sets the level for the transmitted (IP-to-PSTN) signal.

Parameter Name	Type	Provisioning Type	Description
PCM Input Gain	Integer -31 – 31	Instant	Defines the Pulse-code modulation (PCM) input gain control (in decibels). This parameter sets the level for the received (PSTN-to-IP) signal.
Silence Suppression	Enum Disable, Enable, Enable Without Adaptation	Instant	Silence Suppression is a method for conserving bandwidth on VoIP calls by not sending packets when silence is detected. ▪ Disable – Silence Suppression is disabled. ▪ Enable – Silence Suppression is enabled. ▪ Enable Without Adaptation – a single silence packet is sent during a silence period (applicable only to G.729).

Parameter Name	Type	Provisioning Type	Description
DTMF Transport Type	Enum Mute DTMF, Proprietary DTMF Relay, Transparent DTMF, Relay DTMF Over RTP	Instant	Defines the DTMF transport type. ▪ Mute DTMF - erase digits from the voice stream, do not relay to remote. ▪ Proprietary DTMF Relay - erase digits from the voice stream, relay to remote using proprietary syntax. ▪ Transparent DTMF - digits remain in the voice stream. ▪ Relay DTMF Over RTP - erase digits from the voice stream, relay to remote using RFC 2833 syntax.
Echo Canceller	Enum Disable, Enable	Instant	Defines whether echo cancellation is enabled and therefore, echo from voice calls is removed.
Echo Canceller Length	Integer 0 – 22	Instant	Defines the Echo Canceller length. ▪ 0 – echo canceler is length determined internally to reach maximum channel capacity. ▪ 4 – 32 msec ▪ 11 – 64 msec ▪ 22 – 128 msec.
Max Echo Canceller Length	Enum Ec Length Determined Automatically(0), 32 msec(4), 64 msec(11), 128 msec(22)	Online	Defines the maximum Echo Canceller length capability.

Parameter Name	Type	Provisioning Type	Description
Echo Canceller Aggressive NLP	Enum Disabled, Enabled	Instant	Enables or disables the Aggressive NLP at the first 0.5 second of the call. When enabled, the echo is removed only in the first half a second of the incoming IP signal.
Mediation Transcoding Mode	Enum SmartTranscoding(0), TDMTranscoding(1), RTPSyncTranscoding(2), RTPAsyncTranscoding(3)	Instant	de for mediation between two endpoints: - Smart Transcoding (0) - Transcoding is selected according to channels configuration. If two WB coders, excluding FAX are configured, RTP Sync is selected. Otherwise, TDM Transcoding is selected (Default). - TDM Transcoding (1) - packets are sent via channel activation per internal (TDM) clock. - RTP Sync Transcoding (2) - packets are sent via RTP channels activation (Sync mode), for IP to IP transcoding calls. - RTP Async Transcoding (3) - packet is sent only upon reception of packet from the network, for IP to IP transcoding calls.
Network Echo Suppressor Enable	Enum Disable, Enable	Online	This feature removes echoes and sends only the near-end's desired speech signal to the network (i.e., to the far-end party).

Parameter Name	Type	Provisioning Type	Description
Echo Canceller Type	Enum Line,Acoustic	Instant	Defines the echo canceller type. - Line echo canceller = Echo canceller for Tel side (default) - Acoustic echo suppressor = Echo canceller for IP side
Attenuation Intensity	Integer 0-3	Instant	Defines the acoustic echo suppressor signals identified as echo attenuation intensity.
Max ERL Threshold - DB	Integer 0-60	Instant	Defines the acoustic echo suppressor maximum ratio between signal level and returned echo from the phone (in decibels).
Min Reference Delay x10 msec	Integer 0-40	Instant	Defines the acoustic echo suppressor minimum reference delay (in 10-ms units).
Max Reference Delay x10 msec	Integer 0-40	Instant	Defines the acoustic echo suppressor maximum reference delay (in 10-ms units).

Table 39-2:Media Gateway Board's RTP/RTCP Settings

Parameter Name	Type	Provisioning Type	Description
RTP Base UDP Port	Integer 1024 – 65535	Online	Defines the lower boundary of UDP ports used for RTP, RTCP (RTP port + 1) and T.38 (RTP port + 2). The upper boundary is the Base UDP Port +10 * (Number of Channels). The value must be a multiple of 10.
Jitter Buffer Min Delay	Integer 0 – 150	Instant	Defines Jitter Buffer Minimum Delay in milliseconds. The lower you set the Jitter Buffer Minimal Delay, the more significantly the optimization factor influences the error ratio
Jitter Buffer Optimization Factor	Integer 0 – 13	Instant	Defines the factor for dynamic Jitter Buffer frame error/delay optimization.
RFC2833 Receive Payload type	Integer 96 – 127	Instant	Defines the RFC 2833 Receive Relay RTP Payload type.
RFC2833 Transmit Payload type	Integer 96 – 127	Instant	Defines the RFC 2833 Transmit Relay RTP Payload type.
RTP RFC2198 Redundancy	Integer 1 – 5	Instant	Defines whether the Media Gateway generates RFC 2198 redundancy packets. 0 – Disable. 1 – Enable. 5 - five levels of RTP redundancy (according to RFC 2198)
RTP RFC2198 Payload Type	Integer 96 – 127	Instant	Defines the payload type for RFC 2198 redundancy packets.
RTCP Interval (msec)	Integer 100 – 2147483647	Instant	Defines the time interval between the adjacent RTCP report packets.

Parameter Name	Type	Provisioning Type	Description
Default RTCP-XR	Enum Disable, EnableFull, CalculationOnly	Online	Enables voice quality monitoring and RTCP XR reports. ▪ Disable – RTCP-XR reports are disabled ▪ Calculation Only – RTCP-XR statistics are calculated and events are sent to the application; however, RTCP-XR reports are not sent to the network ▪ EnableFull – RTCP-XR reports are enabled.
RTCP Randomize	Enum Randomize, NotRandomize	Online	Defines whether RTCP report intervals are randomized or whether each report interval accords exactly to the parameter defining RTCP Mean Tx Interval (in milliseconds).
VQM Burst Threshold	Integer -1 – 12	Online	Defines excessive burst alert threshold for Voice Quality Monitoring (VQM). If set to -1, no alerts are issued.
VQM Delay Threshold	Integer -1 – 12	Online	Defines excessive delay alert threshold for Voice Quality Monitoring (VQM). If set to -1, no alerts are issued.
VQM EOC Received Delay Threshold	Integer -1 – 12	Online	Defines end of call low quality alert threshold for Voice Quality Monitoring (VQM). If set to -1, no alerts are issued
Minimum Gap Size	Integer 0 – 255	Instant	Voice quality monitoring - minimum gap size (number of frames).
RTCP Activation Mode	Enum ActiveAlways, InactiveOnlyIfRTPInactive	Instant	Disables RTCP traffic when there is no RTP traffic. ▪ Active Always (default) = RTCP is active even during inactive RTP periods. ▪ Inactive Only If RTP Inactive = No RTCP is sent when RTP is inactive.

Parameter Name	Type	Provisioning Type	Description
Standard SID Payload Type	Enum Disable, Enable	Instant	Defines whether Silence Indicator (SID) packets are sent according to RFC 3389. ▪ Disable – G.711 SID packets are sent in a proprietary method. ▪ Enable – SID (comfort noise) packets are sent with the RTP SID payload type according to RFC 3389. Applicable to G.711 and G.726 coders.
Media UDP Checksum	Enum Disable, Enable	Online	Defines whether the Media Gateway inserts a non-zero UDP layer checksum on outgoing packets for UDP streams carrying media content (audio and video).
RTP Payload Format	Enum RTP, ATM	Instant	Defines the voice payload format.

Table 39-3: Media Gateway Board's Fax/Modem Settings

Parameter Name	Type	Provisioning Type	Description
Enable Fax Modem Inband Network Detection	Enum Disabled, Enabled	Instant	Enables or disables in-band network detection related to fax/modem. When this parameter is enabled on Bypass mode, a detection of an Answer Tone from the network triggers a switch to bypass mode in addition to the local Fax/Modem tone detections. However, only a high bit-rate coder voice session effectively detects the Answer Tone sent by a remote Endpoint. This can be useful when, for example, the payload of voice and bypass is the same, allowing the originator to switch to bypass mode as well.
General Fax Transport Method	Enum Transparent, Relay, Bypass, Transparent	Instant	Defines the fax transport method.

Parameter Name	Type	Provisioning Type	Description
	With Events		
TTY Transport Type	Enum Disable(0), Bypass(1), Inband Relay(2)	Instant	Defines the transferring method of TTY signals during a call.
TTY/Fax/Modem Bypass Coder Type	Enum G711 Alaw, G711 Mulaw, G726-32, G726-40	Instant	Defines the TTY/fax/modem bypass coder type.
Fax Bypass Payload Type	Integer 0 – 127	Instant	Defines the fax bypass payload type.
Fax Relay Redundancy Depth	Integer 0 – 2	Instant	Defines the number of times that each T.38 fax relay payload is retransmitted to the network.
T38 Redundancy Depth	Enum No Redundancy, One Packet, Two Packets, Three Packets, Max	Instant	Defines the number of repetitions to be applied to control packets when using the T.38 protocol.
Fax Relay ECM	Enum Disable, Enable	Instant	Defines whether the Error Correction Mode (ECM) mode is used during fax relay.

Table 39-4:Media Gateway Board's Caller ID Settings

Parameter Name	Type	Provisioning Type	Description
V34 Fax Transport Method	Enum Transparent, Relay, Bypass, Transparent With Events	Instant	Defines the V.34 fax transport method.

Parameter Name	Type	Provisioning Type	Description
CNG Detector Mode	Enum Disable, Relay, Events Only	Instant	Defines the Media Gateway behavior upon detection of the fax Calling tone (CNG). ▪ Disable – The originating device doesn't detect CNG; the CNG signal passes transparently to the remote side (default). ▪ Relay – CNG is detected on the originating side. CNG packets are sent to the remote side according to T.38 and the fax session is started. This option is useful, for example, when the originating device is located behind a firewall that blocks incoming T.38 packets on ports that have not yet received T.38 packets from the internal network (i.e., originating device). ▪ Events Only – CNG is detected on the originating side, passes transparently to the remote side and fax session is started. T.38 fax session starts when the 'preamble' signal is detected by the answering side.
CED Transfer Mode	Enum Relay, Tone	Instant	Defines the Media Gateway behavior upon detection of the CED Tone: ▪ Relay – transfer CED in relay mode (default), ▪ Tone – transfer CED in voice/bypass mode and start fax session on V21 preamble
V.21 / V.22 / V.23 / V.32 / V.34 Modem Transport	Enum Transparent, Relay, Bypass, TransparentWithEvents	Instant	Defines the V.21 / V.22 / V.23 / V.32 / V.34 modem transport method.
Modem Bypass Payload Type	Integer 0 – 127	Instant	Defines the RTP payload type for the modem bypass payloads.
Cisco's NSE	Enum Disabled, Enabled	Instant	Enables or disables Cisco's NSE fax / modem automatic pass-through mode.

Parameter Name	Type	Provisioning Type	Description
NSE Payload Type	Integer 96 – 127	Instant	Defines Cisco's NSE packets payload type.

Table 39-5:Media Gateway Board's Coder Settings

Parameter Name	Type	Provisioning Type	Description
Caller ID Transport	Enum Disable, Relay, Reserve, Mute	Instant	Defines the Caller ID detection behavior: - Disable – the caller ID signal is not detected - DTMF digits remain in the voice stream. - Relay – currently not applicable. - Mute – the caller ID signal is detected from the Tel/PSTN side and then erased from the voice stream.
Default Caller ID	Enum Bellcore(0), ETSI(1), NTT(2), British(4), ETSI-ETS(16), Denmark(17), Indian(18), Brazilian(19)	Instant	Defines the default Caller ID type.

Table 39-6: Media Gateway Board's NFS Server Settings

Parameter Name	Type	Provisioning Type	Description
Default Coder	String	Online	Defines default voice coder to be used by the Media Gateway board. Typically voice coder is negotiated via the call control protocol, hence this setting has low importance.
Default Packetization Period	Integer 0 – 200	Instant	Defines the default packetization period.

Table 39-7:Media Gateway Board's No Op Settings

Parameter Name	Type	Provisioning Type	Description
No Op Mode	Enum Disable, Enable	Instant	Enables or disables the transmission of RTP or T.38 No-Op packets. This mechanism ensures that the NAT binding remains open during RTP or T.38 silence periods.
No Op Interval (msec)	Integer 20 – 65000	Instant	Defines the time interval in which RTP or T.38 No-Op packets are sent in the case of silence (no RTP / T.38 traffic) when No-Op packet transmission is enabled.
No Op Payload Type	Integer 96 – 127	Instant	Defines the payload type for No-Op packets.

Table 39-8: Media Gateway Board's NFS Settings

Parameter Name	Type	Provisioning Type	Description
NFS Profile	Integer 0 – 5	Online	Defines the index of the NFS Profile attached to this board. The NFS Profile defines NFS servers that can connect to a specific TP board and transfer files to/from it.
NFS Base Port	Integer 0 – 65535	Online	Defines base UDP port for NFS protocol.

39.1 DSP Templates

The Media Gateway board may be configured to work with up to two DSP templates simultaneously. Each DSP template supports specific voice coders, channel capacity and features.



Note: For the list of supported DSP templates and detailed specification of each DSP template, refer to LTR-90XXX Mediant 5000 and 8000 Release Notes.

A Single DSP template may be configured via the DSP Template Number parameter as described in the previous section. Multiple DSP templates must be defined via the DSP Template objects as described below.

➤ To add and configure the DSP Template:

1. Click  to access the Media Gateway status screen.
2. In the Navigation Pane, select **Media** ➤ **DSP Templates**; the DSP Templates list is displayed.
3. Use the  or  buttons to add or remove entries.
4. Select a specific row and then in the configuration pane, click **DSP Template Settings**; the DSP Template Settings screen is displayed.
5. Configure the DSP Template parameters according to the table 'DSP Template Settings' below.
6. Click the Maintenance icon  and select **Unlock** to activate the configuration.

Table 39-9: DSP Template Settings

Parameter Name	Type	Provisioning Type	Description
DSP Template Number	Enum G723(0), AMR(1), EVRC(2), iLBC(3), AMRWB(4), EVRCB(5), G729EV12(6), EG711iLBC(7), G729EV32(8), RTANB(9),T38Ver3(10), RTAWB(11)	Online	Defines the DSP template to be used by the Media Gateway board. Each DSP template supports specific voice coders, channel capacity and features.

Parameter Name	Type	Provisioning Type	Description
DSP Resources Percentage	Integer 0-100	Online	Defines how many of the Media Gateway board's DSP channels this template will be applied

39.2 AMR Coder Policy

AMR voice coder supports adaptive rate change according to the network performance and voice quality. The voice quality is determined by measuring the packet loss. When one side of the call detects the significant change in voice quality, it sends a special command to the other side requesting the change in the coder rate.

The AMR coder rate policy is defined in the 3G specification 44.318. It may be configured in one of the following ways:

- Pre-configured AMR coder policy provisioned on the Media Gateway board
- Dynamic AMR coder policy configured via the call control protocol (MGCP) by the Media Gateway Controller



Note:

- Pre-configured AMR coder policy is supported for TP-6310/IPM-6310 boards only.
- When AMR coder policy is pre-configured on Media Gateway board, a similar configuration should be applied to both Media Gateways that participate in the call.

39.2.1 Configuring Pre-defined AMR Coder Rate Policy

Pre-defined AMR coder rate policy may be provisioned on the Media Gateway by defining the AMR Profile with a number of AMR Coder Policies. Each AMR Coder Policy corresponds to the specific AMR coder rate and defines network conditions when it's used.

AMR Profiles must be attached to the Media Gateway boards to activate them. A single AMR Profile may be attached to multiple boards. Or, alternatively, separate profiles may be defined for each board.

➤ **To add and configure the AMR Coder Profile:**

1. Click  to access the Media Gateway status screen.
2. In the Navigation pane, select **Media ► AMR Profiles**; the AMR Coder Profiles list is displayed.
3. Use the  or  buttons to add or remove entries.
4. Select a specific row and then in the configuration pane, select **AMR Policies**; the AMR Policy Rules list is displayed, showing all AMR policy rules defined for a specific AMR Profile.
5. Use the  or  buttons to add or remove entries.
6. Select a specific row and then in the configuration pane, click **AMR Codec Policy Settings**; the AMR Policy Rule Settings screen is displayed.
7. Configure the AMR Policy Rules according to the following rules:
 - For each AMR Policy Rule, ensure that the Current Threshold value is greater than the current Hysteresis value.
 - Ensure that AMR Policy Rules are defined in an descending Rate order – i.e. from high to low rate
 - Ensure that AMR Policy Rules are defined in a descending Thresholds order – i.e. from high to low threshold
 - Ensure that AMR Policy Rules are defined in a descending Hysteresis order – i.e. from high to low hysteresis
8. Unlock the AMR Policy Rule to activate the new configuration.

➤ **To attach the AMR Coder Profile to the specific Media Gateway board:**

1. Click  to access the Media Gateway status screen.
2. Select the specific Media Gateway board.
3. In the Navigation pane, select **Media ► AMR Profiles** and then in the configuration pane, click **AMR Codec Profile Settings**; the AMR Codec Profile Settings screen is displayed.
4. Configure the **Profile Name** parameter to match the specific AMR Coder Profile.

Table 39-10: AMR Coder Profile Settings

Parameter Name	Type	Provisioning Type	Description
Profile Name	String Up to 40 chars	Instant	Defines a textual name of the AMR Coder Profile enabling user to easily identify it.
Referenced By	String Up to 255 chars	Read-Only	Indicates VoP boards associated with this AMR Coder Profile.

Table 39-11: AMR Coder Policy Settings

Parameter Name	Type	Provisioning Type	Description
Rule Name	String Up to 20 chars	Instant	Defines a textual name for the AMR Codec Policy enabling user to easily identify it.
Current Rate	Integer 0 – 8	Read-Only	Indicates the current AMR Rate.
Current Redundancy Level	Integer 0 – 3	Read-Only	Indicates the current Redundancy Level.
Current Threshold	Integer 0 – 63	Read-Only	Indicates the current Frame Loss Ratio (FLR) threshold.
Current Hysteresis	Integer 0 – 15	Read-Only	Indicates the current Hysteresis of FLR threshold.
Rate	Integer 0 – 8	Online	Defines the new AMR Rate. Upon successful Unlock action, this value is copied to the Current Rate parameter and applied to all related boards.
Redundancy Level	Integer 0 – 3	Online	Defines the new Redundancy Level. Upon successful Unlock action, this value is copied to the Current Redundancy Level parameter and applied to all related boards.

Parameter Name	Type	Provisioning Type	Description
Threshold	Integer 0 – 63	Online	Defines the new Frame Loss Ratio (FLR) threshold. Upon successful Unlock action, this value is copied to the Current Threshold parameter and applied to all related boards.
Hysteresis	Integer 0 – 15	Online	Defines the new Hysteresis of FLR threshold. Upon successful Unlock action, this value is copied to the Current Hysteresis parameter and applied to all related boards.

This page is intentionally left blank.

Part V

Configuring and Operating the Media Gateway (Part 3)-SIP Subsystem

This part describes the hardware overview of the Mediant 8000 chassis.

SIP (**S**ession **I**nitiation **P**rotocol) is a standards-based application-layer call control protocol defined by IETF RFC 3261. SIP is used on the Media Gateway for creating, modifying, and terminating sessions with one or more participants. These sessions can include Internet telephone calls, media announcements and conferences.

The Mediant 8000 supports the following SIP applications:

- PSTN Gateway – provides gateway functionality between the PSTN and IP networks
- IP-to-IP – provides IP-to-IP call routing functionality
- SBC – provides Session Border Controller (SBC) functionality

Each Media Gateway board operates as a stand-alone SIP Media Gateway. Therefore, the SIP configuration is performed independently for each Media Gateway board.

SIP subsystem configuration consists of the following categories:

- General SIP configuration – applicable to all applications (see page [547](#))
- PSTN Gateway and IP-to-IP configuration – applicable to PSTN Gateway and IP-to-IP applications (see page [649](#))
- SAS Configuration (see page [715](#))
- SBC configuration – applicable to SBC application (see page [725](#))

40 General SIP Configuration

The general SIP configuration includes the following objects:

- SIP Proxy Configuration
- SIP Registrar Configuration
- SIP Protocol Settings
- Coders Table
- IP Group Table
- IP Profile Table
- Account Group Table
- Internal DNS Table
- SIP SRV to IP Table
- SRD Table
- SIP Interfaces Table
- NAT Translation Table
- Least Cost Routing (LCR)Table

40.1 The SIP Proxy

The **SIP Proxy** servers are used by Media Gateway board to perform the routing of the SIP requests. Although you can configure internal SIP routing rules inside the Media Gateway board, a centralized architecture in which routing is performed by a SIP Proxy server (or a group of servers) is recommended for the typical Mediant 8000 installation.

40.1.1 SIP Proxy Set

The SIP Proxy Set is a group of SIP Proxy servers defined by IP address or fully qualified domain name (FQDN). You can define up to six Proxy Sets, each with a unique ID number and each containing up to five Proxy server addresses. For each Proxy server address, you can define the transport type (i.e., UDP, TCP, or TLS). In addition, Proxy load balancing and redundancy mechanisms can be applied per Proxy Set (if a Proxy Set contains more than one Proxy address).

Proxy Sets can later be assigned to IP Groups of type SERVER only (see 'IP Groups Table' on page 611). When the device sends an INVITE message to an IP Group, it is sent to the IP address/domain name defined for the Proxy Set that is associated with the specific IP Group. In other words, the Proxy Set represents the destination of the call.

Typically, for IP-to-IP call routing, at least two Proxy Sets are defined for the call destination – one for each leg (IP Group) of the call (i.e., both directions). For example, one Proxy Set for the Internet Telephony Service provider (ITSP) interfacing with one 'leg' of the device and another Proxy Set for the second SIP entity (e.g., ITSP) interfacing with the other 'leg' of the device.

40.1.2 Redundancy Mechanisms

For each Proxy set, one of the following mechanisms for switching between SIP Proxy server addresses are available:

■ Proxy Keep Alive Redundancy

Media Gateway board periodically sends keep-alive messages to the SIP Proxy Server. If there is no response from the Primary Proxy, Media Gateway board tries to communicate with Redundant Proxies. When a Redundant Proxy is found, the Media Gateway starts using it. When connection with the Primary Proxy is restored, Media Gateway board may either immediately revert to it or continue using the current Redundant Proxy until a failure occurs.

See the parameters **Enable Proxy Keep Alive** and **Redundancy Mode**.

■ Proxy Hot Swap Redundancy

Media Gateway board can also provide real-time switching (Hot Swap) between the Primary and Redundant Proxies (see **Enable Proxy Hot Swap** parameter). If the first Proxy does not respond to an INVITE message, the same INVITE message is immediately sent to the second Proxy. See the parameters **Enable Proxy Hot Swap** and **Proxy Hot Swap Retx**.

40.1.3 DNS Service Records (SRV)

DNS Service Records (SRV) may be used to discover the SIP Proxy servers when their **Proxy IP** parameter contains a domain name. See the parameter **DNS Query Type** in the SIP Protocol Settings table.

For fallback routing, when communication with the SIP Proxy is lost, or for traffic load balancing, you can use internal routing tables (Tel to IP) inside the Media Gateway board. See the parameters **Preferred Routing Table** and **Always Use Proxy** in the SIP Proxy Set table.

40.1.4 SIP Proxy Sets

This section describes how to configure SIP Proxy sets.

➤ To configure SIP Proxy sets:

1. Click  to access the Media Gateway status screen.
2. Select the desired Media Gateway SIP board.
3. In the Navigation pane, select **SIP ► SIP General** and then in the configuration pane, click **SIP Protocol Settings**; the SIP Protocol Settings screen is displayed.
4. In the **Proxy Settings** tab, set **Enable Proxy** to Yes and configure additional parameters as described in the table "SIP Proxy Settings" below.
5. In the Navigation pane, select **SIP ► SIP General ► Proxy Set**; the SIP Proxy Sets list is displayed.
6. Use the  or  buttons to add or remove entries.
7. Select a specific row in the Proxy Sets list and then in the configuration pane, select **Proxy Set Settings**; the Proxy Set Settings screen is displayed.

8. In the **General Settings** tab, configure Proxy Set parameters as described in the table “SIP Proxy Set Settings” below.
9. In the **Proxy Servers** tab, configure the IP address of the SIP Proxy Server as described in table “SIP Proxy Server Parameters” below. For the redundant SIP Proxies configuration, add as many SIP Proxy Servers as required.
10. Unlock the SIP Proxy Set by selecting the corresponding row in the SIP Proxy Sets list and, in the Actions bar, clicking **Unlock**.

Table 40-1: SIP Proxy Set Parameters

Parameter Name	Type	Provisioning Type	Description
Enable Proxy	Enum No, Yes	Instant	Enables use of the SIP Proxy Server: - No – Proxy isn't used and the internal routing table is used instead. - Yes – Proxy is used.
Proxy Name	String Up to 49 chars	Instant	Defines the Home Proxy Domain Name. If specified, the name is used as Request-URI in REGISTER, INVITE and other SIP messages. If not specified, the Proxy IP address is used instead.
Is Trusted Proxy	Enum Disable, Enable	Instant	Defines whether the SIP Proxy is trusted or not. If the Proxy is not trusted, the P-asserted header is not used.
CRLF Keep Alive	Enum Disable, Enable	Instant	Enables or disables use of the CRLF keep-alive mode as per RFC 5626. The option is valid for TCP and TLS SIP transport types only.
CRLF Keep Alive Max Interval (sec)	Integer 5 – 2000000	Instant	Defines the maximum CRLF keep-alive interval.
Proxy Redundancy Mode	Enum Parking, Homing	Instant	Defines fall-back behavior of Proxy Keep-Alive Redundancy Mode: - Parking Gateway continues working with the last active Proxy until the next failure - Homing Gateway always tries to work with the primary Proxy server (switches back to the main Proxy whenever it is available). Note: To use Proxy Redundancy Mode, enable Keep-alive with Proxy option ('Enable Proxy Keep Alive').

Parameter Name	Type	Provisioning Type	Description
Number of RTX Before Hot-Swap	Integer 1 – 30	Instant	Defines the number of retransmitted INVITE/REGISTER messages before a call is routed (hot swap) to another Proxy/Registrar. Note: This parameter is also used for alternative routing using the Tel to IP Routing table. If a domain name in the routing table is resolved into two IP addresses, and if there is no response for specified number of retransmissions to the INVITE message that is sent to the first IP address, the gateway immediately initiates a call to the second IP address.
Enable Fallback To Routing Table	Enum Disable, Enable	Instant	Enables or disables use of internal Tel to IP Routing table when Proxy servers are not available. When the gateway falls back to the internal Tel to IP Routing table, it continues scanning for a Proxy. When the gateway locates an active Proxy, it switches from internal routing back to Proxy routing.
Prefer Routing Table	Enum Disable, Enable	Instant	Defines if the local Tel to IP routing table takes precedence over a Proxy for routing calls: - Disable – only Proxy is used to route calls (default). - Enable – the Proxy checks the 'Destination IP Address' field in the 'Tel to IP Routing' table for a match with the outgoing call. Only if a match is not found, a Proxy is used. Note: Applicable only if Proxy is not always used (i.e. both Always Use Proxy and Send INVITE to Proxy are <i>Disabled</i>).
Always Use Proxy	Enum No, Yes	Instant	Defines SIP messages routing rules when SIP Proxy server is used: - No – use standard SIP routing rules - Yes – send all SIP messages and responses to SIP Proxy Server Note: Applicable only if Proxy server is used.

Parameter Name	Type	Provisioning Type	Description
Use Routing Table For Host Names	Enum Disable, Enable	Instant	Enables use of the internal Tel to IP routing table to obtain the URI Host name and (optionally) an IP profile (per call), even if Proxy server is used.
Redundant Routing Mode	Enum NoRedundant, RoutingTable, RedundantProxy	Instant	Defines the type of redundant routing mechanism to implement when a call can't be completed using the main route.
ReRouting Mode	Enum Standard, Proxy, RoutingTable	Instant	Define the Gateway action as a result of receiving 3xx or Transfer response: - Standard – send Invite according to standard behavior - Proxy – send IINVITE to Proxy. RoutingTable – send INVITE according to Routing Table.
Use Routing Table when Proxy Fails	Enum No, Yes	Instant	Defines SIP messages routing rules when SIP Proxy server fails: - No – Gateway fallback is not used. - Yes – Internal Tel to IP Routing table is used when Proxy servers are not available. When the gateway falls back to the internal Tel to IP Routing table, the gateway continues scanning for a Proxy. When the gateway finds an active Proxy, it switches from internal routing back to Proxy routing.
Send Invite To Proxy	Enum Disable, Enable	Instant	Defines routing rules for SIP 'INVITE' messages: - Disable – INVITE messages, generated as a result of Transfer or Redirect, are sent directly to the URL (according to the refer-to header in the REFER message or contact header in 30x response). - Enable – all INVITE messages, including those generated as a result of Transfer or Redirect are sent to Proxy. Note: Applicable only if Proxy server is used and Always Send to Proxy is <i>Disabled</i> .

Parameter Name	Type	Provisioning Type	Description
Use Gateway Name For Options	Enum Disable, Enable	Instant	Defines Request-URI host part in SIP 'OPTIONS' messages, used for keep-alive with SIP Proxy servers: - Disable – use the gateway's IP address in keep-alive OPTIONS messages (default). - Enable – use 'GatewayName' in keep-alive OPTIONS messages.
Proxy DNS Query Type	Enum A-Record, SRV, NAPTR	Instant	Enables the use of DNS Naming Authority Pointer (NAPTR) and Service Record (SRV) queries to discover Proxy servers: - If set to A-Record, no NAPTR or SRV queries are performed. - If set to SRV and the Proxy IP address parameter contains a domain name without port definition (e.g., ProxyIP = domain.com), an SRV query is performed. The SRV query returns up to four Proxy host names and their weights. The gateway then performs DNS A-record queries for each Proxy host name (according to the received weights) to locate up to four Proxy IP addresses. Therefore, if the first SRV query returns two domain names, and the A-record queries return two IP addresses each, no more searches are performed. - If set to NAPTR, an NAPTR query is performed. If it is successful, an SRV query is sent according to the information received in the NAPTR response. If the NAPTR query fails, an SRV query is performed according to the configured transport type. If the Proxy IP address parameter contains a domain name with port definition (e.g., "domain.com:5080"), the gateway performs a regular DNS A-record query. Note: When enabled, NAPTR/SRV queries are used to discover Proxy servers even if the parameter DNS Query Type is <i>Disabled</i>.

Parameter Name	Type	Provisioning Type	Description
Proxy IP List Refresh Time	Integer 5 – 2000000	Instant	Defines the time interval (in seconds) between refreshes of the Proxy IP list. This parameter is only used for SIP Proxy Sets where Proxy Load Balancing Method is set to <i>RoundRobin</i> .

Table 40-2: SIP Proxy Set Settings

Parameter Name	Type	Provisioning Type	Description
Name	String Up to 20 chars.	Instant	Defines the name of SIP Proxy Set used to identify it easily.
Proxy Load Balancing Method	Enum Disable, RoundRobin, RandomWeights	Instant	Enables usage of the Proxy Load Balancing mechanism: ▪ Disable – disable Proxy Load Balancing ▪ RoundRobin - A list of all possible Proxy IP addresses is compiled. This list includes all entries in the ProxyIP table after necessary DNS resolutions (including NAPTR and SRV, if configured). After this list is compiled, the Proxy Keep-Alive mechanism (according to EnableProxyKeepAlive and ProxyKeepAliveTime parameters) is used to mark each entry as Offline or Online. The balancing is only performed on Proxy servers that are marked as Online. All outgoing messages are equally distributed across the Proxy IP list. REGISTER messages are also distributed unless a RegistrarIP is configured. The Proxy IP list is refreshed according to ProxyIPListRefreshTime. If a change in the order of the entries in the list occurs, all load statistics are erased and balancing starts over again. ▪ Random Weights – the outgoing

Parameter Name	Type	Provisioning Type	Description
			requests are not spread out equally between the Proxies. The weights are received from the DNS server by using SRV records. The gateway sends the requests in such a manner that each Proxy receives a percentage of the requests according to its assigned weight. The Random Weights Load Balancing is not used in the following situations: ▪ The Proxy Set contains more than one Proxy IP address ▪ The ProxyIP parameter of the sole defined SIP Proxy is an IP address and not an FQDN. ▪ SRV usage is not enabled ('Proxy DNS Query Type'). ▪ -SRV response includes several records with a different Priority value.

Parameter Name	Type	Provisioning Type	Description
Enable Proxy Keep Alive	Enum Disable, UsingOptions, UsingRegister, UsingCRLF	Instant	Enables Proxy Keep Alive Redundancy mode (via keep-alive messages): ▪ Disable – disable redundancy ▪ UsingOptions – enable redundancy via OPTIONS messages ▪ UsingRegister – enable redundancy via REGISTER messages ▪ Using CRLF – enable redundancy using carriage return and line feed (CRLF) keep-alives, as per RFC 5626. If set to UsingOptions, the SIP OPTIONS message 'Proxy Keep-Alive Time' is sent every 'Proxy Keep-Alive Time'. If set to UsingRegister, the SIP REGISTER message is sent every 'Registration Time'. Any response from the Proxy server, either success (200 OK) or failure (4xx response), is considered as if the Proxy server is communicating correctly. Notes: ▪ To enable survivability mode for USER-type IP Groups, set this parameter to UsingOptions or UsingRegister ▪ When Proxy redundancy is used, set this parameter to UsingOptions ▪ When the active Proxy doesn't respond to INVITE messages sent by the gateway, the Proxy is marked as Offline. This behavior is similar to the keep-alive failure.
Proxy Keep Alive Time	Integer 5-2000000	Instant	Defines the Proxy keep-alive time interval (in seconds) between OPTIONS messages. Applicable only when Enable Proxy Keep Alive is set to UsingOptions.

Parameter Name	Type	Provisioning Type	Description
Proxy Redundancy Mode	Enum NotConfigured, Parking, Homing	Instant	Defines fall-back behavior of Proxy Set Keep-Alive Redundancy Mode: - Not Configured – use Proxy global parameter - Parking – Media Gateway continues working with the last active Proxy until the next failure - Homing – Media Gateway always tries to work with the primary Proxy server (switches back to the main Proxy whenever it is available). Note: to use Proxy Redundancy Mode, enable keep-alive with Proxy via 'Enable Proxy Keep Alive' parameter.
Is Proxy Hot Swap	Enum No, Yes	Instant	Enables Proxy Hot Swap Redundancy mode: - No – Disable. - Yes – Enable Proxy Keep-Alive Redundancy. If Proxy Hot Swap Redundancy is enabled, the SIP INVITE/REGISTER message is initially sent to the first Proxy/Registrar server. If there is no response from the first Proxy/Registrar server for 'ProxyHotSwapRtx' number of retransmissions, the SIP INVITE/REGISTER message is resent to the next redundant Proxy/Registrar server.
SRD	Integer 0 – 32	Instant	Index of the associated SRD

Parameter Name	Type	Provisioning Type	Description
Classification Input	Enum CompareOnlyIP, CompareIP_Port_TransportType	Instant	Classifies an IP call to a Proxy Set based either on its IP address, or its IP address, port and transport type. ▪ [0] Compare only IP = IP call classified to Proxy Set according to IP address only (default). ▪ [1] Compare IP, port and transport type = IP call classified to Proxy Set according to IP address, port, and transport type.

Table 40-3: SIP Proxy Server Settings

Parameter Name	Type	Provisioning Type	Description
Name	String Up to 20 chars.	Instant	Defines the name of the SIP Proxy Server used to identify it easily.
IP Address	String Up to 49 chars.	Instant	Defines the IP address or domain name (FQDN) of the SIP Proxy Server. Non-default port number may be specified by appending ":" to the IP Address/FQDN, for example: "10.7.3.1:5080".
Transport Type	Enum Undefined, UDP, TCP, TLS	Instant	Defines the transport type of the SIP Proxy Server.

40.2 The SIP Registrar

The SIP board may be configured to send REGISTER messages to SIP Registrar or Proxy servers. The registration request is resent according to the parameters, **Re-registration Timing (%)** and **Registration Time**. For example, if **Re-registration Timing = 70 (%)** and **Registration Time = 3600**, the Media Gateway resends its registration request after $3600 \times 70\% = 2520$ sec.

➤ To configure SIP Registrar:

1. Click  to access the Media Gateway status screen.
2. Select the desired SIP board.
3. In the Navigation pane, select **SIP ▶ SIP General** and then in the configuration pane, click **SIP Protocol Settings**; the SIP Protocol Settings screen is displayed.
4. In the **Registration Options** tab, configure SIP Registration parameters, as described in the table below.

Table 40-4: SIP Registration and Authentication Settings

Parameter Name	Type	Provisioning Type	Description
Enable Registration	Enum No, Yes	Instant	Enables registration with SIP Proxy/Registrar. ▪ No – gateway doesn't register to Proxy/Registrar ▪ Yes – gateway register to Proxy/Registrar at power up

Parameter Name	Type	Provisioning Type	Description
Registrar IP Address	String Up to 15 chars.	Instant	IP address (or FQDN) and optionally port number of Registrar server. If not specified, the Gateway registers to Proxy server. Note: When port number is specified, DNS NAPTR/SRV queries aren't performed, even when 'Proxy DNS Query Type' is set accordingly.
Registration Time	Integer 10-2000000	Instant	Defines the time (in seconds) for which registration to a Proxy server is valid. The value is used in the header 'Expires'. Typically, a value of 3600 should be assigned for one hour registration. The gateway resumes registration according to the parameter 'Re-registration Timing (%)'.
Registration Retry Time	Integer 10-2000000	Instant	Defines the time period (in seconds) after which a Registration request is resent if registration fails with 4xx, or there is no response from the Proxy/Registrar.
Registrar Name	String Up to 49 chars.	Instant	Defines the Registrar Domain Name. If specified, the name is used as Request-URI in REGISTER messages. If not specified, the Registrar IP address or Proxy name or Proxy IP address is used instead.
Re-registration Timing (%)	Integer 30-100	Instant	Defines the re-registration timing (as a percentage). The timing is a percentage of the re-register timing set by the Registration server. For example: If 'Re-registration Timing = 70' (%) and 'Registration Time = 3600', the gateway resends its registration request after $3600 \times 70\% = 2520$ sec.
Gateway Registration Name	String Up to 15 chars.	Instant	Defines the user name that is used in From and To headers of REGISTER messages. If this parameter isn't specified, the 'Username' parameter is used instead.
Gateway Name	String Up to 49 chars.	Instant	Defines the Gateway Name. If specified, the Gateway Name is used as the host part of the SIP URL, in both 'To' and 'From' headers. If not specified, the Gateway IP address is used instead.

Parameter Name	Type	Provisioning Type	Description
Registrar Transport Type	Enum NotConfigured, UDP, TCP, TLS	Instant	Defines the transport layer used for outgoing SIP dialogs initiated by the device to the Registrar.
Registration Time Threshold (Sec)	Integer 0-2000000	Instant	Defines a threshold (in seconds) for re-registration timing. If this parameter is greater than 0, but lower than the time computed according to the Re-Registration Timing (%) parameter, the re-registration timing is set to the time set by the Registration server in the Expires header minus the value of the Registration Time Threshold.
Set Out-Of-Service On Registration Failure	Enum Disable, Enable	Instant	Enables setting a trunk or the entire SIP board (i.e., all endpoints) to out-of-service if registration fails. If the registration is per Endpoint or Account (i.e., AuthenticationMode is set to PerEndpoint) and a specific endpoint/account registration fails (SIP 4xx or no response), then this endpoint is set to out-of-service until a success response is received in a subsequent registration request. When the registration is per the SIP board (i.e., AuthenticationMode is set to PerGateway) and registration fails, all endpoints are set to out-of-service. If all accounts of a specific Trunk Group fail registration and if the Trunk Group comprises a complete trunk, then the trunk is set to out-of-service.
Enable User-Information Usage	Enum Disable, Enable	Instant	Enables or disables usage of the User Information loaded to the gateway via the User Information auxiliary file.
Number Of Active Dialogs	Integer 0 – 20	Instant	Defines the maximum number of active SIP dialogs that are not call related (i.e., REGISTER and SUBSCRIBE). This parameter is used to control the Registration / Subscription rate.
Authentication User Name	String Up to 15 chars	Instant	Defines the username used for Registration and for BASIC/DIGEST authentication process with Proxy. Note: Applicable only if Authentication Mode is <i>Per Gateway</i>.
Authentication	String	Instant	Defines the password used for

Parameter Name	Type	Provisioning Type	Description
Password	Up to 15 chars		BASIC/DIGEST authentication process with Proxy. Single password is used for all gateway ports.
Cnonce	String Up to 15 chars	Instant	Defines a Cnonce string used by the server and client to provide mutual authentication.
Mutual Authentication Mode	Enum Optional, Mandatory	Instant	Defines the mode of operation when Authentication and Key Agreement (AKA) Digest Authentication is used.
Challenge Caching Mode	Enum None, InviteOnly, Full	Instant	Defines the mode used for Challenge Caching. Challenge Caching is used to reduce the number of SIP messages transmitted through the network. The first request to the Proxy is sent without authorization. In return, the Proxy sends a 401/407 response with a challenge. This response is saved for further uses. A new request is resent with the appropriate credentials. Subsequent requests to the Proxy are sent with credentials (calculated from the saved challenge). If the Proxy doesn't accept the new request and sends another challenge instead, the old challenge is replaced with the new one.
Enable User-Information Usage	Enum Disable, Enable	Instant	Enables or disables usage of the User Information loaded to the gateway via the User Information auxiliary file.
Number Of Active Dialogs	Integer 0 – 20	Instant	Defines the maximum number of active SIP dialogs that are not call related (i.e., REGISTER and SUBSCRIBE). This parameter is used to control the Registration / Subscription rate.
Authentication User Name	String Up to 15 chars	Instant	Defines the username used for Registration and for BASIC/DIGEST authentication process with Proxy. Note: Applicable only if Authentication Mode is <i>Per Gateway</i> .
Authentication Password	String Up to 15 chars	Instant	Defines the password used for BASIC/DIGEST authentication process with Proxy. Single password is used for all gateway ports.
Cnonce	String Up to 15 chars	Instant	Defines a Cnonce string used by the server and client to provide mutual authentication.
Mutual	Enum	Instant	Defines the mode of operation when

Parameter Name	Type	Provisioning Type	Description
Authentication Mode	Optional, Mandatory		Authentication and Key Agreement (AKA) Digest Authentication is used.
Challenge Caching Mode	Enum None, InviteOnly, Full	Instant	Defines the mode used for Challenge Caching. Challenge Caching is used to reduce the number of SIP messages transmitted through the network. The first request to the Proxy is sent without authorization. In return, the Proxy sends a 401/407 response with a challenge. This response is saved for further uses. A new request is resent with the appropriate credentials. Subsequent requests to the Proxy are sent with credentials (calculated from the saved challenge). If the Proxy doesn't accept the new request and sends another challenge instead, the old challenge is replaced with the new one.
Authentication Mode	Enum PerGateway, PerEndpoint	Instant	Defines the registration and authentication method used by the SIP board: - Per Endpoint – Registration and Authentication is performed separately for each B-channel. - Per Gateway – Single Registration and Authentication is performed for each SIP board (the recommended configuration).
Add initial Route Header	Enum Disable, Enable	Instant	Determines whether the SIP Route header is included in initial registration or re registration (REGISTER) requests sent by the device. When the device sends a REGISTER message, the Route header includes either the Proxy's FQDN or the IP address and port according to the configured Proxy Set.

40.3 SIP Protocol Settings

The SIP Protocol Settings screen allows you to configure different aspects of the SIP call control protocol implementation, provided by the Mediant 8000.

➤ To configure SIP Protocol Settings:

1. Click  to access the Media Gateway status screen.
2. Select the desired SIP board.
3. In the Navigation pane, select **SIP** ➤ **SIP General** and then in the configuration pane, click **SIP Protocol Settings**; the SIP Protocol Settings screen is displayed.
4. Configure the SIP protocol settings as described in the tables below. Note that parameters in Proxy Settings and Registration and Authentication tabs were already described in previous chapters.

Table 40-5: SIP General Settings

Parameter Name	Type	Provisioning Type	Description
Transport Type	Enum UDP, TCP, TLS	Instant	Defines SIP messages transport type.
Enable SIPS	Enum Disable, Enable	Instant	Enables secured SIP (SIPS) connections over multiple hops. ▪ When Transport Type is <i>TLS</i> and Enable SIPS is <i>Disabled</i>, TLS is used for the next network hop only. ▪ When Transport Type is <i>TLS</i> and Enable SIPS is <i>Enabled</i>, TLS is used through the entire connection (over multiple hops). ▪ When Transport Type is <i>UDP</i> and Enable SIPS is <i>Enabled</i>, the connection fails.
SIP Local Port	Integer 1 – 65535	Instant	Defines local UDP port used to receive SIP messages.
TCP Local Port	Integer 1 – 65535	Instant	Defines local TCP port used to receive SIP messages.
TLS Local Port	Integer 1 – 65535	Instant	Defines local TLS port used to receive SIP messages. The value must differ from TCP Local Port .
SIP Destination Port	Integer 1 – 65535	Instant	Defines SIP destination port for sending initial SIP requests. Note: SIP responses are sent to the port specified in the Via header.

Parameter Name	Type	Provisioning Type	Description
TCP Connection Reuse	Enum Disable, Enable	Instant	Enables the reuse of the same TCP connection for all calls to the same destination.
TCP Timeout (sec)	Integer 0 – 40	Instant	Defines the Timer B (INVITE transaction timeout timer) and Timer F (non-INVITE transaction timeout timer), as defined in RFC 3261, when the SIP Transport Type is TCP.
TLS two-way authentication	Enum Disable, Enable	Instant	Defines the TLS PKI two-way authentication option: - Disable – gateway doesn't require client certificate. - Enable – gateway, when acting as a server for the TLS connection, requires reception of the client certificate to establish the TLS connection.
TLS Re Handshake Interval	Integer 0 – 1500	Instant	Defines the time interval (in minutes) between TLS Re-Handshakes initiated by the Board. Value 0 means that no TLS re-handshake is performed.
TLS Verify Server Certificate	Enum Disable, Enable	Instant	Defines whether the gateway, when acting as client for TLS connections, verifies the Server certificate.

Parameter Name	Type	Provisioning Type	Description
Secure Calls from IP	Enum Disable, SecureIncomingCalls, SecureAllCalls	Instant	Determines the device's handling (allowing or rejecting) of the receipt of IP calls. This feature is useful for preventing unwanted SIP calls, SIP messages, and/or VoIP spam. ▪ [0] Disable = The device accepts all SIP calls (default). ▪ [1] Secure Incoming Calls = The device accepts SIP calls only from IP addresses defined in the 'Outbound IP Routing' table/'Tel to IP Routing' or Proxy Set table, or IP addresses resolved from DNS servers from FQDN which appear in the Proxy Set table. All other incoming calls are rejected. ▪ [2] Secure All Calls = The device accepts SIP calls only from IP addresses (in dotted-decimal notation format) defined in the 'Outbound IP Routing' table or Proxy Set table, and rejects all other incoming calls. In addition, if a fully-qualified domain name (FQDN) is defined in the routing table or Proxy Set table, the call is allowed to be sent only if the resolved DNS IP address appears in one of these table; otherwise it is rejected. Note: If the parameter is set to [2], when using Proxies or Proxy Sets, it's unnecessary to configure the Proxy IP addresses in the routing table. The device allows SIP calls received from the Proxy IP addresses even if these are not configured in the routing table.
Filter Calls to IP	Enum No, Yes	Instant	Enables or disabled filtering for outgoing IP calls. When enabled, the Gateway routes calls only to the IP addresses specified in the Tel to IP routing table. Calls to unknown IP addresses are rejected.
Max Number of Active Calls	Integer 1 – 2016	Instant	Defines the maximum number of calls that the gateway can have active at the same time.

Parameter Name	Type	Provisioning Type	Description
Max Call Duration	Integer 0 – 35791120	Instant	Defines the maximum call duration in minutes. If set to non-zero value and the specified time expires, both sides of the call are released (IP and Tel).
Media Security Behavior	Enum Preferable, Mandatory, PreferableSingleMedia	Instant	Defines the mode of operation when SRTP is used.

Table 40-6: SIP Protocol Settings

Parameter Name	Type	Provisioning Type	Description
DNS Query Type	Enum A-Record, SRV, NAPTR	Instant	Enables the use of DNS Service Record (SRV) queries to discover Proxy servers.
Forking Handling Mode	Enum Sequential, ParallelHandling	Instant	Defines how the device reacts to forking of outgoing INVITE messages by the Proxy. - Sequential Handling – the device opens a voice stream toward the first 18x SIP response that includes an SDP, and disregards any 18x response with an SDP received thereafter. - Parallel Handling – the device opens a voice stream toward the first 18x SIP response that includes an SDP, and re-opens the stream toward any subsequent 18x responses with an SDP. Note: Regardless of the Forking Handling Mode value, once a SIP 200 OK response is received, the device uses the RTP information and re-opens the voice stream, if necessary.

Parameter Name	Type	Provisioning Type	Description
Max SIP Message Length (KB)	Integer 1 – 50	Instant	Defines the maximum length of the SIP message (in Kbytes)
SDP Version Negotiation	Enum Disable, Enable	Instant	This feature enables the flexibility of ignoring a new SDP re-offer (from the media negotiation perspective) in specific scenarios (such as session expires). According to RFC 3264, once an SDP session is established, a new SDP offer is considered a new offer only when the SDP origin value is incremented. In scenarios such as session expires, SDP negotiation is irrelevant and thus, the origin field is not changed. Even though some SIP devices don't follow this behavior and don't increment the origin value, even in scenarios where they want to re-negotiate, the device can now assume that the remote party operates according to RFC 3264, and in cases where the origin field is not incremented, the device does not re-negotiate SDP capabilities. ▪ [0] Disable = The device negotiates any new SDP re-offer, regardless of the origin field (default). ▪ [1] Enable = The device negotiates only an SDP re-offer with an incremented origin field.
Add Subject Header	String Up to 200 chars	Instant	Defines the value of the Subject header in outgoing INVITE messages. If not specified, the Subject header isn't included.

Parameter Name	Type	Provisioning Type	Description
Asserted ID Mode	Enum No Header Added, P-Asserted Id RFC3325, P-Preferred Id RFC3325	Instant	Defines the header that is used to convey the Caller ID in the generated INVITE requests. In addition to the P-asserted or P-preferred Privacy header is generated as follows: ▪ If Caller ID is restricted, the 'Privacy: id' will be added to the INVITE request. ▪ Otherwise, the 'Privacy: none' will be used.
Use Tel URI for Asserted Identity	Enum Disabled, Enabled	Instant	Defines the format of the URI in the P-Asserted-Identity and P-Preferred-Identity headers. ▪ Disable – 'sip:' ▪ Enable – 'tel:'
"User=Phone" in URL	Enum No, Yes	Instant	Defines whether ";user=phone" string is included in SIP URL.
"User=Phone" in From	Enum No, Yes	Instant	Defines whether ";user=phone" string is included in From header.
User-Agent Information	String Up to 50 chars	Instant	Defines the string that is used in the SIP request header 'User-Agent' and SIP response header 'Server'. If not configured, the default string 'AudioCodes product-name s/w-version' is used (e.g., User-Agent: Audiocodes-Sip-Gateway-TP6310/v.6.00.004.008). When configured, the string 'UserAgentDisplayInfo s/w-version' is used (e.g., User-Agent: MyNewOEM/v.6.00.004.008). Note that the version number can't be modified.

Parameter Name	Type	Provisioning Type	Description
Source Number Preference	String Up to 10 chars	Instant	Defines the SIP header used to determine the Source Number in incoming INVITE messages. ▪ P-Asserted - Use device's internal logic for header preference (default). ▪ FROM - Use the Source Number received in the From header.
Enable Contact Restriction	Enum Disabled, Enabled	Instant	Defines whether the gateway sets the Contact header of outgoing INVITE requests to 'anonymous' for restricted calls.
Reason Header	Enum Disable, Enable	Instant	Enables or disables the usage of the SIP Reason header.
RTP Only Mode	Enum Disable, TransmitAndReceive, Transmit Only, ReceiveOnly	Instant	Enables the device to start sending and/or receiving RTP packets to and from remote endpoints without the need to establish a SIP session. The remote IP address is determined according to the Outbound IP Routing table. The port is the same port as the local RTP port (configured by the parameter BaseUDPPort (see page 600) and the channel on which the call is received). ▪ [0] Disable (default) ▪ [1] Transmit & Receive = Send and receive RTP ▪ [2] Transmit Only= Send RTP only ▪ [3] Receive Only= Receive RTP only
Enable RPI Header	Enum No, Yes	Instant	Enables or disables the usage of Remote-Party-ID Headers for calling and called numbers for Tel to IP calls.

Parameter Name	Type	Provisioning Type	Description
Add Type and Number Plan to Remote Party ID Header	Enum Disable, Enable	Instant	Defines whether Type and Number Plan parameters are included in the Remote-Party-ID Header.
X Channel Header	Enum Disable, Enable	Instant	Defines whether X-Channel header, with trunk/B-channel information, is added to the INVITE requests and/or 183/180/200 OK responses.
Retry-After Time	Integer 0 – 3600	Instant	Defines the time (in seconds) used in the Retry-After header when a 503 (Service Unavailable) response is generated by the gateway.

Parameter Name	Type	Provisioning Type	Description
History Info Header	Enum Disable, Enable	Instant	Enables usage of the History-Info header. User Agent Client (UAC) Behavior: Initial request: The History-Info header is equal to the Request URI. If a PSTN Redirect number is received, it is added as an additional History-Info header with an appropriate reason. Upon receiving the final failure response, the gateway copies the History-Info as is, adds the reason of the failure response to the last entry, and concatenates a new destination to it (if an additional request is sent). The order of the reasons is as follows: Q.850 Reason SIP Reason SIP Response code Upon receiving the final (success or failure) response, the gateway searches for a Redirect reason in the History-Info (i.e., 3xx/4xx SIP Reason). If found, it is passed to ISDN according to the following table: 302 – Call Forward Universal (CFU) 408, 480, 487 – Call Forward No Answer (CFNA) 486, 600 – Call Forward Busy (CFB) If history reason is a Q.850 reason, it is translated to the SIP reason (according to the SIP-ISDN tables) and then to ISDN Redirect reason according to the table above. User Agent Server (UAS) Behavior: History-Info is sent in the final response only.
Version 6.6	571		October 2014 Upon receiving a request with History-Info, the UAS checks the policy in the request. If 'session', 'header', or 'history' policy tag is found, the (final) response is sent without History-Info. Otherwise, it

Parameter Name	Type	Provisioning Type	Description
Diversion Header Format	Enum Tel, SIP	Instant	Defines the URI format in the Diversion header. If History User Header exists, it is used instead of Diversion header.
Prefix to Redirect Number	String Up to 8 chars	Instant	Defines a string Prefix that is added to the Redirect number which is received from the Tel side. This Prefix is added to the Redirect Number in the Diversion header.
Enable P-Charging Vector	Enum Disabled, Enabled	Instant	Enables the addition of a P-Charging-Vector header to all outgoing INVITE messages.

Parameter Name	Type	Provisioning Type	Description
Enable GRUU	Enum Disable, Enable	Instant	Determines whether or not the GRUU mechanism is used. The gateway obtains a GRUU by generating a normal REGISTER request. This request contains a Supported header field with the value gruu. The gateway includes a '+sip.instance' Contact header field parameter for each contact for which the GRUU is required. This Contact parameter contains a globally unique ID that identifies the media server instance. The global unique ID is as follows: If registration is per endpoint, it is the MAC address of the device concatenated with the phone number of the endpoint. If the registration is per Media Gateway board it is only the MAC address. When the User Information mechanism is used, the globally unique ID is the MAC address concatenated with the phone number of the endpoint (defined in the User-Info file). If the Registrar/Proxy supports GRUU, the REGISTER responses contain the 'gruu' parameter in each Contact header field. The Registrar/Proxy provides the same GRUU for the same AOR and instance-id in case of sending REGISTER again after expiration of the registration. The device places the GRUU in any header field which contains a URI. It uses the GRUU in the following messages: INVITE requests, 2xx responses to INVITE, SUBSCRIBE requests, 2xx responses to SUBSCRIBE, NOTIFY requests, REFER requests, and 2xx responses to REFER.
Version 6.6	573		October 2014 Note: If the GRUU contains the 'opaque' URI parameter, the device obtains the AOR for the user by stripping the parameter. The resulting URI is the AOR.

Parameter Name	Type	Provisioning Type	Description
Sip Session Expires	Integer 0 – 1999999	Instant	Defines the numerical value that is sent in the Session-Expires header in the first INVITE request or response (if the call is answered). Value 0 disables use of the Session-Expires header.
Minimum Session-Expires (sec)	Integer 10 – 100000	Instant	Defines the time (in seconds) that is used in the Min-SE header. This header defines the minimum time that the user agent refreshes the session.
Session Expires Method	Enum ReInvite, Update	Instant	Defines the SIP method used for session-timer updates. Notes: The gateway can receive session-timer refreshes using both methods. The UPDATE message used for session timer updates lacks the SDP body.
Prack Mode	Enum Disabled, Supported, Required	Instant	Defines PRACK (Provisional Acknowledgment) mechanism mode for 1xx SIP reliable responses. Notes: The Supported and Required headers contain the '100rel' tag. The gateway sends PRACK messages if 180/183 responses are received with '100rel' in the Supported or Required headers.
Sip 183 Behaviour	Enum Disable, Enable	Instant	Defines the ISDN message that is sent when 183 Session Progress message is received for IP to Tel calls. Disable – progress message Enable – alert message
Use 180 Response For Call Waiting	Enum Disable, Enable	Instant	Defines whether gateway responds with 180 instead of 182 progress message for Call Waiting.

Parameter Name	Type	Provisioning Type	Description
Esc Transport Type	Enum UDP,TCP,TLS	Instant	Determines the transport layer used for outgoing SIP dialogs initiated by the device to the RTCP XR Collection Server.
T38 Session Immediate Start	Enum Disable, Enable, EnableforT38andAudio	Instant	Enables fax transmission of T.38 “no-signal” packets to the terminating fax machine. ▪ [0] Disable (default) ▪ [1] Enable ▪ [2] EnableforT38andAudio This parameter is used for the transmission from fax machines (connected to the device) located inside a Network Address Translation (NAT). Generally, the firewall blocks T.38 (and other) packets received from the WAN, unless the device behind the NAT sends at least one IP packet from the LAN to the WAN through the firewall. If the firewall blocks T.38 packets sent from the termination IP fax, the fax fails. To overcome this, the device sends No-Op (“no-signal”) packets to open a pinhole in the NAT for the answering fax machine. The originating fax does not wait for an answer, but immediately starts sending T.38 packets to the terminating fax machine.
SIP T38 Version SIP Protocol	Enum T38Ver_0, T38 Ver_3	Instant	Selects the T.38 fax relay version.

Parameter Name	Type	Provisioning Type	Description
QoS statistics in SIP Release Call	Enum Disable, Enable	Instant	Determines whether the device includes call quality of service (QoS) statistics in SIP BYE and SIP 200 OK response to BYE, using the proprietary SIP header, X-RTP-Stat. ▪ [0] = Disable (default) ▪ [1] = Enable The X-RTP-Stat header provides the following statistics: ▪ Number of received and sent voice packets ▪ Number of received and sent voice octets ▪ Received packet loss, jitter (in ms), and latency (in ms) The X-RTP-Stat header contains the following fields: ▪ PS=<voice packets sent> ▪ OS=<voice octets sent> ▪ PR=<voice packets received> ▪ OR=<voice octets received> ▪ PL=<receive packet loss> ▪ JI=<jitter in ms> ▪ LA=<latency in ms>

Parameter Name	Type	Provisioning Type	Description
T1 Retransmit Time	Integer 500 – 4000	Instant	Defines the time interval (in msec) between the first transmission of a SIP message and the first retransmission of the same message. Note: The time interval between subsequent retransmissions of the same SIP message starts with SipT1Rtx and is multiplied by two until SipT2Rtx. For example (assuming that SipT1Rtx = 500 and SipT2Rtx = 4000): The first retransmission is sent after 500 msec. The second retransmission is sent after 1000 (2*500) msec. The third retransmission is sent after 2000 (2*1000) msec. The fourth retransmission and subsequent retransmissions until SIPMaxRtx are sent after 4000 (2*2000) msec.
T2 Retransmit Time	Integer 4000 – 10000	Instant	Defines the maximum interval (in msec) between retransmission of SIP messages. Note: The time interval between subsequent retransmissions of the same SIP message starts with SipT1Rtx and is multiplied by two until SipT2Rtx.
Maximal Number of Retransmissions	Integer 1 – 30	Instant	Defines maximum number of UDP retransmissions of SIP messages.

Table 40-7: SIP Routing Settings

Parameter Name	Type	Provisioning Type	Description
Add Trunk Group Id as Prefix	Enum No, Yes	Instant	Defines whether the gateway's Trunk Group ID is added as prefix to the destination phone number (i.e., called number) for Tel-to-IP calls Notes: - This option can be used to define various routing rules. - To use this feature, you must configure the Trunk Group IDs.
Add Trunk Id as Prefix	Enum No, Yes	Instant	Defines whether the Trunk ID is added as a prefix to the called number for Tel-to-IP calls. If enabled, the Trunk ID (single digit in the range 1 to 83) is added as a prefix to the called (destination) phone number. This option can be used to define various routing rules.
Replace Empty Dst With Port Number	Enum Disable, Enable	Instant	Defines whether the internal channel number is used as the destination number if the called number is missing. Note: applicable only for Tel-to-IP calls and if the called number is missing.

Parameter Name	Type	Provisioning Type	Description
Remove Prefix on IP to Tel Calls	Enum No, Yes	Instant	Determines whether the gateway removes the prefix from the destination number for IP-to-Tel calls. - No – Don't remove prefix - Yes – Remove the prefix (defined in the 'IP to Trunk Group Routing' table) from a telephone number for an IP-to-Tel call, before forwarding it to Tel. For example: To route an incoming IP-to-Tel call with destination number 21100, the 'IP to Trunk Group Routing' table is scanned for a matching prefix. If such a prefix is found (e.g., 21), then before the call is routed to the corresponding Trunk Group, the prefix (21) is removed from the original number, and therefore, only 100 remains. Notes: Applicable only if number manipulation is performed after call routing for IP-to-Tel calls (i.e., IP to TEL Routing Mode is set to Route Before Map). Similar operation (of removing the prefix) is also achieved by using the usual number Operation rules.
TEL to IP routing mode	Enum Route Before Map, Route After Map	Instant	Defines order between routing incoming calls to IP, using routing table, and manipulation of destination number.
IP to TEL routing mode	Enum Route Before Map, Route After Map	Instant	Defines order between routing calls to Trunk group and manipulation of destination number.
Default Destination Number	Integer 0 – 999999	Instant	Defines the default destination phone number used if the received message doesn't contain a called party number and no phone number is configured in the 'Trunk Group' table. The parameter is used as a starting number for the list of channels comprising all the device's Trunk Groups.

Parameter Name	Type	Provisioning Type	Description
SourceIP Address Input	Enum Auto Decision, SIP Contact Header, Layer 3 Source IP	Instant	Defines the IP address that the gateway uses to determine the source of incoming INVITE messages for IP-to-Tel routing. - Auto Decision – if the IP-to-IP feature is enabled, this parameter is automatically set to Layer 3 Source IP. If the IPto-IP feature is disabled, this parameter is automatically set to SIP Contact Header. - SIP Contact Header – use the IP address in the Contact header of the incoming INVITE message. - Layer 3 Source IP – Use the actual IP address (Layer 3) from which the SIP packet was received.
Tel to IP NO answer Timeout (Sec)	Integer 0 – 3600	Instant	Defines the time (in seconds) that the gateway waits for a 200 OK response from the called party (IP side) after sending an INVITE message. If the timer expires, the call is released.
Replace Calling With Redirect Number	Enum Disable, Enable	Instant	Enables replacing the calling number with the redirect number in ISDN-to-IP calls. When such a replacement occurs, the calling name is deleted and left blank. The outgoing INVITE message does not include the redirect number that was used to replace the calling number. The replacement is performed only if a redirect number is present in the incoming call.
Tel2IP Call Forking Mode	Enum Disable, Enable	Instant	Enables the Tel-to-IP Call Forking feature; the device can send a Tel call to multiple IP destinations. An incoming Tel call with multiple matched routing rules (e.g., all with the same source prefix numbers) can be sent (forked) to multiple IP destinations if the rules are defined with a Forking Group in the SIP Routing Tel to IP table .
Enable Alternative Manipulation Tel2IP	Enum Disable, Enable	Instant	Enables different number manipulation rules for redundant calls.
Enable Alternative Routing	Enum No, Yes	Instant	Enables or disables the Alternative Routing feature for Tel-to-IP calls.

Parameter Name	Type	Provisioning Type	Description
Alternative Routing Mode	Enum None, Conn, QoS, All	Instant	Determines the event(s) reason for triggering Alternative Routing. - None – Alternative routing is not used. - Connectivity – Alternative routing is performed if ping to initial destination fails. - QoS – Alternative routing is performed if poor QoS is detected. - Both – Alternative routing is performed if either ping to initial destination fails, poor Quality of Service is detected, or DNS host name is not resolved. Note: QoS is quantified according to delay and packet loss calculated according to previous calls. QoS statistics are reset if no new data is received within two minutes.
Max Allowed Packet Lost	Integer 0 – 100	Instant	Defines the packet loss percentage at which the IP connection is considered a failure.
Max Allowed Delay	Integer 0 – 10000	Instant	Defines transmission delay (in msec) at which the IP connection is considered a failure.
Alternate Routing Tel to IP Connectivity Method	Enum ICMP Ping, SIP Options	Instant	Defines the method used by the gateway for periodically querying the connectivity status of a destination IP address. - ICMP Ping – Internet Control Message Protocol (ICMP) ping messages. - SIP OPTIONS – The remote destination is considered offline if the latest OPTIONS transaction timed out. Any response to an OPTIONS request, even if indicating an error, brings the connectivity status to online.
Alternate Routing Tel to IP Keep Alive Time (Sec)	Integer 5 – 2000000	Instant	Defines the time interval (in seconds) between SIP OPTIONS Keep-Alive messages used for the IP Connectivity application.

Table 40-8: SIP Supplementary Services Settings

Parameter Name	Type	Provisioning Type	Description
Behavior 3xx	Enum Forward, Redirect	Instant	Defines the gateways behavior when a 3xx response is received for an outgoing INVITE request. The gateway can either use the same call identifiers (CallID, branch, to and from tags) or change them in the new initiated INVITE. - Forward – Use different call identifiers for a redirected INVITE message. - Redirect – Use the same call identifiers.
Enable Semi Attended Transfer	Enum Disable, Enable	Instant	Defines the gateway behavior when Transfer is initiated while still in Alerting state. - Disable – Send REFER with Replaces (default). - Enable – Send CANCEL and after a 487 response is received, send REFER without Replaces.
Wait For Busy Time	Integer 0 – 20000000	Instant	Defines the time to wait to detect busy and reorder tones. Currently used in semi-supervised PBX transfer.
Transfer Prefix	String Up to 9 chars	Instant	Defines the string that is added as a prefix to the transferred / forwarded called number when the REFER / 3xx message is received. This parameter can be used to apply different Operation rules to differentiate transferred number from the originally dialed number.
Trunk Transfer Mode	Enum None, CAS NFA, ISDN, CAS Normal, QSIG IP2TelBlindTransfer, 4ESSFreeOOBBlindTransfer	Instant	Defines the type type of transfer the PSTN/PBX supports. - None – Not supported (default). - CAS NFA – Supports CAS NFA DMS-100 transfer.

Parameter Name	Type	Provisioning Type	Description
			When a SIP REFER message is received, the gateway performs a Blind Transfer by executing a CAS Wink, waits for an acknowledge Wink from the remote side, dials the Refer-to number to the switch, and then releases the call. Note: A specific NFA CAS table is required. ■ ISDN – Supports ISDN transfer: Release Link Trunk (RLT) (DMS-100), Two B Channel Transfer (TBCT) (NI2), Explicit Call Transfer (ECT) (EURO ISDN) and Path Replacement (QSIG). When a SIP REFER message is received, the gateway performs a transfer by sending FACILITY messages to the PBX with the necessary information on the call's legs that are to be connected. The different ISDN variants use slightly different methods (using FACILITY messages) to perform the transfer. ■ CAS Normal – Supports CAS Normal transfer. When a SIP REFER message is received, the gateway performs a Blind Transfer by executing a CAS Wink, dialing the Refer-to number to the switch, and then releasing the call. ■ QSIG – Supports QSIG Single Step transfer: IP-to-Tel: When a SIP REFER message is received, the gateway performs a transfer by sending a FACILITY message to the PBX, initiating Single Step transfer. Once a success return result

Parameter Name	Type	Provisioning Type	Description
			is received, the transfer is completed. - IP-to-Tel Blind Transfer mode supported for ISDN PRI/BRI protocols and implemented according to AT&T Toll Free Transfer Connect Service (TR 50075) "Courtesy Transfer-Human-No Data". When the board receives a SIP REFER message, it performs a blind transfer by first dialing the DTMF digits (transfer prefix) defined by the parameter XferPrefixIP2Tel (configured to "*8" for AT&T service), and then (after 500 msec), the board dials the DTMF of the number (referred) from the Refer-To header sip:URI userpart. If the hostpart of the Refer-To sip:URI contains the board's IP address, and if the Trunk Group selected according to the IP to Tel Routing table is the same Trunk Group as the original call, then the board performs the in-band DTMF transfer; otherwise, the board sends the INVITE according to regular transfer rules. After completing the in-band transfer, the board waits for the ISDN Disconnect message. If the Disconnect message is received during the first 5 seconds, the board sends a SIP NOTIFY with 200 OK message; otherwise, the board sends a NOTIFY with 4xx message. 4ESSFreeOOBBlindTransfer - Supports AT&T Toll Free Out-Of-Band blind transfer for 4ESS protocol.

Parameter Name	Type	Provisioning Type	Description
Swap Redirect and Called Numbers	Enum No, Yes	Instant	Defines whether the redirect number is used instead of the called number for incoming ISDN calls.
Copy Destination to Redirect Number	Enum Do Not Copy, Copy After Manipulation, Copy Before Manipulation	Instant	Defines whether the gateway copies the received ISDN called number to the outgoing SIP Diversion header for Tel-to-IP calls (even if a Redirecting Number IE is not received in the ISDN Setup message). Therefore, the called number is used as a redirect number. Call redirection information is typically used for Unified Messaging and voice mail services to identify the recipient of a message. - Do Not Copy – Do not copy the number. - Copy After Manipulation - Copies the called number after manipulation. The gateway first performs Tel-to-IP destination phone number manipulation (i.e., on the SIP To header), and only then copies the manipulated called number to the SIP Diversion header for the Tel-to-IP call. Therefore, with this option the called and redirected numbers are identical. - Copy Before Manipulation – Copies the called number before manipulation. The gateway first copies the original called number to the SIP Diversion header, and then perform Tel-to-IP destination phone number manipulation. Therefore, this allows you to have different numbers for the called (i.e., SIP To header) and

Parameter Name	Type	Provisioning Type	Description
			redirected (i.e., SIP Diversion header) numbers. Notes: If the incoming ISDN-to-IP call includes a Redirect Number, this number is overridden by the new called number if this parameter is set to Copy After Manipulation or Copy Before Manipulation. This parameter can also be configured for IP Profiles.
SIP Hold to ISDN	Enum Disabled, Enabled	Instant	Enables interworking of the Hold and retrieve supplementary service from PRI to SIP and vice versa. Notes: This feature is only supported for the QSIG and Euro ISDN PRI variants. For EuroISDN, it is only supported from TE (user) to NT (network).
Held Timeout (Sec)	Integer -1 – 2400	Instant	Defines the time interval that the gateway can allow a call to remain on hold. If a Resume (un-hold Re-INVITE) message is received before the timer expires, the call is renewed. If this timer expires, the call is released. Value -1 means that the call is placed on hold indefinitely until the initiator of on hold retrieves the call again.
Voice Mail Interface	Enum None(0), QSIG(3)	Instant	Enables the voice mail application on the gateway and determines the communication method used between the PBX and the gateway.

Table 40-9: SIP PSTN Settings

Parameter Name	Type	Provisioning Type	Description
Channel Select Mode	Enum By Phone Number, Cyclic Ascending, Cyclic Descending, Number And Cyclic Ascending, According To Source Number, Trunk Cyclic Ascending, ISDN SuppServTable, DestNumberAscending	Instant	Defines common rule of port allocation for IP to TEL calls. - By Destination Phone Number - Select the media server port according to the called number (see the note below). - Cyclic Ascending – Select the next available channel in an ascending cycle order. Always select the next higher channel number in the Trunk Group. When the media server reaches the highest channel number in the Trunk Group, it selects the lowest channel number in the Trunk Group and then starts ascending again. - Ascending – Select the lowest available channel. Always start at the lowest channel number in the Trunk Group and if that channel is not available, select the next higher channel. - Cyclic Descending – Select the next available channel in descending cycle order. Always select the next lower channel number in the Trunk Group. When the media server reaches the lowest channel number in the Trunk Group, it selects the highest channel number in the Trunk Group and then start descending again. - Descending – Select the highest available channel. Always start at the highest channel number in the Trunk Group and if that channel is not available, select the next lower channel. - Number + Cyclic Ascending – First select the media server port according to the called number (see the note below). If the called number isn't found, then select the next available channel in ascending cyclic order. Note that if the called number is found, but the port associated with this number is busy, the call is released. - By Source Phone Number – Select the media server port according to the calling number (see the note below).

Parameter Name	Type	Provisioning Type	Description
			- Trunk Cyclic Ascending – Select the media server port from the first channel of the next trunk (next to the trunk from which the previous channel was allocated). - ISDN SuppServ Table - The BRI port/module is selected according to the settings in the ISDN Supplementary Services table , allowing the routing of IP-to-Tel calls to specific BRI endpoints - Dest Number Ascending -The device allocates a channels to incoming IP-to-Tel calls as follows: - The device attempts to route the call to the channel that is associated with the destination (called) number. If located, the call is sent to that channel. - If the number is not located or the channel is unavailable (e.g., busy), the device searches in ascending order for the next available channel in the Trunk Group. If located, the call is sent to that channel. - If all the channels are unavailable, the call is released. - Note: If this parameter is not configured for the Trunk Group, then its channel select method is according to the global parameter, ChannelSelectMode.
Use EndPoint Number As Calling Number Tel2IP	Enum Enable,Disable	Instant	Enables the use of the B-channel number as the calling number (sent in the From header of the INVITE) instead of the number received in the Q.931 Setup message, for Tel-to-IP calls. For example, if the incoming calling party number in the Q.931 Setup message is "12345" and the B-channel number is 17, then the outgoing INVITE From header is set to "17" instead of "12345". Note: When enabled, this feature is applied before routing and manipulation on the source number.

Parameter Name	Type	Provisioning Type	Description
Use EndPoint Number As Calling Number IP2Tel	Enum Enable,Disable	Instant	Enables the use of the B-channel number as the calling party number (sent in the Q.931 Setup message) instead of the number received in the From header of the INVITE, for IP-to-Tel calls. For example, if the incoming INVITE From header contains "12345" and the destined B-channel number is 17, then the outgoing calling party number in the Q.931 Setup message is set to "17" instead of "12345". Note: When enabled, this feature is applied after routing and manipulation on the source number (i.e., just before sending to the Tel side).
Progress Indicator to ISDN	Enum Not Set(-1), Local RB(0), Remote RB(1), Remote RB(8)	Instant	Defines the value of Progress Indicator (PI) sent to the ISDN side. - Not Set – the PI in ISDN messages is set according to the parameter Play Ringback Tone to Tel. - Local RB – PI is not sent to ISDN. - Remote RB(1), Remote RB (8) – the PI value is sent to PSTN in Q.931/Proceeding and Alerting messages. Typically, the PSTN/PBX cuts through the audio channel without playing local Ringback tone, enabling the originating party to hear remote Call Progress Tones or network announcements

Parameter Name	Type	Provisioning Type	Description
Progress Indicator to IP	Enum Not Set(-1), Local RB(0), Remote RB(1), Remote RB(8)	Instant	Defines the value of Progress Indicator (PI) sent to the IP side. - Not Set – the PIS in IP messages is set according to the parameter Play Ringback Tone to IP. - Local RB – For IP-to-Tel calls, the gateway sends 180 Ringing SIP response to IP after receiving ISDN Alert or (for CAS) after placing a call to PBX/PSTN. - Remote RB(1), Remote RB (8) – For IP-to-Tel calls, if early media is enabled, the gateway sends 180 Ringing with SDP in response to an ISDN Alert or it sends a 183 Session Progress message with SDP in response to only the first received ISDN Proceeding or Progress message after a call is placed to PBX/PSTN over the trunk.
Set PI in Rx Disconnect Message	Enum Not Set(-1), Local RB(0), Remote RB(1), Remote RB(8)	Instant	Defines the behavior when a Disconnect message is received from the ISDN before a Connect message is received. - Not Set – Sends a 183 SIP response according to the received progress indicator (PI) in the ISDN Disconnect message. If PI = 1 or 8, the device sends a 183 response, enabling the PSTN to play a voice announcement to the IP side. If there isn't a PI in the Disconnect message, the call is released. - Local RB(0) – Doesn't send a 183 response to IP. The call is released. - Remote RB(1), Remote RB(8) –Sends a 183 response to IP.

Parameter Name	Type	Provisioning Type	Description
Play Ringback Tone to IP	Enum Disable, Enable	Instant	Defines whether or not the ringback tone (RBT) is played to the IP side for IP-to-Tel calls. If configured to Enable and early media is enabled, the gateway plays a ringback tone according to the following: - For CAS interfaces: the gateway opens a voice channel, sends a 183+SDP response, and then plays a ringback tone to IP. - For ISDN interfaces: if a Progress or an Alerting message with PI (1 or 8) is received from the ISDN, the gateway opens a voice channel, sends a 183+SDP or 180+SDP response, but doesn't play a ringback tone to IP. If PI (1 or 8) is received from the ISDN, the gateway assumes that ringback tone is played by the ISDN switch. Otherwise, the gateway plays a ringback tone to IP after receiving an Alerting message from the ISDN. It sends a 180+SDP response, signaling to the calling party to open a voice channel to hear the played ringback tone. Notes: To enable the gateway to send a 183/180+SDP responses, set Enable Early Media to Enable. If Enable Digit Delivery is Enabled, the gateway doesn't play a ringback tone to IP and doesn't send 183 or 180+SDP responses.

Parameter Name	Type	Provisioning Type	Description
Play Ringback Tone to IP	Enum Do Not Play, Play Local, Play According To Early Media, Play According To Received Media	Instant	Enables play of ringback tone (RBT) to the Tel side and determines the method for playing the RBT. It applies to all trunks that are not configured by the parameter Play Ringback Tone to Trunk. - Do Not Play – RBT is not played. - Play Local – RBT is played to the Tel side of the call when a SIP 180/183 response is received. - Play According to Early Media – RBT is played to the Tel side only if a 180/183 response without SDP is received. If 180/183 with SDP message is received, the Board cuts through the voice channel and doesn't play RBT (default). - Play According To Received Media – The behaviour is similar to • Play According to Early Media. If a SIP 180 response is received and the voice channel is already open (due to a previous 183 early media response or due to an SDP in the current 180 response), the Board plays a local RBT if there are no prior received RTP packets. The Board stops playing the local RBT as soon as it starts receiving RTP packets. At this stage, if the Board receives additional 18x responses, it does not resume playing the local RBT. Note: For ISDN trunks, this option is applicable only if Local ISDN Ringback Source is set to Gateway.
Local ISDN Ringback Source	Enum PBX, Gateway	Instant	Defines whether Ringback tone is played to the ISDN by the PBX / PSTN or by the gateway.

Parameter Name	Type	Provisioning Type	Description
Trunk RTP Only Mode	Enum Disable, Transmit, Receive, Transmit	Instant	Enables the device to start sending and/or receiving RTP packets to and from remote endpoints without the need to establish a SIP session. This is configured per trunk. The remote IP address is determined according to the 'Outbound IP Routing' table. The port is the same port as the local RTP port (configured by the parameter BaseUDPPort (see page 600) and the channel on which the call is received). ▪ [0] Disable ▪ [1] Transmit & Receive = send and receive RTP packets ▪ [2] Transmit = send RTP packets only
RTCP XR Collection Server	Enum Disable, Enable	Instant	Determines the transport layer used for outgoing SIP dialogs initiated by the device to the RTCP XR Collection Server.
Send Screening Indicator to IP	Enum Not Overwritten(-1), User Provided(0), User Passed(1), User Failed(2), Network Provided(3)	Instant	Defines how the screening indicator of the calling party's number (CPN) is generated for Tel-to-IP calls. ▪ Not Overwritten – not configured (interworking from ISDN to IP) or set to 0 for CAS. ▪ User Provided – CPN set by user, but not screened (verified). ▪ User Passed – CPN set by user, verified and passed. ▪ User Failed – CPN set by user, verified and failed. Network Provided – CPN set by network. Note: This parameter is applicable only if the Remote Party ID (RPID) header is enabled.

Parameter Name	Type	Provisioning Type	Description
Send Screening Indicator to ISDN	Enum Not Overwrited(-1), User Provided(0), User Passed(1), User Failed(2), Network Provided(3)	Instant	Defines how the screening indicator of the calling party's number (CPN) is generated for IP-to-Tel calls. - Not Overwrited – not configured (interworking from IP to ISDN) or set to 0 for CAS. - User Provided – CPN set by user, but not screened (verified). - User Passed – CPN set by user, verified and passed. - User Failed – CPN set by user, verified and failed. - Network Provided – CPN set by network.
Play Busy Tone to Tel	Enum Do Not Play, Play When Disconnecting, Play Before Disconnect	Instant	Enables the device to play a busy or reorder tone to the PSTN after a Tel-to-IP call is released. - Don't Play – Immediately sends an ISDN Disconnect message. - Play when Disconnecting – Sends an ISDN Disconnect message with PI = 8 and plays a busy or reorder tone to the PSTN (depending on the release cause). - Play before Disconnect – Delays the sending of an ISDN Disconnect message for a user-defined time and plays a busy or reorder tone to the PSTN. Applicable only if the call is released from the IP [Busy Here (486) or Not Found (404)] before it reaches the Connect state; otherwise, the Disconnect message is sent immediately and no tones are played.

Parameter Name	Type	Provisioning Type	Description
Enable Busy Out	Enum Disabled, Enabled	Instant	Defines whether the Busy Out feature is enabled. When Busy Out is enabled and certain scenarios exist, the device performs the following: All E1/T1 trunks are automatically taken out of service by taking down the D-Channel or by sending a Service Out message for T1 PRI trunks supporting these messages (NI-2, 4/5-ESS, DMS-100, and Meridian). These behaviors are performed due to one of the following scenarios: - Physically disconnected from the network (i.e., Ethernet cable is disconnected). - The device can't communicate with the proxy (according to the Proxy Keep-Alive mechanism) and no other alternative route exists to send the call. - The IP Connectivity mechanism is enabled and there is no connectivity to any destination IP address. Notes: The Busy Out behavior varies between different protocol types. The Busy-Out condition can also be applied to a specific Trunk Group. If there is no connectivity to the Serving IP Group of a specific Trunk Group, all the physical trunks pertaining to that Trunk Group are set to the Busy-Out condition. Each trunk uses the proper Out-Of-Service method according to the selected ISDN/CAS variant. You can use the parameter Digital Out-Of-Service Behavior to select the method for setting digital trunks to Out-Of-Service.
ISDN Disconnect On Busy Tone Detection	Enum No, Yes	Instant	Defines whether an ISDN call is disconnected upon detection of a busy tone.

Parameter Name	Type	Provisioning Type	Description
Default Release Cause	Integer 1 – 350	Instant	Defines the default Release Cause to IP for IP to Tel calls. Used when the gateway initiates a call release. If an explicit matching cause for this release isn't found, a default release cause can be configured: The default release cause is NO_ROUTE_TO_DESTINATION(3). Other common values are NO CIRCUIT AVAILABLE (34), DESTINATION OUT OF ORDER (27), etc. Note: The default release cause is described in the Q.931 notation, and is translated to corresponding SIP 40x or 50x values. For example, 404 for 3, 503 for 34, and 502 for 27.

Parameter Name	Type	Provisioning Type	Description
Use Trunk Group Information	Enum Disable, Send Only, Send And Receive URC2008,Hotline Extended	Instant	Defines whether the SIP 'tgrp' parameter is used, which specifies the Trunk Group to which the call belongs, according to RFC 4904. For example: INVITE sip:+16305550100; tgrp=1; trunkcontext=example.com@10.1.0.3; user=phone SIP/2.0 ▪ Disable – 'tgrp' parameter is not used. ▪ Send Only – the trunk group number is added as the 'tgrp' parameter to the Contact header of outgoing SIP messages. If a trunk group number is not associated with the call, the 'tgrp' parameter isn't included. If a 'tgrp' value is specified in incoming messages, it is ignored. ▪ Send And Receive – The functionality of outgoing SIP messages is identical to the functionality described in Send Only option. In addition, for incoming SIP messages, if the Request-URI includes a 'tgrp' parameter, the gateway routes the call according to that value (if possible). If the Contact header includes a 'tgrp' parameter, it is copied to the corresponding outgoing messages in that dialog. ▪ UCR 2008 = Interworks the hotline "Off Hook Indicator" parameter between SIP and ISDN. ▪ Hotline Extended = Interworks the ISDN Setup messages hotline "OffHook Indicator" Information Element (IE) to SIP INVITEs Request-URI and Contact headers.

Parameter Name	Type	Provisioning Type	Description
Out-of-Service Behavior	Enum Default, ISDN Service Msg, ISDN D-Channel, Alarm, CAS Block	Instant	Defines the method for setting digital trunks to Out-Of-Service state per device. - Default – The default behavior is as follows: - For ISDN: Use Service messages on supporting variants and Alarm on non-supporting variants. - For CAS: Use Alarm. - ISDN Service Msg – Sends ISDN In or Out of Service (only for ISDN protocols that support Service message). - ISDN D-Channel – Takes D-Channel down or up (ISDN only). - Alarm – Sends or clears PSTN AIS Alarm (ISDN and CAS). - CAS Block – Blocks trunk (CAS only). Notes: To determine the method for setting Out-Of-Service state per trunk, use the Trunk Out-Of-Service Behavior parameter (see "Trunk/SIP Parameters Settings").
Enable CIC	Enum No, Yes	Instant	Defines whether Carrier Identification Code (CIC) is relayed to ISDN. If enabled, the CIC code (received in an INVITE Request-URI) is included in a TNS IE in the ISDN SETUP message.
ISub Number Of Digits	Integer 0 – 36	Instant	Defines number of digits that are taken from the end of the phone number for the Sub Address.
B-Channel Negotiation	Enum Preferred, Exclusive, Any	Instant	Defines the ISDN B-channel negotiation mode. Applicable to ISDN protocols. The option 'Any' is only applicable to the User side.
Enable ISDN UUI to SIP	Enum Disable, Enable	Instant	Enables transfer of User-to-User Information Element (UUIE) from PRI Setup message to SIP INVITE message. The IE is transferred using a proprietary 'X-UserToUser' SIP header.
Enable SIP UUI to ISDN	Enum Disable, Enable	Instant	Enables transfer of (UUIE) from SIP INVITE message to PRI Setup message. The IE is received using a proprietary 'X-UserToUser' SIP header.

Parameter Name	Type	Provisioning Type	Description
Optional IE in SETUP	String Up to 99 chars	Instant	Enables the adding of an optional Information Element data (in hex format) to the ISDN SETUP message. For example, to add the following IE: '0x20,0x02,0x00,0xe1', set this parameter to "200200e1". Note: This IE is sent from the Trunk Groups with parameter Send Optional IE set to Enabled.
Enable Calling Party Category	Enum Disable, Enable	Instant	Defines whether the Calling Party Category is relayed between SIP and PRI.
PSTN Alert Timeout	Integer 1 – 600	Instant	Defines the Alert Timeout value (in seconds) – ISDN T301 timer – for IP to Tel calls. This timer is used between the time a SETUP message is sent to the Tel side and a CONNECT message is received. If an ALERTING message is received, the timer is restarted.
Send Metering to IP	Enum Disable, Enable	Instant	Enables sending of metering messages to IP on detection of metering pulses.
CAS Disconnect On Detection of Busy Tone	Enum No, Yes	Instant	Enables disconnect of CAS calls on busy tone.
MFC R2 Category	Integer 1 – 15	Instant	Defines MFC R2 Calling Party Category (CPC). Provides information on calling party such as National or International call, Operator or subscriber and Subscriber priority.
TDM Over IP	Enum Disable, Enable	Instant	Enables TDM tunneling. When TDM Tunneling is enabled, the originating device automatically initiates SIP calls from all enabled B-channels pertaining to E1/T1/J1 spans that are configured with the 'Transparent' protocol. The called number of each call is the internal phone number of the B-channel from where the call originates. The 'IP to Trunk Group' routing table is used to define the destination IP address of the terminating device. The terminating device automatically answers these calls if its E1/T1 protocol is set to 'Transparent'.

Parameter Name	Type	Provisioning Type	Description
TDMoIP Trunk Busy Out/ Min Calls For Activation	Integer 0 – 30	Instant	Enables the TDMoIP Trunk Busy Out feature (when set to non-zero value) and defines the Min SIP active calls before clearing AIS and Trunk reactivation.
ISDN Tunnel to IP	Enum Disable, Enable, EnableByUsingBody	Instant	Enables the ISDN Tunneling from Tel side to IP side. When ISDN Tunneling is enabled, the gateway sends all ISDN PRI messages using the correlated SIP messages. Setup is tunneled using INVITE, all mid-call messages are tunneled using INFO, and Disconnect/Release is tunneled using BYE. The raw data from the ISDN is inserted into a proprietary SIP header (X-ISDNTunnelingInfo) or a dedicated message body (application/isdn) in the SIP messages.
IP Tunnel to ISDN	Enum Disable, Enable, EnableByUsingBody	Instant	Enable ISDN Tunneling from IP side to Tel side. When ISDN Tunneling is enabled, the media server extracts the raw data received in a proprietary SIP header (X-ISDNTunnelingInfo) or a dedicated message body (application/isdn) in the SIP messages and sends the data as ISDN messages to the PSTN side.
QSIG Tunneling	Enum Disable, Enable	Instant	Enables QSIG Tunneling in both directions.
QSIG Path Replacement Mode	Enum IP2QSIGTransfer, QSIG2IPTTransfer	Instant	QSIG Path Replacement Mode: the device can interwork consultation call transfer requests for ISDN QSIG-to-IP calls. When the device receives a request for a consultation call transfer from the PBX, the device sends a SIP REFER message with a Replaces Header to the SIP UA to transfer it to another SIP UA. Once the two SIP UA parties are successfully connected, the device requests the PBX to disconnect the ISDN call, thereby freeing resources on the PBX.

Table 40-10: SIP Media Settings

Parameter Name	Type	Provisioning Type	Description
Enable Early Media	Enum Disable, Enable	Instant	Enables the gateway to send a 183 Session Progress response with SDP (instead of 180 Ringing), allowing the media stream to be established prior to the answering of the call. Sending a 183 response depends on the Progress Indicator (PI). It is sent only if PI is set to 1 or 8 in the received Proceeding or Alert PRI messages. For CAS devices, see the Progress Indicator To IP Parameter.
Comfort Noise Negotiation	Enum Disable, Enable	Instant	Enables negotiation and usage of Comfort Noise (CN). The use of CN is indicated by including a payload type for CN on the media description line of the SDP. The device can use CN with a codec whose RTP time stamp clock rate is 8,000 Hz (G.711/G.726). The static payload type 13 is used. The use of CN is negotiated between sides. Therefore, if the remote side doesn't support CN, it is not used. Note: Silence Suppression must be enabled to generate CN.
RTCP-XR Esc IP	String Up to 49 chars	Instant	Defines the IP address of the Event State Compositor (ESC). The media server sends RTCP-XR reports using PUBLISH messages to this server. The address can be configured as a numerical IP address or as a domain name.
RTCP-XR Report Mode	Enum Disable, End Call, End Call And Periodic	Instant	Defines whether or not RTCP-XR reports are sent to the Event State Compositor (ESC) and if so, defines the interval in which they are sent. - Disable – RTCP-XR reports are not sent to the ESC - End Call – RTCP-XR reports are sent to the ESC at the end of each call - End Call And Periodic – RTCP-XR reports are sent to the ESC at the end of each call and periodically according to the parameter RTCP Interval
Media IP Version	Enum PreferIPv6, PreferIPv4,	Instant	Defines the preferred RTP media IP addressing version for outgoing SIP calls. This is indicated in the "c=" field

Parameter Name	Type	Provisioning Type	Description
Preference	IPv6Only, IPv4Only		(Connection) of the SDP. - Only IPv4 – offer includes only IPv4 media IP addresses (default). - Only IPv6 – offer includes only IPv6 media IPs addresses. - Prefer IPv4 – offer includes both IPv4 and IPv6 media IP addresses, but the first media is IPv4. - Prefer IPv6 – offer includes both IPv4 and IPv6 media IP addresses, but the first media is IPv6. Notes: - This parameter is applicable only when the device offers an SDP. - The IP addressing version is determined according to the first SDP "m=" field. - This parameter can be also configured per IP Profile ID.
Enable Ptime	Enum Disable, Enable	Instant	Defines whether the ptime header is included in the SDP.
Multi Ptime Format	Enum None, Packet Cable	Instant	Defines whether the 'mptime' attribute is included in the outgoing SDP. The 'mptime' attribute enables the gateway to define a separate packetization period for each negotiated coder in the SDP. The 'mptime' attribute is only included if this parameter is enabled, even if the remote side includes it in the SDP offer. On receipt, each coder receives its 'ptime' value in the following precedence: - From 'mptime' attribute. - From 'ptime' attribute.
SDP Session Owner	String Up to 39 chars	Instant	Defines the value of the Session Owner line ('o' field) in outgoing SDP bodies.
Fax Signaling Method	Enum No Fax Negotiation Using SIP Signaling, Initiates T38 Fax Relay, Initiates Fax Using G.711, Initiates T38 Fax Relay With G.711	Instant	Defines the SIP signaling method for establishing and transmitting a fax session after a fax is detected. - No Fax Negotiation – No fax negotiation using SIP signaling. Fax transport method is according to the parameter Fax Transport Mode. - Initiates T.38 Relay – Initiates T.38 fax relay.

Parameter Name	Type	Provisioning Type	Description
	On Failure		- Initiates G.711 Transport – Initiates fax / modem using the coder G.711 A-law/μ-law with adaptations (see Note below). - Initiates T38 Fax Relay With G.711 On Failure – Initiates T.38 fax relay. If the T.38 negotiation fails, the device re-initiates a fax session using the coder G.711 A-law/μ-law with adaptations (see the Note below). Notes: Fax adaptations (for last two options): - Echo Canceller = On - Silence Compression = Off - Echo Canceller Non-Linear Processor Mode = Off - Dynamic Jitter Buffer Minimum Delay = 40 - Dynamic Jitter Buffer Optimization Factor = 13 If the device initiates a fax session using G.711 (for last two options) , a 'gpmd' attribute is added to the SDP in the following format: - For A-law: 'a=gpmd:8 vbd=yes;ecan=on' - For Mu-law: 'a=gpmd:0 vbd=yes;ecan=on'
Detect Fax on Answer Tone	Enum Disable, Enable	Instant	Enables Detection of Fax on Answer Tone.
Enable Fax Re-Routing	Enum Disable, Enable	Instant	Enables or disables re-routing of Tel-to-IP calls that are identified as fax calls. If a CNG tone is detected on the Tel side of a Tel-to-IP call, a "FAX" prefix is appended to the destination number before routing and manipulations occur. Standard Tel-to-IP routing table mechanism is then used to route the call, and the destination number manipulation mechanism is used to remove the "FAX" prefix, if required. If the initial INVITE that is used to establish the voice call (not Fax) was already sent, a CANCEL (if not connected yet) or a BYE (if already connected) is sent to tear down the voice call.

Parameter Name	Type	Provisioning Type	Description
Fax CNG Relay Mode	Enum Do Not Send ReInvite, Send ReInvite	Instant	Defines whether gateway sends re-INVITE upon detection of a fax CNG tone, when CNG Detector Mode is set to Relay.

Table 40-11:SIP Media Server Settings

Parameter Name	Type	Provisioning Type	Description
Number of Media Channels	Integer 0 – 2016	Online	Defines the number of DSP channels that are allocated for IP conferences, IP streaming and IP Transcoding (other DSP channels can be used for PSTN Gateway). Note: The allocated media channels are counted from the upper limit. For example: if 'MediaChannels=30', the channel range used for IP media is 91-120
MSCML ID	String Up to 15 chars	Instant	Defines MSCML identification string. To start an MSCML session the application server sends a regular SIP INVITE message with a SIP URI that includes this string. For example: INVITE sip:mscml@10.2.3.4 Subsequent INFO message(s) carry the requests and responses.
NetAnn Announcer ID	String Up to 15 chars	Instant	Defines NetAnn identification string, used to play an announcement using the NetAnn interface. The application server sends a regular SIP INVITE message with SIP URI that includes this identifier string and a play= parameter that identifies the necessary announcement. For example: INVITE sip:_sip-annc@10.2.3.4;play=http://localhost/1 .
Media Streaming ID	String Up to 16 chars	Instant	Defines Media Streaming identification string. To start an announcement / record session, the application server sends a regular SIP INVITE message with SIP URI that includes this identifier string. For example: INVITE sip:play_record@10.2.3.4 Subsequent INFO message(s) carry the announcement execution script..

Parameter Name	Type	Provisioning Type	Description
Play From ID	String Up to 15 chars	Instant	Defines HTTP streaming identification prefix that is used for identifying a specific announcements in an HTTP server.
Record To ID	String Up to 15 chars	Instant	Defines HTTP streaming identification prefix that is used for recording a specific announcements to an HTTP server.
Announcement ID	String Up to 15 chars	Instant	Defines announcement identification string, used for identifying a specific announcement in the local Voice Prompts file.
Tone ID	String Up to 15 chars	Instant	Defines call progress tone identification string, used for identifying a specific announcement in the local Call Progress Tone file.
Conference ID	String Up to 15 chars	Instant	Defines conference identification string. To join a conference, the INVITE URI must include the Conference ID string preceded by the number of the participants in the conference, and terminated by a unique number. For example: INVITE sip:4MyConference1234@10.1.10.10. INVITE messages with the same URI join the same conference.
Transcoding ID	String Up to 15 chars	Instant	Defines transcoding identification string, used for identifying an incoming Transcoding call.
URL Check for Local Alias	Enum Disable, Enable	Instant	Defines if play requests for remote URLs should first be checked for local segments with the same alias as the URL. ▪ Disable – device will not check the local audio first for play requests using URLs. ▪ Enable – device will try to find the URL locally first, and if the audio is not found locally, the device will try to play the audio from the remote URL.

Table 40-12: SIP Radius Settings

Parameter Name	Type	Provisioning Type	Description
AAA Indications	Enum No Indications(0), Accounting Only(3)	Instant	Defines the use of the Authentication, Authorization and Accounting (AAA) indications.
RADIUS Accounting Type	Enum On Call Release, On Call Connect And Release, On Call Setup And Release	Instant	Defines when a RADIUS accounting report is issued.

Table 40-13: SIP Emergency Gateway Setting

Parameter Name	Type	Provisioning Type	Description
Emergency Getway Mode	Enum Disable,Enable	Instant	Enables E911 to NG911 gateway and ELIN handling.
Emergency Callback Timeout	Integer 1-60	Instant	Emergency Callback timeout in minutes. Should be able direct a callback from the Emergency services to the user who made the original emergency call. Therefore the Media Gateway stores for a period of 30 minutes (configurable 10-60) the SIP INVITE "from" header to be used for call back calls.

Parameter Name	Type	Provisioning Type	Description
Emergency Numbers		Instant	Defines a list of Emergency numbers. These emergency numbers are used for the preemption of E911 IP-to-Tel calls when there are unavailable or busy channels. In this scenario, the device terminates one of the busy channels and sends the emergency call to this channel. This feature is enabled by setting the CallPriorityMode parameter (see below) to 2 (Emergency). The list can include up to four different numbers, where each number can be up to four digits long. Example: EmergencyNumbers =100,911,102,101.
Emergency Special Release Cause	Enum Disable,Enable	Instant	When an emergency number is detected, the 4xx release causes should be converted to "Service Unavailable" (503).
Call Priority Mode	Enum Disable, Emergency	Instant	Enables priority calls handling. Disable = Disable (default). Emergency = Preemption of IP-to-Tel E911 emergency calls. If the device receives an E911 call and there are unavailable channels to receive the call, the device terminates one of the channel calls and sends the E911 call to this channel. The preemption is done only on a channel pertaining to the same Trunk Group for which the E911 call was initially destined and if the channel select mode (configured by the ChannelSelectMode parameter) is set to a value other than "By Dest Number" (0). The pre-emption is done only if the incoming IP-to-Tel call is identified as an emergency call. The device identifies emergency calls by one of the following: The destination number of the IP call matches one of the numbers defined by the EmergencyNumbers parameter. (For E911, you must define this parameter with the value "911".) The incoming SIP INVITE message contains the "emergency" value in the Priority header.

40.4 Configuring Coder Groups

The Coder Group Settings page allows you to define up to 10 groups of coders (termed Coder Groups). For each Coder Group, you can define up to 10 coders configured with packetization time (ptime), rate, payload type, and silence suppression. The first coder in the Coder Group table has the highest priority and is used by the device whenever possible. If the remote side cannot use the first coder, the device attempts to use the next coder, and so on.

Coder Groups can be used as follows:

- Assigned to Tel Profiles in the Tel Profiles table (see Configuring Tel Profiles. This is applicable only to the GW/IP-to-IP application.
- Assigned to IP Profiles in the IP Profiles table (see 'Configuring IP Profiles' In this setup, they can be used as Extension coders and Allowed coders for the SBC application.



Note:

- A specific coder can be selected only once per Coder Group.
- For a list of supported coders, see 'Configuring Coders Table' on page 609.
- The Coder Group Settings table can also be configured using the table ini file parameter, CodersGroup.

➤ To configure Coder Groups:

1. Click the  button to access the Media Gateway status screen.
2. Select the desired SIP board.
3. In the Navigation pane, select **SIP** ➤ **SIP General** ➤ **Coders Group**; the SIP Coders Group List is displayed.
4. Use the  or  buttons to add or remove entries.
5. Select a specific row, and then in the Configuration pane, select **SIP Coders Group Settings**; the SIP Coders Group Settings screen is displayed.
6. Configure Coder Group Name.
7. Click the Maintenance icon  and select **Unlock** to activate the configuration.

40.5 Configuring Coders Table

When configuring the Coder's table, note the following:

- Each coder may be defined in the Coders table only once.
- The gateway always uses the packetization time requested by the remote side for sending RTP packets. If not specified, the packetization time (ptime) is assigned the default value.
- Only the packetization of the first coder in the defined coder list is declared in INVITE / 200 OK SDP, even if multiple coders are defined.
- If the coder G.729 is selected and silence suppression is enabled (for this coder), the gateway includes the string 'annexb=no' in the SDP of the relevant SIP messages. If silence suppression is set to 'Enable w/o Adaptations', 'annexb=yes' is included. An exception to this logic is when the remote gateway is a Cisco device (refer to 'Is Cisco SCE Mode' parameter).

➤ **To configure Coders Table:**

1. In the Navigation pane, select **SIP ► SIP General ► Coders Group**; the SIP Coders Group List is displayed.
2. Use the  or  buttons to add or remove entries.
3. Select a specific row, and then in the Navigation pane, select **Coders**; the SIP Coder List is displayed.
4. Use the  or  buttons to add or remove entries.
5. Select a specific row, and then in the Configuration pane, click **SIP Coders Settings**; the SIP Coders Settings screen is displayed.
6. Configure the Coder parameters according to the table 'Coder Parameters' below.
7. Click the Maintenance icon  and select **Unlock** to activate the configuration.

Table 40-14: Coder Parameters

Parameter Name	Type	Provisioning Type	Description
Name	String Up to 20 chars.	Online	Easily identifiable user-defined Coder name
Coder Name	Enum G.711 A-law, G.711 U-law, G.729, G.723.1, G.726, GSM-FR, GSM-EFR, MS-GSM, NetCoder, AMR, EVRC, Transparent, QCELP, iLBC, EVRC-B 4GV, G.722, AMR-WB, T.38, G.711A-law_VBD, G.711U-law_VBD, EG.711 A-law, EG.711 U-law, G.729.1, MS RTA NB, MS RTA WB	Online	Defines Coder name. Each Coder Name may appear in Coder Table only once.
Packetization Time	Enum default, t10ms, t20ms, t30ms, t40ms, t50ms, t60ms, t70ms, t80ms, t90ms, t100ms, t110ms, t120ms, t130ms, t140ms, t150ms	Online	Defines packetization time (in milliseconds). Determines how many coder payloads are combined into a single RTP packet. If not specified, the <i>ptime</i> gets a default value. The <i>ptime</i> specifies the packetization time the gateway expects to receive. The gateway always uses the <i>ptime</i> requested by the remote side for sending RTP packets.
Coder Rate(kbps)	Enum 0 – 64000	Online	Defines coder bit rate (in Kbps).
Payload Type	Integer 0-120	Online	Defines payload type. Applicable to coders with dynamic payload only. Specifies the format of the RTP payload. If not specified – a default is used.
Silence Suppression	Enum Disable, Enable, EnableWithoutAdaptations	Online	Enables/disables the silence suppression. For G.729 it is also possible to select the silence suppression without adaptations.

40.6 IP Groups Table

Use the IP Groups table to define logical entities that represent a group of SIP users (e.g. IP phones, gateways or proxy servers) that communicate with the Mediant 8000.

The IP Groups can be used as follows:

- To determine the destination entity in the 'Tel to IP / Outbound Routing' and 'Account Group' tables
- To identify source entity in the 'IP to Tel / Inbound Routing' table

Each IP Group may be assigned with various parameters that affect formatting of the SIP messages headers and/or other SIP protocol-specific behavior.

40.6.1 Configuring the IP Group Table

This section describes how to configure the IP Group Table.

➤ To configure the IP Group Table:

1. Click  to access the Media Gateway status screen.
2. Select the desired SIP board.
3. In the Navigation pane, select **SIP ► SIP General ► SIP Control Network ► IP Groups**; the IP Groups list is displayed.
4. Use the  or  buttons to add or remove entries.
5. Select a specific row and then in the configuration pane, click **IP Group Settings**; the IP Group Settings screen is displayed. .

The IP Group configuration frame is divided into the following tabs:

- **General Settings** – these settings are relevant for all SIP applications: Gateway, IP-to-IP, SAS, and SBC.
- **Gateway Setting**- The parameters under this tab can be configured for the Gateway and IP-to-IP applications only.
- **SBC Settings**- The parameters under this tab can be configured for the SBC application only.

6. Configure the IP Groups parameters according to the table 'IP Group Parameters' below.
7. Click the Maintenance icon , and then select **Unlock** to activate the configuration.

Table 40-15: IP Group Parameters

Parameter Name	Type	Provisioning Type	Description
Name	String Up to 20 chars.	Instant	User-defined name (Textual), assigned to the IP Group, enabling users to identify it intuitively and easily.
IP Group Type	Enum Server, User, Gateway	Instant	The IP Group type: ▪ SERVER – used when the destination address (configured by the Proxy Set) of the IP Group (e.g., ITSP, Proxy, IP-PBX, or Application server) is known. ▪ USER – represents a group of users (such as IP phones and softphones) where their location is dynamically obtained by the device when REGISTER requests and responses traverse (or are terminated) by the device. These users are considered remote (far-end) users. Typically, this IP Group is configured with a Serving IP Group that represents an IP-PBX, Application or Proxy server that serves this USER-type IP Group. Each SIP request sent by a user of this IP Group is proxied to the Serving IP Group. For registrations, the device updates its internal database with the AOR and contacts of the users. Digest authentication using SIP 401/407 responses (if needed) is performed by the Serving IP Group. The device forwards these responses directly to the SIP users. To route a call to a registered

Parameter Name	Type	Provisioning Type	Description
			user, a rule must be configured in the 'Tel to IP/Outbound Routing' table. The device searches the dynamic database (by using the request URI) for an entry that matches a registered AOR or Contact. Once an entry is found, the IP destination is obtained from this entry, and a SIP request is sent to the destination. The device also supports NAT traversal for the SIP clients that are behind a NAT. In this case, the device must be defined with a global IP address. ▪ GATEWAY – used to indicate that a specific group is used for the Tel-to-IP application only.
Proxy Set	Integer 0-32	Instant	Selects the Proxy Set (defined in 'Proxy Sets Table') to associate with the IP Group. All INVITE messages configured to be 'sent' to the specific IP Group are sent to the IP address associated with this Proxy Set. Note: The Proxy Set is only defined for SERVER type IP Groups.

Parameter Name	Type	Provisioning Type	Description
SIP Group Name	String Up to 49 chars.	Instant	The request URI host name used in INVITE and REGISTER messages that are sent to this IP Group, or the host name in the From header of INVITE messages received from this IP Group. If not specified, the value of the global parameter Proxy Name (see 'Proxy / Registration Parameters') is used instead. Note: If the IP Group is of type USER, this parameter is used internally as a hostname in the request URI for TDM-to-IP initiated calls. For example, if an incoming call from the device's T1 trunk is routed to a USER-type IP Group, the device first forms the request URI (destination_number@SIPGroupName), and then it searches the User's internal database for a match.
Serving IP Group	Integer -1 (Not Defined) or 1-32	Instant	If configured, INVITE messages initiated from the IP Group are sent to this Serving IP Group. In other words, the INVITEs are sent to the address defined for the Proxy Set associated with this Serving IP Group. The Request URI host name in these INVITE messages are set to the value of the parameter 'SIP Group Name' defined for the Serving IP Group. Notes: ▪ If the parameter Prefer Route Table is Enable, the routing rules in the 'Tel to IP/Outbound IP Routing' table takes precedence over this parameter. ▪ If this parameter is not configured, the INVITE messages are sent to the default Proxy or according to the 'Tel to IP/Outbound IP Routing' table.

Parameter Name	Type	Provisioning Type	Description
Enable Survivability	Enum Disabled, Enabled AlwaysTerminate Register	Instant	Determines whether Survivability mode is enabled for USER-type IP Groups. When survivability mode is enabled, the device records in its local database the registration messages sent by the clients belonging to the USER-type IP Group. If communication with the Serving IP Group (e.g., IP-PBX) fails, the USER-type IP Group enters into Survivability mode in which the device uses its database for routing calls between the clients (e.g., IP phones) of the USER-type IP Group. The RTP packets between the IP phones in Survivability mode always traverse through the device. In Survivability mode, the device is capable of receiving new registrations. When the Serving IP Group is available again, the device returns to normal mode, sending INVITE and REGISTER messages to the Serving IP Group. Note: this parameter is applicable only to USER-type IP Groups.
Contact User	String Up to 50 chars.	Instant	Defines the user part for the From, To, and Contact headers of SIP REGISTER messages, and the user part for the Contact header of INVITE messages that are received from this IP Group and forwarded by the device to another IP Group. Note: this parameter is overridden by the 'Contact User' parameter (if configured) in the 'Account Group' table.
IP Profile	Integer 0-9	Instant	Defines the IP Profile associated with the IP group.
Media Realm	String Up to 40 chars.	Instant	Defines the media realm associated with the IP group.

Parameter Name	Type	Provisioning Type	Description
Always Use Route Table	Enum Disabled, Enabled	Instant	Determines the Request URI host name in outgoing INVITE messages. When set to Enabled, the device uses the IP address (or domain name) defined in the 'Tel to IP/Outbound Routing' table as the Request URI host name in outgoing INVITE messages, instead of the value entered in the 'SIP Group Name' field.
Routing Mode	Enum NotConfigured, RoutingTable, ServingIPGroup, RequestURI	Instant	Defines the routing mode for outgoing SIP INVITE messages. - Not Configured – the routing is done according to the selected Serving IP Group. If no Serving IP Group is selected, the device routes the call according to the 'Tel to IP/Outbound IP Routing' table. - Routing Table – the device routes the call according to the 'Tel to IP/Outbound IP Routing' table. - Serving IP Group – the device sends the SIP INVITE to the selected Serving IP Group. If no Serving IP Group is selected, the default IP Group is used. If the Proxy server(s) associated with the destination IP Group is not alive, the device uses the 'Tel to IP/Outbound IP Routing' table (if fallback enabled - see 'Proxy / Registration Parameters'). - Request-URI – the device sends the SIP INVITE to the IP address according to the received SIP Request-URI host name.

Parameter Name	Type	Provisioning Type	Description
SIP Re Routing Mode	Enum Standard, Proxy, RoutingTable	Instant	Determines the routing mode after a call redirection (i.e., a 3xx SIP response is received) or transfer (i.e., a SIP REFER request is received). - Standard – INVITE messages that are generated as a result of Transfer or Redirect are sent directly to the URI, according to the Refer-To header in the REFER message or Contact header in the 3xx response (default). - Proxy – sends a new INVITE to the Proxy. Applicable only if a Proxy server is used and the parameter Always Send To Proxy is Disabled. - Routing Table – uses the Routing table to locate the destination and then sends a new INVITE to this destination. Notes: - When this parameter is set to Proxy and the INVITE sent to the Proxy fails, the device re-routes the call according to the Standard mode. - When this parameter is set to Routing Table and the INVITE fails, the device re-routes the call according to the Standard mode. If DNS resolution fails, the device attempts to route the call to the Proxy. If routing to the Proxy also fails, the Redirect / Transfer request is rejected. - When this parameter is set to Routing Table, the XferPrefix parameter can be used to define different routing rules for redirected calls. - This parameter is disregarded if the parameter Always Send To Proxy is Enabled.

Parameter Name	Type	Provisioning Type	Description
Media Realm	Integer 0-16	Instant	Defines the media realm associated with the IP group.
SRD Name	Integer 0 – 32	Instant	Defines the SRD associated with the IP Group.
Classify By Proxy Set	Enum Disabled, Enabled	Instant	Defines whether the incoming INVITE is classified to an IP Group according to the Proxy Set. This classification occurs only if classification according to the device's database fails for locating whether the INVITE arrived from a registered user. The classification proceeds with checking whether the INVITE's IP address (if host names, then according to the dynamically resolved IP address list) is defined in the IP Group's Proxy Set ID (in the Proxy Set table). If the IP address is listed, then the INVITE is assigned to this IP Group. Note: This classification is not relevant in cases where multiple IP Groups use the same Proxy Set.
Max Num Of Reg Users	Integer -1 – 10000	Instant	Defines the maximum number of registered users. Value -1 indicates that no limit is applied.

Parameter Name	Type	Provisioning Type	Description
Inbound Message Manipulation Set	Integer -1 – 19	Instant	Message Manipulation Set (rule) that you want to assign to this IP Group for SIP message manipulation rule on the inbound message.
Outbound Message Manipulation Set	Integer -1 – 19	Instant	Message Manipulation Set (rule) that you want to assign to this IP Group for SIP message manipulation on the outbound message.
Source URI	Enum NotConfigured,From,To,RequestURI, PAssertedFirstHeader, PAssertedSecondHeader, PPreferred, Route, Diversion, HistoryInfo, PAssociatedURI, PCalledPartyID, Contact	Instant	The source URI input used in the (CMR) Classify-Manipulate-Route process in SBC. Defining source URI: ▪ Request ▪ If REGISTER request – use the TO header as the source URI ▪ For all other requests, perform the following steps: ▪ -Use P-Preferred header if exist. If not, go to step 2. ▪ -Use the first header in the P-Asserted headers list, if exist. If not, go to step 3. ▪ -Use FROM header as source URI. ▪ Response ▪ Use the TO header as the source URI
Destination URI	Enum NotConfigured,From,To,RequestURI, PAssertedFirstHeader, PAssertedSecondHeader, PPreferred, Route, Diversion, HistoryInfo, PAssociatedURI, PCalledPartyID, Contact	Instant	The destination URI input used in the (CMR) Classify-Manipulate-Route process in SBC. Defining destination URI: ▪ Use Request-URI header as the destination URI (applies for all message types)

Parameter Name	Type	Provisioning Type	Description
Registration Mode	Enum UserInitRegistrations,SBCInitRegistrations,NoRegistrations	Instant	Defines the registration mode for an IP Group: - User initiates registrations (default) - SBC initiate registrations (works only with User Info file) = Used when the device serves as a client (e.g., with an IP PBX). No registrations needed = The device adds users to its database in active state.
Authentication Mode	Enum UserAuthenticates,SBCAuthenticateClient,SBCAuthenticatesServer	Instant	Defines the authentication mode: - User Authenticates (default) = The device does not handle the authentication; however passes the authentication messages between the SIP user agents. - SBC Authenticates (as client) = The device authenticates as a client. It receives the 401/407 response from the proxy requesting for authentication. The device then sends the proxy, the authorization credentials (i.e., user name and password) according to one of the following: - Account defined in the Account table (only if authenticating SERVER-type IP Group), - Global username and password parameters (only if authenticating SERVER-type IP Group), - User Information file, or - Sends request to users requesting credentials (only if authenticating USER-type IP Group). - SBC Authenticates (as server) = The device authenticates as a server (using the User Information file).

Parameter Name	Type	Provisioning Type	Description
Authentication Method List	String 256 char	Instant	Defines SIP methods that the device must challenge. Multiple entries are separated by the forward slash "/". If none is defined (default), no methods are challenged.
Enable SBC Client Forking	Enum No, Yes	Instant	Enables call forking for USER-type IP Groups. No (default) Yes = The device forks INVITE messages (to up to five separate SIP outgoing legs)
Contact Name	String 299 char	Instant	Local Host Name. If configured, the gateway uses the Contact Name string in its Contact and Via headers as a host name . It is used for working with a specific IP group. If this IP group parameter is empty, the Contact header includes the gateway numerical IP address (default). This feature is applicable for Via/Contact headers in outgoing INVITE to the specific IP group, and the Contact header in 18x/200OK responses for incoming INVITE from the specific IP Group. The IP2TEL routing table can be used to identify the source IP group, from where the INVITE message was received. Note: To enable proper gateway operation, the Contact Name should be a valid FQDN.

40.7 Account Group

Use the Account Groups table to define accounts per Trunk Groups (referred to as Served Trunk Group) or to a Served IP Group for registration and/or digest authentication (user name and password) to a destination IP address (Serving IP Group). The Account Group can be used, for example, to register to an Internet Telephony Service Provider (ITSP) on behalf of an IP-PBX to which the device is connected. The registrations are sent to the Proxy Set associated with these Serving IP Groups. A Trunk Group can register to more than one Serving IP Group (e.g., ITSP's), by configuring multiple entries in this Account Groups table with the same Served Trunk Group, however with different Serving IP Groups, user name/password, Host Name, and Contact User parameters.

40.7.1 Configuring Account Group

This section describes how to configure account groups.

➤ **To configure Account Groups:**

1. Click  to access the Media Gateway status screen.
2. Select the desired SIP board.
3. In the Navigation pane, select **SIP ► SIP General ► Account Groups**; the Account Groups list is displayed.
4. Use the  or  buttons to add or remove entries.
5. Select a specific row and then in the configuration pane, click **Account Group Settings**; the Account Group Settings screen is displayed.
6. Configure the Account Group parameters according to the table 'Account Group Parameters' below.
7. Click the Maintenance icon  and select **Unlock** to activate the configuration.

Table 40-16: Account Group Parameters

Parameter Name	Type	Provisioning Type	Description
Name	String Up to 20 chars.	Instant	Textual, user-defined name assigned to the IP Group, enabling users to identify it intuitively and easily.

Parameter Name	Type	Provisioning Type	Description
Served Trunk Group	Integer -1 (Not Defined) or 1-100	Instant	The Trunk Group for which the device performs registration and/or authentication to a destination IP Group (i.e., Serving IP Group). For Tel-to-IP calls, the Served Trunk Group is the source Trunk Group from where the call initiated. For IP-to-Tel calls, the Served Trunk Group is the 'Trunk Group' defined in the 'IP to Tel / Inbound Routing' table. Note: for IP-to-IP call routing, this parameter must be set to Not Defined.
Served IP Group	Integer -1 (Not Defined) or 1-32	Instant	The Source IP Group (e.g., IP-PBX) for which registration and/or authentication is performed. Note: for Tel-to-IP call routing, this parameter must be set to Not Defined.
Serving IP Group	Integer -1 (Not Defined) or 1-32	Instant	The destination IP Group ID to where the REGISTER requests (if enabled) are sent or Authentication is performed. The actual destination to where the REGISTER requests are sent is the IP address defined for the Proxy Set associated with this IP Group. This occurs only in the following conditions: ▪ The parameter 'Registration Mode' is set to 'Per Account' in the 'Trunk Group Settings' table. ▪ The parameter 'Register' in this table is enabled. In addition, for a SIP call that is identified by both, Served Trunk Group/ Served IP Group and Serving IP Group, the username and password for digest authentication defined in this table is used. For Tel-to-IP calls, the Serving IP Group is the destination IP Group defined in the 'Trunk Group Settings' table or 'Tel to IP / Outbound Routing' table. For IP-to-Tel calls, the Serving IP Group is the 'Source IP Group' defined in the 'IP to Tel / Inbound Routing' table. Note: if no match is found in this table for incoming or outgoing calls – the username and password global parameters, defined in the 'Proxy / Registration' are used.
Username	String Up to 50 chars.	Instant	Digest MD5 Authentication user name (up to 50 characters).
Password	String Up to 50 chars.	Instant	Digest MD5 Authentication password (up to 50 characters).

Parameter Name	Type	Provisioning Type	Description
Host Name	String Up to 49 chars	Instant	Defines the Address of Record (AOR) host name. It appears in REGISTER From/To headers as ContactUser@HostName. For successful registrations, this HostName is also included in the INVITE requests' From header URI. If not configured or if registration fails, the 'SIP Group Name' parameter from the 'IP Group' table is used instead.
Register	Enum No, Yes	Instant	Enables registration. When enabled, the device sends REGISTER requests to the Serving IP Group. In addition, to activate registration, you also need to set the parameter 'Registration Mode' to 'Per Account' in the 'Trunk Group Settings' table for the specific Trunk Group. The Host Name (i.e., host name in SIP From/To headers) and Contact User (user in From/To and Contact headers) are taken from this table upon a successful registration. Notes: - The Trunk Group account registration is not effected by the parameter Is Register Needed. - You can configure this table so that a specific IP Group can register to multiple ITSP's. This is performed by defining several rows in this table containing the same Served IP Group, but with different Serving IP Groups, user/password, Host Name and Contact User parameters. - If registration to an IP Group(s) fails for all the accounts defined in this table for a specific Trunk Group, and if this Trunk Group includes all the channels in the Trunk, the Trunk Group is set to Out-Of-Service if the parameter Set Out-Of-Service On Registration Failure is enabled.
Contact User	String Up to 50 chars	Instant	Defines the AOR user name that appears in REGISTER From/To headers as ContactUser@HostName, and in INVITE/200 OK Contact headers as ContactUser@<device's IP address>. If not configured, the 'Contact User' parameter from the 'IP Group Table' page is used instead. Note: If registration fails, then the userpart in the INVITE Contact header contains the source party number.

Parameter Name	Type	Provisioning Type	Description
Application Type	Enum Gwlp2ip(0), SBC(2)	Instant	Defines the type of application per account.

40.8 SIP Routing DNS Table

The internal DNS table, similar to a DNS resolution, translates hostnames into IP addresses. This table is used when hostname translation is required (e.g., 'Tel to IP Routing' table). Two different IP addresses can be assigned to the same hostname. If the hostname isn't found in this table, the gateway communicates with an external DNS server.

Assigning two IP addresses to hostname can be used for alternative routing (using the 'Tel to IP Routing' table).

40.8.1 Configuring the Internal DNS Table

This section describes how to configure the internal DNS table.

➤ To configure the SIP routing DNS settings:

1. Click  to access the Media Gateway status screen.
2. Select the desired SIP board.
3. In the Navigation pane, select **SIP ► SIP General ► DNS**; the SIP DNS list is displayed.
4. Use the  or  buttons to add or remove entries.
5. Select a specific row and then in the configuration pane, click **DNS Settings**; the DNS Settings screen is displayed.
6. Configure the DNS Table entry parameters as described in table 'Internal DNS Table Parameters' below.
7. Click the Maintenance icon  and select **Unlock** to activate the configuration.

Table 40-17: SIP Routing DNS Settings Parameters

Parameter Name	Type	Provisioning Type	Description
Name	String Up to 20 chars.	Online	Textual, user-defined name assigned to the entity (MO), enabling users to identify it intuitively and easily.

Parameter Name	Type	Provisioning Type	Description
Domain Name	String Up to 31 chars.	Instant	If the internal DNS table is configured, the gateway first tries to resolve a domain name using this table. If the domain name isn't found, the gateway performs a DNS resolution using an external DNS server.
First / Second / Third / Fourth IP Address	IP Address	Instant	Up to four IP address assigned to a hostname. Also supports IPV6.

40.9 SIP SRV to IP Table

The Internal SRV table provides a table for resolving host names to DNS A-Records. Three different A-Records can be assigned to each host name. Each A-Record contains the host name, priority, weight, and port.

If the Internal SRV table is configured, the Mediant 8000 initially attempts to resolve a domain name using this table. If the domain name isn't found, the Service Record (SRV) resolution is performed using an external DNS server.

40.9.1 Configuring the SIP SRV to IP Table

This section describes how to configure the SIP SRV to IP table.

➤ To configure the Internal SRV Table:

1. Click  to access the Media Gateway status screen.
2. Double-click the desired SIP board.
3. In the Navigation pane, select **SIP** ➤ **SIP General** ➤ **SRV**; the SIP SRV to IP list is displayed.
4. Use the  or  buttons to add or remove entries.
5. Select a specific row and then in the configuration pane, click **SIP SRV to IP Settings**; the SIP SRV to IP Settings provisioning screen is displayed.
6. Configure the SIP SRV to IP Table entry parameters as described in the table 'SIP SRV to IP Table Parameters' below.
7. Click the Maintenance icon  and select **Unlock** to activate the configuration.

Table 40-18: SIP SRV to IP Table Parameters

Parameter Name	Type	Provisioning Type	Description
Name	String Up to 20 chars.	Online	Textual, user-defined name assigned to the entity (MO), enabling users to identify it intuitively and easily.
Domain Name	String Up to 70 chars.	Instant	The host name to be translated.
Transport Type	Enum UDP, TCP, TLS	Instant	Transport type of the SRV query.
DNS Name 1 / 2 / 3	String Up to 98 chars.	Instant	Up to three DNS A-Records to which the host name is translated.
Priority 1 / 2 / 3	Integer 0-65535	Instant	Priority of the corresponding entry in the SRV table.
Weight 1 / 2 / 3	Integer 0-65535	Instant	Weight of the corresponding entry in the SRV table.
Port 1 / 2 / 3	Integer 0-65535	Instant	IP port of the corresponding entry in the SRV table.

40.10 SRD Table

The Signaling Routing Domain (SRD) is a set of definitions of IP interfaces, resources, SIP behaviors and other definitions that partition a single SIP board into multiple virtual multi service gateways.

SRD provides the following capabilities:

- Provides different SIP signaling (SRD associated with a SIP Interface) and RTP media (associated with a Media Realm) interfaces for multiple Layer-3 networks
- Enables separation of SIP signaling traffic between different customers; multiple gateway customers may reside either in the same or different Layer-3 networks as the device.

Once configured, the following actions can be performed on the SRD:

- Associate to a SIP Interface (see 'SIP Interfaces Table' on page [630](#))
- Associate to an IP Group (see 'IP Groups Table' on page [611](#))
- Associate to a Proxy Set (see 'SIP Proxy Settings Table' on page [547](#))
- Define as a Classification parameter to associate the incoming SIP request with a specific IP Group (see 'Source IP Group Classification' on page [745](#))
- Define as an IP to IP Destination rule (see 'SBC Routing' on page [745](#))
- Apply an Admission Control rule to a specific SRD (see 'SBC Admission Control' on page [768](#)).

40.10.1 Configuring the SRD Table

This section describes how to configure the SRD table.

➤ **To configure the SRD Table:**

1. Click  to access the Media Gateway status screen.
2. Select the desired SIP board.
3. In the **Navigation Pane** select **SIP ► SIP General ► SRD**; the SRD list is displayed.
4. Use the  or  buttons to add or remove entries.
5. Select a specific row and then in the configuration pane,; click **SRD Settings**; the SRD Settings screen is displayed.
6. Configure SRD parameters according to the table 'SRD Parameters' below.
7. Click the Maintenance icon  and select **Unlock** to activate the configuration.

Table 40-19: SRD Parameters

Parameter Name	Type	Provisioning Type	Description
Name	String Up to 20 chars.	Instant	User-defined name (Textual), assigned to the SRD, enabling users to identify it intuitively and easily.
Media Realm	Integer 0-8	Instant	Defines the Media Realm (range of UDP ports in the media subnet) associated with this SRD.
Intra SRD Media Anchoring	Enum Anchor Media, Don't Anchor Media	Instant	Defines the SRD internal media anchoring behavior: - Anchor Media – don't support direct Media calls. - Don't Anchor Media – the calls between two user agents belonging to the same SRD (source and destination) are direct Media calls.
Max Num Of Reg Users	Integer -1 – 10000	Instant	Defines the maximum number of registered users.
Block UnReg Users	Enum No, Yes	Instant	Defines whether unregistered users are blocked.
Enable UnAuthenticated Registrations	Enum No, Yes	Instant	Enables/disables unauthenticated registrations.

40.11 SIP Interfaces Table

A SIP Interface represents a single SIP signaling entity, which is a combination of UDP, TCP, and TLS ports relating to a single IP address (in the control subnet). The SIP Interface is configured with a corresponding SRD. This interface allows User Agents on the network to communicate with a specific SRD using the SIP Interface associated with it.

Each SRD may be associated with up to 2 SIP Interfaces (one per application type – Gateway/IP-to-IP and SBC). Each SIP Interface must have a unique signaling port (i.e. no port overlapping is allowed).

SIP Interfaces provide the following capabilities:

- Uses different SIP signaling ports.
- Differentiates between the different applications supported by the device (i.e. Gateway/IP2IP and SBC).
- Separates signaling traffic of different customers to use different routing tables, manipulations, SIP definitions, etc.

40.11.1 Configuring the SIP Interfaces Table

This section describes how to configure the SIP Interfaces table.

➤ **To configure the SIP Interfaces Table:**

1. Click  to access the Media Gateway status screen.
2. Select the desired SIP board.
3. In the Navigation Pane, select **SIP ► SIP General ► SIP Interface**; the SIP Interface list is displayed.
4. Use the  or  buttons to add or remove entries.
5. Select a specific row and then in the configuration pane, click **SIP Interface Settings**; the SIP Interface Settings screen is displayed.
6. Configure SIP Interface parameters according to the table 'SIP Interface Parameters' below.
7. Click the Maintenance icon  and select **Unlock** to activate the configuration.

Table 40-20: SIP Interface Parameters

Parameter Name	Type	Provisioning Type	Description
Board IP Address Index	Integer 0-10	Instant	Control Subnet index, as configured in the Board's IP Address table.

Parameter Name	Type	Provisioning Type	Description
Application Type	Enum Gwlp2Ip, SAS, SBC	Instant	Defines the application type associated with this SIP interface. GW/IP2IP – IP-to-IP routing application and regular gateway functionality SAS – Stand-Alone Survivability (SAS) application SBC – Session Border Controller application
UDP Port	Integer 1-65534	Instant	Defines the listening and source UDP port. Note: This port must be outside of the RTP port range.
TCP Port	Integer 1-65534	Instant	Defines the listening TCP port. Note: This port must be outside of the RTP port range.
TLS Port	Integer 1-65534	Instant	Defines the listening TLS port. Note: This port must be outside of the RTP port range.
SRD	Integer 0-32	Instant	Index of the associated SRD.
Message Policy	Integer 1-5	Instant	Associates Message Policy to SIP interface.

40.12 NAT Translation Table

This table's parameters define multiple NATs for SIP control and RTP media using Static NAT rules. This table creates NAT rules for translating a source IP address per VoIP interface (SIP control and RTP media traffic) into NAT IP addresses. This allows, for example, the separation of VoIP traffic between different ISTP's, and topology hiding (of internal IP addresses to the "public" network). Each IP interface (configured in the Multiple Interface table - InterfaceTable parameter) can be associated with a NAT rule in this table, translating the source IP address and port of the outgoing packet into the NAT address (IP address and port range).

40.12.1 Configuring the NAT Translation Table

This section describes how to configure the NAT Translation Table

➤ **To configure the NAT Translation Table:**

1. Click  to access the Media Gateway status screen.
2. Select the desired SIP board.
3. In the Navigation Pane, select **SIP ► SIP General ► NAT Translation**; the NAT Translation list is displayed.
4. Use the  or  buttons to add or remove entries.
5. Select a specific row and in the Configuration pane, click **SIP NAT Translation**; the SIP NAT Translation screen is displayed.
6. Configure SIP NAT Translation parameters according to the table NAT Translation Parameters' below.
7. Click the Maintenance icon  and select **Unlock** to activate the configuration.

Table 40-21: NAT Translation Parameters

Parameter Name	Type	Provisioning Type	Description
Subnet Name	String up to 255 chars	Online	Subnet name as defined in the Boards Network.
Global IP address	String up to 20 chars	Online	Global IP address which is represented by NAT.
Source Start Port	Integer 1-65535	Online	Optional port range (1-65535) of the IP interface. If no ports are required, leave this field blank.
Source End Port	Integer 1-65535	Online	Optional port range (1-65535) of the IP interface. If no ports are required, leave this field blank.

Table 40-21: NAT Translation Parameters

Parameter Name	Type	Provisioning Type	Description
Global IP Start Port	Integer 1-65535	Online	Optional port range (1-65535) of the global address. If no ports are required, leave this field blank.
Global IP End Port	Integer 1-65535	Online	Optional port range (1-65535) of the global address. If no ports are required, leave this field blank.

40.13 Least Cost Routing (LCR) Table

The LCR feature enables the device to choose the outbound IP destination routing rule based on lowest call cost. This is useful in that it enables service providers to optimize routing costs for customers. For example, you may wish to define different call costs for local and international calls, or different call costs for weekends and weekdays (specifying even the time of call). The device sends the calculated cost of the call to a Syslog server (as Information messages), thereby enabling billing by third-party vendors.

LCR is implemented by defining Cost Groups and assigning them to routing rules in the Outbound IP Routing table. The device searches this routing table for matching routing rules, and then selects the rule with the lowest call cost. If two routing rules have identical costs, then the rule appearing higher up in the table is used (i.e., first-matched rule). If a selected route is unavailable, the device selects the next least-cost routing rule. However, even if a matched rule is not assigned a Cost Group, the device can select it as the preferred route over other matched rules with Cost Groups. This is determined according to the settings of the Default Cost parameter in the Routing Rule Groups table.

The Cost Group defines a fixed connection cost (*connection cost*) and a charge per minute (*minute cost*). Cost Groups can also be configured with time segments (*time bands*), which define connection cost and minute cost based on specific days of the week and time of day (e.g., from Saturday through Sunday, between 6:00 and 18:00). If multiple time bands are configured per Cost Group and a call spans multiple time bands, the call cost is calculated using only the time band in which the call was initially established.

In addition to Cost Groups, the device can calculate the call cost using an optional, user-defined average call duration value. The logic in using this option is that a Cost Group may be cheap if the call duration is short, but due to its high minute cost, may prove very expensive if the duration is lengthy. Thus, together with Cost Groups, the device can use this option to determine least cost routing. The device calculates the Cost Group call cost as follows: Total Call Cost = Connection Cost + (Minute Cost * Average Call Duration).

The following steps should be performed to configure LCR:

1. Routing Rule Groups Table - Enable LCR feature and configure the average call duration and default connection cost.
2. Cost Group Table - Configuring Cost Groups
3. Time Band Table - Configuring Time Bands for Cost Groups
4. Tel to IP / Outbound Table - Assign Cost Groups to outbound IP routing or IPtoIP routing rules.

40.13.1 Configuring the Routing Rule Groups Table

This section describes how to configure the routing rule groups table.

➤ To configure the Routing Rule Groups Table:

1. Click  to access the Media Gateway status screen.
2. Select the desired SIP board.
3. In the Navigation Pane, select **SIP** ➤ **SIP General** ➤ **Least Cost Routing** ➤ **Routing Rule Groups**; the Routing Rule Groups list is displayed.
4. Use the  or  buttons to add or remove entries. **Note** – only one can be added.
5. Select a specific row and in the Configuration pane, click **SIP Routing Rule Group Frame**; the SIP Routing Rule Groups screen is displayed.
6. Configure SIP Routing Rule Groups parameters according to the table Routing Rule Groups Parameters' below.
7. Click the Maintenance icon  and select **Unlock** to activate the configuration.



Routing Rule Groups Parameters

Parameter Name	Type	Provisioning Type	Description
LCR Enable	Enum Disabled, Enabled	Instant	Enables The Lcr Feature.
Average Call Length	Integer 0-30000	Instant	Defines The Average Call Duration (in Minutes) And Is Used To Calculate The Variable Portion Of The Call Cost.
Default Cost	Enum Lowestcost, Highestcost	Instant	Determines whether routing rules Routing table without an assigned Cost Group are considered a higher cost or lower cost route compared to other matched routing rules that are assigned Cost Groups.

40.13.2 Configuring the Cost Group Table

The following table has a child table Time Bands table. The Cost Group table can't be removed until the Time Bands table is removed. When the Cost Group table is locked, all associated Time Bands tables are also locked..

➤ **To configure the Cost Group Table:**

1. Click  to access the Media Gateway status screen.
2. Select the desired SIP board.
3. In the Navigation Pane, select **SIP ► SIP General ► Least Cost Routing ► Cost Group**; the Cost Group list is displayed.
4. Use the  or  buttons to add or remove entries. **Note** – only one can be added.
5. Select a specific row and in the Configuration pane, click **SIP Cost Group Group Frame**; the SIP Cost Group screen is displayed.
6. Configure Cost Group parameters according to the table Cost Group Parameters' below.
7. Click the Maintenance icon  and select **Unlock** to activate the configuration.

Cost Group Parameters

Parameter Name	Type	Provisioning Type	Description
Cost Group Name	String up to 30 chars	Instant	Defines An Unique Name For The Cost Group.
Default Connect Cost	Integer 0- 3000	Instant	Defines The Call Connection Cost (added As A Fixed Charge To The Call) For A Call Outside The Time Bands.
Default Time Cost	Integer 0- 3000	Instant	Defines the call charge per minute for a call outside the time bands.

40.13.3 Configuring the Time Band Table

The purpose of Time Band table is to configure Time Bands for Cost Group. The time bands defines the day and time range for which the time band is applicable (e.g. from Monday 05:00 to Friday 16:00) as well as the fixed call connection charge and call rate per minute for this interval.

➤ **To configure the Time Band Table:**

1. Click  to access the Media Gateway status screen.
2. Select the desired SIP board.
3. In the Navigation Pane, select **SIP SIP General ▶ Least Cost Routing ▶ Cost Group ▶ Time Band**; the Time Band list is displayed.
4. Use the  or  buttons to add or remove entries. **Note** – only one can be added.
5. Select a specific row and in the Configuration pane, click **SIP Cost Group Group Time Band Frame**; the SIP Cost Group screen is displayed.
6. Configure Time Band parameters according to the table Time Band Parameters' below.
7. Click the Maintenance icon  and select **Unlock** to activate the configuration.

Time Band Parameters

Parameter Name	Type	Provisioning Type	Description
Start Time (ddd:hh:mm)	String up to 9 chars	Instant	Defines The Day And Time Of Day From When This Time Band Is Applicable. The Format Is Ddd:hh:mm (e.g., Sun:06:00), Where: <i>Ddd</i> Is The Day (i.e., Sun, Mon, Tue, Wed, Thu, Fri, Or Sat) <i>Hh</i> And <i>Mm</i> Denote The Time Of Day, Where <i>Hh</i> Is The Hour (00-23) And <i>Mm</i> The Minutes (00-59)
End Time (ddd:hh:mm)	String Up To 9 Chars	Instant	Defines The Day And Time Of Day Until When This Time Band Is Applicable. The Format Is Ddd:hh:mm (e.g., Sun:06:00), Where: <i>Ddd</i> Is The Day (i.e., Sun, Mon, Tue, Wed, Thu, Fri, Or Sat) <i>Hh</i> And <i>Mm</i> Denote The Time Of Day, Where <i>Hh</i> Is The Hour (00-23) And <i>Mm</i> The Minutes (00-59)
Connection Cost	Integer 0-65533	Instant	Defines The Call Connection Cost During This Time Band. This Is Added As A Fixed Charge To The Call.

Time Band Parameters

Parameter Name	Type	Provisioning Type	Description
Minute Cost	Integer 0-65533	Instant	Defines the call cost per minute charge during this timeband.

40.14 SIP Message Policy Table

This feature provides support for defining SIP message policies for blocking (blacklist) unwanted incoming SIP messages and allowing (whitelist) receipt of desired messages. This feature allows you to define legal and illegal characteristics of a SIP message. The message policy can apply globally (default) or per signaling domain (i.e., assigned to a SIP interface in the SIP Interface table).

This feature is helpful against VoIP fuzzing (also known as robustness testing), which sends different types of packets to its "victims" for finding bugs and vulnerabilities. For example, the attacker might try sending a SIP message containing either an oversized parameter or too many occurrences of a parameter.

Perform the following steps to configure the SIP Message Policy:

1. Configuring Message Policy Rule
2. Assign Message Policy Rule to SIP Interface

40.14.1 Configuring the SIP Message Policy Table

This section describes how to configure the SIP Message Policy table.

➤ To configure the SIP Message Policy Table:

1. Click  to access the Media Gateway status screen.
2. Select the desired SIP board.
3. In the Navigation Pane, select **SIP ► SIP General ► SIP Message Policy**; the SIP Message Policy list is displayed.
4. Use the  or  buttons to add or remove entries.
5. Select a specific row and in the Configuration pane, click **SIP Message Policy Settings Frame**; the SIP Message Policy Settings screen is displayed.
6. Configure SIP Message Policy parameters according to the table 'SIP Message Policy Parameters' below.
7. Click the Maintenance icon  and select **Unlock** to activate the configuration.

Table 40-22: SIP Message Policy Parameter

Parameter Name	Type	Provisioning Type	Description
Max Message Length	Integer 0-32768	Instant	Defines the maximum SIP message length.
Max Header Length	Integer 0-256	Instant	Defines the maximum SIP header length.
Max Body Length	Integer 0-512	Instant	Defines the maximum SIP message body length. This is the value of the Content-Length header.
Max Num Headers	Integer 1-16	Instant	Defines the maximum number of headers.
Max Num Bodies	Integer 0-2	Instant	Defines the maximum number of bodies.
Send Rejection	Enum PolicyReject,PolicyDrop	Instant	Determines whether the device sends a 400 "Bad Request" response if a message request is rejected. 0 - Policy Reject - If the message is a request, then the device sends a response to reject the request. 1- Policy Drop - The device ignores the message without sending any response.
Method List Type	Enum Blacklist,Whitelist	Instant	Determines the policy for the SIP methods. 0- Policy Blacklist = The specified methods (in the 'Method List' field) are rejected by the policy. 1- Policy Whitelist = The specified methods (in the 'Method List' field) are allowed by the policy.
Method List	String up to 256 chars	Instant	Defines the SIP methods (e.g., "INVITE\BYE") to which the rule applies. The syntax for entering the methods is as follows: Methods must be separated by a forward slash (/).

Parameter Name	Type	Provisioning Type	Description
Body List Type	Enum Blacklist,Whitelist	Instant	Determines the policy for the defined SIP body. ▪ 0-Policy Blacklist =The specified SIP body (in the 'Body List' field) is rejected by the policy. ▪ 1-Policy Whitelist = The specified SIP body (in the 'Body List' field) is allowed by the policy.
Body List	String up to 256 chars	Instant	Defines the SIP message body list (i.e., value of the Content-Type header) to which the rule applies. Must be separated by a forward slash (\). application/sdp \ audio/telephone-event.

40.15 Routing Based on LDAP Active Directory Queries

The device supports Lightweight Directory Access Protocol (LDAP), enabling call routing decisions based on information stored on a third-party LDAP server (or Microsoft's Active Directory™ Enterprise Directory server). This feature enables the usage of a single common, popular database to manage and maintain information regarding user's availability, presence, and location.

The basic LDAP mechanism is described below:

- **Connection:** The device connects and binds to the remote LDAP server either during the service's initialization (at device start-up) or whenever the LDAP server's IP address and port is changed. The LDAP Service makes 10 attempts to connect and bind to the remote LDAP server with a timeout of 20 seconds between the attempts. If the connection fails, the service remains in the disconnected state until either the LDAP server's IP address or port is changed.

If connection to the LDAP server later fails, the service attempts to reconnect. The SNMP alarm is sent when the connection is broken. Upon successful reconnection, the alarm is cleared.

Binding to the LDAP server can be anonymous or not. For anonymous binding, the LDAPBindDN and LDAPPASSWORD parameters must not be defined or set to an empty string.

The address of the LDAP server can be a DNS name / FQDN configured by the LDAP Server Domain Name parameter, or an IP address configured by the LDAP Server IP parameter.

Up to five LDAP servers can be provisioned in the Mediant 8000/Mediant 5000 system, where each Media Gateway SIP board can be assigned with one LDAP server.



Note: If you configure an FQDN, make sure that the LDAPServerIP parameter is left empty.

- **Search:** For the device to run a search using the LDAP service, the path to the directory's subtree (or DN) where the search is to be performed must be configured using the LDAP Search DN parameter. Up to three DNs can be configured. The search key, or filter in LDAP references, which define the exact DN to be found and one or more attributes whose values should be returned, must also be defined.

If the connection to the LDAP server is disrupted during the search, all search requests are dropped and an alarm indicating a failed status is sent to client applications.

40.15.1 Configuring LDAP Server Parameters

This section describes how to configure the LDAP server .Up to five LDAP servers can be configured. Each Media Gateway SIP board can be associated with one LDAP server

➤ ☐ To configure the LDAP Servers Table:

1. Click  to access the Media Gateway status screen.
2. In the Navigation pane, select **Services** ➤ **LDAP**; the SIP LDAP Servers list is displayed.
3. Use the  or  buttons to add or remove entries.
4. Select a specific row, and then in the Configuration pane, click **LDAP Server Settings** ; the LDAP Server Settings screen is displayed.
5. Configure LDAP server parameters according to the table 'LDAP server settings' below.
6. Click the Maintenance icon , and then select **Unlock** to activate the configuration.

Table 40-23: LDAP Server Parameters

Parameter Name	Type	Provisioning Type	Description
Name	String	Online	Defines name of LDAP server.
LDAP Server IP		Online	Defines the LDAP server's address as an IP address (in dotted-decimal notation, e.g., 192.10.1.255). The default is 0.0.0.0..

Parameter Name	Type	Provisioning Type	Description
LDAP Server Port	Integer	Online	Defines the LDAP server's port number. The valid value range is 0 to 65535. The default port number is 389
LDAP Server Domane Name		Online	Defines the host name (FQDN) of the LDAP server. The device tries to connect to the LDAP server according to the IP address list received in the DNS query. If there is no connection to the LDAP server or the connection to the LDAP server fails, the device tries to connect to the LDAP server with the next IP address in the DNS query list. Note: The 'LDAP Server IP' parameter takes precedence over this parameter. Thus, if you want to use an FQDN, keep the 'LDAP Server IP' parameter empty.
LDAP Search DN	String	Online	Defines up to three search DN's for LDAP search queries. These are the DN subtrees where the search is done. This parameter is mandatory for the search. The format of this parameter is as follows: OU=QA,DC=SIPLDAP,DC=NET In this example, the DN path is defined by the LDAP names, ou (organizational unit) and dc (domain component).
LDAP Password	String	Online	Defines the LDAP server's user password.
LDAP Bind Dn	String	Online	Defines the LDAP server's bind Distinguished Name (DN). This is used as the username during connection and binding to the server. For example: LDAPBindDN = CN=Search user,OU=Labs,DC=OCSR2,DC=local Note: The DN is used to uniquely name an Active Directory object.

40.15.2 Querying the AD and Routing Priority

The device queries the AD using the initial destination number (i.e., called number). The query can return up to four user phone numbers, each pertaining to one of the IP domains (i.e., private number, Lync / OCS number, PBX / IP PBX number, and mobile number). The configuration parameters listed in the table below are used to configure the query attribute keys that define the AD attribute that you wish to query in the AD:

Table 40-24: Parameters for Configuring Query Attribute Key

Parameter	Queried User Domain (Attribute) in AD	Query or Query Result Example
LDAPPBXNumAttributeName	PBX or IP PBX number (e.g., "telephoneNumber" - default)	telephoneNumber=+3233554447
LDAPOCSTNumAttributeName	Mediation Server / Lync client number (e.g., "msRTCSIP-line")	msRTCSIP-line=john.smith@company.com
LDAPMobileNumAttributeName	Mobile number (e.g., "mobile")	mobile=+3247647156
LDAPPrivateNumAttributeName	Any attribute (e.g., "msRTCSIP-PrivateLine") Note: Used only if set to same value as Primary or Secondary key.	msRTCSIP-PrivateLine=+3233554480
LDAPPrimaryKey	Primary Key query search instead of PBX key - can be any AD attribute	msRTCSIP-PrivateLine=+3233554480
LDAPSecondaryKey	Secondary Key query key search if Primary Key fails - can be any attribute	-

The process for querying the AD and subsequent routing based on the query results is as follows:

1. If the Primary Key is configured, it uses the defined string as a primary key instead of the one defined in MSLDAPPBXNumAttributeName. It requests the attributes which are described below.
2. If the primary query is not found in the AD and the Secondary Key is configured, it performs a second query for the destination number using a second AD attribute key name, configured by the 'MSLDAPSecondaryKey' parameter.
3. If none of the queries are successful, it routes the call to the original dialed destination number according to the routing rule matching the LDAP_ERR destination prefix number value, or rejects the call with a SIP 404 "Not Found" response.

4. For each query (primary or secondary), it requests to query the following attributes (if they're not configured as an empty string):

- LDAPPBXNumAttributeName
- LDAPOCSNumAttributeName
- LDAPMobileNumAttributeName

In addition, it queries the special attribute defined in 'LDAPPrivateNumAttributeName', only if the query key (primary or secondary) is equal to its value.

5. If the query is found: the AD returns up to four attributes - Lync / OCS, PBX / IP PBX, private (only if it equals Primary or Secondary key), and mobile.
6. The device adds unique prefix keywords to the query results to identify the query type (i.e., IP domain). These prefixes are used as the prefix destination number value in the Outbound IP Routing table to denote the IP domains:
 - "PRIVATE" (PRIVATE:<private_number>): used to match a routing rule based on query results of the private number (MSLDAPPrivateNumAttributeName)
 - "OCS" (OCS:<Lync_number>): used to match a routing rule based on query results of the Lync client number (MSLDAPOCSNumAttributeName)
 - "PBX" (PBX:<PBX_number>): used to match a routing rule based on query results of the PBX / IP PBX number (MSLDAPPBXNumAttributeName)
 - "MOBILE" (MOBILE:<mobile_number>): used to match a routing rule based on query results of the mobile number (MSLDAPMobileNumAttributeName)
 - "LDAP_ERR": used to match a routing rule based on a failed query result when no attribute is found in the AD



Note: These prefixes are involved only in the routing and manipulation processes; they are not used as the final destination number.

7. The device uses the Outbound IP Routing table to route the call based on the LDAP query result. The device routes the call according to the following priority:
 - a. **Private line:** If the query is done for the private attribute and it's found, then the device routes the call according to this attribute.
 - b. **Mediation Server SIP address (Lync / OCS):** If the private attribute does not exist or is not queried, then the device routes the call to the Mediation Server (which then routes the call to the Lync client).
 - c. **PBX / IP PBX:** If the Lync / OCS client is not found in the AD, it routes the call to the PBX / IP PBX.
 - d. **Mobile number:** If the Lync / OCS client (or Mediation Server) is unavailable (e.g., SIP response 404 "Not Found" upon INVITE sent to Lync client), and the PBX / IP PBX is also unavailable, then the device routes the call to the user's mobile number (if exists in the AD).

8. **Alternative route:** If the call routing to all the above fails (e.g., due to unavailable destination - call busy), the device can route the call to an alternative destination if an alternative routing rule is configured.
9. **"Redundant" route:** If the query fails (i.e., no attribute found in the AD), the device uses the routing rule matching the "LDAP_ERR" prefix destination **number** value.

40.15.3 Configuring Query Attribute Key

This section describes how to configure the query attribute key.



1. Click  to access the Media Gateway status screen.
2. In the Navigation pane, select VoIP board, in the Navigation pane, select **SIP** ► **SIP General**, and then in the Configuration pane, select **SIP Protocol Settings**.
3. In the **LDAP** tab, Configure LDAP Query Attributes.

Table 40-25: Query Attribute Key

Parameter Name	Type	Provisioning Type	Description
LDAP Server	ENUM	Offline	This parameter associates VOIP Board with LDAP server. A server name could be selected from previously configured LDAP servers list.
LDAP Server Connection Status		Read only parameter	The parameter describes connection status between VOIP board and LDAP server. The possible statuses are: NotApplicable The LDAP server not configured or board isn't associated to LDAP server ConnectionBroken, Connecting,Connected
LDAP PBX NUM Attribute Name	String Default: telephoneNumber	Instant	This attribute <i>telephoneNumber</i> represents PBX telephone number in Active Directory.
LDAP Lync NUM Attribute Name	String Default: msRTCSIP-Line	Instant	This attribute <i>msRTCSIP-Line</i> represents Lync number in Active Directory.
LDAP Mobile NUM Attribute Name	String Default: mobile	Instant	This attribute <i>mobile</i> represents mobile number in Active Directory.

Parameter Name	Type	Provisioning Type	Description
LDAP Private NUM Attribute Name	String Default: msRTCSIP-PrivateLine	Instant	This attribute <i>msRTCSIP-PrivateLine</i> represents user private line number in Active Directory.
LDAP Private key	String Default: empty string	Instant	if the Primary Key is configured, it uses the defined string as a primary key instead of the one defined in LDAPPBXNumAttributeName. It requests the attributes which are described below.
LDAP secondary key	String Default: empty string	Instant	If the primary query is not found in the AD and the Secondary Key is configured, it does a second query for the destination number using a second AD attribute key name, configured by the LDAPSecondaryKey parameter

40.15.4 Configuring AD-Based Routing Rules

The procedure below describes how to configure Tel-to-IP routing based on LDAP queries.

➤ **To configure LDAP-based Tel-to-IP routing for Lync Server 2010:**

1. Configure the LDAP server parameters, as described in 'Configuring LDAP Server Parameters' on page 640.
2. Configure the AD attribute names used in the LDAP query.
 - a. Configure the LDAP attribute names as desired.
3. For the Gateway/IP-to-IP application: Configure AD-based Tel-to-IP routing rules:
 - a. Select the relevant VoIP board, and then open the Tel to IP routing table (**SIP ► GW/IP to IP ► Routing ► Telephone to IP / Outbound**).
 - b. Configure query-result routing rules for each IP domain (private, PBX / IP PBX, Lync / OCS clients, and mobile), using the LDAP keywords (case-sensitive) for the prefix destination number:

Table 40-26: Destination Username Prefixes

AD Object	Description
PRIVATE	Private number
OCS	Lync / OCS client number
PBX	PBX / IP PBX number

AD Object	Description
MOBILE	Mobile number
LDAP_ERR	LDAP query failure

- c. Configure a routing rule for routing the initial Tel call to the LDAP server, using the value "LDAP" for denoting the IP address of the LDAP server.
 - d. For alternative routing, enable the alternative routing mechanism and configure corresponding SIP reasons for alternative routing. For this feature, alternative routing starts from the table row located under the LDAP query row.
4. For the SBC application: Configure AD-based IP-to-IP routing rules:
 - a. Open the IP-to-IP Routing Table.
 - b. Select the relevant VoIP board, and then open the IP-to-IP routing table (**SIP ► SBC ► SBC Routing ► IP-to-IP Routing Table**).
 - c. Configure query-result routing rules for each IP domain (private, PBX / IP PBX, Lync / OCS clients, and mobile), using the LDAP keywords (case-sensitive) in the Destination Username Prefix field:

Table 40-27: Destination Username Prefixes

AD Object	Description
PRIVATE	Private number
OCS	Lync / OCS client number
PBX	PBX / IP PBX number
MOBILE	Mobile number
LDAP_ERR	LDAP query failure

- d. Configure a routing rule for routing the initial call (LDAP query) to the LDAP server, by setting the 'Destination Type' field to LDAP for denoting the IP address of the LDAP server.
- e. For alternative routing, enable the alternative routing mechanism and configure corresponding SIP reasons for alternative routing. For this feature, alternative routing starts from the table row located under the LDAP query row.

The table below shows an example for configuring AD-based Tel-to-IP routing rules in the Outbound IP Routing Table:

Table 40-28: AD-Based Tel-to-IP Routing Rule Configuration Examples

Index	Dest. Phone Prefix	Dest. IP Address
1	PRIVATE:	10.33.45.60
2	PBX:	10.33.45.65
3	OCS:	10.33.45.68
4	MOBILE:	10.33.45.100
5	LDAP_ERR	10.33.45.80
6	*	LDAP
7	*	10.33.45.72

The table below shows an example for configuring AD-based SBC routing rules in the IP-to-IP Routing Table:

Table 40-29: AD-Based SBC IP-to-IP Routing Rule Configuration Examples

Index	Destination Username Prefix	Destination Type	Destination Address
1	PRIVATE:	Dest Address	10.33.45.60
2	PBX:	Dest Address	10.33.45.65
3	OCS:	Dest Address	10.33.45.68
4	MOBILE:	Dest Address	10.33.45.100
5	LDAP_ERR	Dest Address	10.33.45.80
6	*	LDAP	
7	*	Dest Address	10.33.45.72

The configured routing rule example is explained below:

- **Rule 1:** Sends call to private telephone line (at 10.33.45.60) upon successful AD query result for the private attribute.
- **Rule 2:** Sends call to IP PBX (at 10.33.45.65) upon successful AD query result for the PBX attribute.
- **Rule 3:** Sends call to Lync client (i.e., Mediation Server at 10.33.45.68) upon successful AD query result for the Lync attribute.
- **Rule 4:** Sends call to user's mobile phone number (to PSTN through the device's IP address at 10.33.45.100) upon successful AD query result for the Mobile attribute.
- **Rule 5:** Sends call to IP address of device (10.33.45.80) if AD query failure (e.g., no response from LDAP server or attribute not found).

- **Rule 6:** Sends query for original destination number of received call to the LDAP server.
- **Rule 7:** Alternative routing rule that sends the call of original dialed number to IP destination 10.33.45.72. This rule is applied in any of the following cases:
 - LDAP functionality is disabled.
 - LDAP query is successful but call fails (due to, for example to a busy line) to all the relevant attribute destinations (private, Lync, PBX, and mobile), and a relevant **Tel-to-IP Release Reason (see Alternative Routing for Tel-to-IP Calls) or SBC Alternative Routing Reason (see Configuring Alternative Routing Reasons)** has been configured.

Once the device receives the original incoming call, the first rule that it uses is Rule 6, which queries the AD server. When the AD replies, the device searches the table, from the first rule down, for the matching destination phone prefix (i.e., "PRIVATE:", "PBX:", "OCS:", "MOBILE:", and "LDAP_ERR:"), and then sends the call to the appropriate destination.

41 PSTN Gateway and IP-to-IP Applications

This section describes PSTN Gateway and IP-to-IP applications.

41.1 PSTN Gateway Application

The Mediant 8000 supports the PSTN Gateway application that enables customers to establish calls between PSTN and SIP networks.

41.2 IP-to-IP Application

The Mediant 8000 supports IP-to-IP call routing functionality. This functionality, for example, enables enterprises to seamlessly connect their IP-PBX to a SIP trunk provided by an Internet Telephony Service Provider (ITSP), thereby supporting extensive transcoding capabilities for voice, fax, and modems, as well as RTP to SRTP translations.

➤ **To enable IP-to-IP call routing functionality:**

1. Pre-load the SIP boards with a License Key that enables the IP-to-IP feature. See 'Updating License Key' on page 259 for details.
2. Click  to access the Media Gateway status screen.
3. Select the SIP board.
4. In the **Navigation Pane**, select **SIP ► GW/IP to IP**.
5. Click the **Configuration** button; the SIP IP to IP Settings screen is displayed.
6. Configure SIP IP-to-IP parameters as described below.

Table 41-1: SIP IP-to-IP Parameters

Parameter Name	Type	Provisioning Type	Description
Enable IP to IP	Enum Enabled, Disable	Online	Determines whether to enable IP-to-IP functionality. Note that prior to enabling the IP-to-IP application, the SIP board must be pre-loaded with a License Key with the IP-to-IP feature enabled.
Enable RFC4117 Transcoding Mode	Enum Disable, Enable	Online	Enables transcoding of calls according to RFC 4117.

Parameter Name	Type	Provisioning Type	Description
IP to IP Transcoding Mode	Enum IfRequired,Force	Instant	Defines the voice transcoding mode (media negotiation) between two user agents for the IP-to-IP application. [0] Only if Required = Do not force. Media settings (such as gain control) are not implemented on the voice stream; the device passes packets RTP to RTP without any processing. [1] Force = Force transcoding on outgoing IP leg. The device interworks the media by implementing DSP transcoding (default).

41.3 Trunk Groups Table

Use the Trunk Group table to assign trunk groups, profiles and logical telephone numbers to the gateway's E1/T1 B-channels. Trunk Groups are used for routing IP to Tel calls with common rules. Channels that are not defined are disabled.

41.3.1 Configuring the Trunk Group Table

This section describes how to configure the trunk group table.

➤ To configure Trunk Group Table:

1. Click  to access the Media Gateway status screen.
2. Select the desired SIP board.
3. In the Navigation pane, select **SIP ► GW/IP to IP ► Trunk Groups ► Trunk Group**; the SIP Trunk Group list is displayed.
4. Use the  or  buttons to add or remove entries correspondingly.
5. Select a specific row and then in the configuration pane, click **SIP Trunk Group Settings**; the SIP Trunk Group Settings screen is displayed.
6. Configure the Trunk Group parameters according to the table 'Trunk Group Parameters' below.
7. Click the Maintenance icon  and select **Unlock** to activate the configuration.

Table 41-2: Trunk Group Parameters

Parameter Name	Type	Provisioning Type	Description
Name	String Up to 20 chars.	Instant	Textual, user-defined name assigned to the Trunk Group enabling users to identify it intuitively and easily.
Trunk Group ID	Integer 1-99	Instant	Trunk Group ID assigned to the channels. The same trunk group ID can be used for more than one group of channels. Trunk group ID is used to define a group of common behavior channels that are used for routing IP to Tel calls. If an IP to Tel call is assigned to a trunk group, the call is routed to the channel or channels that correspond to the trunk group ID. You can configure the Trunk Group Settings table to determine the method in which new calls are assigned to channels within the trunk groups. Note: You must configure the IP to Tel / Inbound Routing Table to assign incoming IP calls to the appropriate trunk group, otherwise calls will not complete.
First Trunk ID	Integer 1-84	Instant	Starting physical trunk number.
Last Trunk ID	Integer 1-84	Instant	Ending physical trunk number.
Starting Channel	Integer 1-31	Instant	Starting trunk's B-channel.
Ending Channel	Integer 1-31	Instant	Ending trunk's B-channel. Note: The number of defined channels must not exceed the number of the trunk's B-channels (1-24 for T1 spans and 1-31 for E1 spans).

Parameter Name	Type	Provisioning Type	Description
Starting Phone Number	String Up to 19 chars.	Instant	The first telephone number assigned to the first channel defined in the 'Channels' fields. Subsequent channels are assigned the next consecutive phone number. If the 'Phone Number' field includes alphabetical characters and the phone number is defined for a range of channels (e.g., 1-4), then the phone number must end with a number (e.g., 'user1'). Note: This field is optional. The logical numbers defined in this field are used when an incoming PSTN / PBX call doesn't contain the calling number or called number (the latter being determined by the parameter 'Replace Empty Dst With Port Number'), these numbers are used to replace them. These logical numbers are also used for B-channel allocation for IP-to-Tel calls, if the trunk group's 'Channel Select Mode' is set to 'By Phone Number' (in Trunk Group Setting Table).

41.4 Trunk Group Settings Table

The Trunk Group Settings Table is used to determine the method in which new calls are assigned to B-channels within each Trunk Group. If such a rule does not exist (for a specific Trunk group), the global rule, defined by the **Channel Select Mode** parameter applies.

(See **SIP > GW/IP to IP > Trunk Group Settings**).

41.4.1 Configuring Trunk Group Settings Table

This section describes how to configure Trunk Groups.

➤ To configure the Trunk Group Settings table:

1. Click  to access the Media Gateway status screen.
2. Select the desired SIP board.
3. In the Navigation pane, select **SIP > GW/IP to IP > Trunk Group > Trunk Group Settings**; the SIP Trunk Group Settings list is displayed.
4. Use the  or  buttons to add or remove entries correspondingly.
5. Select a specific row and then in the configuration pane, click **SIP Trunk Groups Settings**; the 'SIP Trunk Groups Settings' screen is displayed.
6. Configure the Trunk Group Settings parameters according to the table 'SIP Trunk Group Settings' Parameters below.
7. Click the Maintenance icon  and select **Unlock** to activate the configuration.

Table 41-3: SIP Trunk Group Settings Parameters

Parameter Name	Type	Provisioning Type	Description
Name	String Up to 20 chars.	Instant	Textual, user-defined name assigned to the Trunk Group Settings, enabling users to identify it intuitively and easily.
Trunk Group ID	Integer 1-99	Instant	Trunk Group ID number.
Channel Select Mode	Enum (see description)	Instant	Defines common rule of port allocation for IP to TEL calls. ▪ By Destination Phone Number - Select the media server port according to the called number (see the note below). ▪ Cyclic Ascending – Select the next available channel in an ascending cycle order. Always select the next higher channel number in the Trunk Group. When the media server

Parameter Name	Type	Provisioning Type	Description
			reaches the highest channel number in the Trunk Group, it selects the lowest channel number in the Trunk Group and then starts ascending again. ▪ Ascending – Select the lowest available channel. Always start at the lowest channel number in the Trunk Group and if that channel is not available, select the next higher channel. ▪ Cyclic Descending – Select the next available channel in descending cycle order. Always select the next lower channel number in the Trunk Group. When the media server reaches the lowest channel number in the Trunk Group, it selects the highest channel number in the Trunk Group and then start descending again. ▪ Descending – Select the highest available channel. Always start at the highest channel number in the Trunk Group and if that channel is not available, select the next lower channel. ▪ Number + Cyclic Ascending – First select the media server port according to the called number (see the note below). If the called number isn't found, then select the next available channel in ascending cyclic order. Note that if the called number is found, but the port associated with this number is busy, the call is released. ▪ By Source Phone Number – Select the media server port according to the calling number (see the note below). ▪ Trunk Cyclic Ascending – Select the media server port from the first channel of the next trunk (next to the trunk from which the previous channel was allocated). ▪ ISDN SuppServ Table - The BRI port/module is selected according to the settings in the ISDN Supplementary Services table , allowing the routing of IP-to-Tel calls to

Parameter Name	Type	Provisioning Type	Description
			specific BRI endpoints ▪ Dest Number Ascending -The device allocates a channels to incoming IP-to-Tel calls as follows: ▪ The device attempts to route the call to the channel that is associated with the destination (called) number. If located, the call is sent to that channel. ▪ If the number is not located or the channel is unavailable (e.g., busy), the device searches in ascending order for the next available channel in the Trunk Group. If located, the call is sent to that channel. ▪ If all the channels are unavailable, the call is released. ▪ Note: If this parameter is not configured for the Trunk Group, then its channel select method is according to the global parameter, ChannelSelectMode.
Registration Mode	Enum (see description)	Instant	Registration mode per Trunk Group: ▪ Per Gateway – Single registration for the entire device (default). This mode is applicable only if a default Proxy or Registrar IP are configured, and Registration is enabled. In this mode, the URI userpart in the From, To, and Contact headers is set to the value of the global registration parameter Gateway Registration Name or username if the Gateway Registration Name is not configured. ▪ Per Endpoint – Each channel in the Trunk Group registers individually. The registrations are sent to the Serving IP Group if defined in the table, otherwise to the default Proxy, and if no default Proxy exists, then to the Registrar IP. ▪ Don't Register – No registrations are sent by endpoints pertaining to the Trunk Group. For example, if the device is configured globally to register all its endpoints (using the

Parameter Name	Type	Provisioning Type	Description
			global parameter Authentication Mode), you can exclude some endpoints from being registered by assigning them to a Trunk Group and configuring the Trunk Group registration mode to 'Don't Register'. - Per Account – Registrations are sent (or not) to an IP Group, according to the settings in the Account table Notes: - To enable Trunk Group registrations, configure the global Enable Registration parameter to Yes. This is unnecessary for 'Per Account' registration mode. - If no mode is selected, the registration is performed according to the global parameter Authentication Mode. - If the Media Gateway is configured globally (via the Authentication Mode parameter) to register Per Endpoint, and a Trunk Group comprised of four channels is configured to register Per Gateway, the media gateway registers all channels except the first four channels. The Trunk Group of these four channels sends a single registration request.
Serving IP Group	Integer -1 (Not Defined) or 1-32	Instant	The Serving IP Group ID to where INVITE messages initiated by this Trunk Group's endpoints are sent. The actual destination to where these INVITE messages are sent is to the Proxy Set ID (see 'Proxy Sets Table') associated with this Serving IP Group. The Request URI hostname in the INVITE and REGISTER messages (except for 'Per Account' registration modes) is set to the value of the field 'SIP Group Name' defined in the 'IP Group'. If no Serving IP Group ID is selected, the INVITE messages are sent to the default Proxy or according to the 'Tel to IP Routing Table' or 'Tel to IP/Outbound IP Routing Table'. Note: If the parameter PreferRouteTable

Parameter Name	Type	Provisioning Type	Description
			is Yes, the routing rules in the 'Tel to IP/ Outbound Routing Table' prevail over the selected Serving IP Group.
Gateway Name	String Up to 50 chars.	Instant	The host name used in the From header in INVITE messages, and as a host name in From/To headers in REGISTER requests. If not configured, the global parameter 'Gateway Name' is used instead.
Contact User	String Up to 50 chars.	Instant	The string used as the user part in the Contact URI in INVITE messages, and as a user part in From, To, and Contact headers in REGISTER requests. Applicable only if the field 'Registration Mode' is set to 'Per Account', and the Registration through the Account table is successful. Notes: ▪ If registration fails, then the userpart in the INVITE Contact header contains the source party number. ▪ The 'ContactUser' parameter in the 'Account Table' page overrides this parameter.
Trunk Group Name	String Up to 21 chars.	Instant	Trunk Group Name.

41.5 Manipulation Tables

The Mediant 8000 provides Manipulation tables for incoming and outgoing calls. These tables are used to modify the destination and source telephone numbers or names so that the calls can be routed correctly.

The following tables are available:

- Destination Phone Number Manipulation Table for IP to Tel calls
- Destination Phone Number Manipulation Table for Tel to IP call
- Source Phone Number Manipulation Table for IP to Tel calls
- Source Phone Number Manipulation Table for Tel to IP calls
- Calling Name Manipulation Table for IP to Tel calls
- Calling Name Manipulation Table for Tel to IP calls
- Redirect Number Manipulation Table for IP to Tel calls
- Redirect Number Manipulation Table for Tel to IP calls

41.5.1 Possible Uses for the Number Manipulation Tables

Possible uses for the Number Manipulation Tables include the following:

- Strip/add dialing plan digits from/to the number. For example, a user could dial 9 in front of each number to indicate an external line. This number (9) can be removed before (or after) the call is setup.
- Assignment of NPI/TON to IP to Tel calls. The Mediant 8000 can use a single global setting for NPI/TON classification or it can use the setting in this table on a call by call basis.
- Allow / disallow Caller ID information to be sent according to destination / source prefixes.

41.5.2 Manipulation on all Inbound/Outbound SIP INVITE

This feature provides support for SIP INVITE message manipulation for the Gateway / IP2IP application. This is similar to the SIP message manipulation capabilities supported for the SBC application (see Section 'SBC Message Manipulation' on page 761)

The message manipulation rules are configured in the **SBC Message Manipulation table** (see Section 'SBC Message Manipulation' on page 761). The logic for applying message manipulation rules (Manipulation Set ID) are as follows:

- For manipulation on all **inbound** SIP INVITE messages, the Manipulation Set ID is selected using the **GW Inbound Manipulation Set** parameter.
- For manipulation on **outbound** SIP INVITE messages, the Manipulation Set ID is selected using the following logic:
 - According to the settings of the Outbound Message Manipulation Set parameter of the destination IP Group. In other words, manipulation can be done per destination IP Group. If this parameter is not configured, see bullet below.
 - According to the settings of **GW Outbound Manipulation Set** parameter. If this parameter is also not configured, no manipulation is performed.

➤ **To configure inbound/outbound Manipulation Set:**

1. Click  to access the Media Gateway status screen.
2. Select the desired SIP board.
3. In the Navigation pane, select **SIP ► Gateway/IP to IP ► Manipulation** and in the Configuration frame, select **GW Manipulation Frame**; the GW Manipulation Settings screen is displayed.
4. Configure the GW inbound/outbound Manipulation set ID parameters according to the GW inbound/outbound Manipulation set ID Parameters' below.

Table 41-4: GW Inbound/Outbound Manipulation Set ID Parameter

Parameter Name	Type	Provisioning Type	Description
GW Inbound Manipulation Set	Integer -1 (Not Defined) to 19	Instant	Inbound manipulation set ID for GW. If configured, applies for all incoming INVITE requests.
GW Outbound Manipulation Set	Integer -1 (Not Defined) to 19	Instant	Outbound manipulation set ID for GW. If configured, applies for all incoming INVITE requests.

➤ **To configure Calling Name Manipulation Table for IP to Tel Tables:**

1. Click  to access the Media Gateway status screen.
2. Select the desired SIP board.
3. In the Navigation pane, select **SIP ► Gateway/IP to IP ► Manipulation ► Calling Name Manipulation Table for IP to Tel**; the Calling Name Manipulations IP to Tel table is displayed.
4. Use the  or  buttons to add or remove entries correspondingly.
5. Select a specific row in the Calling Name Manipulation Table for IP to Tel Table and in the Configuration pane, click the corresponding link; the corresponding Calling Name Manipulation Table for IP to Tel Settings screen is displayed.
6. Configure the Calling Name Manipulation Table for IP to Tel Table entry parameters according to the table Calling Name Manipulation Table for IP to Tel Table Parameters' below.
7. Click the Maintenance icon  and select **Unlock** to activate the configuration.

Table 41-5: Calling Name Manipulation Table for IP to Tel Table Parameter

Parameter Name	Type	Provisioning Type	Description
Destination Prefix	String Up to 101 chars.	Instant	Destination Prefix
Redirect Prefix	String Up to 101 chars.	Instant	Redirect Prefix
Calling Name Prefix	String Up to 101 chars.	Instant	Calling Name Prefix
Source Address	String Up to 101 chars.	Instant	Source Address
Remove from Left	Integer 0-211	Instant	Stripped Digits From Left
Remove from Right	Integer 0-211	Instant	Stripped Digits From Right
Leave from Right	Integer 0-255	Instant	Number of Digits to Leave
Prefix2Add	String Up to 101 chars.	Instant	Prefix to Add
Suffix2Add	String Up to 101 chars.	Instant	Suffix to Add

41.5.3 Configuring the Calling Name Manipulation Table for Tel to IP Routing

This section describes how to configure the calling name manipulation table for Tel to IP routing.

➤ **To configure Calling Name Manipulation Table for Tel to IP Tables:**

1. Click  to access the Media Gateway status screen.
2. Select the desired SIP board.
3. In the Navigation pane, select **SIP ► Gateway/IP to IP ► Manipulation ► Calling Name Manipulation Table for Tel to IP**; the Calling Name Manipulation Table for Tel to IP list screen is displayed.
4. Use the  or  buttons to add or remove entries correspondingly.
5. Select a specific row in the Calling Name Manipulation Table for Tel to IP Table and in the Configuration pane, click the corresponding link; the corresponding Calling Name Manipulation Table for Tel to IP Settings screen is displayed.
6. Configure the Calling Name Manipulation Table for Tel to IP Table entry parameters according to the table Calling Name Manipulation Table for Tel to IP Table Parameters' below.
7. Click the Maintenance icon  and select Unlock to activate the configuration.

Table 41-6: Calling Name Manipulation Table for Tel to IP Table Parameter

Parameter Name	Type	Provisioning Type	Description
Destination Prefix	String Up to 101 chars.	Instant	Destination Prefix
Source Prefix	String Up to 101 chars.	Instant	Source Prefix
Calling Name Prefix	String Up to 101 chars.	Instant	Calling Name Prefix
Source Trunk Group ID	Integer 0-101	Instant	Source Trunk Group ID
Source IP Group ID	Integer 0-32	Instant	Source IP Group ID
Remove from Left	Integer 0-211	Instant	Stripped Digits From Left
Remove from Right	Integer 0-211	Instant	Stripped Digits From Right

Parameter Name	Type	Provisioning Type	Description
Leave from Right	Integer 0-255	Instant	Number of Digits to Leave
Prefix2Add	String Up to 101 chars.	Instant	Prefix to Add
Suffix2Add	String Up to 101 chars.	Instant	Suffix to Add

41.5.4 Configuring the Redirect Number Manipulation IP to Tel Routing

This section describes how to configure the redirect number manipulation IP to Tel routing.

➤ **To configure Redirect Number Manipulation IP to Tel Tables:**

1. Click  to access the Media Gateway status screen.
2. Select the desired SIP board.
3. In the Navigation pane, select **SIP ► Gateway/IP to IP ► Manipulation Redirect Number Manipulation IP to Tel**; the Redirect Number Manipulation IP to Tel list screen is displayed.
4. Use the  or  buttons to add or remove entries correspondingly
5. Select a specific row in the Redirect Number Manipulation IP to Tel table and in the Configuration pane, click the corresponding link; the corresponding Redirect Number Manipulation IP to Tel Settings screen is displayed.
6. Configure the **Redirect Number Manipulation IP to Tel Table** entry parameters according to the table Redirect Number Manipulation IP to Tel table parameters' below.
7. Click the Maintenance icon  and select **Unlock** to activate the configuration.

Table 41-7: Redirect Number Manipulation IP to Tel Table Parameter

Parameter Name	Type	Provisioning Type	Description
Destination Prefix	String Up to 101 chars.	Instant	Destination Prefix
Redirect Prefix	String Up to 101 chars.	Instant	Redirect Prefix

Parameter Name	Type	Provisioning Type	Description
Source IP Address	String Up to 101 chars.	Instant	Source IP Address
Number Type	Enum NotIncluded, Unknown, InternationalLevel2Regional, NationalLevel1Regional, NetworkSpecificNetworkPISN, SubscriberLevel0Regional, Abbreviated, NotConfigured	Instant	TON : Select the Number Type assigned to this entry. See 'Numbering Plans and Type of Number' on page 666 for the allowed combinations of Number Plan and Number Type parameters.
Number Plan	Enum NotIncluded, Unknown, E164Public, Private, NotConfigured	Instant	NPI : Select the Number Plan assigned to this entry.
Remove from Left	Integer 0-211	Instant	Stripped Digits From Left
Remove from Right	Integer 0-211	Instant	Stripped Digits From Right
Leave from Right	Integer 0-255	Instant	Number of Digits to Leave
Prefix2Add	String Up to 101 chars.	Instant	Prefix to Add
Suffix2Add	String Up to 101 chars.	Instant	Suffix to Add

41.5.5 Configuring the Redirect Number Manipulation Tel to IP Routing

This section describes how to configure the Redirect Number Manipulation Tel to IP routing.

➤ **To configure Redirect Number Manipulation Tel to IP Tables:**

1. Click  to access the Media Gateway status screen.
2. Select the desired SIP board.
3. In the Navigation pane, select **SIP ► Gateway/IP to IP ► Manipulation ► Redirect Number Manipulation Tel to IP**; the Redirect Number Manipulation Tel to IP list screen is displayed.
4. Use the  or  buttons to add or remove entries correspondingly

5. Select a specific row in the Redirect Number Manipulation Tel to IP Table and in the Configuration pane, click the corresponding link; the corresponding Redirect Number Manipulation Tel to IP Settings screen is displayed.
6. Configure the Redirect Number Manipulation Tel to IP Table entry parameters according to the table Redirect Number Manipulation Tel to IP Table Parameters' below.
7. Click the Maintenance icon  and select **Unlock** to activate the configuration.

Table 41-8: Redirect Number Manipulation Tel to IP Table Parameter

Parameter Name	Type	Provisioning Type	Description
Destination Prefix	String Up to 101 chars.	Instant	Destination Prefix
Redirect Prefix	String Up to 101 chars.	Instant	Redirect Prefix
Source Trunk Group ID	Integer 0-101	Instant	Source Trunk Group ID
Source IP Group ID	Integer 0-32	Instant	Source IP Group ID
Number Type	Enum NotIncluded, Unknown, InternationalLevel2Regional, NationalLevel1Regional, NetworkSpecificNetworkPIS N, SubscriberLevel0Regional, Abbreviated, NotConfigured	Instant	TON : Select the Number Type assigned to this entry. See "Numbering Plans and Type of Number" on page 666 for the allowed combinations of Number Plan and Number Type parameters.
Number Plan	Enum NotIncluded, Unknown, E164Public, Private, NotConfigured	Instant	NPI : Select the Number Plan assigned to this entry.
Remove from Left	Integer 0-211	Instant	Stripped Digits From Left
Remove from Right	Integer 0-211	Instant	Stripped Digits From Right
Leave from Right	Integer 0-255	Instant	Number of Digits to Leave
Prefix2Add	String Up to 101 chars.	Instant	Prefix to Add
Suffix2Add	String Up to 101 chars.	Instant	Suffix to Add

Parameter Name	Type	Provisioning Type	Description
Is Presentation Restricted	Enum Allowed,Restricted,NotConfigured	Instant	Presentation

41.5.6 Operation Rules

The Operation rules are applied to any incoming call whose:

- Destination number prefix matches the prefix defined in the 'Destination Number' field.
- Source number prefix matches the prefix defined in the 'Source Prefix' field.
- Source IP address matches the IP address defined in the 'Source IP' field (if applicable).
- The number manipulation can be performed using a combination of each of the above criteria, or using each criterion independently.
- The Operation rules are executed in the following order:
 1. Num of stripped digits
 2. Number of digits to leave
 3. Prefix / suffix to add
- For Destination Number Manipulation, up to 50 entries can be configured.
- For Source Number Manipulation, up to 20 entries can be configured.

For available notations that represent multiple numbers, see 'Dialing Plan Notation' on page 666.



Note: A number manipulation can be performed either before or after a routing decision is made. For example, you can route a call to a specific trunk group according to its original number, and then you can remove/add a prefix to that number before it is routed.

To control when number manipulation is performed, configure **TEL to IP routing mode** and **IP to TEL routing mode** parameters in the 'SIP Routing Properties' screen.

41.5.7 Dialing Plan Notation

The dialing plan notation applies to the four Manipulation tables and to the 'Telephone to IP Routing table' on page 669 and 'IP to Telephone Routing table' on page 675.

When entering a number in the destination and source 'Prefix' columns, you can create an entry that represents multiple numbers using the following notation:

- [n-m] represents a range of numbers
- [n,m] represents multiple numbers. This notation only supports single digit numbers.
- x represents any single digit

(that terminates the number) represents the end of a number A single asterisk (*) represents any number For example:

- [5551200-5551300]# represents all numbers from 5551200 to 5551300
- [2,3,4]xxx# represents four-digit numbers that start with 2, 3 or 4
- 54324 represents any number that starts with 54324
- 54324xx# represents a 7 digit number that starts with 54324
- 123[100-200]# represents all numbers from 123100 to 123200.

The Mediant 8000 matches the rules starting at the top of the table. For this reason, enter more specific rules above more generic rules. For example, if you enter 551 in entry 1 and 55 in entry 2, the Mediant 8000 applies rule 1 to numbers that starts with 551 and applies rule 2 to numbers that start with 550, 552, 553, 554, 555, 556, 557, 558 and 559. However if you enter 55 in entry 1 and 551 in entry 2, the Mediant 8000 applies rule 1 to all numbers that start with 55 including numbers that start with 551.

41.5.8 Numbering Plans and Type of Number

Numbers are classified by their Numbering Plan Indication (NPI) and their Type of Number (TON). The Mediant 8000 supports all NPI/TON classifications used in the standard. The list of ISDN ETSI NPI/TON values is shown in the table below.

Table 41-9: NPI/TON Values for ISDN ETSI

NPI	TON	Description
Unknown [0]	Unknown [0]	A valid classification, but one that has no information about the numbering plan.
E.164 Public [1]	Unknown [0]	A public number in E.164 format, but no information on what kind of E.164 number.
	International [1]	A public number in complete international E.164 format. For example: 16135551234
	National [2]	A public number in complete national E.164 format. For example: 6135551234

NPI	TON	Description
	Subscriber [4]	A public number in complete E.164 format representing a local subscriber. For example: 5551234
Private [9]	Unknown [0]	A private number, but with no further information about the numbering plan
	Level 2 Regional [1]	
	Level 1 Regional [2]	A private number with a location. For example: 3932200
	PISN Specific [3]	
	Level 0 Regional (local) [4]	A private local extension number. For example: 2200

For NI-2 and DMS-100 ISDN variants the valid combinations of TON and NPI for calling and called numbers are (Plan/Type):

- 0/0 - Unknown/Unknown
- 1/1 - International number in ISDN/Telephony numbering plan
- 1/2 - National number in ISDN/Telephony numbering plan
- 1/4 - Subscriber (local) number in ISDN/Telephony numbering plan
- 9/4 - Subscriber (local) number in Private numbering plan

41.6 The Routing Tables

The Mediant 8000 provides the following routing tables:

Table 41-10: SIP Routing Table

SIP Routing Table	EMS Path
Routing Settings	SIP ► GW/IP to IP ► Routing
Telephone to IP / Outbound Routing Table	SIP ► GW/IP to IP ► Routing >Telephone to IP / Outbound
IP To Telephone / Inbound Routing Table	SIP ► GW/IP to IP ► Routing ► IP to Telephone / Inbound
DNS Routing Table	SIP ► SIP General ► DNS
SRV to IP Table	SIP ► SIP General ► SRV
Reasons for Alternative Telephone To IP Routing Table	SIP ► GW/IP to IP ► Routing ► Alternate Tel to IP
Reasons for Alternative IP To Telephone Routing Table	SIP ► GW/IP to IP ► Routing ► Alternate IP to Tel

41.6.1 Telephone to IP/Outbound Routing Table

The Tel to IP/OutBound Routing Table is used to route incoming Tel calls to IP addresses. This routing table associates a called / calling telephone number's prefixes with a destination IP address or with an FQDN (Fully Qualified Domain Name). When a call is routed through the Mediant 8000 (Proxy is not used), the called and calling numbers are compared to the list of prefixes on the IP Routing Table (up to 50 prefixes can be configured); Calls that match these prefixes are sent to the IP address or IP Group. If the number dialed does not match these prefixes, the call is not made.

The Tel to IP / Outbound Routing Table may also be used for IP-to-IP calls to perform "outbound routing" – i.e. to determine a destination IP address or IP Group where specific IP-to-IP calls will be sent.

When using a Proxy server, you do not need to configure the Telephone to IP Routing Table. However, if you want to use fallback routing when communication with Proxy is lost, or to use the 'Filter Calls to IP' and IP Security features, or to obtain different SIP URI host names (per called number), you need to configure the IP Routing Table.

For the Telephone to IP Routing table to take precedence over a Proxy for routing calls, In the SIP Routing Settings screen, set the **Prefer Routing Table** parameter to *Enable*. The Mediant 8000 checks the Destination IP Address field in the Telephone to IP Routing table for a match with the outgoing call. Only if a match is not found, a Proxy is used.

41.6.1.1 Telephone to IP/Outbound Routing Provisioning Rules

The Telephone to IP / Outbound Routing table consists of the following two parts:

- Matching Rules
- Destination Rules

All calls that match all or any combination of the "matching rules" are subsequently sent to the destination IP address or IP Group, defined by the "destination rules".

For alternative routing, additional entries of the same prefixes can be configured.

For available notations that represent multiple numbers, see 'Dialing Plan Notation' on page 666.

41.6.1.2 Possible Uses for Telephone to IP/Outbound Routing

Possible uses for Telephone-to-IP/Outbound routing include the following:

- **Proxy Fallback** – Fallback to internal routing table if there is no communication with the Proxy.
- **Call Restriction** – (when Proxy is not used), reject all outgoing Tel to IP calls that are associated with the destination IP address: 0.0.0.0. (See the SIP Protocol Definition screen ► Call Security tab ► Secure Calls from IP parameter.)
- **IP Security** – When the IP Security feature is enabled (Secure Calls From IP = Yes), the Mediant 8000 accepts only those IP to Tel calls with a source IP address identical to one of the IP addresses entered in the Telephone to IP Routing Table.

- **Filter Calls to IP** – When a Proxy is used, the gateway checks the Tel to IP routing table before a telephone number is routed to the Proxy. If the number is not allowed (number is not listed or a Call Restriction routing rule was applied), the call
- **Always Use Routing Table** – When this feature is enabled (Always Use Routing Table = Enable), even if a Proxy server is used, the SIP URI host name in the sent INVITE message is obtained from this table. Using this feature, users are able to assign a different SIP URI host name for different called and/or calling numbers.
- **Alternative Routing** – (When a Proxy is not used) an alternative IP destination for telephone number prefixes is available. To associate an alternative IP address to called telephone number prefix, assign it with an additional entry (with a different IP address), or use an FQDN that resolves to two IP addresses.

The call is sent to the alternative destination when one of the following occurs:

- No ping to the initial destination is available, or when poor Quality of Service (QoS) (delay or packet loss, calculated according to previous calls) is detected, or when a DNS host name is not resolved. For detailed information, see 'Alternative Routing Provisioning Rules' on page 679.
- When a release reason that is defined in the 'Reasons for Alternative Tel to IP Routing' table is received. For detailed information, see 'Reasons for Alternative Routing' on page 679.

Alternative routing (using this table) is commonly implemented when there is no response to an INVITE message (after INVITE retransmissions). The Mediant 8000 then issues an internal 408 'No Response' implicit release reason. If this reason is included in the Alternate Tel to IP table, the Mediant 8000 immediately initiates a call to the redundant destination using the next matched entry in the Tel to IP Routing table.

If a domain name in this table is resolved to two IP addresses, the timeout for INVITE retransmissions can be reduced by using the parameter, **Proxy Hot Swap Rtx** in **SIP Proxy settings**. See the table, 'SIP Proxy Settings' on page 547 for details.

If the alternative routing destination is the gateway itself, the call can be configured to be routed back to PSTN. This feature is referred to as 'PSTN Fallback', meaning that if sufficient voice quality is not available over the IP network, the call is routed through legacy telephony system (PSTN).



Note: Tel to IP routing can be performed either before or after applying the number Operation rules. Tel to IP routing can be performed either before or after applying the number Operation rules.

To control when number manipulation is carried out, set the **TEL to IP routing mode** parameter SIP Protocol Settings screen.

41.6.1.3 Configuring Telephone to IP/Outbound Routing

This section describes how to configure Telephone to IP/Outbound Routing.

➤ **To configure Telephone to IP /Outbound Routing:**

1. Click  to access the Media Gateway status screen.
2. Select the desired SIP board.
3. In the Navigation pane, select **SIP ► GW/IP to IP ► Routing ► Telephone to IP / Outbound**; the Telephone to IP/Outbound Routing list is displayed.
4. Use the  or  buttons to add or remove entries.
5. Select a specific row and then in the configuration pane, click **SIP Routing Tel to IP Settings**; the SIP Routing Tel to IP Settings screen is displayed.
6. Configure Telephone to IP / Outbound Routing entry parameters according to the tables below.
7. Click the Maintenance icon  and select **Unlock** to activate the configuration.

Table 41-11: Telephone to IP / Outbound Routing Table "Matching Rules"

Parameter Name	Type	Provisioning Type	Description
Source IP Group	Integer -1 (Not Defined) or 1-32	Instant	For Tel-to-IP calls, set this parameter to -1 (Not Defined). For IP-to-IP calls, specify the IP Group from where the call originated. Typically, the IP Group of an incoming INVITE is determined/classified using the 'IP to Tel / Inbound Routing' table. To denote any IP Group, set to -1 (Not Defined) If the Source IP Group has a Serving IP Group, then all calls originating from this Source IP Group are sent to the Serving IP Group. In this scenario, this table is used only if in the SIP Routing Settings screen, the Prefer Routing Table parameter is set to Enabled.
Source Host Prefix	String Up to 50 chars.	Instant	For Tel-to-IP calls, leave this field empty. For IP-to-IP calls, specify the prefix of the SIP URI host name in the From header of the incoming SIP INVITE message. To denote any source host leave the field empty or use asterisk (*) symbol.
Destination Host Prefix	String Up to 50 chars.	Instant	For Tel-to-IP calls, leave this field empty. For IP-to-IP calls, specify the request SIP URI host name prefix of the incoming SIP INVITE message. To denote any destination host leave the field empty or use asterisk (*) symbol.
Source Trunk Group	Integer 0 (Not Defined) or 1-100	Instant	For Tel-to-IP calls, specify the source Trunk Group. To denote any Trunk Group, set to -1 (Not Defined). For IP-to-IP calls, set to -1 (Not Defined).
Dest Phone Prefix	String Up to 19 chars.	Instant	Represents a called telephone number prefix. An asterisk (*) represents all numbers.
Source Phone Prefix	String Up to 19 chars.	Instant	Represents a calling telephone number prefix. An asterisk (*) represents all numbers.

Table 41-12: Telephone to IP / Outbound Routing Table "Destination Rules"

Parameter Name	Type	Provisioning Type	Description
Destination IP Address	String Up to 50 chars	Instant	The destination IP address (in dotted decimal notation) to where the calls will be sent. Domain names (e.g., domain.com) can be used instead of IP addresses. If the Destination IP Group is defined, leave this field empty (it will not be used anyway). To discard outgoing IP calls of a specific Tel-to-IP / Outbound routing rule, enter 0.0.0.0.
Destination Port	Integer 1-65535	Instant	The destination IP port to where the calls will be sent.
Transport Type	Enum NotConfigured, UDP, TCP, TLS	Instant	The transport type for sending the Tel-to-IP calls. When set to "Not Configured", the Transport Type defined in SIP Proxy Parameters is used.
Destination IP Group	Integer 1 (Not Defined) or 1-9	Instant	The IP Group to where you want to route the call. The SIP INVITE messages are sent to the IP address(es) of the Proxy Set that is associated with the selected IP Group. If you select an IP Group, it is unnecessary to configure a destination IP address (in the 'Dest IP Address' field). However, if both parameters are configured, the INVITE message is sent only to the IP Group. If the parameter AlwaysUseRouteTable is enabled (in the 'IP Group' table), the request URI host name in the INVITE message is set to the value of the parameter 'Dest IP Address'; otherwise, it is set to the value of the parameter 'SIP Group Name'.
Destination SRD	Integer 0 – 31	Instant	The SRD to where you wish to route the call.
IP Profile	Integer 0 (Not Defined) or 1-9	Instant	The number of the Tel profile that is assigned to the source address.

Parameter Name	Type	Provisioning Type	Description
Cost Group	String Up to 30 chars	Instant	Associates a Cost Group with the routing rule for determining the cost of the call.
Forking Group ID	Integer -1 (Not Defined) or 1-99	Instant	Defines a forking group ID for the routing rule. This enables forking of incoming Tel calls to two or more IP destinations. The device sends simultaneous INVITE messages and handles multiple SIP dialogs until one of the calls is answered. When a call is answered, the other calls are dropped. To enable Tel-to-IP call forking, you must set the 'Tel2IP Call Forking Mode' parameter to 'Enable'.

41.6.2 IP to Telephone/Inbound Routing Table

The IP to Tel / Inbound Routing Table is used to route incoming IP calls to groups of E1/T1 B channels called Trunk Groups. Calls are assigned to trunk groups according to any one of the following criteria (or a combination of thereof):

- Destination and source host prefix
- Destination and source phone prefix
- Source IP address

Once the call is routed to the specific Trunk Group, the call is sent to the Mediant 8000 channels assigned to this specific trunk group. The specific channel, within a trunk group, where the call is sent, is determined according to the trunk group's channel selection mode, which is defined in the 'Trunk Group Settings Table' on page 653, or according to the global parameter **Channel Select Mode**.

When a release reason that is defined in the 'Reasons for Alternative IP to Tel Routing' table is received for a specific IP to Tel call, an alternative trunk group for that call is available. To associate an alternative trunk group to an incoming IP call, assign it with an additional entry in the 'IP to Trunk Group Routing' table (repeat the same routing rules with a different trunk group ID). For detailed information, see 'Reasons for Alternative Routing' on page 679.

IP to Tel / Inbound Routing Table may also be used for IP-to-IP calls to perform "inbound routing" – i.e. to identify the received call as an inbound IP-to-IP call and to assign it to the specific IP Group.

41.6.2.1 IP to Telephone/Inbound Routing Provisioning Rules

IP to Telephone / Inbound Routing table consists of the following two parts:

- Matching Rules
- Destination Rules

All calls that match all or any combination of the "matching rules" are subsequently sent to the destination Trunk IP Group or assigned to a specific inbound IP Group.

The IP address can include wildcards. The 'x' wildcard is used to represent single digits, e.g., 10.8.8.xx represents all addresses between 10.8.8.10 to 10.8.8.99. The '*' wildcard represents any number between 0 and 255, e.g., 10.8.8.* represents all addresses between 10.8.8.0 and 10.8.8.255.

For available notations that represent multiple numbers, see 'Dialing Plan Notation' on page 666.

41.6.2.2 Configuring IP to Telephone/Inbound Routing

This section describes how to configure IP to Telephone/Inbound Routing.

➤ To configure IP to Telephone/Inbound Routing:

1. Click  button to access the Media Gateway status screen.
2. Select the desired SIP board.
3. In the Navigation pane, select **SIP ▶ GW/IP to IP ▶ Routing ▶ IP to Telephone / Inbound**; the IP to Telephone/Inbound Routing list screen is displayed.
4. Use the  or  buttons to add or remove entries.
5. Select a specific row and then in the configuration pane, click **SIP Routing IP to Telephone Settings**; the SIP Routing IP to Telephone Settings screen is displayed.
6. Configure IP to Telephone/Inbound Routing entry parameters according to the tables below.
7. Click the Maintenance icon  and select **Unlock** to activate the configuration.

Table 41-13: IP to Telephone / Inbound Routing Table "Matching Rules"

Parameter Name	Type	Provisioning Type	Description
TPM Association	Enum None, Master, Slave, Both	Instant	Not applicable to TP-6310 and TP-8410 boards, therefore leave it set to 'Both'.
Destination Host Prefix	String Up to 50 chars.	Instant	The Request URI host name prefix of the incoming SIP INVITE message. To denote any destination host leave the field empty. Note: the asterisk (*) wildcard cannot be used to denote any destination host prefix.
Source Host Prefix	String Up to 50 chars	Instant	The From header URI host name prefix of the incoming INVITE message. To denote any source host leave the field empty. Note: the asterisk (*) wildcard cannot be used to denote any source host prefix.
Destination Phone Prefix	String Up to 49 chars.	Instant	Represents a called telephone number prefix.
Source Phone Prefix	String Up to 49 chars.	Instant	Represents a calling telephone number prefix
Source Address	String Up to 50 chars.	Instant	The Source IP address (obtained from the Contact header in the INVITE message).

Table 41-14: IP to Telephone / Inbound Routing Table "Destination Rules"

Parameter Name	Type	Provisioning Type	Description
Trunk Group ID	Integer 0 (Not Defined) or 1-100	Instant	The Trunk Group to which calls that match a specific rule will be routed.
IP Profile	Integer 0 (Not Defined) or 1-9	Instant	The IP Profile that will be assigned to the calls that match a specific rule.

Parameter Name	Type	Provisioning Type	Description
Source IP Group	Integer 1 (Not Defined) or 1-32	Instant	The IP Group that will be assigned to the IP-to-IP calls that match a specific rule. This IP Group can later be used in the 'Tel to IP / Outbound IP Routing' table, and as the Serving IP Group in the 'Account Groups' table for obtaining the authentication user name/password for this call.
Dest Trunk ID	Integer 0 (Not Defined) or 1-84	Instant	Allow routing of incoming SIP call to specific Trunk ID using the IP2TEL routing table. This trunk can be part of a specific trunk group that is used in a different IP2TEL routing rule

41.6.3 Reasons for Alternative Routing

The Reasons for Alternative Routing are defined via the following two tables:

- Alternate Tel to IP
- Alternate IP to Tel

Each alternative routing table enables you to define up to 4 different release reasons. If a call is released as a result of one of these reasons, the Mediant 8000 tries to find an alternative route to that call. The release reason for IP to Tel calls is provided in Q.931 notation. The release reason for Tel to IP calls is provided in SIP 4xx, 5xx and 6xx response codes. For Tel to IP calls an alternative IP address, for IP to Tel calls an alternative trunk group.

See 'Telephone to IP Routing Table' on page 669 for information on defining an alternative IP address. See 'IP to Telephone Routing Table' on page 675 for information on defining an alternative trunk group.

41.6.3.1 Alternative Routing Provisioning Rules

- Each Alternative Routing table enables you to define up to 4 different release reasons.
- To enable Alternative Routing, set **Enable Alternative Routing** parameter to **Yes** in SIP Protocol Routing Settings screen.

41.6.3.2 Configuring Alternate Routing

This section describes how to configure alternative routing.

➤ To configure Alternative Routing:

1. Click  to access the Media Gateway status screen.
2. Select the desired SIP board. The Board Status screen is displayed.
3. In the Navigation pane, select **SIP ► GW/IP to IP ► Routing** and then select the alternative Routing table that you wish to configure (either **Alternate Tel to IP** or **Alternate IP to Tel**). The Alternative Routing Table list is displayed.
4. Use the  or  buttons to add or remove entries.
5. Select a specific row and then in the configuration pane, click the corresponding button; The corresponding Alternative Routing Settings screen is displayed.
6. Configure the Alternate Routing Table entry parameters according to the table 'Alternative Routing Parameters' below.
7. Click the Maintenance icon  and select **Unlock** to activate the configuration.

Table 41-15: Alternative Routing Parameters

Parameter Name	Type	Provisioning Type	Description
Name	String Up to 20 chars.	Online	Textual, user-defined name assigned to the entity (MO), enabling users to identify it intuitively and easily.
Release Cause	Integer 0-232	Read-Only	Read-only parameter indicating the release cause of the call that initiates alternative routing. ▪ For Tel to IP Alternate Routing, configure SIP response number (e.g. 408 – No Response). ▪ For IP to Tel Alternate Routing, configure Q.850 release causes (e.g. 17 – Destination Busy).

41.6.4 SIP to ISDN and ISDN to Release Cause Mapping

The SIP to ISDN and ISDN to SIP Release Cause Mapping tables enable the Mediant 8000 to map (up to 12) different SIP Responses to Q.850 Release Causes and vice versa, thereby overriding the hard-coded mapping mechanism (described in the Mediant 8000 *Programmer's User Manual - Document # LTRT-914xx*).

The following release cause mapping tables are supported:

- SIP to ISDN Cause Mapping
- ISDN to SIP Cause Mapping

41.6.4.1 Configuring SIP / ISDN Cause Mapping

This section describes how to configure SIP / ISDN Cause Mapping.

➤ To configure SIP / ISDN Cause Mapping:

1. Click  to access the Media Gateway status screen.
2. Select the desired SIP board.
3. In the Navigation pane, select **SIP ► GW/IP to IP ► Trunk Groups** and then select the SIP / ISDN Cause Mapping table that you wish to configure (either **ISDN to SIP Cause Map** or **SIP to ISDN Cause Map**); the corresponding SIP / ISDN Cause Mapping Table list is displayed.
4. Use the  or  buttons to add or remove entries.
5. Select a specific row and then in the configuration pane, click **Release Cause Settings**; the corresponding Release Cause Settings screen is displayed.
6. Configure the relevant table entry parameters according to the tables below.
7. Click the Maintenance icon  and select **Unlock** to activate the configuration.

Table 41-16: SIP to ISDN Cause Mapping Parameters

Parameter Name	Type	Provisioning Type	Description
Name	String Up to 20 chars.	Online	Define a name (string) to be assigned to the entity.
SIP Response	Integer 400-700	Instant	Defines a flexible mapping of SIP Responses and Q.850 Release Causes. When a SIP response is received (from the IP side), the gateway searches this mapping table for a match. If a match is found, corresponding Q.850 Release Cause is sent to the PSTN side. If no match is found, the default static mapping is used.
Q850 Cause	Integer 0-127	Instant	Defines a flexible mapping of SIP Responses and Q.850 Release Causes.

Table 41-17: ISDN to SIP Cause Mapping Parameters

Parameter Name	Type	Provisioning Type	Description
Name	String Up to 20 chars.	Online	Define a name (string) to be assigned to the entity.
Q850 Cause	Integer 0-127	Instant	Defines a flexible mapping of Q.850 Release Causes and SIP Responses. When a Release Cause is received (from the PSTN side), the gateway searches this mapping table for a match. If a match is found, corresponding SIP response is sent to the IP side. If no match is found, the default static mapping is used.
SIP Response	Integer 400-700	Instant	Defines a flexible mapping of Q.850 Release Causes and SIP Responses.

41.7 Profiles Tables

The Profiles tables provide the Mediant 8000 with high-level adaptation when connected to a variety of equipment (at both Tel and IP sides) and protocols, each of which requires different system behavior.

You can assign different Profiles (behavior) on a per-call basis, using the 'Tel to IP / Outbound Routing' and 'IP to Tel / Inbound Routing' tables. In addition you can associate different Profiles to the gateway's B-channels.

Each profile contains a set of parameters such as coders, T.38 Relay, Voice and DTMF Gains, Silence Suppression, Echo Canceler, RTP DiffServ, Current Disconnect and more. The Profiles feature allows you to customize these parameters or to turn them on or off, per source or destination routing and/or the specific gateway's trunks (channels). For example, a specific E1/T1 trunk can be designated to have a profile which always uses G.711 codec.

Each call can be associated with one or two Profiles: Tel Profile and/or IP Profile. If both IP and Tel profiles apply to the same call, the coders and other common parameters of the preferred Profile (determined by the Preference option) are applied to that call. If the Preference of the Tel and IP Profiles is identical, the Tel Profile parameters are applied.

The following profile tables are supported:

- Telephone Profile Table
- IP Profile Table

41.7.1 Tel Profile Table

Use the Tel Profile table to define up to nine different Tel Profiles. You can then assign these Tel Profiles to the Media Gateway channels (in the Trunk Group table), thereby applying different configurations to different channels.

➤ To configure the Tel Profile:

1. Click the  button to access the Media Gateway status screen.
2. Select the desired SIP board.
3. In the Navigation pane, select **SIP ► GW/IP to IP ► Trunk Groups ► Tel Profile**; the Tel Profile list is displayed.
4. Use the  or  buttons to add or remove entries.
5. Select a specific row and then in the configuration pane, click **Tel Profile Settings**; the Tel Profile Settings screen is displayed.
6. Configure the **Tel Profile** parameters according to the table 'Tel Profile Parameters' below.
7. Click the Maintenance icon  and select **Unlock** to activate the configuration.

Table 41-18: Tel Profile Parameters

Parameter Name	Type	Provisioning Type	Description
Name	String Up to 20 chars.	Instant	Textual, user-defined name assigned to the Tel Profile, enabling users to identify it intuitively and easily.
Preference	Integer 0-20	Instant	Used to determine the priority of the profile, where '20' is the highest preference value. If both IP and Tel profiles apply to the same call, the coders and other common parameters (noted by an asterisk) of the preferred Profile are applied to that call. If the Preference of the Tel and IP Profiles is identical, the Tel Profile parameters are applied.
Coders Group ID	Integer 1-5	Instant	Used to assign different coders to profiles. For each group, you can define the first to fifth preferred coders (and their attributes) for the gateway. The first coder is the highest priority coder and is used by the gateway whenever possible. If the far end gateway cannot use the coder assigned as the first coder, the gateway attempts to use the next coder and so forth.

Parameter Name	Type	Provisioning Type	Description
Is Fax Used	Enum NoFax, T38, G711, FallBack	Instant	Determines the SIP signaling method used to establish and convey a fax session after a fax is detected. NoFax = No fax negotiation using SIP signaling (default). T38 = Initiates T.38 fax relay. G711 = Initiates fax using the coder G.711 A-law/m-law with adaptations (see note). FallBack = Initiates T.38 fax relay. If the T.38 negotiation fails, the gateway re-initiates a fax session using the coder G.711 A-Law/m-Law with adaptations (see note). Notes ▪ Fax adaptations: ▪ -Echo Cancellor = On ▪ -Silence Compression = Off ▪ -Echo Canceler Non-Linear Processor Mode = Off ▪ -Dynamic Jitter Buffer Minimum Delay = 40 ▪ -Dynamic Jitter Buffer Optimization Factor = 13 ▪ If the gateway initiates a fax session using G.711 , a 'gpmd' attribute is added to the SDP in the following format: ▪ -For A-law: 'a=gpmd:0 vbd=yes;ecan=on'. ▪ -For m-law: 'a=gpmd:8 vbd=yes;ecan=on'. ▪ When 'IsFaxUsed' is set to any value besides NoFax the parameter 'FaxTransportMode' is ignored. ▪ When the value of IsFaxUsed is other than T38, T.38 might still be used without the control protocol's involvement. To completely disable T.38, set FaxTransportMode to a value other than 1.
DJ Buf Min Delay	Integer 0-150	Instant	Dynamic jitter buffer minimum delay in msec.
DJ Buf Opt Factor	Integer 0-13	Instant	Dynamic Jitter Buffer frame error / delay optimization factor. Note: Set to 13 for data (fax & modem) calls.

Parameter Name	Type	Provisioning Type	Description
IP Diff Serv	Integer 0-63	Instant	Sets the Diff Serv value for Premium Media service class content (only if IP Diff Serv is not set in the selected IP Profile). Note: The value for the Premium Control Diff Serv is determined by (according to priority): 1. IPDiffServ value in the selected IP Profile. 2. Premium Service Class Media Diff Serv.
Sig IP Diff Serv	Integer 0-63	Instant	Sets the Diff Serv value for Premium Control service class content (only if parameter 'Control IP Diff serv' is not set in the selected IP Profile). Note: The value for the Premium Control Diff Serv is determined by (according to priority): 1. 'Control IP Diff serv' value in the selected IP Profile. 2. Premium Service Class Control Diff Serv.
Voice Volume	Integer 0-63	Instant	Voice gain control in dB. Sets the level for the transmitted (IP to PSTN) signal.
DTMF Volume	Integer 0-31	Instant	DTMF gain control in dBm.
Input Gain	Integer 0-63	Instant	PCM input gain control in dB. Sets the level for the received (PSTN-IP) signal. Note: This parameter is intended for advanced users. Changing it affects other gateway functionalities.
Enable Digit Delivery	Enum Disable, Enable	Instant	The digit delivery feature enables sending of DTMF digits to the destination IP address after the Tel-IP call was answered. To enable this feature, modify the called number to include at least one 'p' character. The gateway uses the digits before the 'p' character in the initial INVITE message. After the call was answered the gateway waits for the required time (# of 'p' * 1.5 seconds) and then sends the rest of the DTMF digits using the method chosen (in-band, out-of-band). Note: The called number can include several 'p' characters (1.5 seconds pause). For example, the called number can be as follows: 1001pp699, 8888p9p300.

Parameter Name	Type	Provisioning Type	Description
ECE	Enum Disable, Enable	Instant	Enable/disable Echo Canceler.
Flash Hook Period	Integer 5-1500	Instant	Defines the flash-hook period (in msec)
Enable Early Media	Enum Disable, Enable	Instant	If enabled, the gateway sends 183 Session Progress response with SDP (instead of 180 Ringing), allowing the media stream to be set up prior to the answering of the call. Note: Sending 183 response depends on the Progress Indicator. It is sent only if PI=1 or PI=8 was received in Proceeding or Alert PRI messages. For CAS gateways see the ProgressIndicator2IP parameter.
Progress Indicator to IP	Enum NotConfigured, NoPI, PI=1, PI=8	Instant	Progress Indicator to IP - NotConfigured - for ISDN spans, the progress indicator (PI) that is received in ISDN Proceeding, Progress and Alert messages is used as described in the options below. - NoPI - For IP-Tel call, the gateway sends '180 Ringing' SIP response to IP after receiving ISDN Alert or (for CAS) after placing a call to PBX/PSTN. - PI=1, PI=8 - For IP-Tel call, if 'EnableEarlyMedia=1', the gateway sends '180 Ringing' with SDP in response to an ISDN alert, or it sends a '183 session in progress' message with SDP in response to only the first received ISDN Proceeding or Progress message, after a call is placed to PBX/PSTN over the trunk.
Disconnect On Busy Tone	Enum NotConfigured, No, Yes	Instant	Determines whether a call is disconnected upon detection of a busy tone.

Parameter Name	Type	Provisioning Type	Description
Dial Plan Index	Enum None, Plan1, Plan2, Plan3, Plan4, Plan5, Plan6, Plan7, Plan8	Instant	Defines which dial plan index to use in the external Dial Plan file. The Dial Plan file is loaded to the Board as a *.dat file - converted using AudioCodes DConvert utility. The dial plan index can be assigned per Tel Profile. Notes: ▪ If this parameter is used to select a dial plan index (from the Dial Plan file), the settings of the parameter Digit Mapping are ignored. ▪ This parameter is applicable to ISDN E1/T1 with overlap dialing (Receive Overlap Dialing is set to Enabled). ▪ For E1 CAS MFC-R2 variants (which don't support terminating digit for the called party number, usually I-15), this parameter and the Digit Mapping parameter are ignored. Instead, you can define a Dial Plan template per trunk in the 'Trunk Settings' page.

41.7.2 IP Profile Table

Use the Tel Profile table to define up to four different IP Profiles. These Profiles are used in the Tel to IP and IP to Tel Routing tables to associate different Profiles to routing rules. IP Profiles can also be used when working with Proxy server (set 'AlwaysUseRouteTable' to 1).

➤ **To configure IP Profile table:**

1. Click the  button to access the Media Gateway status screen.
2. Select the desired SIP board.
3. In the Navigation pane, select **SIP ► SIP General ► SIP Control Network ► IP Profile**; the IP Profiles list is displayed.

The IP Profile configuration frame is divided into the following tabs:

- General Settings – these settings are relevant for all SIP applications: Gateway, IP-to-IP, SAS, and SBC.
- Gateway Setting- The parameters in this tab can be applied only for Gateway and IP-to-IP applications.
- SBC Settings- These parameters can only be applied for the SBC application only.

4. Use the  or  buttons to add or remove entries.
5. Select a specific row, and then in the Configuration pane, click **IP Profile Settings**; the IP Profile Settings screen is displayed.
6. Configure the **IP Profile** parameters according to the table 'IP Profiles Parameters' below.
7. Click the Maintenance icon  and select **Unlock** to activate the configuration.

Table 41-19: IP Profiles Parameters

Parameter Name	Type	Provisioning Type	Description
Name	String Up to 20 chars.	Instant	Textual, user-defined name assigned to the IP Profile, enabling users to identify it intuitively and easily.
Preference	Integer -20	Instant	Used to determine the priority of the profile, where '20' is the highest preference value. If both IP and Tel profiles apply to the same call, the coders and other common parameters (noted by an asterisk) of the preferred Profile are applied to that call. If the Preference of the Tel and IP Profiles is identical, the Tel Profile parameters are applied.
Coders Group ID	Integer 1-5	Instant	Used to assign different coders to profiles. For each group, you can define the first to fifth preferred coders (and their attributes) for the gateway. The first coder is the highest priority coder and is used by the gateway whenever possible. If the far end gateway cannot use the coder assigned as the first coder, the gateway attempts to use the next coder and so forth.

Parameter Name	Type	Provisioning Type	Description
Is Fax Used.	Enum NoFax, T38, G711, FallBack	Instant	Determines the SIP signaling method used to establish and convey a fax session after a fax is detected. NoFax = No fax negotiation using SIP signaling (default). T38 = Initiates T.38 fax relay. G711 = Initiates fax using the coder G.711 A-law/m-law with adaptations (see note). FallBack = Initiates T.38 fax relay. If the T.38 negotiation fails, the gateway re-initiates a fax session using the coder G.711 A-Law/m-Law with adaptations (see note 1). Notes: ▪ Fax adaptations: ▪ -Echo Celler = On ▪ -Silence Compression = Off ▪ -Echo Celler Non-Linear Processor Mode = Off ▪ -Dynamic Jitter Buffer Minimum Delay = 40 ▪ -Dynamic Jitter Buffer Optimization Factor = 13 ▪ If the gateway initiates a fax session using G.711, a 'gpmid' attribute is added to the SDP in the following format: ▪ -For A-law: 'a=gpmid:0 vbd=yes;ecan=on'. ▪ -For m-law: 'a=gpmid:8 vbd=yes;ecan=on'. ▪ When 'IsFaxUsed' is set to any value besides NoFax the parameter 'FaxTransportMode' is ignored. ▪ When the value of IsFaxUsed is other than T38,
Version 6.6		691	T.38 might still be used without the control protocol's involvement. To completely disable T.38, set FaxTransportMode to a value other than 1. October 2014

Parameter Name	Type	Provisioning Type	Description
DJ Buf Min	Delay Integer 0-150	Instant	Dynamic jitter buffer minimum delay in msec.
DJ Buf Opt Factor	Integer 0-13	Instant	Dynamic Jitter Buffer frame error / delay optimization factor. Note: Set to 13 for data (fax & modem) calls.
IP Diff Serv	Integer 0-63	Instant	Sets the Diff Serv value for Premium Media service class content (only if IP Diff Serv is not set in the selected IP Profile). Note: The value for the Premium Control Diff Serv is determined by (according to priority): 1. IPDiffServ value in the selected IP Profile. 2. Premium Service Class Media Diff Serv.
Sig IP Diff Serv	Integer 0-63	Instant	Sets the Diff Serv value for Premium Control service class content (only if parameter 'Control IP Diff serv' is not set in the selected IP Profile). Note: The value for the Premium Control Diff Serv is determined by (according to priority): 1. 'Control IP Diff serv' value in the selected IP Profile. 2. Premium Service Class Control Diff Serv.

Parameter Name	Type	Provisioning Type	Description
Silence Suppression Mode	Integer 0-2	Instant	Silence Suppression Mode 0 - Silence Suppression disabled. 1 - Silence Suppression enabled. 2 - Enable without adaptation. A single silence packet is sent during silence period (applicable only to G.729). Note: If the selected coder is G.729, the following rules determine the value of the 'annexb' parameter of the fmtp attribute in the SDP. EnableSilenceSuppression = 0 to 'annexb=no'. EnableSilenceSuppression = 1 to 'annexb=yes'. EnableSilenceSuppression = 2 and IsCiscoSCEMode = 0 to 'annexb=yes'. EnableSilenceSuppression = 2 and IsCiscoSCEMode = 1 to 'annexb=no'.
RTP Redundancy Depth	Integer 0-1	Instant	RTP Redundancy Depth. 0 - disable generation of redundant packets 1 - enable generation of RFC 2198 redundancy packets.

Parameter Name	Type	Provisioning Type	Description
Remote Base UDP Port	Integer 0-64000	Instant	Determines the lower boundary of UDP ports used for RTP, RTCP and T.38 by a remote gateway. If this parameter is set to a non-zero value, ThroughPacket is enabled. Note that the value of RemoteBaseUDPPort on the local gateway must equal the value of BaseUDPPort of the remote gateway. The gateway uses these parameters to identify and distribute the payloads from the received multiplexed IP packet to the relevant channels.

Parameter Name	Type	Provisioning Type	Description
CNG Mode	Enum Disable, Relay, EventsOnly	Instant	Comfort Noise Generation Mode ▪ Disable - The originating gateway doesn't detect CNG, the CNG signal passes transparently to the remote side. ▪ Relay - CNG is detected on the originating side. CNG packets are sent to the remote side according to T.38 (if IsFaxUsed=1), a Re-INVITE message isn't sent and the fax session starts by the terminating gateway. This option is useful (for example) when the originating gateway is located behind a firewall that blocks incoming T.38 packets on ports that have not yet received T.38 packets from the internal network (i.e., originating gateway). ▪ Events Only - CNG is detected on the originating side. The CNG signal passes transparently to the remote side and fax session is started by the originating side using Re-INVITE message. Usually T.38 fax session starts when the 'preamble' signal is detected by the answering side. Some SIP gateways don't support the detection of this fax signal on the answering side, thus, for these cases it is possible to configure the gateways to start the T.38 fax session when the CNG tone is detected by the originating side. However, this mode is not recommended.

Parameter Name	Type	Provisioning Type	Description
Vxx Transport Type	Enum Disable, Relay, Bypass, EventsOnly	Instant	V.21/V.22/V.23/V.32/V.34 Modem Transport Type

Parameter Name	Type	Provisioning Type	Description
NSE Mode	Enum Disable, Enable	Instant	Enables/disables Cisco compatible fax and modem bypass mode. - This feature can be used only if <code>VxxModemTransportType=2</code> (Bypass) - If NSE mode is enabled the SDP contains the following line: <code>'a=rtpmap:100 X-NSE/8000'</code> To use this feature: - The Cisco gateway must include the following definition: <code>'modem passthrough nse payload-type 100 codec g711alaw'</code>. - Set the Modem transport type to Bypass mode for all modems. - Configure the gateway parameter <code>NSEPayloadType=100</code> - In NSE bypass mode the gateway starts using G.711 A-Law (default) or G.711u-Law, according to the parameter <code>FaxModemBypassCoderType</code>. The payload type used with these G.711 coders is a standard one (8 for G.711 A-Law and 0 for G.711 u-Law). The parameters defining payload type for the 'old' <code>AudioCodes Bypass mode FaxBypassPayloadType</code> and <code>ModemBypassPayloadType</code> are not used with NSE Bypass. The bypass packet interval is selected according to the parameter <code>FaxModemBypassBasicRtpPacketInterval</code>

Parameter Name	Type	Provisioning Type	Description
Play RB Tone to IP	Enum Disable, Enable	Instant	Enables/disables play ofringback tone to the IP side of the call after SIP 183 session progress response is sent. If enabled and EnableEarlyMedia=1, for IP-to-Tel calls the gateway may play a ringback tone to IP, according to the following: For CAS interfaces, the gateway opens a voice channel, sends a 183+SDP response and plays a Ringback tone to IP. For ISDN interfaces, if a Progress or an Alert message with PI (1 or 8) is received from the ISDN, the gateway opens a voice channel, sends a 183+SDP or 180+SDP response, but it doesn't play a Ringback tone to IP. If PI (1 or 8) is received from the ISDN, the gateway assumes that Ringback tone is played by the ISDN Switch. Otherwise, the fateway plays a Ringback tone to IP after receiving an Alert message from the ISDN. It sends a 180+SDP response, signaling to the originating party to open a voice channel to hear the played Ringback tone. Notes: ▪ To enable the gateway to send a 183/180+SDP responses, set EnableEarlyMedia to 1. ▪ If EnableDigitDelivery = 1, the gateway doesn't play a Ringback tone to IP and doesn't send 183 or 180+SDP responses.

Parameter Name	Type	Provisioning Type	Description
Enable Early Media	Enum Disable, Enable	Instant	If enabled, the gateway sends 183 Session Progress response with SDP (instead of 180 Ringing), allowing the media stream to be set up prior to the answering of the call. Note: Sending 183 response depends on the Progress Indicator. It is sent only if PI=1 or PI=8 was received in Proceeding or Alert PRI messages. For CAS gateways see the ProgressIndicator2IP parameter.
Progress Indicator to IP	Enum NotConfigured, NoPI, PI=1, PI=8	Instant	- NotConfigured - for ISDN spans, the progress indicator (PI) that is received in ISDN Proceeding, Progress and Alert messages is used as described in the options below. - NoPI - For IP-Tel call, the gateway sends '180 Ringing' SIP response to IP after receiving ISDN Alert or (for CAS) after placing a call to PBX/PSTN. - PI=1, PI=8 - For IP-Tel call, if 'EnableEarlyMedia=1', the gateway sends '180 Ringing' with SDP in response to an ISDN alert, or it sends a '183 session in progress' message with SDP in response to only the first received ISDN Proceeding or Progress message, after a call is placed to PBX/PSTN over the trunk.
Echo Cancellor	Enum Disable, Enable	Instant	Enables/disables echo canceller

Parameter Name	Type	Provisioning Type	Description
GW Media Security Behaviour	Enum Not Configured, Preferable, Mandatory, PreferableSingleMedia	Instant	Determines the device's mode of operation when SRTP is used (Board's "Enable Media Security" = Enable). - Not Configured – use the default settings - Preferable – The device initiates encrypted calls. If negotiation of the cipher suite fails, an unencrypted call is established. Incoming calls that don't include encryption information are accepted. - Mandatory – The device initiates encrypted calls, but if negotiation of the cipher suite fails, the call is terminated. Incoming calls that don't include encryption information are rejected.
Disconnect On Broken Connection	Enum Not Configured, Disable, Enable	Instant	Determines whether the device releases the call if RTP packets are not received within a user-defined timeout. The timeout is set by the parameter <code>BrokenConnectionEventTimeout</code>.
Copy Dest to Redirect Number	Enum NotConfigured, Disabled, AfterManipulation, BeforeManipulation	Instant	Determines whether and when the call destination is copied to the Redirect Number.

Parameter Name	Type	Provisioning Type	Description
Number of Calls Limit	Integer -1 – 2147483647	Instant	The Maximum number of concurrent calls. If the profile is set to a specific limit, the device maintains the number of concurrent calls (incoming and outgoing) pertaining to the specific profile. A limit value of '-1' indicates that there is no calls limitation for this profile (default). When the parameter value is '0', all calls are rejected. All concurrent calls which exceed the limit will be rejected.
Media IP Version Preference	Enum OnlyIPv4, OnlyIPv6, PreferIPv4, PreferIPv6	Instant	Determines the preferred RTP media IP addressing version for outgoing SIP calls. This is indicated in the "c=" field (Connection) of the SDP. - Only IPv4 = offer includes only IPv4 media IP addresses (default). - Only IPv6 = offer includes only IPv6 media IPs addresses. - Prefer IPv4 = offer includes both IPv4 and IPv6 media IP addresses; however, the first media is IPv4. - Prefer IPv6 = offer includes both IPv4 and IPv6 media IP addresses; however, the first media is IPv6. Notes: - This parameter is applicable only when the device offers an SDP. - The IP addressing version is determined according to the first SDP "m=" field. - This parameter can be configured per IP Profile ID.

Parameter Name	Type	Provisioning Type	Description
1 st DTMF 2833 Negotiation Option	Enum NotConfigured, NotSupported, InfoNortel, Notify, InfoCisco, Rfc2833, InfoKorea	Instant	Determines a single or several preferred transmit DTMF negotiation methods. - Not configured – use the global parameter; (default). - Not Supported – No negotiation - DTMF digits are sent according to the parameters DTMFTransportType and RFC2833PayloadType. - INFO (Nortel) – Sends DTMF digits according to IETF <draft-choudhuri-sip-info-digit-00>. - NOTIFY – Sends DTMF digits according to <draft-mahy-sipping-signaled-digits-01>. - INFO (Cisco) – Sends DTMF digits according to Cisco format. - RFC 2833 – Sends DTMF according to RFC 2833. - INFO (Korea) – Sends DTMF digits according to Korea Telecom format.

Parameter Name	Type	Provisioning Type	Description
2 nd DTMF 2833 Negotiation Option	Enum NotConfigured, NotSupported, InfoNortel, Notify, InfoCisco, Rfc2833, InfoKorea	Instant	Determines a single or several preferred transmit DTMF negotiation methods. - Not configured – use the global parameter; (default). - Not Supported – No negotiation - DTMF digits are sent according to the parameters DTMFTransportType and RFC2833PayloadType. - INFO (Nortel) – Sends DTMF digits according to IETF <draft-choudhuri-sip-info-digit-00>. - NOTIFY – Sends DTMF digits according to <draft-mahy-sipping-signaled-digits-01>. - INFO (Cisco) – Sends DTMF digits according to Cisco format. - RFC 2833 – Sends DTMF according to RFC 2833. - INFO (Korea) – Sends DTMF digits according to Korea Telecom format.
Declare RFC2833 in SDP	Enum NotConfigured, DontDeclare, Declare	Instant	Defines the supported Receive DTMF negotiation method. - Not Configured – use the global parameter; - Don't Declare – don't declare RFC 2833 telephony-event in SDP. - Declare – declare RFC 2833 telephony-event in SDP.

Parameter Name	Type	Provisioning Type	Description
RFC2833 Payload Type	Integer 96 – 127	Instant	Defines the RFC 2833 DTMF relay dynamic payload type. Cisco equipment uses payload type 101 for RFC 2833. The 100 and 102 to 105 range is allocated for proprietary usage. Note: When RFC 2833 payload type negotiation is used, this payload type is used for the received DTMF packets. If negotiation isn't used, this payload type is used for receive and for transmit.
Add IE in SETUP	String Up to 10 chars	Instant	Defines an optional Information Element (IE) data (in hex format) to be added to the ISDN SETUP messages. For example, to add IE '0x20,0x02,0x00,0xe1', use '200200e1' value.
Input Gain	Integer -32 – 31	Instant	Defines the input gain control (in decibels) for the received (PSTN-to-IP) signal.
Voice Volume	Integer -32 – 31	Instant	Defines the output gain control (in decibels) for the transmitted (IP-to-PSTN) signal.

Parameter Name	Type	Provisioning Type	Description
SBC Extension Coders Group	Integer 0 – 10	Instant	Defines the Coder Group ID for extended (additional) coders. This is used when transcoding is required between two user agents (i.e., the SDP answer from one user agent doesn't include any coder included in the offer previously sent by the other user agent). Therefore, to allow user agents of different IP Groups to communicate with each other (regardless of their capabilities), an extended coders table with at least one coder that is supported by each IP Groups' user agents needs to be assigned to each IP Group. Therefore, each offer destined to specific IP Groups includes this coder.
Transcoding Mode	Enum OnlyIfRequired, Force	Instant	Defines the voice transcoding mode (media negotiation) for the SBC application, between the two SBC legs. - Only if Required – Do not force. Many of the media settings (such as gain control) are not implemented on the voice stream. The SBC application passes packets RTP to RTP without any processing. - Force – Force transcoding on outgoing SBC leg. The device's SBC application interworks the media by implementing DSP transcoding.

Parameter Name	Type	Provisioning Type	Description
SBC Media Security Behavior	Enum AsIs, SRTP, RTP, Both	Instant	Defines the Board's SBC mode of operation when SRTP is used. - As Is – Incoming calls (either encrypted or not) are forwarded transparently. - SRTP – The board initiates encrypted calls only, if negotiation of the cipher suite fails, the call is terminated. - RTP – The Board initiates unencrypted calls only. - Both – The Board can initiate encrypted or unencrypted calls, if negotiation of the cipher suite fails, the call is unencrypted.
SBC RFC2833 Behavior	Enum AsIs, SRTP, RTP,Both	Instant	Determines the Board's SBC mode of operation when SRTP is used (Board's "SRTP Media Security" = Enable). [0] As Is (Default) = Incoming calls (either encrypted or not) are forwarded transparent. [1] SRTP = The Board initiates encrypted calls only; if negotiation of the cipher suite fails, the call is terminated. [2] RTP = The Board initiates unencrypted calls only. [3] Both = The Board can initiate encrypted or unencrypted calls, if negotiation of the cipher suite fails, the call is unencrypted.

Parameter Name	Type	Provisioning Type	Description
SBC Alternative DTMF Method	Enum Transparent, InBand, INFOCisco, INFONortel, INFOKorea	Instant	The devices first priority for DTMF method at each leg is RFC 2833. Therefore, if a specific leg negotiates RFC 2833 successfully, then the chosen DTMF method for this leg is RFC 2833. For legs where RFC 2833 is not negotiated successfully, the device uses this parameter to determine the DTMF method for the leg.
SBC Assert Identity	Enum NotConfigured, DontCare, AddPAssertedIdentity, RemovePAssertedIdentity	Instant	SBC Assert Identity.
SBC Allowed Coders Group ID	Integer 0 – 5	Instant	Select Allowed Coders Group table
SBC Allowed Coders Mode	Enum Restriction, Preference, RestrictionAndPreference	Instant	Determines the application behavior refer to the Allowed Coder Group. ▪ Restriction: Removes coders from the SDP that are not in the Allowed Coders Group#. ▪ Preference: Organizes the coders in the SDP according the order of coder in Allowed Coders Group#. ▪ Restriction And Preference: Restriction &Preference is performed.
SBC Diversion Mode	Enum Disable, Add, Remove	Instant	Defines the Diversion header behavior
SBC History Info Mode	Enum Disable, AddInfo, RemoveInfo	Instant	Defines the History Info header behavior.

Parameter Name	Type	Provisioning Type	Description
SBC Prack Mode	Enum Optional,Mandatory,Transparent	Instant	The SBC will be able to intervene into call establish procedure between end-users in the scope of 100Rel functionality. This intervention will be configurable per SBC LEG. - TRANSPARENT (default) – in other words "AS IS". Once the LEG configured by such an option, no intervention into either Alert responses or to the Invite request and the PRACK procedure will be necessary. - OPTIONAL – The LEG will allow the PRACK procedure and will help to complete it successfully if necessary. - MANDATORY – the LEG requires that the remote users support PRACK procedure.
SBC Fax Coders Group ID	Integer 0-5	Instant	Selects the supported fax coders (Coders Group ID) for fax negotiation. Coders Groups are configured in the Coders Group Settings table.

Parameter Name	Type	Provisioning Type	Description
SBC Fax Behavior	Enum AsIs,HandleAlways,HandleOnReINVITE	Instant	Defines the negotiation method for a fax offer: - AsIs = Pass fax transparently, without interference (default). - Handle Always = Handle fax according to fax settings in the IP Profile for all offer-answer transactions (including the initial INVITE). - Handle On ReINVITE = Handle fax according to fax settings in the IP Profile for all re-INVITE offer-answer transactions (except for initial INVITE)
SBC Fax Offer Mode	Enum AllCoders,SingleCoder	Instant	Defines the coders included in the outgoing SDP offer (sent to the called "fax"). - All = Use only (and all) the coders of the selected Coders Group ID configured using the SBCFaxCodersGroupID parameter. (Default) - Single = Use only one coder. If a coder in the incoming offer (from the calling "fax") matches a coder in the SBCFaxCodersGroupID, then the device uses this coder. If no match exists, then the device uses the first coder listed in the Coders Group ID (SBCFaxCodersGroupID).

Parameter Name	Type	Provisioning Type	Description
SBC Fax Answer Mode	Enum AllCoders,SingleCoder	Instant	Defines the coders included in the outgoing SDP answer (sent to the calling "fax"). - All = Use matched coders between the incoming offer coders (from the calling "fax") and the coders of the selected Coders Group ID (configured using the SBCFaxCodersGroupID parameter). - Single = Use only one coder. If the incoming answer (from the called "fax") includes a coder that matches a coder match between the incoming offer coders (from the calling "fax") and the coders of the selected Coders Group ID (SBCFaxCodersGroupID, then the device uses this coder. If no match exists, then the device uses the first listed coder of the matched coders between the incoming offer coders (from the calling "fax") and the coders of the selected Coders Group ID (Default).
SBC Remote Early Media Support	Enum NotSupported,Supported	Instant	This feature provides support for interworking early media between SIP UAs (IP Groups) that support and do not support receipt of early media. It determines whether a remote side can accept early media or not. [0] Not Supported = Early media is not supported. [1] Supported = (Default) Early media is supported.

Parameter Name	Type	Provisioning Type	Description
SBC Remote Early Media Response Type	Enum Transparent,Res180,Res183	Instant	This feature provides support for determining the SIP provisional response type – 180 or 183 – to forward the early media to the caller. ▪ [0] Transparent = (Default) All early media response types are supported; the E-SBC forwards all responses as is (unchanged). ▪ [1] 180 = Early media is sent as 180 response only. ▪ [2] 183 = Early media is sent as 183 response only.
SBC Remote Multiple 18x Support	Enum NotSupported,Supported	Instant	This feature provides support for determining whether multiple 18x responses (including 180 Ringing, 181 Call is Being Forwarded, 182 Call Queued, and 183 Session Progress) are forwarded to the caller. ▪ [0] Not Supported = Only the first 18x response is forwarded to the caller. ▪ [1] Supported = (Default) Multiple 18x responses are forwarded to the caller.

Parameter Name	Type	Provisioning Type	Description
SBC Remote Early Media RTP	Enum Immediate ,Delayed	Instant	This feature provides support for interworking with remote clients that send 18x responses with early media, but consequent RTP is delayed (e.g. Lync), while others do not support this and require RTP to follow the 18x response immediately. [0] Immediate = (Default) Remote client sends RTP immediately after it sends 18x response with early media. [1] Delayed = After sending 18x response, the remote client waits before sending RTP (e.g., Microsoft Lync environment).
SBC Remote Supports RFC 3960	Enum NotSupported,Supported	Instant	Remote client is capable of receiving 18x messages with delayed RTP. [0] Not Supported = (Default) Remote client does not support receipt of 18x messages with delayed RTP. [1] Supported = Remote client is capable of receiving 18x messages with delayed RTP.
SBC Remote Can Play Ringback	Enum Yes,No	Instant	Remote client can play local ringback tone. If not, we must send 18x with early media. [0] No [1] Yes (Default)

Parameter Name	Type	Provisioning Type	Description
SBC Remote Re-Invite Support	Enum NotSupported,Supported	Instant	Determines whether the destination of the re-INVITE request supports re-INVITE messages and if so, whether it supports re-INVITE with or without SDP. ▪ [0] Not Supported = re-INVITE is not supported. ▪ [1] Supported with SDP = re-INVITE is supported, but only with SDP. If the re-INVITE arrives without SDP, the E-SBC creates an SDP and adds it to the re-INVITE. ▪ [2] Supported = (Default) re-INVITE is supported with or without SDP.
SBC Remote Update Support	Enum NotSupported,AfterConnect,Supported	Instant	There are sip trunks that don't support RE-INVITE or UPDATE or both. In case the SBC receives a RE-INVITE or UPDATE requests, it will always try to forward the request to the remote side, depending on the remote side support. If it can't forward the request as is, it can convert the request or add SDP if necessary, but if the remote side doesn't support both RE-INVITE and UPDATE it handles the request locally. The converted event (request/response) will contain all the headers of the original message, except the URI and Cseq headers that have to be compatible to the method.

Parameter Name	Type	Provisioning Type	Description
SBC Remote Delayed Offer Support	Enum NotSupported,Supported	Instant	Determines whether the remote endpoint supports delayed offer (i.e., initial INVITEs without an SDP offer): [0] Not Supported = Initial INVITE requests without SDP are not supported. [1] Supported = (Default) Initial INVITE requests without SDP are supported.
SBC Remote Refer Behavior	Enum NotConfigured,Regular,DB,IPGroupName,HandleLocally	Instant	[0] Regular = (Default) Refer-To header is unchanged. [1] Reroute through SBC = SBC changes the Refer-To header so that the re-routed INVITE is sent through the SBC. [2] Group Name = Sets the host part to the name defined for the IP Group in the IP Group table. [3] Handle Locally = Device handles the REFER request itself without forwarding the REFER request.
SBC Remote 3xx Behavior	Enum NotConfigured,Transparent,DB,HandleLocally	Instant	[-1] Not Configured (default) = According to the settings of the SBC3xxBehavior parameter. [0] Transparent = Forwards the SIP Contact header as is. [1] Reroute through SBC = SBC changes the Contact header so that the re-route request is sent through the SBC. [2] Handle Locally = E-SBC handles the 3xx response and forwards the 3xx response.

42 Stand-Alone Survivability (SAS) Application

This section describes the Stand-Alone Survivability (SAS) application.

42.1 Overview

Stand-Alone Survivability (SAS) feature ensures telephony communication continuity (survivability) for enterprises using hosted IP services (such as IP Centrex) or IP-PBX; in cases of failure of these entities. In case of failure of the IP Centrex, IP-PBX servers (or even WAN connection and access Internet modem), the Enterprise internal telephony service at any branch is lost between its offices, and with the external environment. In addition, these failures prevent emergency calls from being made (e.g., 911 in North America). Despite these possible points of failures, the SAS feature ensures that the Enterprise's telephony services (e.g., SIP IP phones or soft phones) are maintained, by routing calls to the PSTN (i.e., providing PSTN fallback).

The maximum number of SAS registered users supported by the board is 2000.



Notes:

- The SAS application is available only if the board is installed with the SAS Feature Key.
- The SAS feature is not HA supported.

42.2 SAS Modes

The SAS feature operates in one of two modes:

- **Normal:** Initially, the device's SAS agent serves as a registrar (and an outbound Proxy server) to which every VoIP CPE (e.g., IP phones) within the Enterprise's LAN registers. The SAS agent at the same time sends all these registration requests to the Proxy server (e.g., IP-Centrex or IP-PBX). This ensures registration redundancy by the SAS agent for all telephony equipment. Therefore, the SAS agent functions as a stateful proxy, passing all SIP requests received from the Enterprise to the Proxy and vice versa. In parallel, the SAS agent continuously maintains a keep-alive "handshake" with the Proxy server, using SIP OPTIONS or re-INVITE messages.
- **Emergency:** The SAS agent switches to this mode if it detects (from the keep-alive responses) that the connection with the Proxy is lost. This can occur due to Proxy server failure or WAN problems. In this mode, when the connection with the Proxy server is down, the SAS agent handles all internal calls within the enterprise LAN. In the case of outgoing calls, the SAS agent forwards these to a local VoIP gateway (this can be the device itself or a separate analog or digital gateway). For PSTN fallback, the local VoIP gateway should be equipped with analog (FXO) lines or digital (E1/T1) trunk(s) for PSTN connectivity. In this way, the enterprise preserves its capability for internal and outgoing calls.

The call routing rules for SAS is configured in the 'IP2IP Routing Table' (see Section 'Configuring the SBC IP to IP Routing Table'). This table provides enhanced call routing capabilities (such as built-in ENUM queries and redundant SAS proxy server load balancing) for routing received SIP INVITE messages.

42.2.1 The SAS Configuration

This chapter describes the basic configuration of the SAS application.

➤ To configure the SAS application:

1. Click the  button to access the Media Gateway status screen.
2. Select the SIP board.
3. In the **Navigation pane**, select **SIP ► SAS**.
4. In the Toolbar, click **Configuration**; the SIP SAS Settings screen is displayed.
5. Configure the SIP SAS parameters according to the table 'SIP SAS Parameters' described below.
6. Click the Maintenance icon  and select **Unlock** to activate the configuration.

SIP SAS Parameters

Parameter Name	Type	Provisioning Type	Description
Enable SAS	Enum Enabled, Disable	Online	Enables or disables SAS functionality. Note that prior to enabling the SAS application, the SIP board must be pre-loaded with a License Key that enables this feature.

SIP SAS Parameters

Parameter Name	Type	Provisioning Type	Description
SAS Survivability Mode	Enum Standard, AlwaysEmergency, IgnoreRegister, AutoAnswerREGISTER, RoutingTableOnly	Instant	Determines the Survivability mode used by the SAS application. - Standard = Incoming INVITE and REGISTER requests are forwarded to the defined Proxy list of SASProxySet in Normal mode and handled by the SAS application in Emergency mode (default). - Always Emergency = The SAS application does not use Keep-Alive messages towards the SASProxySet, instead it always operates in Emergency mode (as if no Proxy in the SASProxySet is available). - Ignore Register = Use regular SAS Normal/Emergency logic (same as option Standard); however when in Normal mode incoming REGISTER requests are ignored. - Auto-answer REGISTER = When in Normal mode, the device responds to received REGISTER requests by sending a SIP 200 OK (instead of relaying the registration requests to a Proxy), and enters the registrations in its SAS database. - Use Routing Table only in Normal mode = The device uses the IP-to-IP Routing table to route IP-to-IP SAS calls only when in SAS Normal mode (and is unavailable when SAS is in Emergency mode). This allows routing of SAS IP-to-IP calls to different destinations (and not only to the SAS Proxy Set).
SAS Local SIP UDP Port	Integer 1 – 65,534	Instant	Defines Local UDP port for sending and receiving SIP messages for SAS. The SIP entities in the local network need to send the registration requests to this port. When forwarding the requests to the proxy ('Normal Mode'), this port serves as the source port.

SIP SAS Parameters

Parameter Name	Type	Provisioning Type	Description
SAS Default Gateway IP	IP String Up to 50 chars	Instant	Defines the default gateway used in SAS 'Emergency Mode'. When an incoming SIP INVITE is received and the destination Address-Of-Record is not included in the SAS database, the request is immediately sent to this default gateway. The address can be configured as an IP address (dotted-decimal notation) or as a domain name (up to 50 characters). The default is a null string, which is interpreted as the local IP address of the gateway.
SAS Registration Time	Integer 1- 2,000,000	Instant	Defines the value of the SIP Expires header that is sent in a 200 OK response to an incoming REGISTER message when in SAS 'Emergency Mode'.
SAS Local SIP TCP Port	Integer 1 – 65,534	Instant	Defines the local TCP port used to send/receive SIP messages for the SAS application. The SIP entities in the local network need to send the registration requests to this port. When forwarding the requests to the proxy ('Normal Mode'), this port serves as the source port.
SAS Local SIP TLS Port	Integer 1 – 65,534	Instant	Local TLS port used to send/receive SIP messages for the SAS application. The SIP entities in the local network need to send the registration requests to this port. When forwarding the requests to the proxy ('Normal Mode'), this port serves as the source port.

SIP SAS Parameters

Parameter Name	Type	Provisioning Type	Description
Enable Record-Route	Enum Enabled, Disable	Instant	Determines whether the device's SAS application adds the SIP Record-Route header to SIP requests. This ensures that SIP messages traverse the device's SAS agent by including the SAS IP address in the Record-Route header. ▪ [0] Disable (default) ▪ [1] Enable The Record-Route header is inserted in a request by a SAS proxy to force future requests in the dialog session to be routed through the SAS agent. Each traversed proxy in the path can insert this header, causing all future dialogs in the session to pass through it as well. When this feature is enabled, the SIP Record-Route header includes the URI "lr" parameter. The presence of this parameter indicates loose routing; the lack of 'lr' indicates strict routing. For example: Loose routing: Record-Route: <sip:server10.biloxi.com;lr> Strict routing: Record-Route: <sip:bigbox3.site3.atlanta.com>
SAS Proxy Set	Integer 0 - 32	Instant	Determines the Proxy Set used in SAS Normal mode to forward REGISTER and INVITE requests from users that are served by the SAS application.

SIP SAS Parameters

Parameter Name	Type	Provisioning Type	Description
Redundant SAS Proxy Set	Integer 0 - 32	Instant	Determines the Proxy Set used in SAS Emergency mode for fallback when the user is not found in the Registered Users database. Each time a new SIP request arrives, the SAS application checks whether the user is listed in the registration database. If the user is located in the database, the request is sent to the user. If the user is not found, the request is forwarded to the Redundant SAS Proxy Set. If this SAS Proxy IP appears in the Via header of the request, it is not forwarded (thereby, preventing loops in the request's course). If no such redundant SAS exists, the SAS sends the request to its default gateway.
SAS Block Unregistered Users	Enum UnBlock, Block	Instant	Determines whether the device rejects SIP INVITE requests received from unregistered SAS users. This applies to SAS Normal and Emergency modes. ▪ [0] Un-Block = Allow INVITE from unregistered SAS users (default). ▪ [1] Block = Reject dialog-establishment requests from un-registered SAS users.

SIP SAS Parameters

Parameter Name	Type	Provisioning Type	Description
SAS Contact Replace	Enum Enabled, Disable	Instant	Enables the device to change the SIP Contact header so that it points to the SAS host and therefore, the top-most SIP Via header and the Contact header point to the same host. ▪ [0] (default) = Disable - when relaying requests, the SAS agent adds a new Via header (with the SAS IP address) as the top-most Via header and retains the original Contact header. Thus, the top-most Via header and the Contact header point to different hosts. ▪ [1] Enable - the device changes the Contact header so that it points to the SAS host and therefore, the top-most Via header and the Contact header point to the same host. Note: Operating in this mode causes all incoming dialog requests to traverse the SAS, which may cause load problems.
SAS Binding Mode	Enum URI, User Part only	Instant	Determines the SAS application database binding mode. ▪ [0] URI = If the incoming AoR in the INVITE requests is using a 'tel:' URI or 'user=phone' is defined, the binding is performed according to the user part of the URI only. Otherwise, the binding is according to the entire URI, i.e., User@Host (default). ▪ [1] User Part only = The binding is always performed according to the User Part only.

SIP SAS Parameters

Parameter Name	Type	Provisioning Type	Description
SAS Emergency Prefix	String Up to 200 chars	Instant	Defines a prefix that is added to the Request-URI user part of the INVITE message that is sent by the device's SAS agent when in Emergency mode to the default gateway or to any other destination (using the 'IP2IP Routing' table, see <i>Section Configuring the SBC IP to IP Routing</i> table on page). This parameter is required to differentiate between normal SAS calls routed to the default gateway and emergency SAS calls. Therefore, this allows you to define different manipulation rules for normal and emergency calls.
SAS Emergency Numbers	String Up to 20 chars	Instant	Defines emergency numbers for the device's SAS application. When the device's SAS agent receives a SIP INVITE (from an IP phone) that includes one of the emergency numbers (in the SIP user part), it forwards the INVITE to the default gateway (configured by the parameter SASDefaultGatewayIP), i.e., the device itself, which sends the call directly to the PSTN. This is important for routing emergency numbers, such as 911 (in North America) directly to the PSTN. This is applicable to SAS operating in Normal and Emergency modes. Up to four emergency numbers can be defined, where each number can be up to four digits. Default - empty Separator – ","
SAS Connection Reuse	Enum Disable,Enable	Instant	Enables the re-use of the TCP/TLS connection in the SAS application.If SASconnectionReuse is enabled, the SAS tries to reuse the connection without regards to the "alias" parameter. If "SASconnectionReuse" is disabled, then reuse according to the "alias" parameter.

42.3 SAS Registration Manipulation

This table is used by the SAS application to manipulate the SIP Request-URI user part of incoming INVITE messages and of incoming REGISTER request AoR (To header), before saving it to the registered users database. Currently, the SAS Registration Manipulation table holds one index entry (1 row only).

➤ To configure the SAS Registration Manipulation Table:

1. Click the  button to access the Media Gateway status screen.
2. Select the SIP board.
3. In the Navigation pane, select **SIP ► SAS**.
4. In the Toolbar, click **SAS Registration Manipulation**; the SAS Registration Manipulation List screen is displayed.
5. Use the  or  buttons to add or remove entries.
6. Select a specific row and in the Configuration pane, click **SIP SAS Registration Manipulation**; the SIP SAS Registration Manipulation screen is displayed.
7. Configure the **SIP SAS Registration Manipulation** parameters according to the table ' SIP SAS Registration Manipulation below.
8. Click the Maintenance icon  and select **Unlock** to activate the configuration.

SIP SAS Registration Manipulation Table

Parameter Name	Type	Provisioning Type	Description
Remove From Right	Integer 0 - 30	Online	Number of digits removed from the right side of the user part before saving to the registered user database.
Leave From Right	Integer 0 - 30	Instant	Number of digits to keep from the right side.

This page is intentionally left blank.

43 Session Border Controller (SBC) Application

This section describes the Session Border Controller (SBC) application.

43.1 Overview

The Session Border Controller (SBC) application provides the following functionality:

- VoIP firewall and security for both signaling and media.
- Topology hiding
- Admission Control
- Routing:
 - IP-to-IP routing translations of SIP, UDP, TCP, TLS (when extensive transcoding is not required)
 - Load balancing and redundancy of SIP servers
 - Routing according to Request-URI\Specific IP address\Proxy\FQDN
 - Alternative routing
 - Routing between different Layer-3 networks (e.g., LAN and WAN)
- ITSP accounts
- SIP URI user and host name manipulations.
- Coder Transcoding.

➤ **To enable the SBC application:**

1. Pre-load the SIP boards with a License Key that enables the SBC feature. Refer to Updating License Key for details.
2. In the SBC Configuration Settings, set the **Enable SBC Application** parameter to **Enabled**. See Section "SBC Application" on page [723](#) for details.

43.2 VoIP Firewall

The SBC application implements the following firewall features:

- SIP signaling:
 - Deep and stateful inspection of all SIP signaling packets
 - SIP dialog initiations may be rejected based on values of incoming SIP INVITE message and other Layer-3 characteristics
 - Packets not belonging to an authorized SIP dialog are discarded
- RTP:
 - Opening pinholes (ports) in the device's firewall based on Offer-Answer SDP negotiations
 - Deep packet inspection of all RTP packets

- Late rouge detection - if a SIP session was gracefully terminated and someone tries to "ride on it" with rouge traffic from the already terminated RTP and SIP context, the VoIP Firewall will prevent this from occurring
- Disconnects call (after user-defined time) if the RTP connection is broken
- Black/White lists for both Layer-3 firewall and SIP classification.

43.3 Topology Hiding

The SBC application implements Topology Hiding by limiting the amount of topology information displayed to external parties. For example, IP addresses of ITSPs' equipment (e.g. proxies, gateways, and application servers) can be hidden from outside parties.

The topology hiding is provided by implementing back-to-back user agent (SBC) leg routing:

- Strips all incoming SIP Via header fields and creates a new Via value for the outgoing message.
- Each leg has its own Route/Record Route set
- Modifies SIP To, From, and Request-URI host names
- Generates a new SIP Call-ID header value (different between legs)
- Changes the SIP Contact header to the device's own address
- Layer-3 topology hiding, by modifying source IP address in the SIP IP header

43.4 SIP Normalization

The SBC application can overcome interoperability problems between SIP user agents. This is achieved by the following:

- Manipulations of SIP URI user part and host part.
- Connection to ITSP SIP trunks on behalf of an IP-PBX – the board can register and utilize a user name and password to authenticate for the IP-PBX.

43.5 The SBC Configuration

This chapter describes the basic configuration of the SBC application.

➤ **To configure the SBC application:**

1. Click the  button to access the Media Gateway status screen.
2. Select the SIP board.
3. In the **Navigation Pane**, select **SIP ► SBC**.
4. In the Toolbar, click **Configuration**; the SIP SBC Settings screen is displayed.
5. Configure the SIP SBC parameters according to the table 'SIP SBC Parameters' described below.
6. Click the Maintenance icon  and select **Unlock** to activate the configuration.

Table 43-1: SIP SBC Parameters

Parameter Name	Type	Provisioning Type	Description
Enable SBC Application	Enum Enabled, Disable	Online	Enables or disables SBC functionality. Note that prior to enabling the SBC application, the SIP board must be pre-loaded with a License Key that enables this feature.
SBC Transcoding Mode	Enum If Required, Force	Instant	Defines the voice transcoding mode (media negotiation) for the SBC application, between the two SBC legs. ▪ If Required – Do not force (default). Many of the media settings (such as gain control) are not implemented on the voice stream. The SBC application passes packets RTP to RTP without any processing. ▪ Force – Force transcoding on outgoing SBC leg. The device's SBC application interworks the media by implementing DSP transcoding. Note: This parameter can also be defined for an IP Profile (using the IP Profile parameter).

Parameter Name	Type	Provisioning Type	Description
SBC Unclassified Calls	Enum Reject, Allow	Instant	Defines treatment for calls (incoming packets) that cannot be classified into a Source IP Group (i.e. classification process fails). - Reject – the call is rejected if classification fails. - Allow – if classification fails, the incoming packet is assigned to the default IP Group of the default SRD (and the call is subsequently processed).
SBC Direct Media	Enum Disable, Enable	Instant	Defines the SBC media anchoring behavior: - Disable – all cross SRD's calls via SBC are not direct media (internal SRD calls are according to the SRD configuration). - Enable – all calls via SBC are direct media.
SBC No Answer Timeout [Sec]	Integer 0 - 3600	Instant	Defines the timeout (in seconds) for SBC outgoing (outbound IP routing) SIP INVITE messages. If the called IP party does not answer the call within this user-defined interval, the device disconnects the session. The device starts the timeout count upon receipt of a SIP 180 Ringing response from the called party. If no other SIP response (for example, 200 OK) is received thereafter within this timeout, the call is released.

Parameter Name	Type	Provisioning Type	Description
SBC P-Asserted-Identity Handle	Enum AlwaysAdd,AlwaysRemove	Instant	Determines the device's privacy handling of the PAsserted Identity header. This indicates how the outgoing SIP message asserts identity. ▪ [1] Add PAsserted Identity Header = Adds a P-Asserted-Identity header. The header's values are taken from the source URL. ▪ [2] Remove PAsserted Identity Header = Removes the PAsserted Identity header. Notes: This parameter affects only the initial INVITE request. The configuration of privacy handling in the IP Group table takes precedence over the settings of this global parameter. If in the IP Group this parameter is set to 'Don't care', then the settings of this global parameter is used. If this global parameter and the IP Group are set to 'Don't care', the device uses the same P-Asserted-Identity header (if present) in the incoming message for the outgoing message.

Parameter Name	Type	Provisioning Type	Description
SBC Refer Behavior	Enum Regular,UseDB	Instant	Defines how the device handles REFER requests. [0] = Refer To header is unchanged (default). [1] = Uses the database for Refer To as described below. When enabled, the device handles REFERs as follows: Before passing on the REFER request, the device changes the host part to the device's IP address and adds a special prefix ("T-&R_") to the Contact user part. The incoming INVITE is identified as a REFER-resultant INVITE according to the special prefix. The device replaces the host part (in the Request-URI) with the host from the REFER contact. The prefix ("T-&R_") remains in the user part for regular classification, manipulation, and routing. The special prefix can be used for specific routing rules for REFER-resultant INVITES. The prefix is removed before the resultant INVITE is sent to the destination.
SBC Xfer Prefix	String Up to 255 chars	Instant	When the SBCReferBehavior is set to 1, the device, while interworking the SIP REFER message, adds the prefix "T-&R-" to the user part of the URI in the Refer-To header. After this, the device can receive an INVITE with such a prefix (the INVITE is sent by the UA that receives the REFER message or 302 response). If the device receives an INVITE with such a prefix, it replaces the prefix with the value defined for the SBCXferPrefix parameter.

Parameter Name	Type	Provisioning Type	Description
SBC 3xx Behavior	Enum Transparent,UseDB	Instant	Determines the device's handling of SIP 3xx responses. When enabled, the device handles SIP redirections between different subnets (e.g., between LAN and WAN sides). This is required where the new address provided by the redirector (Redirect sever) may not be reachable by the far-end user (FEU) that is located in another subnet. For example, a far-end user (FEU) in the WAN sends a SIP request via the device to a Redirect server in the LAN, and the Redirect server replies with a SIP 3xx response to a PBX in the LAN in the Contact header. If the device sends this response as is (i.e., with the original Contact header), the FEU is unable to reach the new destination. ▪ [0] (default) = The device sends the received SIP 3xx response without changing the Contact header (transparent handling). ▪ [1] = The device changes the URI in the Contact header of the received SIP 3xx response to its own URI and adds a special user prefix ("T~&R_"), which is then sent to the FEU. The FEU then sends a new INVITE to the device, which the device then sends to the correct destination. Notes: When this parameter is changed from 1 to 0, new 3xx Contact headers remain unchanged. However, requests with the special prefix continue using the device's database to locate the new destination. Only one database entry is supported for the same host, port, and transport combination. For example, the following URIs cannot be distinguished by the device: sip:10.10.10.10:5060;transport=tc p;param=a sip:10.10.10.10:5060;transport=tc
Version 6.6	731		Copyright 2014

Parameter Name	Type	Provisioning Type	Description
SBC GRUU Mode	Enum NoGRUU,AsProxy,TemporaryOnly,PublicOnly,Both	Instant	Determines the Globally Routable User Agent (UA) URI (GRUU) support (according to RFC 5627). ▪ [0] None = No GRUU is supplied to users. ▪ [1] As Proxy = The device provides the same GRUU types as the proxy provided the device's GRUU clients. (default) ▪ [2] Temporary only = Supply only temporary GRUU to users. (Currently not supported.) ▪ [3] Public only = The device provides only public GRUU to users. ▪ [4] Both = The device provides temporary and public GRUU to users.
SBC Max Forwards Limit	Integer 1 - 70	Instant	Defines the value of the Max-Forwards SIP header. The valid value range is 1-70. The default is 10. This parameter affects the Max-Forwards header in the received message, as follows: If the received header's original value is 0, the message is not passed on and is rejected. If the received header's original value is less than the user-defined parameter, the header's value is decremented before being sent on. If the received header's original value is greater than the user-defined parameter, the header's value is replaced by the user-defined parameter's value

Parameter Name	Type	Provisioning Type	Description
SBC Minimum Session-Expires [Sec]	Integer 0 - 1,000,000	Instant	Defines the minimum amount of time (in seconds) between session refresh requests in a dialog before the session is considered timed out. This value is conveyed in the SIP Min-SE header. The valid range is 0 (default) to 1,000,000 (where 0 means that the device does not limit Session-Expires).
SBC User Registration Time [Sec]	Integer 0 - 2,000,000	Instant	Defines the duration of the periodic registrations between the user and the SBC (SBC responds with this value to user). When set to 0, the SBC does not change the Expires value received in the user's REGISTER request. If no Expires header is received in the REGISTER and SBCUserRegistrationTime = 0, the Expires value is set to 180 seconds (by default). The valid range is 0 to 2,000,000 seconds.
SBC Proxy Registration Time [Sec]	Integer 0 - 2,000,000	Instant	Defines the duration for which the user is registered in the proxy database (after the device forwarded the REGISTER). When set to 0, the SBC sends the Expires value as received from the user to the proxy. The valid range is 0 to 2,000,000 seconds.

Parameter Name	Type	Provisioning Type	Description
SBC Survivability Registration Time [Sec]	Integer 0 - 2,000,000	Instant	Defines the duration of the periodic registrations between the user and SBC, when the SBC is in survivability state (i.e., when REGISTER requests cannot be forwarded to the proxy, and is terminated by the SBC). When set to 0, the SBC uses the value of the parameter <i>SBCUserRegistrationTime</i> for the SBC response. The valid range is 0 to 2,000,000 seconds.
Keep original user in Register	Enum Disable, EnableDisable, Enable	Instant	Determines whether the device replaces the Contact user with a unique Contact user in the outgoing message in response to a REGISTER request. [0] Disable = (default) The device replaces the original Contact user with a unique Contact user, for example: Received Contact: <sip:123@domain.com> Outgoing (unique) Contact: <sip:FEU1_7_1@SBC> [1] Enable = The original Contact user is retained and used in the outgoing REGISTER request.

Parameter Name	Type	Provisioning Type	Description
SBC Coders Preferences Mode	Enum NoExtentions,IncludeExtentions	Instant	Determines the order of the Extension coders (coders added if there are no common coders between SDP offered coders and Allowed coders) and Allowed coders (defined in the Allowed Coders Group table) in the outgoing SIP message (in the SDP). ▪ [NoExtentions] Doesn't Include Extensions = (Default) Extension coders are added at the end of the coder list. ▪ [IncludeExtentions] Include Extensions = Extension coders and Allowed coders are arranged according to their order of appearance in the Allowed Coders Group table. Note: If the 'SBC Extension Coders Group' parameter of the IP Profile table is set to 'None' (the coder group isn't selected), this parameter is not applicable.
SBC Bye Authentication	Enum Disable,Enable	Instant	Enables the authentication of a SIP BYE request before the call is disconnected. . This feature prevents, for example, a scenario in which the SBC SIP client receives a BYE request from a third-party imposer assuming the identity of a participant in the call and as a consequence, the call between the first and second parties is inappropriately disconnected.

Parameter Name	Type	Provisioning Type	Description
SBC Forking Handling Mode	Enum LatchOnFirst, Sequential	Instant	Defines the handling of 18x responses received due to call forking of an INVITE. • [0] Latch On First = (Default) Only the first 18x is forwarded to the INVITE-initiating UA. If SIP 18x with SDP is received, the device opens a voice stream according to the received SDP and disregards any subsequent 18x forking responses (with or without SDP). If the first response is 180 without SDP, the device responds according to the PlayRBTone2TEL parameter and disregards the subsequent forking 18x responses. • [1] Sequential = All 18x responses are forwarded, one at a time (sequentially) to the INVITE-initiating UA. If 18x arrives with an offer only, then only the first offer is forwarded to the INVITE-initiating UA (and subsequent 18x responses are discarded).

43.6 SIP Network Definitions

The following SIP network definitions are used for configuring the SBC application:

- Signaling Routing Domain (SRD) (see Section 43.6.1 on page 737)
- SIP Interfaces (see Section 43.6.2 on page 738)
- Media Realms (see Section 43.6.3 on page 738)

43.6.1 Signaling Routing Domain (SRD)

Signaling Routing Domain (SRD) is a set of definitions of IP interfaces, resources, SIP behaviors and other definitions that partition a single SIP board into multiple virtual multi service gateways.

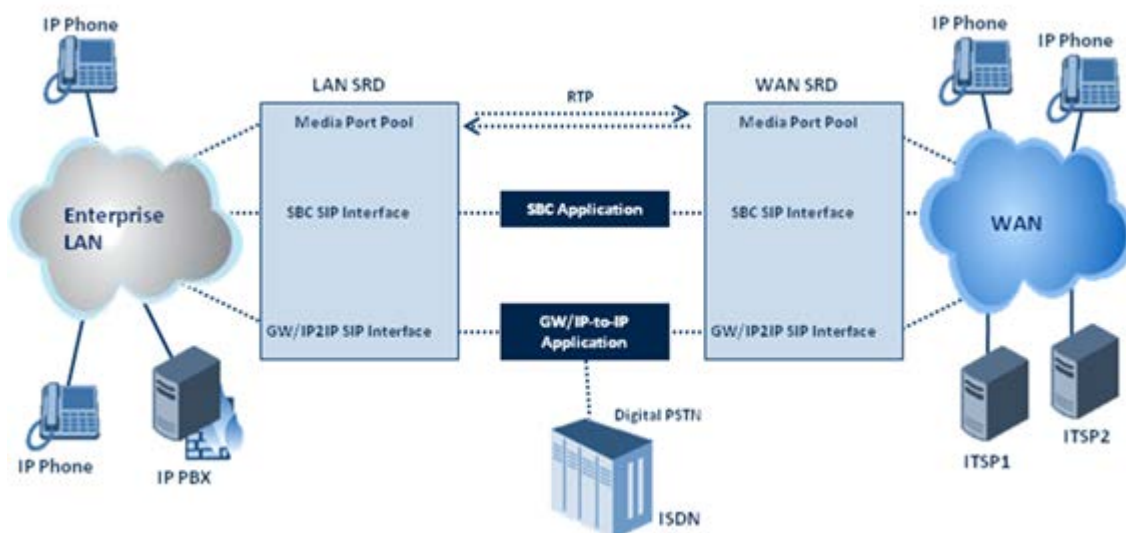
Refer to 'SRD Table' on page 628 for a detailed description of SRD table and its configuration.

For a typical SBC application, the following SRDs are configured:

- One WAN SRD
- One or more LAN SRD (for each group of SIP User Agents – e.g. proxies, IP phones, application servers etc.)

Routing from one SRD to another is possible, whereby each routing destination (IP Group or destination address) indicates the SRD to which it belongs.

Figure 43-1: Example of SRD and SIP Interfaces Configuration for SBC Application



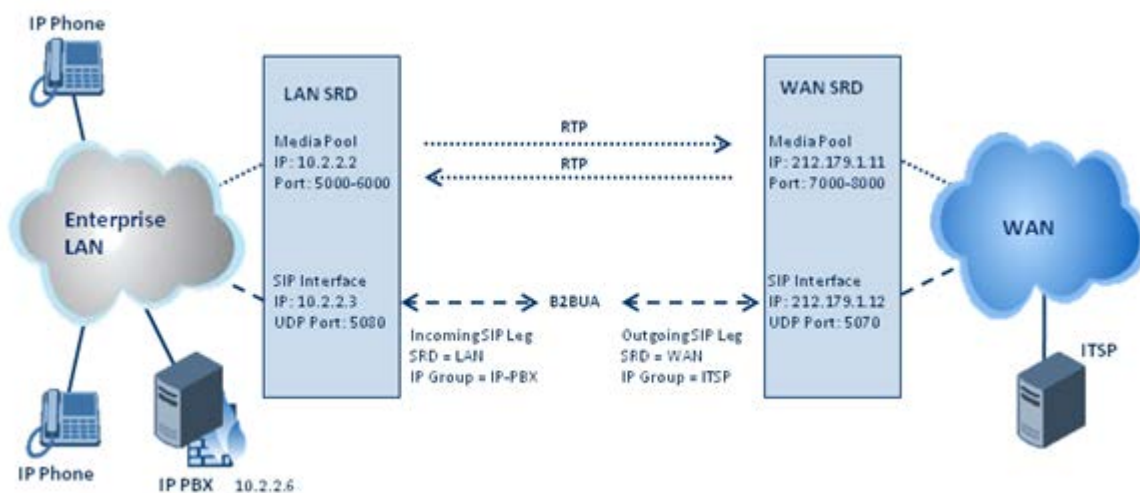
43.6.2 SIP Interfaces

A SIP Interface represents a single SIP signaling entity, which is a combination of UDP, TCP, and TLS ports relating to a single specific IP address (in the control subnet). The SIP Interface is configured with a SRD. This allows User Agents on the network to communicate with a specific SRD, using the SIP Interface associated with it.

Refer to the 'SIP Interfaces Table' on page 630 for a detailed description of the SIP Interfaces table and its configuration.

The figure below illustrates the SBC application call flow between an enterprise LAN (IP PBX) and an ITSP (WAN), implementing different interfaces (IP addresses and ports) for RTP packets and SIP signaling.

Figure 43-2: Example of an SBC application Call Flow



43.6.3 Media Realms

Media Realms enable definition of pools of media interfaces, where each realm is associated with a Media Subnet and is specified by an UDP port range.

Refer to 'Configuring Media Realms' on page 210 for a detailed description.

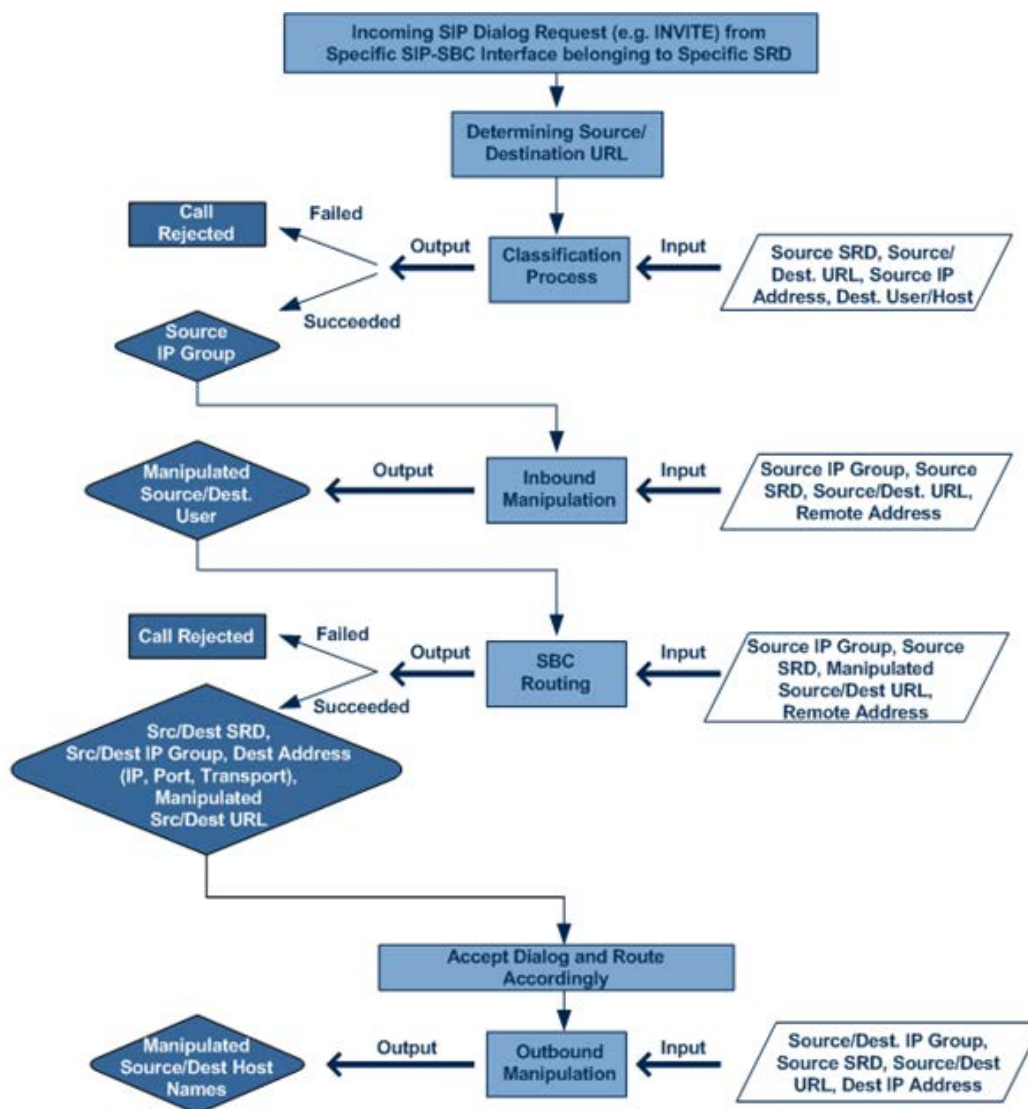
43.7 SIP Dialog Initiation Process

The SBC application performs a SIP dialog initiation process for all incoming SIP dialog initiation requests. This includes the SIP methods such as INVITE, SUBSCRIBE, OPTIONS, REFER, INFO, UNSOLICITED NOTIFY, MESSAGE, and REGISTER.

The SIP dialog initiation process consists of the following stages:

- Determining Source and Destination URL
- Source IP Group Classification
- SBC Routing
- SBC Inbound and Outbound Manipulation

Figure 43-3: SBC Application SIP Dialog Initiation Process



43.8 Determining Source and Destination URL

The SIP protocol has more than one URL in a dialog establishing request that might represent the source and destination URL. When handling an incoming request, the device determines which SIP headers are used for source and destination URL's. Once these URL's are determined, the input user and host are taken from these URLs.

- INVITE dialogs:
 - Source URL: if exists, obtained from the P-Asserted\Preferred-Identity header; otherwise, from the From header
 - Destination URL: obtained from the Request URI
- REGISTER dialogs:
 - Source URL: obtained from the To header
 - Destination URL: obtained from the Request URI

43.9 Source IP Group Classification

The SBC application performs a classification process to associate the incoming SIP request with a specific IP Group. Once determined, this IP Group is used for the following purposes:

- Input for the SBC manipulation and routing processes
- Definition of SIP behavior via the IP Profile, Media Realm and Account

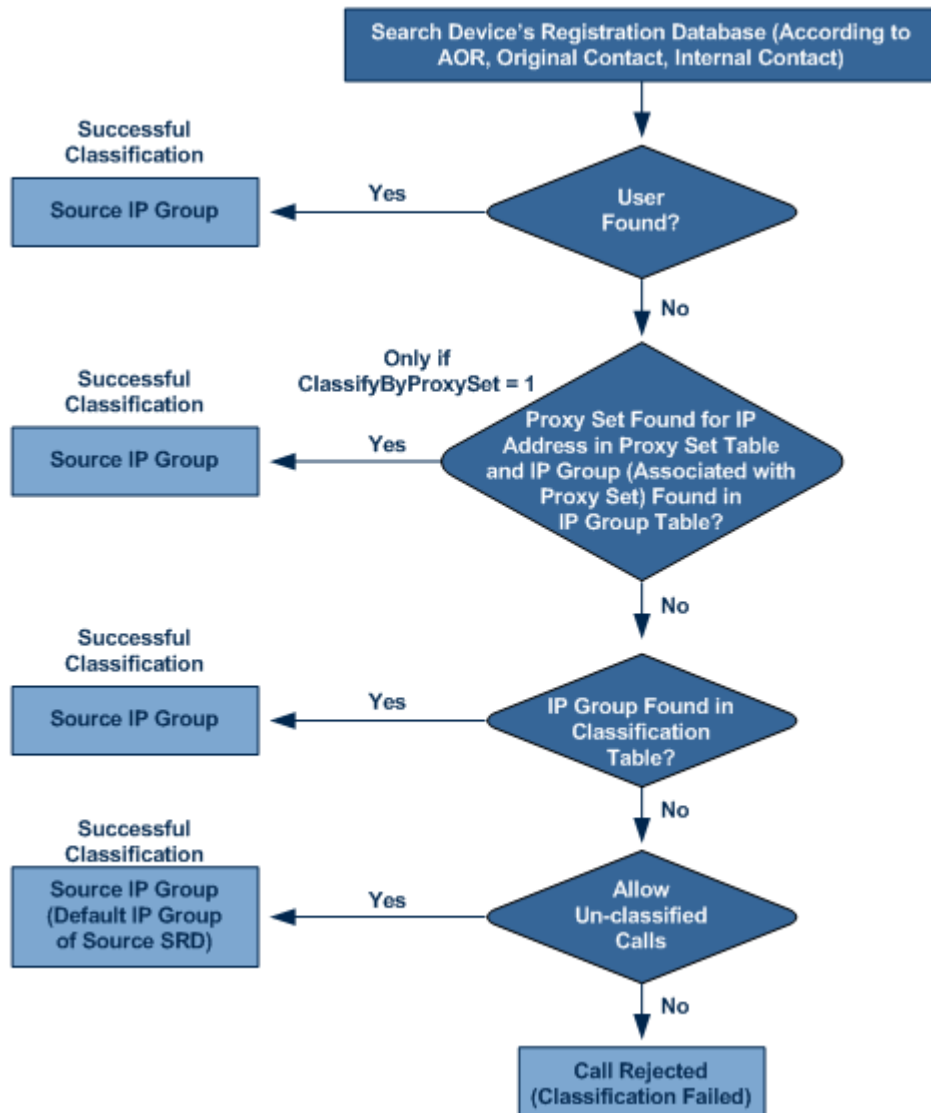
The classification begins by matching the incoming SIP request with the Registrations Database.

If the registration database search is unsuccessful, the classification proceeds with locating a Proxy Set (associated with the SIP dialog request's IP address) and then searches for a match with a IP Group in the IP Groups table. Each IP Group can be classified according to its Proxy Set (if the parameter **Classify By Proxy Set** in IP Group is set to *enabled*). Note that this classification is not relevant in cases where multiple IP Groups use the same Proxy Set.

If the classification based on the Proxy Set is unsuccessful, the device proceeds to the SBC Classification table, where it searches for a source IP Group based on the following matching rules: Source IP Address, Source Username Prefix, Source Host Prefix, Destination Username Prefix, Destination Host and Source SRD.

If all attempts to classify the incoming SIP request fail, the call can either be rejected, or allowed and processed (by assigning it to the default IP Group of the default SRD). This behavior is determined by the **SBC Unclassified Calls** parameter in the SBC configuration screen.

Figure 43-4: SBC Application Classification Process



The SBC Classification table is used as part of the generic classification process, described above to associate the incoming SIP request with a specific IP Group.

➤ **To configure the SBC Classification:**

1. Click the  button to access the Media Gateway status screen.
2. Select the SIP board.
3. In the **Navigation Pane**, select **SIP ► SBC ► SBC Classification**; the SBC Classifications list is displayed.
4. Use the  or  buttons to add or remove entries.
5. Select a specific row and in the Configuration pane, click **SBC Classification Settings**; the SBC Classification Settings screen is displayed.
6. Configure SBC Classification parameters according to the table 'SBC Classification Parameters' below.
7. Click the Maintenance icon  and select **Unlock** to activate the configuration.

Table 43-2: SBC Classification Parameters “Matching Rules”

Parameter Name	Type	Provisioning Type	Description
Source SRD	Integer -1 – 4	Instant	Defines the index of the source SRD. The source SRD is defined according to the UDP/TCP/TLS port at which the incoming INVITE is received. The SIP Interface table defines the UDP/TCP/TLS ports per SRD.
Source Username Prefix	String Up to 20 chars	Instant	Defines the prefix of the user part of the incoming INVITE's source URI (usually the From URI).
Source Host	String Up to 50 chars	Instant	Defines the From header URI host name prefix of the incoming INVITE message. If this routing rule is not required, leave the field empty. The asterisk (*) symbol can be used to depict any source host prefix.
Destination Username Prefix	String Up to 50 chars	Instant	Defines the prefix of the incoming SIP INVITE's destination URI (usually the Request URI) user part.
Destination Host	String Up to 50 chars	Instant	Defines the Request URI host name prefix of the incoming SIP INVITE message. If this routing rule is not required, leave the field empty. The asterisk (*) symbol can be used to depict any destination host prefix.

Parameter Name	Type	Provisioning Type	Description
Message Condition	Integer 0-20	Instant	Defines the index of the condition to which to associate. The classification is used only if the classification rule and its associated condition rule are matched.
Source Port	Integer 0-65534	Instant	Defines the Source Port of the incoming SIP message.
Source Transport Type	Enum Udp, Tcp, Tls	Instant	Defines the Source Transport Type of the incoming SIP message.
Action Type	Enum Deny, Allow	Instant	Defines SIP application-layer access lists. It offers greater flexibility in the security mechanism of the SBC by allowing the user to configure whitelists (allowed messages) and blacklists (deny messages) based on classification rules. If the incoming SIP dialog cannot be classified according to the classification table, the call is accepted or rejected based on the settings of the existing parameter "SBC Unclassified Calls".

Table 43-3: SBC Classification Parameters “Operation Rules”

Parameter Name	Type	Provisioning Type	Description
Source IP Group	Integer 0-32	Instant	Defines the index of the IP Group to be associated with the call as a result of classification process and is used for SBC routing and manipulations. The IP Group must be associated with the Source SRD.

43.10 SBC Condition Table

The SBC Condition table is used as part of the generic classification process.

This classification is used only if the classification rule and its associated condition rule are matched.

➤ To configure the SBC Condition:

1. Click the  button to access the Media Gateway status screen.
2. Select the SIP board.
3. In the **Navigation Pane**, select **SIP ▶ SBC ▶ SBC Condition**; the SBC Condition s list is displayed.
4. Use the  or  buttons to add or remove entries.
5. Select a specific row and in the Condition pane, click **SBC Condition Settings**; the SBC Condition Settings screen is displayed.
6. Configure SBC Condition parameters according to the table 'SBC Condition Parameters' below.
7. Click the Maintenance icon  and select **Unlock** to activate the configuration.

Table 43-4: SBC Condition Parameter

Parameter Name	Type	Provisioning Type	Description
Condition	String Up to 299 chars	Instant	The defined condition. For example : "header.from.url.user == '1000' AND header.from.url.user == '8000'".
Description	String Up to 60 chars	Instant	Description of the condition

43.11 SBC Routing

The SBC application employs a comprehensive and flexible routing scheme:

- Routing rules according to Layer 3 and SIP characteristics
- Routing to multiple destination types:
 - Request-URI (of incoming SIP dialog initiating requests)
 - Specific destination IP address
 - Specific FQDN (NAPTR/SRV/A-Record Resolutions)
 - Registered Contact in device's database (User-type IP Groups)
 - IP Group (address defined for Proxy Set associated with the IP Group), with the ability of load balancing and redundancy
- Alternative Routing
- Routing between two different Layer-3 networks (LAN-WAN etc.)
- Transport protocol translator (UDP to TCP to TLS)
- Source and destination user name manipulation (pre/post routing)

43.11.1 SBC IP to IP Routing Table

The SBC IP to IP Routing table provides enhanced IP-to-IP call routing capabilities for routing received SIP messages (such as INVITE or REGISTER) to a destination IP address. The routing rule must match one of the following input characteristics: Source IP Group, Source Phone Prefix, and/or Source Host Prefix.



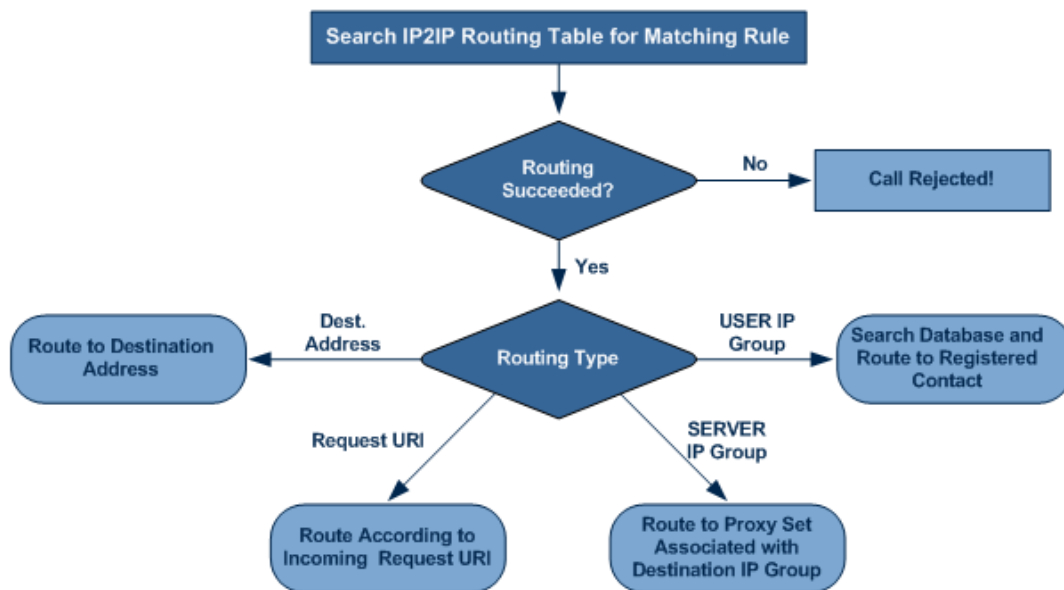
Note: SIP REGISTER messages are routed only by using Destination IP Groups defined in the SBC IP-to-IP routing rules.

The IP2IP Routing table determines the destination route according to any one of the following:

- Registered User Contact listed in the device's database (only for USER IP Groups)
- Destination IP Group's associated Proxy Set (allows redundancy/load balancing)
- Specific destination address (can be based on IP address, Host name, port, transport type, and/or SRD). Routing to a host name can be resolved using NAPTR/SRV/A-Record.
- Incoming Request URI

For all destination types listed above, except destination IP Group, the IP Group can optionally be configured to provide the destination SRD and/or IP Profile. If neither the destination SRD nor destination IP Group are defined, the destination SRD is the source SRD and the destination IP Group is its default IP Group.

Figure 43-5: SBC Application IP to IP Routing Types



In addition to the alternative routing/load balancing provided by the Destination's IP Group's associated Proxy Set, the SIP IP to IP Routing table also allows the configuration of alternative routes, whereby if a route fails, the next adjacent rule in the table that is configured as 'Alt Route Ignore/Consider Inputs' are used. The alternative routes rules can be set to enforce the input matching criteria or to ignore any matching criteria. For alternative routing, alternative SBC routing reasons (i.e., 4xx, 5xx, and 6xx SIP responses) must be configured in the 'SBC Alternative Routing Reasons' table.

If no matching rule is located in the table, the call is rejected.

43.11.2 Configuring the SBC IP to IP Routing Table

The SBC IP to IP Routing table consists of the following two parts:

- Matching Rules
- Destination Rules

All calls that match all or any combination of the "matching rules" are subsequently sent to the destination IP address or IP Group defined by the "destination rules".

For alternative routing, additional entries of the same prefixes can be configured.

➤ **To configure SBC IP to IP Routing:**

1. Click the  button to access the Media Gateway status screen.
2. Select the SIP board.
3. In the Navigation pane, select **SIP ► SBC ► SBC Routing ► IP to IP Routing**; the SIP IP to IP Routing list is displayed.
4. Use the  or  buttons to add or remove entries.
5. Select a specific row and in the Configuration pane, click **SIP IP to IP Routing Settings**; the SIP IP to IP Routing Settings screen is displayed.
6. Configure SBC IP to IP Routing parameters according to the table 'SBC IP to IP Routing Table Matching Rules' below.
7. Click the Maintenance icon  and select **Unlock** to activate the configuration.

Table 43-5: SBC IP to IP Routing Table "Matching Rules"

Parameter Name	Type	Provisioning Type	Description
Source IP Group	Integer 0-9	Instant	Defines the IP Group from where the call originated. Typically, this IP Group is determined by the Classification process. If this feature is not used (i.e., any IP Group), set to 0 (Any).
Source Username Prefix	String Up to 20 chars	Instant	Defines the prefix of the user part of the incoming INVITE's source URI (usually the From header). To denote any source username prefix leave the field empty or use asterisk (*) symbol.

Parameter Name	Type	Provisioning Type	Description
Source Host	String Up to 50 chars	Instant	Defines the hostname of the incoming INVITE's source URI (usually the From header). To denote any source host leave the field empty or use asterisk (*) symbol.
Destination Username Prefix	String Up to 50 chars	Instant	Defines the prefix of the user part of the incoming SIP INVITE's destination URI (usually the Request URI). To denote any destination username prefix leave the field empty or use asterisk (*) symbol.
Destination Host	String Up to 50 chars	Instant	Defines the hostname of the incoming SIP INVITE's destination URI (usually the Request URI) user part. To denote any destination host leave the field empty or use asterisk (*) symbol.
Message Condition	Integer 0-20	Instant	Defines the index of the condition to which to associate. The classification is used only if the classification rule and its associated condition rule are matched.

Table 43-6: SBC IP to IP Routing Table "Destination Rules"

Parameter Name	Type	Provisioning Type	Description
Destination Type	Enum IPGroup, DestAddress, RequestURI, Enum, HuntGroup, DialPlan,LDAP	Instant	Defines the destination type to which the outgoing INVITE is sent. IP Group – The INVITE is sent to the IP Group's Proxy Set (if the IP Group is of SERVER type) or registered contact from the database (if SERVER type). Dest Address – The INVITE is sent to the address configured in the following fields: 'Destination SRD', 'Destination Address', 'Destination Port', and 'Destination Transport Type'. Request URI – The INVITE is sent to the address indicated in the incoming Request URI. If the fields 'Destination Port' and 'Destination Transport Type' are configured, the incoming Request URI parameters are overridden and these fields take precedence. ENUM – An ENUM query is sent to conclude the destination address. If the fields 'Destination Port' and 'Destination Transport Type' are configured, the incoming Request URI parameters are overridden and these fields take precedence. (This option is currently not supported.)

Parameter Name	Type	Provisioning Type	Description
Destination IP Group	Integer 0-32	Instant	Defines the index of the IP Group to where the outbound IP-to-IP call will be routed. The INVITE messages are sent to the IP address(es) defined for the Proxy Set associated with this IP Group. If you select an IP Group, it is unnecessary to configure a destination IP address (in the 'Destination Address' field). However, if both parameters are configured, the INVITE message is sent only to the IP Group. If the destination IP Group is of USER type, the device searches for a match between the requested URI (of the received INVITE) to an AOR registration record in the device's internal database. The INVITE is then sent to the IP address of the registered contact. Note: This is only relevant if parameter 'Destination Type' is set to IP Group. However, regardless of the settings of the parameter 'Destination Type', the IP Group is still used - only for determining the IP Profile or outgoing SRD. If neither IP Group nor SRD are defined in this table, the destination SRD is determined according to the source SRD associated with the Source IP Group (configured in the 'IP Group' table). If this table does not define an IP Group; however only an SRD, then the first IP Group associated with this SRD (in the 'IP Group' table) is used.
Destination SRD	Integer -1 – 32	Instant	Determines the SRD. Note: The destination IP Group must belong to the destination SRD if both are configured.

Parameter Name	Type	Provisioning Type	Description
Destination Address	String Up to 20 chars	Instant	The destination IP address (or domain name, e.g., domain.com) to where the outbound call is sent. This parameter is applicable only if the parameter 'Destination Type' is set to 'Dest Address'. When using domain names, enter a DNS server IP address or alternatively, define these names in the 'Internal DNS Table'.
Destination Port	Integer 1 – 65534	Instant	Defines the destination port to where the outbound call is sent.
Destination Transport Type	Enum Not Configured, UDP, TCP, TLS	Instant	Defines the transport layer type for sending the outbound SIP IP calls. When this parameter is set to Not Configured, the transport type is determined by the global SIP Transport Type parameter.

Parameter Name	Type	Provisioning Type	Description
Alternate Route Options	Enum Route Row, Alt Route Ignore Inputs, Alt Route Consider Inputs	Instant	Determines whether this routing rule is the main routing rule or an alternative routing rule. Route Row – main routing rule – the device first attempts to route the call to this route if the incoming INVITE's input characteristics matches this rule. Alt Route Ignore Inputs – if the call cannot be routed to the main route (Route Row), the call is routed to this alternative route regardless of the incoming INVITE's input characteristics. Alt Route Consider Inputs – if the call cannot be routed to the main route (Route Row), the call is routed to this alternative route only if the incoming INVITE matches this IP-to-IP routing rule's input characteristics. Notes: The alternative route entry, must be defined in the next consecutive table entry to the Route Row entry (i.e., directly below it). For example, if Index 4 is configured as a Route Row, Index 5 must be configured as the alternative route. Multiple alternative route entries can be configured (e.g., Index 1 is the main route - Route Row - and indices 2 through 4 are configured as alternative routes). Alternative routing applies to INVITE and other dialog initiating SIP messages (except REGISTER messages). For IP-to-IP alternative routing, configure SBC alternative routing reasons upon receipt of 4xx, 5xx, and 6xx SIP responses (in the 'SBC Alternative Routing Reasons' table). If no response, ICMP, or 408 SIP response is received, the device attempts to use the alternative route even if no entries are configured in the 'SBC Alternative Routing Reasons' table.

Parameter Name	Type	Provisioning Type	Description
Request Type	ENUM All, INVITE, REGISTER, SUBSCRIBE, INVITEAndREGISTER, INVITEAndSUBSCRIBE	instant	Defines the type of incoming SIP request.

43.11.3 Configuring SBC Alternative Route Reasons Table

The SBC Alternative Route Reasons table defines reasons for alternative routing rules defined in the SBC IP to IP Routing table.

➤ **To configure SBC Alternative Route Reasons:**

1. Click the  button to access the Media Gateway status screen.
2. Select the SIP board.
3. In the **Navigation Pane**, select **SIP ► SBC ► SBC Routing ► Alternative Route Reasons**; the SIP Alternative Route Reasons list is displayed.
4. Use the  or  buttons to add or remove entries.
5. Select a specific row and in the Configuration pane, click **SBC Alternative Route Reasons Settings**; the SBC Alternative Route Reasons Settings screen is displayed.
6. Configure SBC Alternative Route Reasons parameters according to the table 'SBC Alternative Route Reasons Parameters' below.
7. Click the Maintenance icon  and select **Unlock** to activate the configuration.

Table 43-7: SBC Alternative Route Reasons Parameters

Parameter Name	Type	Provisioning Type	Description
Release Cause	Integer 400-699	Instant	Defines the release cause of the call that initiates alternative routing.

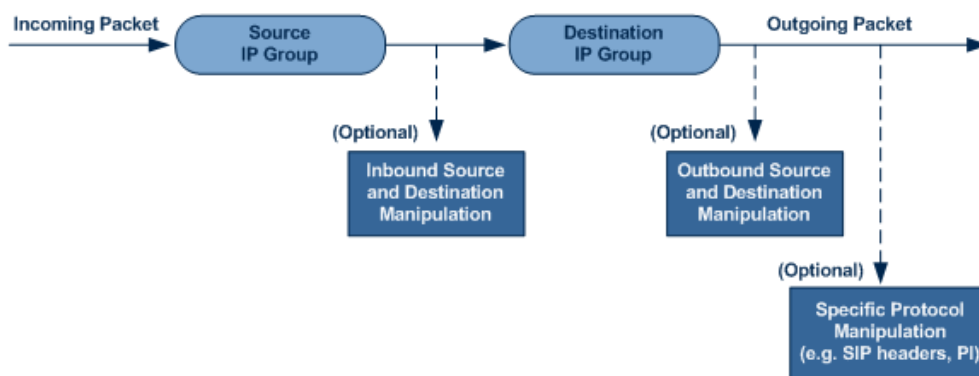
43.12 SBC Inbound and Outbound Manipulation

A manipulation rule is located according to the source IP group, and source and destination host and user prefixes. Since outbound manipulations are performed after routing, the outbound manipulation rule matching can also be done by destination IP Group. The operation rules apply to INVITE, OPTIONS, and SUBSCRIBE messages (not REGISTER messages).

Host name (source and destination) manipulations are simply host name substitutions with the names defined for the source and destination IP Groups respectively (if any, in the IP Group table).

Manipulated destination user and host are performed to the following SIP headers: Request URI, To, and Remote party ID (if exists). Manipulated source user and host are performed to the following SIP headers: From, P-Asserted (if exists), P-Preferred (if exists), and Remote party ID (if exists).

Figure 43-6: SBC Application Inbound and Outbound Manipulation



Below is an example of an SBC call flow and consequent SIP URI manipulations:

Figure 43-7: Example of SBC Application Manipulation



In the example above, the following SIP message manipulations were performed (contributing to typical topology hiding):

Table 43-8: SIP Manipulations Examples

SIP Manipulation	From	To
Inbound Source SIP URI User Name	7000	97000 (blue)
Source IP Group Name (SIP URI Host Name)	10.2.2.6	IP_PBX (blue)
Inbound Destination SIP URI User Name	1000	9721000 (red)
Destination IP Group Name (SIP URI Host Name)	10.2.2.3	ITSP1 (red)

43.12.1 SBC IP to IP Inbound Manipulation Table

The SBC IP to IP Inbound Manipulation table consists of the following two parts:

- Matching Rules
- Operation Rules

All calls that match all or any combination of the "matching rules" are subsequently modified according to the "Operation rules".

➤ To configure SBC IP to IP Inbound Manipulation:

1. Click the  button to access the Media Gateway status screen.
2. Select the SIP board.
3. In the Navigation pane, select **SIP ► SBC ► SBC Manipulation ► IP to IP Inbound Manipulation**; the SIP IP to IP Inbound Manipulation list is displayed.
4. Use the  or  buttons to add or remove entries.
5. Select a specific row and in the Configuration pane, click **SBC IP to IP Inbound Manipulation Settings**; the SBC IP to IP Inbound Manipulation Settings screen is displayed.
6. Configure SBC IP to IP Inbound Manipulation parameters according to the tables 'SBC IP to IP Inbound Manipulation Table Matching Rules' and 'SBC IP to IP Inbound Manipulation Table Operation Rules' below.
7. Click the Maintenance icon  and select **Unlock** to activate the configuration.

Table 43-9: SBC IP to IP Inbound Manipulation Table "Matching Rules"

Parameter Name	Type	Provisioning Type	Description
Source Username Prefix	String Up to 20 chars	Instant	Defines the prefix of the user part of the incoming SIP request's source URI (usually the From header). To denote any source username prefix leave the field empty or use asterisk (*) symbol.
Source Host	String Up to 50 chars	Instant	Defines the hostname of the incoming SIP request's source URI (usually the From header). To denote any source host leave the field empty or use asterisk (*) symbol.
Destination Username Prefix	String Up to 50 chars	Instant	Defines the prefix of the user part of the incoming SIP request's destination URI (usually the Request URI). To denote any destination username prefix leave the field empty or use asterisk (*) symbol.
Destination Host	String Up to 50 chars	Instant	Defines the hostname of the incoming SIP request's destination URI (usually the Request URI) user part. To denote any destination host leave the field empty or use asterisk (*) symbol.
Additional Manipulation	Enum No, Yes	Instant	Defines whether additional SIP URI user part manipulation is performed for the table entry rule listed directly above it. No – Regular manipulation rule (not performed in addition to the rule above it). Yes – If the previous table row entry rule matched the call, consider this row entry as a match as well and perform the manipulation specified by this rule. Note: Additional manipulation can only be performed on a different SIP URI (either source or destination) to the rule configured in the row above (defined by the parameter ManipulatedURI).
Manipulated URI	Enum Source, Destination	Instant	Defines whether the source or destination SIP URI user part is manipulated.
Source IP Group	Integer	Instant	Defines the IP Group from where the call

Parameter Name	Type	Provisioning Type	Description
	0-32		originated. Typically, this IP Group is determined by Classification process. If not used (i.e., any IP Group), set to 0 (Any).

Table 43-10: SBC IP to IP Inbound Manipulation Table "Operation Rules"

Parameter Name	Type	Provisioning Type	Description
Remove From Left	Integer 0-255	Instant	Defines the number of digits to remove from the left of the user name prefix. For example, if you enter 3 and the user name is 'bobby', the new user name is 'by'.
Remove From Right	Integer 0-255	Instant	Defines the number of digits to remove from the right of the user name prefix. For example, if you enter 3 and the user name is 'bobby', the new user name is 'bo'.
Leave From Right	Integer 0-255	Instant	Defines the number of characters to retain from the right of the user name.
Prefix to Add	String Up to 50 chars	Instant	Defines the string to be added in front of the user name. For example, if you enter 'sir' and the user name is 'bobby', the new user name is 'sirbobby'.
Suffix to Add	String Up to 50 chars	Instant	Defines the string to be added to the end of the user name. For example, if you enter '01' and the user name is 'bobby', the new user name is 'bobby01'.

43.12.2 SBC IP to IP Outbound Manipulation Table

The SBC IP to IP Outbound Manipulation table consists of the following two parts:

- Matching Rules
- Operation rules

All calls that match all or any combination of the "matching rules" are subsequently modified according to the "operation rules".

➤ **To configure SBC IP to IP Outbound Manipulation:**

1. Click the  button to access the Media Gateway status screen.
2. Select the SIP board.
3. In the Navigation pane, select **SIP ► SBC ► SBC Manipulation ► IP to IP Outbound Manipulation**; the SIP IP to IP Outbound Manipulation list is displayed.
4. Use the  or  buttons to add or remove entries.
5. Select a specific row and in the Configuration pane, click **SBC IP to IP Outbound Manipulation**; the SBC IP to IP Outbound Manipulation screen is displayed.
6. Configure SBC IP to IP Outbound Manipulation parameters according to the tables 'SBC IP to IP Outbound Manipulation Table Matching Rules' and 'SBC IP to IP Outbound Manipulation Table Operation Rules' below.
7. Click the Maintenance icon  and select **Unlock** to activate the configuration.

Table 43-11: SBC IP to IP Outbound Manipulation Table "Matching Rules"

Parameter Name	Type	Provisioning Type	Description
Source Username Prefix	String Up to 20 chars	Instant	Defines the prefix of the user part of the incoming SIP request's source URI (usually the From header). To denote any source username prefix leave the field empty or use asterisk (*) symbol.
Source Host	String Up to 50 chars	Instant	Defines the hostname of the incoming SIP request's source URI (usually the From header). To denote any source host leave the field empty or use asterisk (*) symbol.

Parameter Name	Type	Provisioning Type	Description
Destination Username Prefix	String Up to 50 chars	Instant	Defines the prefix of the user part of the incoming SIP request's destination URI (usually the Request URI). To denote any destination username prefix leave the field empty or use asterisk (*) symbol.
Destination Host	String Up to 50 chars	Instant	Defines the hostname of the incoming SIP request's destination URI (usually the Request URI) user part. To denote any destination host leave the field empty or use asterisk (*) symbol.
Additional Manipulation	Enum No, Yes	Instant	Defines whether additional SIP URI user part manipulation is performed for the table entry rule listed directly above it. No – Regular manipulation rule (not performed in addition to the rule above it). Yes – If the previous table row entry rule matched the call, consider this row entry as a match as well and perform the manipulation specified by this rule. Note: Additional manipulation can only be performed on a different SIP URI (either source or destination) to the rule configured in the row above (defined by the parameter ManipulatedURI).
Manipulated URI	Enum Source, Destination	Instant	Defines whether the source or destination SIP URI user part is manipulated.
Source IP Group	Integer 0-32	Instant	Defines the IP Group from where the call originated. Typically, this IP Group is determined by the Classification process. For more information, see Source IP Group Classification. If not used (i.e., any IP Group), set to 0 (Any).
Dest IP Group	Integer 0-32	Instant	Defines the destination IP Group to where the call will be sent. Typically, this IP Group is determined by Routing process. If not used (i.e., any IP Group), set to 0 (Any).

Table 43-12: SBC IP to IP Outbound Manipulation Table "Operation Rules"

Parameter Name	Type	Provisioning Type	Description
Remove From Left	Integer 0-255	Instant	Defines the number of digits to remove from the left of the user name prefix. For example, if you enter 3 and the user name is 'bobby', the new user name is 'by'.
Remove From Right	Integer 0-255	Instant	Defines the number of digits to remove from the right of the user name prefix. For example, if you enter 3 and the user name is 'bobby', the new user name is 'bo'.
Leave From Right	Integer 0-255	Instant	Defines the number of characters to retain from the right of the user name.
Prefix to Add	String Up to 50 chars	Instant	Defines the string to be added in front of the user name. For example, if you enter 'sir' and the user name is 'bobby', the new user name is 'sirbobby'.
Suffix to Add	String Up to 50 chars	Instant	Defines the string to be added to the end of the user name. For example, if you enter '01' and the user name is 'bobby', the new user name is 'bobby01'.

43.13 SBC Message Manipulation

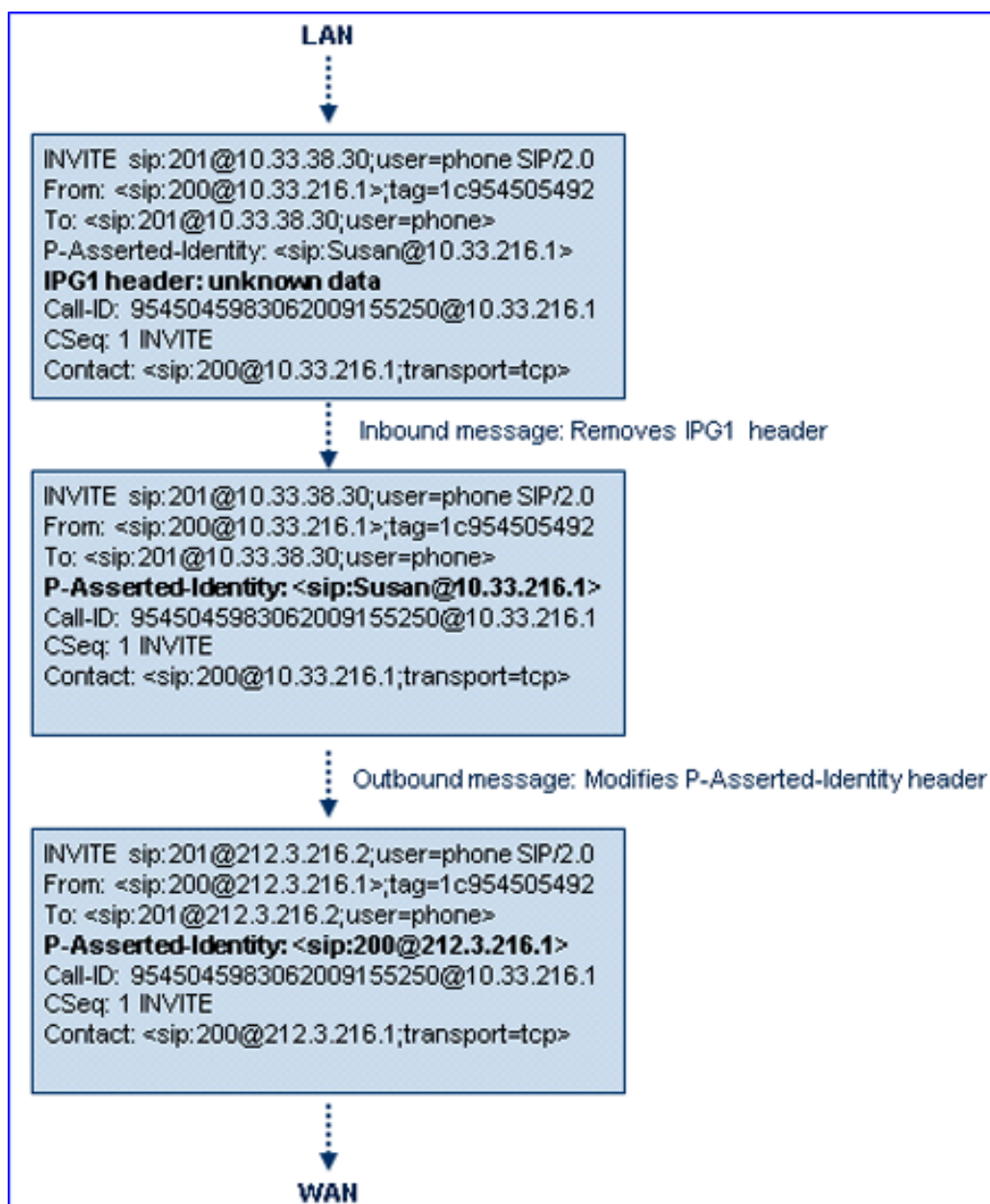
SIP header manipulation enables insertion, removal, and/or modification of SIP headers and parameters. This manipulation is configured in the Message Manipulations table. This feature enables the normalization of SIP messaging fields between communicating network segments. For example, it allows service providers to design their own policies on the SIP messaging fields that must be present before a SIP call enters their network. Similarly, enterprises and small businesses may have policies for the information that can enter or leave their networks for policy or security reasons from a service provider. The manipulations can also be implemented to resolve incompatibilities between SIP devices inside the enterprise network.

SIP messaging manipulation supports the following:

- Addition of new headers.
- Removal of headers ("Black list").
- Modification of header components - value, header value (e.g., URI value of the P-Asserted-Identity header can be copied to the From header), call's parameter values.
- Deletion of SIP body (e.g., if a message body isn't supported at the destination network this body is removed).
- Translating one SIP response code to another.
- Topology hiding (generally present in SIP headers, such as Via, Record Route, Route and Service-Route).
- Configurable identity hiding (information related to identity of subscribers for example, P-Asserted-Identity, Referred-By, Identity and Identity-Info).
- Apply conditions per rule - the condition can be on parts of the message or call's parameters.
- Multiple manipulation rules on the same SIP message.

Example of SBC Header Manipulation

Figure 43-8: SBC Message Manipulation



43.13.1 Configuring the SBC Message Manipulation Table

The manipulation is performed on SIP messages according to the Classification table (source/destination of username/host prefixes and source IP address). The manipulation can be performed on message type (Method, Request/Response, and Response type). Message manipulations are performed only after the classification, inbound manipulations and routing are successfully performed (i.e., manipulations are performed only in the outgoing leg).

SIP Message manipulation rules can be assigned to an IP Group in the IP Group table and it can be determined whether they must be performed for inbound or outbound messages.

➤ **To configure SBC Message Manipulation:**

1. Click the  button to access the Media Gateway status screen.
2. Select the SIP board.
3. In the Navigation pane, select **SIP ► SBC ► SBC Message Manipulation**; the SBC Message Manipulation list is displayed.
4. Use the  or  buttons to add or remove entries.
5. Select a specific row and in the Configuration pane, click **SBC Message Manipulation**; the SIP SBC Message Manipulation screen is displayed.
6. Configure SIP SBC Message Manipulation parameters according to the table SIP SBC Message Manipulation Table Matching Rules' below.
7. Click the Maintenance icon  and select **Unlock** to activate the configuration.

Table 43-13: SIP SBC Message Manipulation Table

Parameter Name	Type	Provisioning Type	Description
Manipulation Set ID	Integer 0-19	Instant	Unique manipulation set ID that you can later assign to an IP Group.
Message Type	String Up to 50 chars	Instant	SIP message type that you want to manipulate. The valid value is a string depicting the SIP message
Condition	String Up to 200 chars	Instant	Condition that must exist for the rule to apply.
Action Subject	String Up to 100 chars	Instant	SIP header upon which the manipulation is performed.

Table 43-13: SIP SBC Message Manipulation Table

Parameter Name	Type	Provisioning Type	Description
Action Type	ENUM Add, Remove, Modify, AddPrefix, AddSuffix, RemoveSuffix, RemovePrefix	Instant	The type of manipulation to perform. ▪ [0] Add (default) = adds new header/param/body (header or parameter elements). ▪ [1] Remove = removes header/param/body (header or parameter elements). ▪ [2] Modify = sets element to the new value (all element types). ▪ [3] Add Prefix = adds value at the beginning of the string (string element only). ▪ [4] Add Suffix = adds value at the end of the string (string element only). ▪ [5] Remove Suffix = removes value from the end of the string (string element only). ▪ [6] Remove Prefix = removes value from the beginning of the string (string element only).
Action Value	String Up to 200 chars	Instant	Value (string) that you want to use in the manipulation. The syntax is as follows: string/<message-element>/<call-param> "+" string/<message-element>/<call-param>
Row Role	ENUM CurrentCondition, PreviousCondition		Determines which condition must be used for the rule of this table row. ▪ [0] Use Current Condition = The condition entered in this row must be matched to perform the defined action (default). ▪ [1] Use Previous Condition = The condition of the rule configured directly above this table row must be used to perform the defined action. This option allows you to configure multiple actions for the same condition.

43.14 User Registration

To allow registrations to traverse the SBC application, one of the IP Groups must be configured with USER type. USER IP Groups represent a group of user agents that share the following characteristics:

- Perform registrations and share the same serving proxy/registrar
- Identical SIP and media behavior
- Reside on the same Layer-3 network and are associated with the same SRD

Typically, the Board functions as the user agent's outbound proxy and is configured (using the SBC IP to IP Routing table) to route requests received from this IP Group to the serving proxy and vice versa. Survivability can be achieved using the alternative routing feature.

43.14.1 Registration Request Processing

Registration requests have different processing policies than other SIP methods:

1. Determining source and destination URL's:
 - The source URL is obtained from the To header
 - The destination URL is obtained from the Request URI
2. Classification: The REGISTER classification process is the same as the general classification process (described in previous sections). The source IP Group must be of type USER. If the classification fails or the source IP Group is not of type USER, the registration is rejected.
3. Routing: The REGISTER routing is performed using the IP2IP Routing table:
 - The destination type can only be an IP Group (i.e., no specific address\Request URI).
 - If the IP Group is of type SERVER, the REGISTER is routed to the IP Group's Proxy Set.
 - If the IP Group is of type USER, then the device replies with a 200 OK response (used for Survivability) and the REGISTER is not forwarded.
4. The Contact of the outgoing REGISTER is populated with a unique Contact generated by the device and associated with this specific registration.



Note: Alternative route and manipulations are not implemented for registrations.

43.14.2 Registrations Database

The board manages a dynamic database that is updated according to registration requests that traverse the SBC application. Each database entry represents a binding between an Address Of Record (AOR) and one or more contacts. Database bindings are added upon successful registration responses. For specific registrations, the AOR is obtained from the SIP To header and the contact is taken from the SIP Contact header.



Note: The Registrations Database is independently maintained by each SIP board. No information is shared between different SIP boards.

Database bindings are deleted in the following cases:

- Successful de-registration responses (REGISTER with Expires header that equals zero)
- Registration failure responses
- Timeout of the Expires header value (in scenarios where the user agent did not send a refresh registration request)

The database has the following limitations:

- Maximum registered users is 200
- Maximum of five contacts per AOR
- The same contact cannot belong to more than one AOR
- Contacts with identical URIs and different ports and transport types are not supported (same key is created)
- Multiple contacts in a single REGISTER is not supported
- One database is shared between all USER-type IP Groups.

43.14.3 Routing using Registrations Database

Typically, routing using the registration database, is applicable to all method types other than registrations. To route to a registered user (using the internal dynamic database) an IP-to-IP routing rule must be configured with the desired input parameters (matching characteristics) and the destination type as IP Group (operation rule). The destination IP Group must be of type USER.

To find a match for these specific rules, the device attempts to locate a match between the incoming request URI and (according to the description order):

- a. Unique contact - the Contact generated by the SBC application and sent in the initial registration request to the serving proxy
- b. Registered AOR - the AOR of the incoming REGISTER request
- c. Registered contact - the Contact of the incoming REGISTER request

If registrations are destined to the database (using the above rules), the device does not attempt to find a database match, however instead replies with 200 OK (used for Survivability). Once a match is found, the request is routed either to the contact received in the initial registration or (if the device identifies that the user agent is behind a NAT) to the source IP address of the initial registration.

43.14.4 Registration Refreshes

Registration refreshes are incoming REGISTER requests that are associated with a specific registered user. The association is performed by searching the internal registration database. These refreshes are routed to the serving proxy only if the serving proxy 'Expires time' is about to expire; otherwise, the device responds with a 200 OK without routing the REGISTER. Each refresh also refreshes the internal timer time set on the device for this specific registration.

43.15 SBC Admission Control

SBC Admission Control functionality allows definition of various limitations on call signaling - for example, limits on the number of concurrent calls, limits on the number of calls per second etc. Different limits/policies may be configured for different IP groups and/or SRDs. The admission control functionality may be used, for example, to enforce SLA policy of a service provider or to prevent DoS attacks from the WAN.

➤ To configure SBC Admission Control:

1. Click the  button to access the Media Gateway status screen.
2. Select the SIP board.
3. In the Navigation pane, select **SIP ► SBC ► SBC Admission Control**; the SIP SBC Admission Control list is displayed.
4. Use the  or  buttons to add or remove entries.
5. Select a specific row and in the Configuration pane, click **SBC Admission Control Settings**; the SBC Admission Control Settings screen is displayed.
6. Configure SBC Admission Control parameters according to the table below.
7. Click the Maintenance icon  and select **Unlock** to activate the configuration.

Table 43-14: SBC Admission Control Settings

Parameter Name	Type	Provisioning Type	Description
Group Type	Enum IP Group, SRD	Instant	Defines which entity the admission control rule applies to – IP Group or SRD.
IP Group ID	Integer -1 – 32	Instant	Defines the IP Group to which this admission control rule applies.
SRD ID	Integer -1 – 32	Instant	Defines the SRD to which this admission control rule applies.
Request Type	Enum All, INVITE, SUBSCRIBE, Other	Instant	Defines the type of SIP dialogs to which this admission control rule applies, based on the SIP dialog initiating request. When set to All – all SIP dialogs are affected.
Request Direction	Enum Both, In, Out	Instant	Defines the direction of the SIP dialog that this admission control rule applies to.
Limit Per Group	Integer -1 – 2147483647	Instant	Defines maximum number of dialogs allowed. Value -1 means that no limit is imposed. Value 0 means that no dialogs are allowed.
Limit Per User	Integer	Instant	Defines maximum number of dialogs

Parameter Name	Type	Provisioning Type	Description
	-1 – 2147483647		allowed per user. Value -1 means that no limit is imposed. Value 0 means that no dialogs are allowed.
Dialogs Rate	Integer 0 – 65536	Instant	Defines limit on dialogs rate. Value 0 means that no limit is imposed.
Max Dialogs Burst	Integer 0 – 65536	Instant	Defines limit of maximum dialogs burst. Value 0 means that no limit is imposed.

43.16 SBC Media Handling

Media behavior includes anything related to the establishment, management and termination of media sessions within the SIP protocol. Media sessions are created using the SIP "offer"/"answer" mechanism. If successful, the result is a bi-directional media (RTP) flow (e.g. audio, fax, modem, DTMF). Each offer/answer may create more than one media session of different types (e.g. audio and fax). In a SIP dialog, multiple offer/answer transactions may occur, where each may change the media sessions characteristics (e.g. IP address, port, coders, media types, and RTP mode).

The media capabilities exchanged in offer/answer transactions include the following:

- Media types (Audio, Secure Audio, Video, Fax, Text...)
- IP addresses and ports of the media flow
- Media flow mode (send receive, receive only, send only, inactive)
- Media coders (coders and there characteristics used in each media flow)
- Other (standard or proprietary) media and session characteristics

Even though the device usually does not change the negotiated media capabilities (mainly performed by the remote user agents), it does examine the media exchange to control negotiated media types (if necessary) and to know how to open the RTP media channels (IP addresses, coder type, payload type etc.).

The device is aware and sometimes active in the offer\answer process due to the following:

- Firewall and security:
 - RTP pin holes - only RTP packets related to a successful offer\answer negotiation traverse the device: when the device initializes, there are no RTP pin holes open, this means that each RTP/RTCP packets destined to the device are discarded. Once an offer/answer transaction ends successfully, an RTP pin hole is opened and RTP/RTCP flows between the two remote user agents. Once a pin hole is open, the payload type and RTP header version is validated for each packet. RTP pin holes close if one of the associated SIP dialogs is closed (this may also be due to a broken connection).
 - Late rogue detection - once a dialog is disconnected, the related pin holes also disconnect
 - Deep Packet inspection of the RTP that flows through the opened pin holes
- Adding media functionality to SIP user agents:
 - Transcoding
 - Broken connection

According to the above functionalities, the call can be configured to operate in one of the following modes:

- **Media Anchoring without Transcoding (Transparent):** RTP traverses the device with minimal RTP packet changes (no DSP resources required). This is typically used to solve NAT, firewall, and security issues. In this mode, all the "audio" coders in the received offer are included in the SBC application outgoing offer. The Coder Table configuration has no effect on the coders in the outgoing offer.
- **Media Anchoring with Transcoding:** RTP traverses the device and each leg uses a different coder or coder parameters (DSP resources are required).

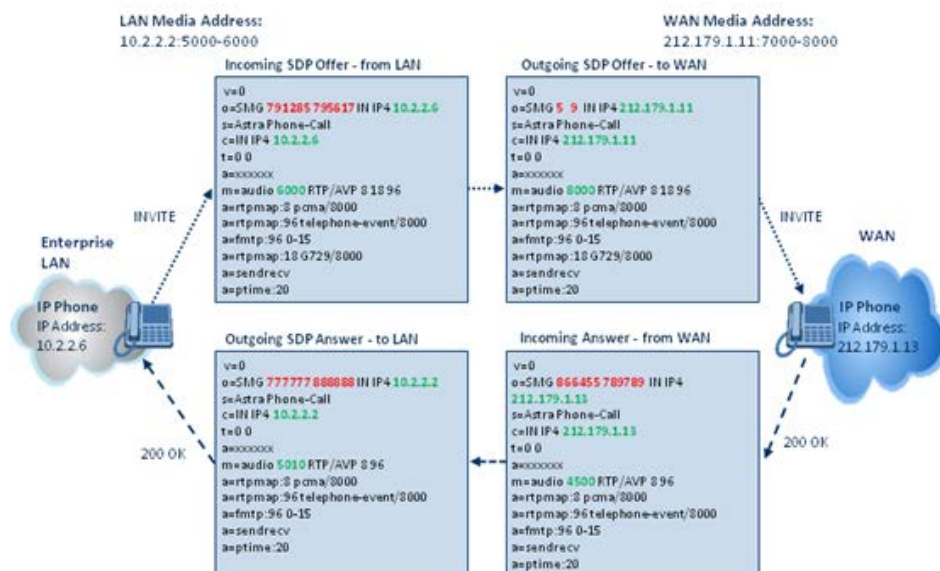
43.16.1 Media Anchoring without Transcoding (Transparent)

To direct the RTP to flow through the device (for NAT traversal, firewall and security), all IP address fields in the SDP are modified:

- Origin: IP address, session and version id
- Session connection attribute ('c=' field)
- Media connection attribute ('c=' field)
- Media port number
- RTCP media attribute IP address and port (if the parameter Enable RTCP Attribute is set to 1)

Each SBC leg allocates and uses the device's local ports (e.g., for RTP\RTCP\fax). The local ports are allocated from a Media Realm associated with each SBC leg. SBC legs are associated with a Media Realm as follows: If the leg's IP Group is configured with a Media Realm, then this is the associated Media Realm; otherwise, the leg's SRD Media Realm is the associated one.

Figure 43-9: Example of a SIP call with Media Anchoring without Transcoding

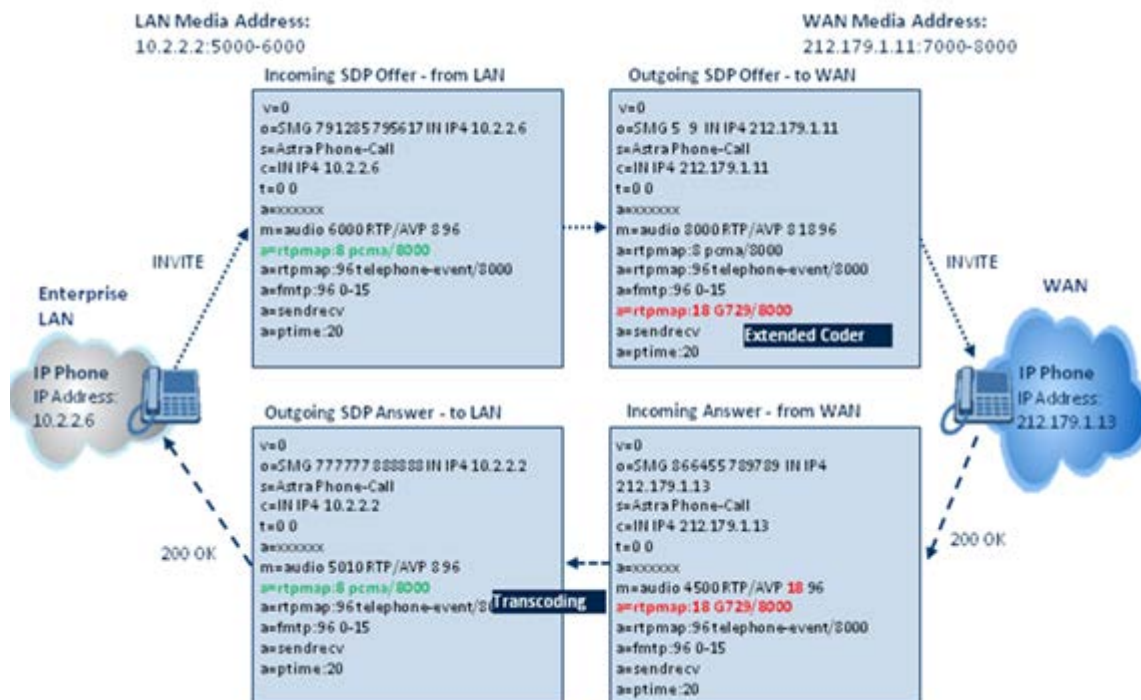


43.16.2 Media Anchoring with Transcoding

The device performs transcoding when there are no common coders between the two user agents (i.e., the SDP answer from one user agent doesn't include any coder included in the offer previously sent by the other user agent). For transcoding, the device can be configured to add media capabilities to user agents pertaining to a specific IP Group, and then perform transcoding in cases where the selected coder in the answer SDP is not one that appears in the original offer. The capabilities that can be added are one or more of the device's supported coders and are configured by using the parameter "SBC Extension Coders Group ID" (points to a coders list) in the IP Profile table (which is assigned to the IP Group). Therefore, to allow user agents of different IP Groups to communicate with each other (regardless of their capabilities), an extended coders table with at least one coder that is supported by each IP Groups' user agents needs to be assigned to each IP Group. Therefore, each offer destined to specific IP Groups includes this coder.

In the scenario depicted in the figure below, the IP phone on the LAN side initiates a call to the IP phone in the WAN. The initial SDP offer (from the LAN leg) includes codec G.711 as its supported codec. Since this is sent to a Destination IP Group that is configured with an extended coder list, on the WAN leg, the device adds another supported codec G.729 to the SDP, which is now offered to the WAN IP phone. The WAN IP phone chooses the extended codec (G.729) in its SDP answer to the device's WAN leg. Since this codec was not included in the original incoming offer, the device performs transcoding (between G.729 and G.711) between its two legs, allowing the streaming of media to occur.

Figure 43-10: Example of SIP call with Media Anchoring with Transcoding



For an SDP offer to provide an extended coder list to a remote user agent, the following prerequisites must be fulfilled:

- An extended coders list has been configured for the user agent's IP Group (i.e., Destination IP Group)
- The incoming offer contains at least one supported coder (otherwise, transcoding can't be performed)
- Both legs have available DSP's
- T.38 doesn't appear in the offer

If the above prerequisites are not met, the SDP offer is sent without the extended coders list. The coders from the extended list are added after the ones from the original offer (decreases transcoding probability). Coders common between the extended coders list and those in the original SDP offer are not added. Transcoding may be performed even in scenarios when the same coder has been chosen - this occurs if the coders use different coder parameters (e.g. rate and packetization time).

The device also supports early media, whereby the first offer\answer transaction is finalized and the media flow starts before the SIP call is connected (before the INVITE 200 OK response).

The offer and answer options can be included in the following SIP messages:

- Offer in first INVITE, answer on 180, and no or same answer in the 200 OK
- Offer in first INVITE, answer on 180, and a different answer in the 200 OK (not standard)
- INVITE without SDP, offer in 180, and answer in PRACK
- PRACK and UPDATE transactions can also be used for initiating subsequent offer\answer transactions before the INVITE 200 OK response.
- In a SIP dialog life time, media characteristics after originally determined by the first offer\answer transaction can be changed by using subsequent offer\answer transactions. These transactions may be carried either in UPDATE or ReINVITE SIP transactions. The media handling is similar to the original offer\answer handling. If the offer is rejected by the remote party, then no media changes occur (e.g. INVITE without SDP, then 200 OK and ACK, offer\answer within an offer\answer, and Hold ReINVITE with IP address of 0.0.0.0 - IP address is unchanged).

43.16.3 Transcoding Modes

The device supports the configuration of the voice transcoding mode (media negotiation) between the two SBC legs. The device can be configured to perform transcoding only when necessary. Typically, the SBC application passes RTP packets transparently (RTP-to-RTP) between the two user agents. If the device is configured to always perform transcoding, then transcoding is performed on the outgoing SBC leg and the device's SBC application interworks the media by implementing Media transcoding (since both legs have different media capabilities).

In the SBC application, forced transcoding of voice in an SBC session allows the device to receive capabilities that are not negotiated between the SBC legs. For example, if you wish to force Gain Control on the SBC session to use voice transcoding, even though both sides of the session have negotiated without SBC intervention (for example coder extension).



Note: To implement transcoding, you must configure the number of required DSP channels used for transcoding via Number of Media Channels parameter in the SIP Configuration screen. Each transcoding session uses two DSP resources.

Part VI

Maintenance

This part describes the Mediant 8000 maintenance procedures.

44 Media Gateway Software Backup/Restore Procedures

A backup of the Media Gateway software should be made at the following times:

- After changing the Media Gateway configuration
- Before performing the Online Software Upgrade (to ensure that an up-to-date backup is available, in the unlikely event of a problem occurring as the result of the software upgrade)
- After completing the Online Software Upgrade

44.1 Backup Procedures

The software backup procedures are performed on the Active SC board and do not interrupt the operation of the SC software. The backup file created on the Active SC board may be restored on both SC boards.

The backup file contains complete configuration data, including IP addresses of the SC and Media Gateway boards. Therefore you should restore the backup file on the same Mediant 8000 system where it was created.

44.2 Backup Types

The Media Gateway software supports two backup types:

- Configuration Backup – contains configuration data and auxiliary files.
- Full Backup – contains software binaries in addition to the configuration data.

Configuration Backup is much smaller than Full Backup and therefore is most commonly used. However, it can be restored only on the SC board that has proper SC software version pre-installed.



Note: The Operating System (OS) image is not part of any backup. Therefore you must ensure that the correct OS version is installed on the SC board prior to restoring the backup on it. See Section 'The Operating System on the SC Boards' on page [226](#) for more information.

44.3 Creating the Media Gateway Software Backup

A backup of the Media Gateway software may be performed via the EMS GUI or, alternatively, via the command line interface (CLI).

➤ To create a backup for the Media Gateway software via the EMS GUI:

1. Click  to access the Media Gateway status screen.
2. In the Actions bar, click **Backup**; the Backup Dialog screen is displayed.

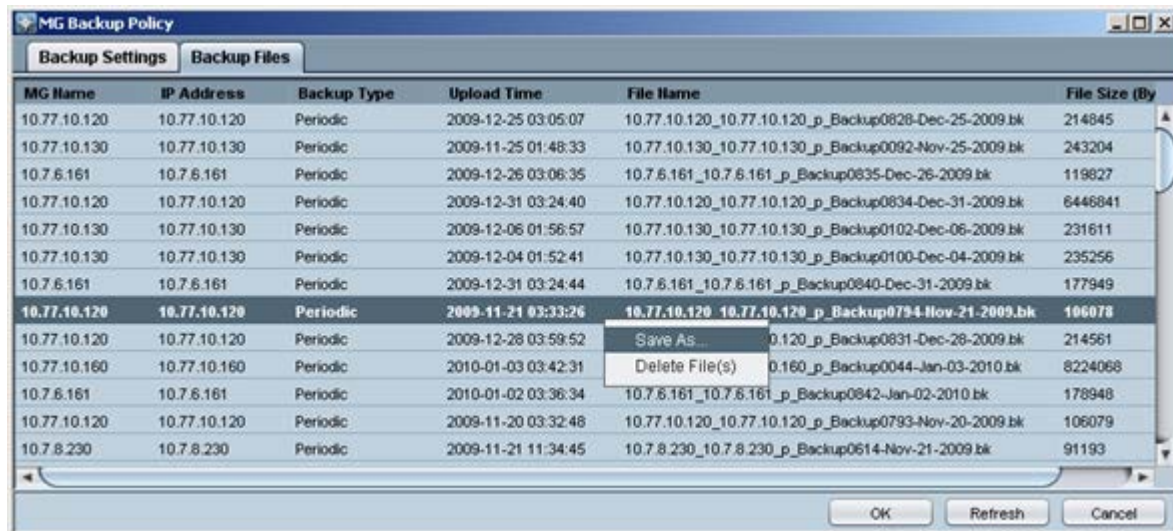
Figure 44-1: Backup Dialog screen



3. Select whether you wish to create **Configuration Backup** or **Full Backup**.
 - **Configuration Backup** – contains configuration data and auxiliary files.
 - **Full Backup** – contains software binaries in addition to the configuration data.
4. Wait patiently while the backup file is created (this may take up to 10 minutes, depending on the Backup Type and amount of configuration data). You will be notified when the backup file is ready.

- The Backup file is stored in the EMS server. To view all available Backup files, in the EMS menu, choose **Tools -> MG Backup Files**.

Figure 44-2: Backup files in the EMS



MG Name	IP Address	Backup Type	Upload Time	File Name	File Size (By)
10.77.10.120	10.77.10.120	Periodic	2009-12-25 03:05:07	10.77.10.120_10.77.10.120_p_Backup0828-Dec-25-2009.bk	214845
10.77.10.130	10.77.10.130	Periodic	2009-11-25 01:48:33	10.77.10.130_10.77.10.130_p_Backup0092-Nov-25-2009.bk	243204
10.7.6.161	10.7.6.161	Periodic	2009-12-26 03:06:35	10.7.6.161_10.7.6.161_p_Backup0835-Dec-26-2009.bk	119827
10.77.10.120	10.77.10.120	Periodic	2009-12-31 03:24:40	10.77.10.120_10.77.10.120_p_Backup0834-Dec-31-2009.bk	8446841
10.77.10.130	10.77.10.130	Periodic	2009-12-06 01:56:57	10.77.10.130_10.77.10.130_p_Backup0102-Dec-06-2009.bk	231611
10.77.10.130	10.77.10.130	Periodic	2009-12-04 01:52:41	10.77.10.130_10.77.10.130_p_Backup0100-Dec-04-2009.bk	235256
10.7.6.161	10.7.6.161	Periodic	2009-12-31 03:24:44	10.7.6.161_10.7.6.161_p_Backup0840-Dec-31-2009.bk	177949
10.77.10.120	10.77.10.120	Periodic	2009-11-21 03:33:26	10.77.10.120_10.77.10.120_p_Backup0794-Nov-21-2009.bk	106078
10.77.10.120	10.77.10.120	Periodic	2009-12-28 03:58:52	10.77.10.120_10.77.10.120_p_Backup0831-Dec-28-2009.bk	214561
10.77.10.160	10.77.10.160	Periodic	2010-01-03 03:42:31	10.77.10.160_10.77.10.160_p_Backup0044-Jan-03-2010.bk	8224068
10.7.6.161	10.7.6.161	Periodic	2010-01-02 03:36:34	10.7.6.161_10.7.6.161_p_Backup0842-Jan-02-2010.bk	178948
10.77.10.120	10.77.10.120	Periodic	2009-11-20 03:32:48	10.77.10.120_10.77.10.120_p_Backup0793-Nov-20-2009.bk	106079
10.7.8.230	10.7.8.230	Periodic	2009-11-21 11:34:45	10.7.8.230_10.7.8.230_p_Backup0614-Nov-21-2009.bk	91193

- You may optionally store a copy of the backup file on an external file server (or on the PC where you run the EMS client). To perform this task, in the **MG Backup Files** screen, select **backup file**, right-click and choose the **Save As** option from the drop-down menu.

➤ **To create a backup for the Media Gateway software via CLI:**

- Connect to the CLI interface on Active SC board. For more information, see Section 'Connecting to the CLI via IP Network' on page 111.
- Login as a regular CLI user with administrative privileges (e.g. **acladmin**) and provide the password. For more information, see Section 'Logging into the Command Line Interface' on page 115.



Note: Backup may also be performed when you are logged in as the **root** user. However, for better accountability and easier backup file transfer, it is recommended to use regular CLI user with administrative privileges for this purpose.

3. At the prompt, type **tools bk** and press **Enter**.

```
client238 -- ~ -- /moGW
•   tools bk
```

The backup sequence is activated. You are prompted to confirm the action. Type **y** and press **Enter**.

```
BACKUP
```

```
This tool will create a complete backup of Media Gateway software
```

```
IMPORTANT: you must run this tool only on ACTIVE SC board!!!
```

```
Make a backup? ([y]/n) : y
```

4. You are prompted to enter a name of the backup file or press ENTER to accept the default file name – **backup.bk**.

In the example below, the chosen backup file name is **backup_12jan2009.bk**. The backup file is created in the home directory of the logged in user (e.g., **/data/acladmin directory** for **acladmin** user) unless you specify a complete file name starting with the "/" symbol (e.g., **/data/shared/12_jan2009.bk**).

It is recommended to end the backup file name with the extension ".bk".

```
Backup file name [backup.bk] : backup_12jan2009.bk
```

5. You are prompted to choose whether you wish to include binary files in the backup or not. Backup without software binary files included is most commonly used due to much smaller size and faster creation time. However it can be restored only on the SC board that has a proper SC software version pre-installed.

```
Do you wish to include binary files in the backup?
Backup without binary files has significantly smaller size, but
it may be restored only on the SC board with correct SC software
version pre-installed on it.
Include binary files? ([y]/n) : y
```


6. Wait patiently till backup process completes. It may take up to 10 minutes to create the backup file.

```
Please wait patiently until backup completes.
```

```
The process may take up to 10 minutes.
```

```
Extracting installation package to temporary directory... done
Building list of files to be backed up... done
Creating backup file... done
Compressing backup file... done
Creating self-extracting backup file... done
```

```
Backup file /data/acladmin/backup_12jan2009.bk was successfully created.
```

7. For safekeeping, transfer the created backup file from the SC board to an external location (e.g. a file server or a regular PC) via the SCP/SFTP/FTP protocol. When prompted for the username and password, provide the name of the CLI user that you used to create the backup file (e.g. **acladmin**) and the password. See Section 'Transferring the Mediant 8000 Installation Package to the SC Boards' on page 130 for additional details.

Transferring Backup File from the SC board via the Command-Line SFTP Client:

```
Microsoft Windows XP [Version 5.1.2600]
© Copyright 1985-2001 Microsoft Corp.

C:\> psftp acladmin@10.7.13.91
Using username "acladmin"

+-----+
| WARNING: To protect systems from unauthorized use and to |
| | ensure that the system is functioning properly, |
| | activities on this system are monitored and recorded and |
| | subject to audit. Use of this system is expressed consent |
| | to such monitoring and recording. Any unauthorized access |
| | or use of this system is prohibited and could be subject |
| | to criminal and civil penalties. |
+-----+

Password: *****
Remote working directory is /data/acladmin
psftp> lcd \Backup
New local directory is c:\Backup
psftp> put backup_12jan2009.bk
local: backup_12jan2009.bk => remote:/data/acladmin/backup_12jan2009.bk

psftp> bye
```



Note: If you transfer the backup file via FTP protocol, ensure to choose "binary file transfer mode" (command **bin** in a console FTP client).

44.4 Restoring the Media Gateway Software from Backup

Restoring the Media Gateway software from a backup file is provided as a precautionary measure and is intended for use in extreme cases only. Restoring the Media Gateway software from a backup file requires restoration on *both* of the SC boards, and, therefore, the entire system must be non-operational for this process.



Note: The Restore procedure must be performed on both of the SC boards.

The Basic IP Network Configuration is not part of the Software Backup and must be manually updated to match the restored configuration prior to running the Restore procedure described below. See 'Configuring the Basic IP Network Parameters of SC Boards' on page 117 for details.

If current IP network configuration of the Mediant 8000 is different from the IP network configuration at the time when backup was created (e.g. there is a difference in VLAN tags or interface separation settings), Mediant 8000 may lose IP connectivity after restoring the backup file. See 'Connecting the Media Gateway to the IP Network' on page 178, for detailed instructions on how to update the network configuration.

Restoration of the Media Gateway software from the backup file may be performed via the EMS GUI or, alternatively, via the command line interface (CLI).

➤ **To restore the Media Gateway software from the backup file via the EMS GUI:**

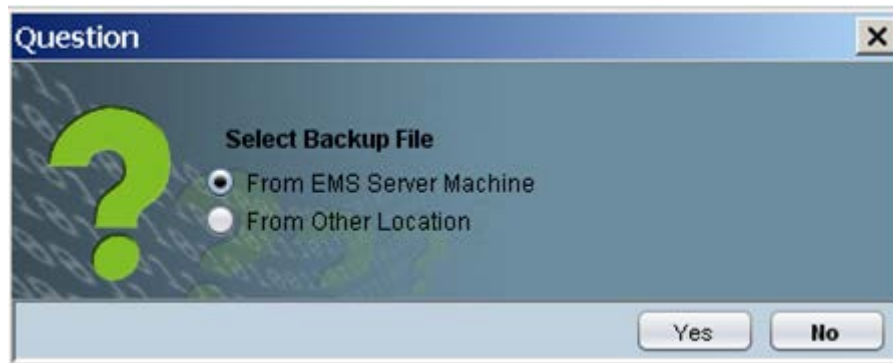
1. Click  to access Media Gateway status screen.
2. Lock the Media Gateway by clicking **Lock** in the Actions bar. Confirm that you wish to lock the Media Gateway by clicking the **Yes** button in the displayed screen.
3. Start the restore procedure by clicking **Restore** in the Actions bar; the Restore Prompt information message is displayed.

Figure 44-3: Gateway Restore Procedure



4. Click **Yes** to continue; the Backup File select prompt is displayed.

Figure 44-4: Select Backup File



Choose whether you wish to restore the backup file that is currently stored on the EMS server, or a file stored in some other location (e.g. on the EMS client PC or on a file server).

5. Choose the backup file and click **OK**.
6. Wait patiently while the Media Gateway software is restored from the backup. When performing the restore operation via the EMS GUI, the backup is restored on both SC boards automatically. The restore operation may take up to 20 minutes, depending on the Backup Type and amount of configuration data.

➤ **To restore the Media Gateway software from the backup file via the CLI:**

1. Transfer the backup file from safekeeping location to both SC boards via the SFTP/SCP/FTP protocol. Use a regular CLI user name and password when prompted (e.g. **acladmin**). See 'transferring the Mediant 8000 Installation Package to the SC Boards' on page 130 for details on how to perform a file transfer.

Transferring the Backup file to the SC board via the Command-line SFTP client

```
Microsoft Windows XP [Version 5.1.2600]
© Copyright 1985-2001 Microsoft Corp.

C:\> psftp acladmin@10.7.13.91
Using username "acladmin"

+-----+
| WARNING: To protect systems from unauthorized use and to | | ensure
| that the system is functioning properly, |
| activities on this system are monitored and recorded and |
| subject to audit. Use of this system is expressed consent |
| to such monitoring and recording. Any unauthorized access |
| or use of this system is prohibited and could be subject |
| to criminal and civil penalties. |
+-----+

Password: *****
Remote working directory is /data/acladmin
psftp> lcd \Backup
New local directory is c:\Backup
psftp> put backup_12jan2009.bk
local: backup_12jan2009.bk => remote:/data/acladmin/backup_12jan2009.bk

psftp> bye
```

2. Connect to the CLI interface on both SC boards . For more information, see Section 'Connecting to the CLI via the IP Network' on page 111.
3. Login as the **root** user. For more information, see Section 'Logging in as a Root User' on page 115. To stop the Media Gateway software on *both* SC boards, at the prompt, type **tools sc dn** and press **Enter**. When prompted to confirm this command, type **y** and press **Enter**.

```
client238::~~# tools sc dn
STOP SC SOFTWARE
```

```
Stop SC software? ([y]/n) : y
```

```
>>> Stop watchdog process...
>>> Wait for application to stop...
```



Note: The Media Gateway software on both SC boards must be stopped (via the **tools sc dn** command) prior to proceeding to the next step. If you attempt to restore the backup file on the Standby SC board, while the Active SC is still operating, the restored configuration database will be erased by the replication mechanism.

4. On the SC board in Slot 1 (designated to be Active board), change the current directory to the place where the **backup** file is stored (typically, the home directory of the CLI user that you used to perform the file transfer) and type the following commands to start the restore process:

```
client238::~~# cd /data/acladmin
client238::~~# chmod u+x backup_12jan2009.bk
client238::~~# ./backup_12jan2009.bk
```

RESTORE

This backup contains the following data:

```
Product type       : Mediant 8000
Software version   : 6.6.15
Binaries included  : Yes
Created at         : Sun Jan 12 18:20:10 2009
Created on         : 10.7.9.245
```

IMPORTANT: Prior to restoring the backup, run 'tools sc dn' command on BOTH SC boards to make sure that Media Gateway software is stopped on both SC boards.

5. When prompted to confirm the restore operation, type **y** and press **Enter**. The restore process begins.

```
Restore? ([y]/n) : y
Please wait patiently until restore completes.
The process may take up to 10 minutes.
```

```
Extracting backup data... done
Uncompressing backup data... done
Uninstalling current SC software... done
Installing backup data... done
Repairing installation... done
```

Media Gateway software was successfully restored from the backup.

6. When the restore completes, you will be prompted to reboot the SC board. Type **y** at the prompt and press **Enter**.

```
This SC board must be rebooted!  
REBOOT now? ([y]/n) : y  
Reboot ...
```

7. The SC board reboots. It typically takes 2 minutes to complete the reboot process. The Media Gateway software starts automatically after the SC board completes the reboot process.
8. After the SC board completes the reboot process, re-connect to its CLI interface and login as a regular CLI user that you used to transfer the backup file (e.g. **acladmin**). Remove the backup file from the SC board via the following command:

```
client238::~~# rm backup_12jan2009.bk
```

9. On the SC board in Slot 2 (designated as the Standby board), repeat steps 4-8.

44.5 Automatic Backups

In addition to user-initiated backups described in 'Creating the Media Gateway Software Backup' on page 778 and 'Restoring Media Gateway Software from Backup' on page 783, the Media Gateway software periodically performs automatic backups.

Automatic backups are performed on a daily or weekly basis at a pre-defined maintenance time (typically at night, when the amount of traffic passing through the Media Gateway is relatively low). Automatic backups contain configuration data only (without binary files) and therefore are relatively small in size. Automatic backup files are stored in the **/backup** directory on both SC boards (they are initially created on the Active SC board and automatically replicated to the Standby SC board). Up to 100 last backup files may be preserved, thus allowing restoration of the Media Gateway's configuration to any of the specific historic backup point.

Automatic backups should be used to restore the Media Gateway configuration in case of severe malfunction or misconfiguration. The procedure for restoring the automatic backup is identical to the one described in 'Restoring Media Gateway Software from Backup' on page 783. The only exception being that there is no need to transfer the backup file from the safekeeping location to the SC board (because the files already reside in /backup directory on both SC boards).

➤ **To customize the Automatic Backup configuration:**

1. Click  to access the Media Gateway status screen.
2. In the Navigation pane, select **Management** and then in the configuration pane, click **Management Settings**; the Management Settings screen is displayed.
3. In the **Backup Settings** tab, configure the Automatic Backup parameters according to the table 'Automatic Backup Parameters' below.

Table 44-1: Automatic Backup Parameters

Parameter Name	Type	Provisioning Type	Description
Enable Automatic Backup	Yes, No	Instant	Enables or disables Automatic Backup functionality. Default: Enabled
Automatic Backup Mode	Enum Daily, Weekly	Instant	Defines the daily or weekly automatic backup mode. Default: Daily
Automatic Backup Day	Enum Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday	Instant	Defines the day of the week when Automatic Backup is performed. Default: Sunday

Parameter Name	Type	Provisioning Type	Description
Automatic Backup Hour	Integer 0-23	Instant	Defines the hour when Automatic Backup is performed. Default: 3 (corresponds to 3:00 AM)
Automatic Backup Minute	Integer 0-59	Instant	Defines the minute when Automatic Backup is performed. Default: 0 (corresponds to 3:00 AM)
Automatic Backup History Size	Integer 1-100	Online	Defines how many "history" backup files are stored in the /backup directory on the Active SC board. Default: 31

This page is intentionally left blank.

45 Hardware Replacement

This section provides instructions for replacing Mediant 8000 components (boards and modules) in case of hardware failure. Use EMS management interface or CLI to determine the cause of failure prior to performing these procedures. Contact AudioCodes Technical Support to order replacement hardware.

The section also contains instructions for adding a new hardware to the Mediant 8000 chassis. See "'Adding Media Gateway Boards to a Mediant 8000 System' on page 797.

45.1 Hardware Replacement Preliminaries

Before starting hardware replacement procedure, be sure to prepare all replacement components and tools to be used in advance.

45.1.1 ESD Requirements



Electrical Component Sensitivity

Electronic components on printed circuit boards are extremely sensitive to static electricity. Normal amounts of static electricity generated by clothing can damage electronic equipment. To reduce the risk of damage due to electrostatic discharge when installing or servicing electronic equipment, use anti-static earthing straps and mats.

➤ Before removing any hardware component from the Mediant 8000 chassis:

1. Locate the ESD (electrostatic discharge) connections on the Mediant 8000 chassis. See the diagrams in 'Front and Back Views of the ' on page 37 Mediant 8000.
2. Attach a wrist strap for electrostatic discharge (ESD) and connect it to an ESD connection on the chassis using a banana plug or an alligator clip.

45.1.2 Slot Assignment



Caution

Board types are assigned to specific slots (see 'Board Assembly Order' on page 87). The midplane behind the slots contains keys that are specific to the board types appropriate for the individual slots. Forcing a board into a slot for which the board is not keyed will damage the board and/or midplane. If a board does not easily slide in the full way, verify that it appropriate for this slot.

45.1.3 Empty Slots Cover Requirements

It is imperative to cover all unoccupied slots in both the front cage and the rear cage of the Mediant 8000 chassis with blank panels to maintain the mandatory high, internal airflow and to ensure continuous compliance with EMC standards.



Note: The front blank panels are baffled panels. Be sure to use this type of blank panel in the front of the chassis and use the blank panel without the baffle in the rear of the chassis only.

Figure 45-1: Baffled Blank Panel for Front Slots

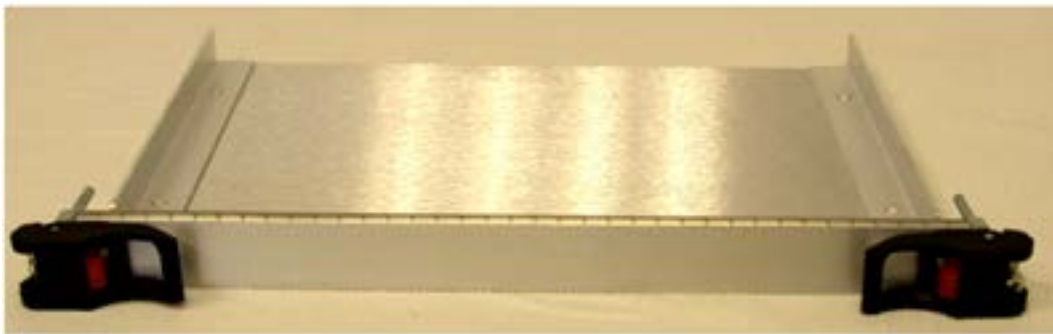


Figure 45-2: Blank Panel for Rear Slots



45.2 SC Board Replacement Procedure

In the unlikely event of a SC board failure, the Mediant 8000 automatically switches to another available SC board and notifies users with an alarm. Replace the failed board as soon as possible to restore the system to its engineered configuration. SC boards are hot-swappable, where the board can be inserted and removed when the Mediant 8000 is under power.

SC board replacement consists of the following steps:

- Replacing the failed SC board with a new board
- Installing the Operating System (OS) on the replaced SC board (this step may be typically skipped, because SC boards normally have OS pre-installed on them)
- Configuring the IP address on the replaced SC board
- Installing software on the replaced SC board and bringing it up

45.2.1 Replacing the Failed SC Board

This section describes how to replace the failed SC board.

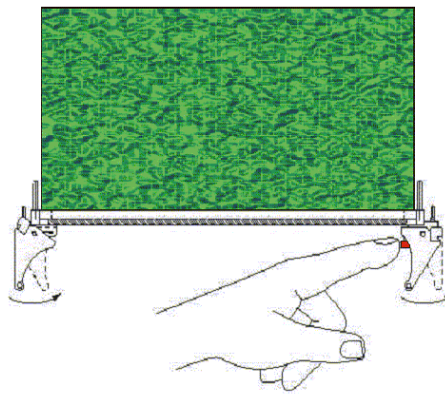


Note: This section describes hardware replacement procedures only. They must be followed by software installation and configuration as described in the following chapters.

➤ **To remove an SC board from the chassis, take these 3 steps:**

1. Unfasten the screws on the plate of the board.
2. Simultaneously press the red ejector buttons on the two black ejector/injector latches on both ends and wait 10 sec for the Hot Swap blue LED to light, indicating that the board can be removed.

Figure 45-3: Red Ejector Buttons on a Board



3. Pull on the two ejector/injector latches and ease out the board from the slot.

➤ To insert an SC board into the chassis, take these 6 steps:

1. Hold the board Vertical with the top of the board pointed upward.
2. With the black ejector/injector latches in the open (pulled out) position, insert the board in the slot, aligning the board on the grooves on each end.
3. Ease the board all the way into the slot until the ejector/injector latches touch the chassis. The blue hot-swap LED is lit.



Note: Push in the board until it is flush with the other boards. The SC board requires extra pressure to ensure it is pushed in back sufficiently.

4. Press the two black ejector/injector latches on both ends inward, toward the middle until you hear a click.
5. Wait for the hot-swap blue LED to turn off.
6. Fasten the screws on the front plate of the board to secure the board to the chassis and to ensure that the board has an earth connection to the chassis.

45.2.2 Installing the Operating System (OS) on the Replaced SC Board

The SC board typically has the proper version of the Operating System (OS) pre-installed on it. Therefore there is usually no need to install the OS on a replaced SC board.

In the unlikely event that your replacement SC board does not have the correct OS version installed, install the correct OS version as described in 'The Operating System on the SC Boards' on page [226](#).

45.2.3 Configuring IP Address on the Replaced SC Board

The replaced SC board must be configured to use the same IP address as the failed one. See 'Configuring the Basic IP Network Parameters of SC Boards' on page [117](#) for a detailed configuration procedure.

45.2.4 Installing the Software on the Replaced SC Board

The Media Gateway software must be installed on a replaced SC board.



WARNING

Be sure to install exactly the same Media Gateway software version on the replaced SC board as was installed on the original SC board prior to failure.

See 'Installing Mediant 8000 Software on the SC Board to Operate as the Standby board' on page 140 for a detailed installation procedure.

45.3 Media Gateway Board Replacement Procedure

In the unlikely event of a Media Gateway board failure, the Mediant 8000 automatically notifies users with an alarm. Replace the failed board as soon as possible to restore the system to its engineered configuration. Media Gateway boards are hot-swappable, meaning that the board can be inserted and removed when the Mediant 8000 is under power.

45.3.1 Replacing the Failed Media Gateway Board

The procedures for replacing the TP-6310 and 8410 Media Gateway boards are identical.

➤ To remove a Media Gateway board from the chassis:

1. In the EMS, lock the Media Gateway board to be replaced. For more information see 'Working with the Media Gateway Boards' on page 245.
2. Unfasten the screws on the plate of the board.
3. Gently pull the two black ejector/injector latches on both ends outwards (not actually removing the board) and wait for the Hot Swap blue LED to light, indicating that the board can be removed.
4. Pull on the two ejector/injector latches and ease out the board from the slot.

➤ To insert a Media Gateway board into the chassis:

1. Hold the board Vertical.
2. With the black ejector/injector latches in the open (pulled out) position, insert the board in the slot, aligning the board on the grooves on each end.
3. Ease the board all the way into the slot until the ejector/injector latches touch the chassis.
4. Press the two black ejector/injector latches on both ends inward, toward the middle until you hear a click.
5. The Blue hotswap LED is lit momentarily. (If the Blue LED does not turn off, see the 'Diagnostics' on page 832.)

6. Fasten the screws on the front plate of the board to secure the board to the chassis and to ensure that the board has an earth connection to the chassis.
7. Using one of the Media Gateway Board Definition Methods discussed above, in the EMS, define the board.
8. In the EMS, unlock the Media Gateway board that has been replaced. For more information, see Section 'Working with the Media Gateway Boards' on page 245.

45.3.2 Replacing the Media Gateway Board's RTM module

The procedures for replacing the 6310/RTM and 8410/RTM Media Gateway Board's RTM modules are identical.



Caution Laser

Note for the 6310/RTM/STM1-OC3, the SONET/SDH interfaces contain a Class 1 Laser device.

➤ To remove the Media Gateway board's RTM from the chassis:

1. In the EMS, lock the Media Gateway board of the RTM to be replaced. For more information see 'Working with the Media Gateway Boards' on page 245.
2. Remove all of the cables attached to the RTM.
3. Unfasten the screws on brackets at both ends of the panel that secure the board to the chassis.
4. Press the red ejector buttons on the two black ejector/injector latches on both ends.
5. Grasp the panel and ease the board out of the slot.

➤ To insert a Media Gateway board's RTM into the chassis:



Caution Laser

Note for the 6310/RTM/STM1-OC3, the SONET/SDH interfaces contain a Class 1 Laser device.

1. Hold the board Vertical.
2. With the black ejector/injector latches in the open (pulled out) position, insert the board in the slot, aligning the board on the grooves on each end.
3. Ease the board all the way into the slot until the ejector/injector latches touch the chassis.
4. Press the two black ejector/injector latches on both ends inward, toward the middle until you hear a click.

5. Fasten the screws on the front plate of the board to secure the board to the chassis and to ensure that the board has an earth connection to the chassis.

Connect the cables as detailed below.

45.3.2.1 Connecting Cables to Media Gateway's RTM Module

See 'Connecting to the PSTN Network' on page 122 for detailed instructions on connecting PSTN cables to Media Gateway boards and RTM modules.

45.4 Adding Media Gateway Boards to a Mediant 8000 System

You can add additional Media Gateway boards to a system that was originally ordered with less than the full capacity of Media Gateway boards.

➤ To add a Media Gateway board to a Mediant 8000 system:

1. Locate the desired empty slot in the Mediant 8000 chassis. See the constraints for adding Media Gateway board listed in the following section.
2. Insert the TP-6310 or 8410Media Gateway board into the designated slot in the front of the chassis. For more information, see Section 'Replacing Media Gateway Boards' on page 795.
3. Insert the RTM module – 6310/RTM or or 8410/RTM – into the designated slot in the rear of the chassis. For more information, see Section 'Replacing the Media Gateway Board's RTM Module' on page 800.
4. To add a board to the Media Gateway software, in the EMS, right-Click the slot and from the popup menu, select **Add Board**. See the **AddBoard** action described in 'Media Gateway Board Actions' on page 247.
5. Provision the Media Gateway board's parameters and relevant applications. See 'Configuring & Operating the Media ' on page 155Gateway for details.
6. When the configuration is complete, to unlock the Media Gateway board, right-Click it and from the popup menu, select **Maintenance>Unlock**.

45.4.1 Constraints for Adding Boards to the Mediant 8000 System

This section describes the constraints for adding boards to the Mediant 8000 system. For more information, see 'Board Assembly Order' on page [87](#).

45.4.1.1 TP-6310 Boards

Slots 7 to 8 and 11 to 17 are used for provisioning up to 9 TP-6310 boards (including the TP-6310 Redundant board in slot 17) according to the customer's requirements. The RTMs are located in the rear cage of the Mediant 8000 Media Gateway in the slot.

In less than a full configuration, place boards from slot 17 to 11 and then 8 to 7, adding boards from the highest slot number to the lowest slot number. Unused slots must be covered using the appropriate blank panel.

45.4.1.2 TP-8410 Boards

Slots 4 and 7 and 11 to 15 are used for provisioning up to 7 TP-8410 boards (including the TP-8410 Redundant board in slot 4) according to the customer's requirements. The RTMs are located in the rear cage of the Mediant 8000 Media Gateway in the slot.

In less than a full configuration, place boards from slot 15 to 11 and then 7 and 4, adding boards from the highest slot number to the lowest slot number. Unused slots must be covered using the appropriate blank panel.

45.4.2 Troubleshooting the Newly installed Media Gateway Board

In rare cases, a newly installed Media Gateway board may not return to service (become Enabled) after the **Unlock** action is performed in the EMS.

➤ **If this occurs, to solve the problem:**

1. In the Troubleshooting screen, change the Board Provisioning Mode parameter to MAC Address.
 - a. Click  to access the Media Gateway status screen.
 - b. In the Navigation pane, select **Troubleshooting** and then in the configuration pane, click **Troubleshooting Settings**; the Troubleshooting Settings screen is displayed.
 - c. Change the **Board Provisioning Mode** parameter to *MAC Address*.
2. Lock the Media Gateway board
 - a. Click  to access the Media Gateway status screen.
 - b. Select the newly added Media Gateway board and in the Action bar, click **Lock**.
3. Ascertain the Media Gateway board's MAC address, that is indicated on a sticker attached to the board.
4. In the Media Gateway board's Network Settings Screen, provision the ascertained MAC addresses.
 - a. Click  to access the Media Gateway status screen.
 - b. Select the newly added Media Gateway board and in the Action bar, click **Unlock**.
 - c. In the Navigation pane, select **Inventory** and then in the configuration pane, click **Media Gateway Info**; the Media Gateway Info screen is displayed.
 - d. Configure MAC Address parameter to match the ascertained MAC address.
5. Unlock the Media Gateway board.
 - a. Click  to access the Media Gateway status screen.
 - b. Select the newly added Media Gateway board and in the Action bar, click **Unlock**.
6. Wait up to 5 minutes until MediaGateway board completes restart and returns to service. When Media Gateway is ready for operation, its **Operational State** is changed to *Enabled* and board is color-coded *Red* in the EMS.
7. When you have completed the configuration, in the Troubleshooting screen return the **Board Provisioning Mode** parameter to *Geographical Address*.
 - a. Click  to access the Media Gateway status screen.
 - b. In the Navigation pane, select **Troubleshooting** and then in the configuration pane, click **Troubleshooting Settings**; the Troubleshooting Settings screen is displayed.
 - c. Change the **Board Provisioning Mode** parameter to *Geographical Address*.

45.5 SA/RTM Replacement Procedure

➤ **To remove an SA/RTM from the chassis:**

1. Remove the connected cables.
2. Unfasten the screws on the plate of the board.
3. Press the two red ejector buttons.
4. Pull on the two ejector/injector latches and ease out the board from the slot.

➤ **To insert an SA/RTM into the chassis:**

1. Hold the board Vertical with the top of the board pointed upward.
2. With the black ejector/injector latches in the open (pulled out) position, insert the board in the slot, aligning the board on the grooves on each end.
3. Ease the board all the way into the slot until the ejector/injector latches touch the chassis and it is flush with the other boards.
4. Press the two black ejector/injector latches on both ends inward, toward the middle until you hear a click.
5. Fasten the screws on the front plate of the board to secure the board to the chassis and to ensure that the board has an earth connection to the chassis.
6. Replace the cable connections.
7. From the EMS, perform a manual switchover so that the SC with the newly installed SA/RTM becomes the Active SC board.
8. Verify that the LEDs on the SA/RTM are lit *Green*.
9. In the EMS, verify that the status reports of the SC board of the replaced SA/RTM indicate that it is operating correctly.

45.6 Ethernet Switch Board Replacement Procedure

ES boards are typically pre-loaded with the required software and, therefore, can be inserted into the chassis followed by the lock/unlock procedure in the EMS, as described below.

45.6.1 Replacing the Ethernet Switch Board

This section describes how to replace the ethernet switch board.



Caution

Do not insert the ES-2 module while the ES/6600/RTM is inserted.

➤ To remove an Ethernet Switch board from the chassis:

1. In the EMS, lock the Ethernet Switch board to be replaced. For more information, see Section 'Working with the Ethernet Switch Boards' on page [261](#).
2. Unfasten the screws on the plate of the board.
3. Gently pull the two black ejector/injector latches on both ends outwards (not actually removing the board) and wait for the Hot Swap blue LED to light, indicating that the board can be removed.
4. Pull on the two ejector/injector latches and ease out the board from the slot.

➤ To insert an Ethernet Switch board into the chassis:

1. Hold the board Vertical with the top of the board pointed upward.
2. With the black ejector/injector latches in the open (pulled out) position, insert the board in the slot, aligning the board on the grooves on each side.
3. Ease the board all the way into the slot until the ejector/injector latches touch the chassis. The blue hot-swap LED is lit.
4. Press the two black ejector/injector latches on both ends inward, toward the middle until you hear a click.
5. Wait for the hot-swap blue LED to turn off.
6. Fasten the screws on the front plate of the board to secure the board to the chassis and to ensure that the board has an earth connection to the chassis.
7. In the EMS, unlock the Ethernet Switch board that has been replaced. For more information see 'Working with the Ethernet Switch Boards' on page [261](#).
8. In the EMS (after 6 minutes for ES/6600 and 1 minute for ES-2), verify that the Ethernet Switch board's **Operational State** is *Enabled*.

45.6.2 Replacing the Ethernet Switch RTM Module

This section describes how to replace the Ethernet Switch RTM module.

➤ **To remove an Ethernet Switch RTM from the chassis:**

1. In the EMS, lock the Ethernet Switch board of the RTM to be replaced. For more information see 'Working with the Ethernet Switch Boards' on page 261.
2. Remove the connected cables.
3. Unfasten the screws on the plate of the board.
4. Pull on the two ejector/injector latches and ease out the board from the slot.

➤ **To insert an Ethernet Switch RTM into the chassis:**

1. Hold the board Vertical with the top of the board pointed upward.
2. With the black ejector/injector latches in the open (pulled out) position, insert the board in the slot, aligning the board on the grooves on each end.
3. Ease the board all the way into the slot until the ejector/injector latches touch the chassis.
4. Press the two black ejector/injector latches on both ends inward, toward the middle until you hear a click.
5. Fasten the screws on the front plate of the board to secure the board to the chassis and to ensure that the board has an earth connection to the chassis.
6. Reconnect the cables according to the IP Separation configuration. See Section 'Ethernet Switch Boards' on page 72.
7. In the EMS, unlock the Ethernet Switch board of which the RTM has been replaced. For more information, see Section 'Working with the Ethernet Switch Boards' on page 261.
8. In the EMS, verify that the Ethernet Switch board's **Operational State** is *Enabled*.
9. In the EMS, double Click the Ethernet Switch board of the RTM that has been replaced. In the status screen that appears, verify that the uplink port's **Operational State** is *Enabled*.

45.6.3 Troubleshooting the ES/6600 Board Installation

If the **Operational State** of the replaced ES board remains *Disabled* (the board is displayed *Red* in the EMS) 10 minutes after inserting the board into the chassis, use the procedure below to restore service on the replaced ES board.



Note: The procedure described below configures a temporary IP address for the replaced ES board. This IP address is used only for the recovery of the ES board after a malfunction. As soon as the full service on the ES board is restored, the provisioned IP address becomes invisible to the other equipment in the IP network.

➤ **To configure a temporary IP address on the ES board:**

1. Connect to the Switch Board's RS232 console.
2. Log in using the username: **admin** and password: **password**.

```
Escape character is '^['.  
PTI CPC6600 (from application)...  
login: admin  
Password: password  
#
```

3. Configure the IP address on Ethernet Switch board (This configuration does not survive reset, hence you should immediately proceed to the software installation as described above).

```
# ip config sw0 10.1.1.35
```

4. In the EMS, open the ES board's Provisioning Screen and provision the same IP address as configured in the previous step. For more information, see Section 'Working with the Ethernet Switch Boards' on page 261.
5. Lock and unlock the ES board.
6. The ES board is reset and new software files will be loaded on it. After 10 minutes, the ES board should complete the restart and restore its service. When this occurs, ES board's **Operational State** is changed to *Enabled*.

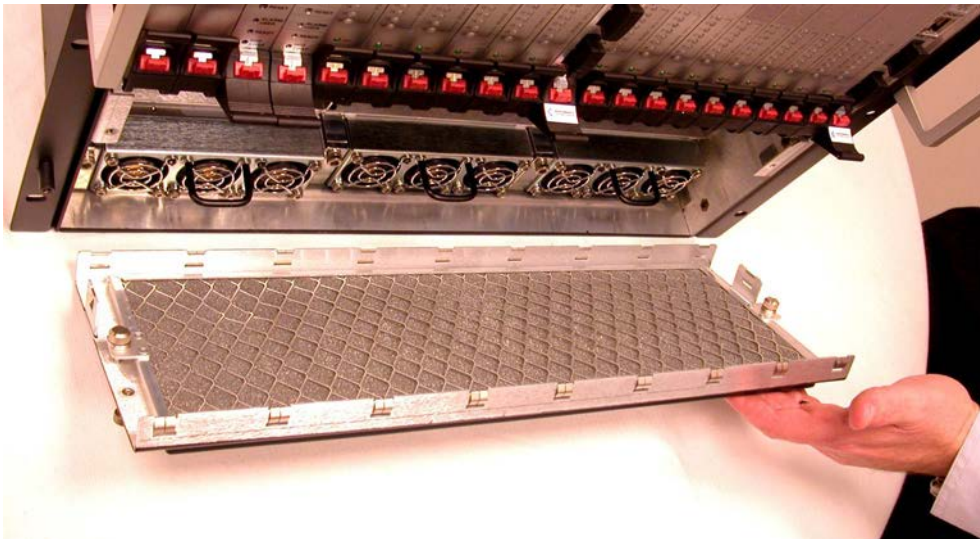
45.7 Power Supply Modules Replacement

This chapter describes the procedure for replacing the Power Supply Module (PS/DC/8K).

➤ **To remove a faulty power supply:**

1. Unfasten the screws of the grill and remove it to access the power supply modules.

Figure 45-4: Opening the Grill to Access the Power Supply Modules



2. Unfasten the screw to the left of the power supply to be removed.

3. Pull on the handle in the middle of the power supply.

Figure 45-5: Removing the PS from the Chassis



➤ **To insert a replacement power supply:**

1. Push in the power supply until the front panel is flush with the chassis plate. The *green* LED lights up.
2. Fasten the screws of the power supply.
3. Close the grill and fasten the screws at both sides.
4. In the EMS main status screen, verify that the Power Supply icon is *green* (as in the figure below). In addition, verify that the Power Supply Alarm is not displayed in the Alarms Browser screen.

Figure 45-6: Power Supply Icon in EMS Status Screen

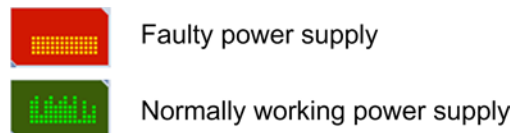


Figure 45-7: Power Supply Alarm in the Alarms Browser

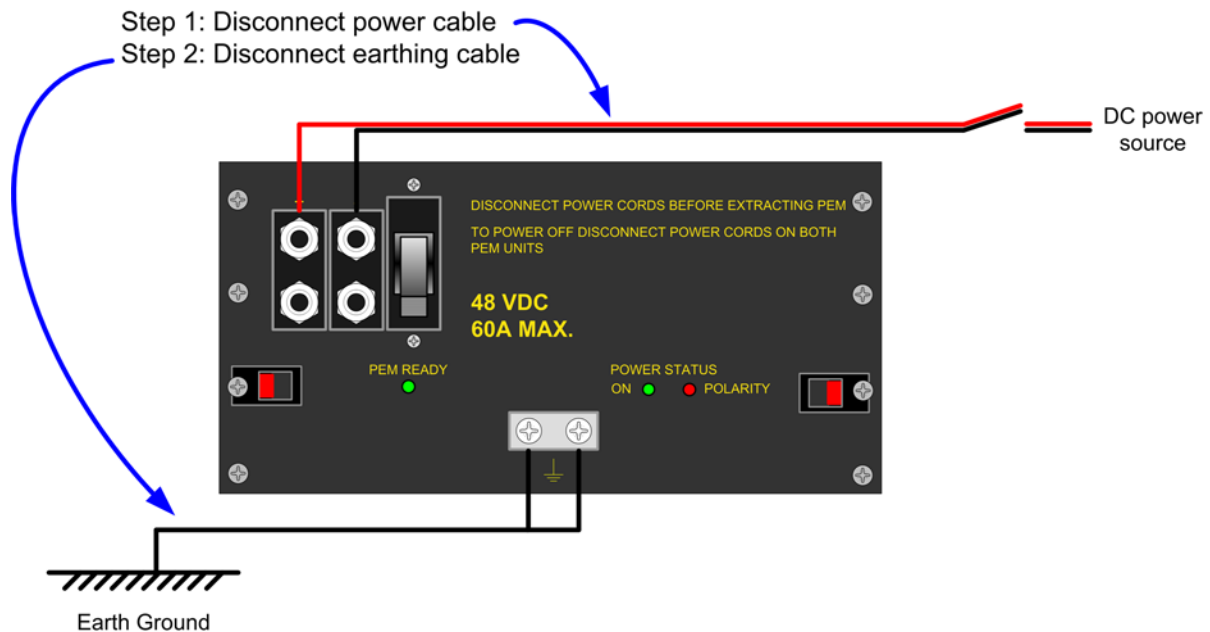
Alarm Browser 4						
View Level: Current Level Alarms						
Ack	Severity	Time	MG Name	Source	Alarm Name	Description
☐	minor	12:34:47 Jul 1...	Ram	SAT/PS/Middle	Power Supply Alarm	Power Supply cassette 2 failure
☐	major	12:34:47 Jul 1...	Ram	SystemClock/...	Operative State Change	SystemClock/TimingModule#2 is DISABLED
☐	minor	12:34:47 Jul 1...	Ram	Board#4	Admin State Change	Board#4 is LOCKED

45.7.1 Replacing the Power Entry Module

This section describes how to replace the power entry module.

➤ To remove a faulty PEM module:

1. Disconnect the power cable from the PEM module.
2. Disconnect earthing cable.



3. Release the screws on the front panel of the PEM module.
4. Release the latch, press the *red* button. Wait for the Swap Ready LED to turn *blue*.
5. Open the latch and slightly pull the PEM module out of the chassis. Wait for 30 seconds and then remove it completely.

➤ To insert a replacement DC PEM module:

1. Insert the replacement PEM module into its slot, until the front panel is flush with the chassis plate and close the latch.



Caution

Verify that the power cord is not connected to the PEM before inserting it.

2. Fasten the screws at both sides of the front panel.
3. Attach the earthing cables.
4. Verify that the power cable is connected to the power source and then connect the cable to the PEM module.
5. Verify that the PEM Power LED is *green*.

45.8 Replacing the Fan Tray Modules

This section describes how to replace the fan tray modules.



Note: To ensure high availability, two operational fan trays are required at all times. Do not leave a fan tray in a partially open position. Under no circumstances should you remove both fan trays at the same time.

➤ **To remove a faulty fan tray:**

1. Release the 2 screws on both sides of the panel covering the Fan Tray units.
2. Release the 2 screws on both sides of the Fan Tray unit.



Caution

When removing a fan tray unit, the fans continue to rotate at a high speed. Use caution not to touch the rotating fan blades.

3. Pull the fan tray unit outward by 2 cm.

Figure 45-8: Replacing the Fan Tray Unit



4. Wait for the fans to stop rotating and then remove the fan tray completely.

➤ **To insert a replacement fan tray unit:**

1. Insert the fan tray unit into its slot, until the front panel is flush with the chassis plate.
2. Secure the Fan Tray in its slot by fastening the screws at both ends of the fan tray unit.
3. Close the Fan Tray cover door and secure it to the chassis by fastening the thumb screws on the cover.

4. In the EMS main status screen, verify that the color of the icon that represents the Fan Tray is green. Verify that Fan Tray Alarm disappeared from the Alarms Browser screen.
5. In the EMS, open the Media Gateways' Advanced Properties screen, and in the Alarm Card Info tab verify that Fan Speeds are within the accepted range.

45.9 Replacing Air Filters

The NEBS compliant air filters should be replaced approximately every 90 days. The figure below indicates the location of the filters and shows the air filter partially removed from the Mediant 8000 chassis.



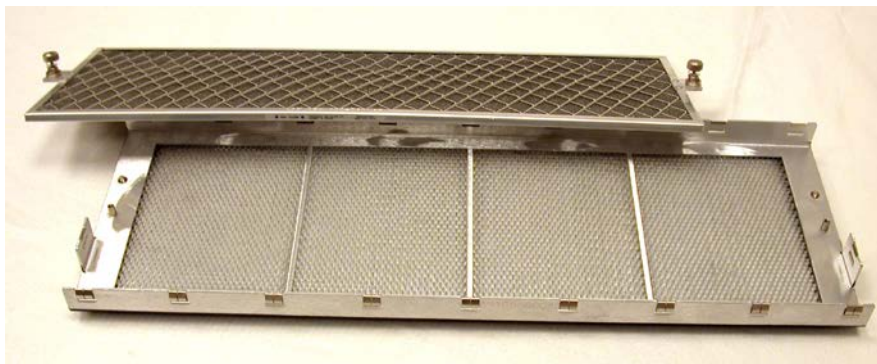
Caution

Be sure to prepare all of the equipment you need to replace the air filter before removing the existing air filter. It is imperative the chassis not remain without the fan tray unit for more than 60 sec.

➤ To remove the air filter:

1. On the front, bottom of the chassis, unscrew to screws at both ends of the grill.
2. Remove the grill.
3. Unscrew the nuts at each end of the air filter.
4. Pull out the filter.

Figure 45-9: Replacing the Air Filter



➤ **To reinsert the air filter:**

1. In the front filter holder, place the filter into the slot, lining up the holes at each end with the pins and fastening the nuts onto the pins.
2. Replace the cable rack, lining it up under the card cage and pushing it into its slot.
3. Fasten the screws at each end of the cable rack.
4. Note the direction-indicator arrow on the edge of the replacement filter. With the direction-indicator arrow in the correct position, place it on the grill so that the placement of the screws at both ends of the grill is aligned correctly.
5. Fasten the screws binding the filter to the grill.
6. Replace the grill on the chassis.
7. Fasten the screws at each end of the grill to the chassis.

This page is intentionally left blank.

46 Online Software Upgrade

The Online Software Upgrade provides a mechanism for upgrading the Mediant 8000 software to a newer version, while preserving the Media Gateway configuration and minimizing the affect on the Media Gateway service during the upgrade.

In this section, the following terms are used:

- **1st SC** – The SC board that is Active before starting the Software upgrade
- **2nd SC** – The SC board that is Standby before starting the Software upgrade

It is recommended to perform the Online Software Upgrade when the SC board in Slot 1 is the Active board and the SC board in Slot 2 is the Standby board. If required, perform SC switchover to achieve this configuration.

46.1 Overview

The Online Software Upgrade is performed when the Mediant 8000 Media Gateway is up and running. The Online Software Upgrade upgrades the software on all the Media Gateway components including:

- System Controller (SC) boards
- Media Gateway boards
- Ethernet Switch (ES) boards

The Media Gateway configuration is preserved throughout the upgrade procedure and the effect on the Media Gateway service is minimized.

After upgrading each major system component (e.g., the SC or Media Gateway board) the Online Software Upgrade process pauses and allows you to verify the basic functionality of the upgraded component. At these "stop points" you can decide whether to proceed with the upgrade or initiate a roll-back.

The Roll-back functionality enables you to return the Mediant 8000 Media Gateway to the pre-upgrade software version and configuration in case of any problem.

The Mediant 8000 Media Gateway continues its operation without interruption during the software upgrade of the SC and ES boards. However, certain calls may be affected during the upgrade of the Media Gateway boards, depending on the upgrade mode being used (see sections Hitless Upgrade Mode and Graceful Shutdown Mode below). To minimize the impact on the Mediant 8000 Media Gateway service, the Media Gateway boards are upgraded one at a time.

46.1.1 Hitless Upgrade Mode

Starting from Version 6.2, Hitless Upgrade mode is supported for the upgrade of Media Gateway boards. In this mode, activity switchover is performed between Normal and Redundant Media Gateway boards. As a consequence, established calls are not affected during the Media Gateway boards upgrade. Calls that have not been established may be dropped.

Although Hitless Upgrade Mode is the preferred upgrade mode, it may be not available due to one of the following reasons:

- Redundant Media Gateway board is not available or out of service during the upgrade;
- Configuration of the specific Media Gateway board doesn't allow hot redundancy;
- New software doesn't support Hitless Upgrade mode for specific current software version;

In all above cases, Graceful Shutdown mode will be used for upgrading affected Media Gateway boards. For more information, see Section 'Graceful Shutdown Mode' on page [812](#).

46.1.2 Graceful Shutdown Mode

Graceful Shutdown mode is available for all Media Gateway boards' without any dependency on the Redundant Media Gateway board's availability or any specific configuration. In this mode, each Media Gateway board is upgraded after a definable Graceful Shutdown period. During this period, no new calls are established on the Media Gateway board; however, the remaining active calls are allowed to complete normally. The Graceful Shutdown period ends when either there are no more active calls on the Media Gateway board, or the defined time period ends. If the defined time period ends and there are still active calls, these calls are dropped and the Media Gateway board is restarted.

The Graceful Shutdown period helps to ensure that a negligible number of calls are dropped during a Media Gateway board's upgrade. In any case, the Media Gateway capacity is never reduced by more than a single Media Gateway board's capacity. To further minimize the effect of a Media Gateway board upgrade, it is recommended that you distribute customer trunks across at least two different Media Gateway boards.



Note: To further minimize call traffic loss during the Media Gateway boards' upgrade, perform this procedure when low call traffic is known to occur.

46.2 Pre-Upgrade Configuration Backup

Prior to performing the Online Software Upgrade, you must manually perform a full Media Gateway software backup and store it on a third-party server. This backup maintains the ability to rollback the Media Gateway to the pre-upgrade state in the event of abnormal hardware and/or software failure during the upgrade.



Note: This backup should be used in emergency cases only, since Online Software Upgrade has a built-in rollback functionality that enables roll-back to the pre-upgrade software version and configuration.

For details on performing a backup, see 'Media Gateway Software Backup/Restore Procedures' on page 774.

46.3 Preparing for the Online Software Upgrade

46.3.1 Preparing the Media Gateway

The following conditions must be met prior to starting the Online Software Upgrade procedure:

- Both SC boards are in service.
- Both ES boards are in service and have up-links properly connected.
- All Media Gateway boards are either in service or manually LOCKED.



Note: There is no HA functionality available during Online Software Upgrade, therefore all Media Gateway components must be stable during the upgrade. Remove or LOCK any unstable board prior to starting the upgrade.

46.3.2 Preparing the IP Network

To perform Online Software Upgrade, the IP network must be configured to provide a bandwidth rate of at least 2 Mbps between the EMS server and the Media Gateway chassis (SC boards).

The IP network speed mainly affects the time of the Media Gateway Software package transfer between the EMS client, the EMS server and the SC boards. Use the following formula to estimate the time of the Media Gateway Software package transfer by the available IP network bandwidth:

$$T_{upload} = \frac{25}{B} \text{ min}$$

where B is available bandwidth in Mbps.

For example, for a bandwidth rate of 2 Mbps, the Media Gateway Software package transfer takes approximately 13 minutes. Similarly, for a bandwidth rate of 10 Mbps, the transfer takes approximately 2.5 minutes.

46.3.3 Verifying that the Online Software Upgrade is Supported

Make sure that an upgrade from the specific Media Gateway version is supported. AudioCodes officially supports upgrade to Version 6.6 from the last two major software versions (Version 6.2) only.

For additional information and clarifications contact Tech Support.

46.3.4 Planning the Maintenance Time Period

To minimize the effect of any problem that may occur during Online Software Upgrade, it is recommended to perform the upgrade during the *upgrade maintenance time period* when low call traffic is known to occur.

It is important to properly estimate the time of the Online Software Upgrade and plan the *upgrade maintenance time period* accordingly, so that there is enough time for both the upgrade itself and for the appropriate acceptance tests of the new software version.

The time of the Online Software Upgrade may be estimated using the following formula (all values are measured in *minutes*):

$$T_{upgrade} = 15 \text{ min} + 2 \times T_{upload} + T_{MGboard} \times N_{MGboard} + 2 \times T_{OSpatch} + 2 \times T_{ESboard}$$

where:

- T_{upload} is the time of the Media Gateway Software package transfer over the network. The transfer is performed twice – first between the EMS client and the EMS server (during version upload to the EMS server's "**Files Manager**") and after that between the EMS server and the SC boards (during the Welcome stage of the Online Software Upgrade Wizard). The time may be estimated based on the available IP network bandwidth as described in 'Preparing the IP Network' on page 814. To reduce this time, transfer software package prior to the *maintenance time period* as described in 'Transferring the SC Software Package to the SC Boards' on page 823.
- $N_{MGboard}$ is the number of unlocked Media Gateway boards. If the Media Gateway is not "in service", you may lock the entire Media Gateway (and all of its boards) prior to starting the Online Software Upgrade to minimize the upgrade time. After the upgrade is finished, unlock the Media Gateway to complete upgrade of Media Gateway boards to the new software version.
- $T_{MGboard}$ is the time of a Media Gateway board's upgrade. For Hitless Upgrade mode, it approximately equals 5 minutes. For Graceful Shutdown mode, it may be calculated using the following formula $T_{MGboard} = 2 + T_{GracefulShutdown}$ where $T_{GracefulShutdown}$ is the Graceful Shutdown time (in minutes) that is configured in the Online Software Upgrade Wizard's "Welcome Questionnaire" screen. The default value of Graceful Shutdown time is 6 minutes. To reduce the Media Gateway board's upgrade time, configure a smaller Graceful Shutdown period.
- $T_{OSpatch}$ is the time required for OS patches installation on a single SC board. OS patches must be installed on both SC boards. The Online Software Upgrade process determines the exact number of OS patches to be installed and indicates the number at the early stages of the Online Software Upgrade wizard, together with the estimated installation time. If you upgrade between major software versions on SC Rev.1 boards (using the Solaris OS), the OS patch installation may take more than 1 hour on each SC board. For SC Rev.2 boards (using the Linux OS), the OS patches installation typically takes less than 5 minutes. To reduce the time of OS patches installation on SC Rev.1 boards, pre-install the OS patches as described in 'Pre-installing OS Patches' on page 817.
- $T_{ESboard}$ is the time of ES board's upgrade. If you upgrade between major software versions, it takes approximately 6 minutes to upgrade each ES board. However, if you are upgrading between minor software versions (maintenance releases) and the version of ES board's software is not altered, this value is zero (no upgrade of ES boards is needed).

For example, you can use the above formula to estimate a time of the upgrade of the Mediant 8000 chassis with SC Rev.1 boards (using the Solaris OS) and 3 Media Gateway boards in a typical IP network, as follows:

$$T_{upload} = 2.5 \text{ min}$$

$$N_{MGboard} = 3$$

$$T_{MGboard} = 4 \text{ min}$$

$$T_{OSpatch} = 60 \text{ min}$$

$$T_{ESboard} = 6 \text{ min}$$

$$T_{upgrade} = 15 + 2 \times 2.5 + 4 \times 3 + 2 \times 60 + 2 \times 6 \text{ min} \cong 2h \ 45 \text{ min}$$



Note: Even when you choose Hitless Upgrade as the preferred upgrade mechanism, some Media Gateway boards may be upgraded via the Graceful Shutdown mechanism (for more information, see Section 'Overview' on page [811](#)). Therefore, when you plan a maintenance time period, perform estimations of the Graceful Shutdown mechanism scenario as well.

46.3.5 Pre-installing OS Patches

When upgrading between major software versions, a considerable amount of OS patches must be installed on each SC board. These OS patches provide better security and overall system stability.

The time of the OS patches installation varies depending on the hardware revision of the SC boards installed in your chassis. For SC Rev.1 boards, the OS patches installation may take up to 1 hour for each SC board. For SC-.2 boards, the OS patches installation typically takes less than 5 minutes.



Note: Upgrade between major software versions on a chassis with SC Rev.1 boards (using the Solaris OS) may take more than 3 hours due to the amount of OS patches that must be installed on each SC board. Plan your *upgrade maintenance time period* accordingly or pre-install the OS patches prior to starting the upgrade as described in this section.

To reduce Online Software Upgrade time, you may pre-install OS patches on both SC boards prior to starting the Online Software Upgrade. The pre-installation of OS patches does not interrupt Media Gateway service. Old software continues to run normally on a system with new OS patches installed.

The Online Software Upgrade is significantly faster if OS patches are pre-installed beforehand. It will typically take approximately 1 hour depending on the amount of Media Gateway boards and the configured Graceful Shutdown period.

See 'Installing OS Security Patches from a Latest Installation Package' on page [313](#).

46.3.6 EMS Verifications

Before performing the Online Software Upgrade, verify the following in EMS:

- Both SC boards are **Unlocked** and **Enabled** (boards are color-coded *Green* in the EMS GUI).
- Both Ethernet Switch (ES) boards are **Unlocked** and **Enabled** (boards are color-coded *Green* in the EMS GUI).
- All Media Gateway boards are either **Unlocked** and **Enabled** (boards are color-coded *Green* in the EMS GUI) or **Locked** (boards are color-coded *Gray* in the EMS GUI).

46.3.6.1 Configuring the EMS and ROOT Passwords of the Mediant 8000 in the EMS

The EMS server uses **ems** and **root** user accounts to communicate with SC boards during the Online Software Upgrade. Therefore SC boards **ems** and **root** user passwords must be properly configured in the EMS prior to starting the Online Software Upgrade.

Default passwords of **ems** and **root** users on SC boards match the default settings of the EMS server. However for security reasons it is recommended to change these passwords to some other value. See 'Changing the Password of EMS User' on page 365 and 'Changing the ROOT User Password' on page 362 for detailed instructions on how to change **ems** and **root** passwords.

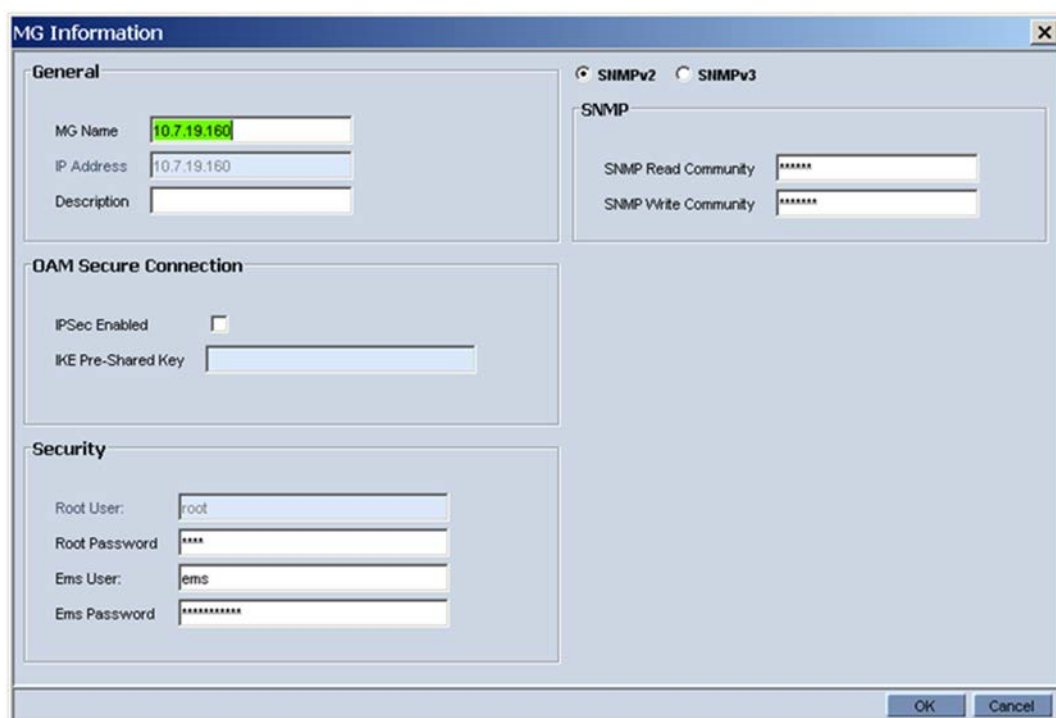


Note : Both SC boards must have the same **ems** and **root** passwords configured.

➤ To configure the EMS and ROOT user passwords in the EMS:

1. Select the Media Gateway in the MG Tree.
2. Right-click the specific Gateway and from the pop-up menu select **Details**; the MG Information dialog screen is displayed.

Figure 46-1: MG Information dialog



The MG Information dialog box is shown with the following fields and controls:

- General Tab:**
 - MG Name: 10.7.19.160
 - IP Address: 10.7.19.160
 - Description: (empty)
- DAM Secure Connection Tab:**
 - IPSec Enabled: ☐
 - IKE Pre-Shared Key: (empty)
- Security Tab:**
 - Root User: root
 - Root Password: ****
 - Ems User: ems
 - Ems Password: ****
- SNMP Section:**
 - SNMPv2 (selected) / SNMPv3
 - SNMP Read Community: ****
 - SNMP Write Community: ****
- Buttons:** OK, Cancel

3. In the **Ems Password** field, change the password to match the current password for the **ems** user configured on both SC boards.
4. In the **Ems User** field, ensure that the **ems** user name is set.
5. In the **Root Password** field, change the password to match the current password for the **root** user configured on both SC boards.
6. Click **OK**.

46.3.6.2 Adding the Media Gateway Software to the EMS Server

The Media Gateway software package must be added to the EMS Files Manager prior to starting the Online Software Upgrade. During this process, the Media Gateway software package is transferred from the EMS client to the EMS server. No affect on the Media Gateway operation occurs during this transfer.

The Media Gateway software package transfer takes a few minutes in a typical IP network environment (with 10 Mbps or better bandwidth). However, it may take much longer if the IP network connection between EMS server and client has limited bandwidth. Therefore, to minimize the upgrade maintenance time, it is recommended to add the Media Gateway software package to the EMS server well in advance.

➤ **To add the Media Gateway Software to the EMS server:**

1. Insert the Installation CD into the CD-ROM drive of your PC.
2. In the EMS menu, select **Tools -> Software Manager**.



3. Click the **Add File** icon; the Add Files dialog is displayed.
4. In the "M5K/M8K/IPM5K/IPM8K Software" pane, select the EMS file (e.g. tg_Version 6.6.16.ems) and the installation package file (e.g tg_Version 6.6.16.install) located on the Installation CD and press OK.

46.4 Performing the Online Software Upgrade

The Online Software Upgrade Wizard guides you through the Online Software Upgrade process. It includes the following stages:

1. Starting the Online Software Upgrade Wizard
2. Welcome Questionnaire
3. Upgrading the 2nd SC Board
4. Upgrading the Media Gateway Boards
5. Upgrading the ES boards
6. Upgrading the 1st SC Board
7. Finish

The upgrade process pauses after completing each of the major stages. You may perform some tests to verify that upgrade proceeds as expected and click **Next** to continue to the next stage.

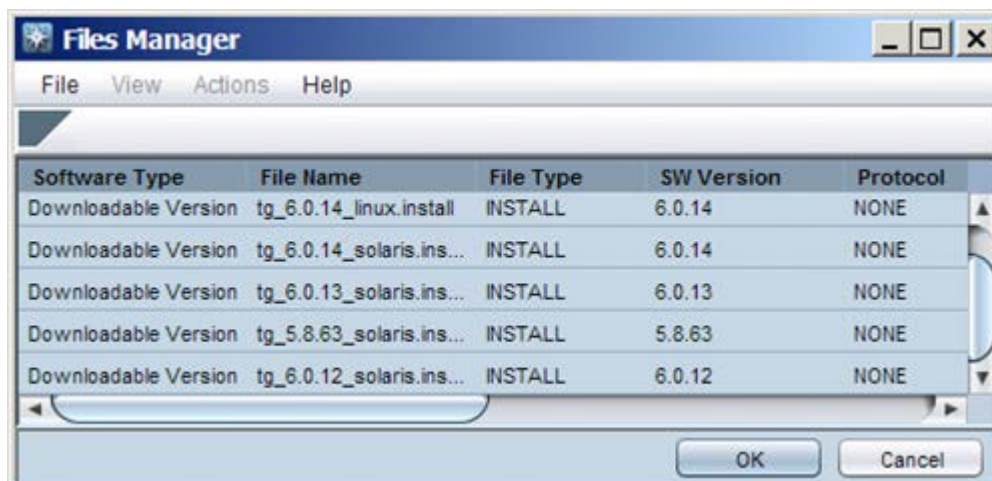
46.4.1 Starting the Online Software Upgrade Wizard

The Online Software Upgrade is performed via the Online Software Upgrade Wizard that is opened from the EMS client application. A single instance of the Online Software Upgrade Wizard performs the upgrade of the specified Media Gateway. Multiple instances of Online Software Upgrade Wizard may be opened for upgrading multiple Media Gateways at the same time.

➤ **To start the Online Software Upgrade Wizard:**

1. Click the  button to access the Media Gateway status screen.
2. In the Action bar, select **Sw Upgrade**; the Files Manager screen is displayed.

Figure 46-2: File Manager Screen



3. In the Files Manager screen, select the Media Gateway software version to which you want to upgrade and click **OK**. The Software Upgrade Wizard opens and guides you through the process.

46.4.2 Welcome Questionnaire

The Welcome Questionnaire screen contains basic configuration parameters that affect the software upgrade process.

Figure 46-3: Welcome Questionnaire

The screenshot shows the 'Online Software Upgrade Wizard' window. On the left, a 'Wizard Stages' pane lists: Welcome (selected), Secondary SC Upgrade, VoP Boards Upgrade, Switch Boards Upgrade, Primary SC Upgrade, and Finish. The main area contains a welcome message and a list of parameters to be configured:

- VoP Boards Upgrade Mechanism: Hitless Upgrade (dropdown)
- VoP Boards Upgrade Mode: Non-interactive (dropdown)
- Graceful Shutdown Timeout (in sec): 300 (text input)
- Graceful Shutdown Timeout for Abort (in sec): 60 (text input)

A note states: 'Note: Graceful Shutdown Timeouts are counted independently for each VoP board.' At the bottom right are 'Abort' and 'Next >>' buttons. Below the main area is a 'Summary' section with a table header: Action, Time, SC IP, Action Description, and Repair Action.

In this screen, configure the following parameters:

- **VoP Board Upgrade Mechanism** – preferred upgrade mechanism used for upgrading the Media Gateway boards. The following options are available:
 - **Hitless Upgrade** – Media Gateway boards are upgraded via activity switchover between normal and redundant Media Gateway boards; all established calls are preserved.
 - **Graceful Shutdown** – Media Gateway boards are upgraded one-by-one; a Graceful Shutdown mechanism is used to minimize amount of the affected calls.

When the Hitless Upgrade mechanism is selected, it is still possible that the Graceful Shutdown mechanism will be used for certain Media Gateway boards. For more information, see Section 'Overview' on page 811.

- **VoP Board Upgrade Mode** – level of user interaction while upgrading Media Gateway boards; the following options are available:
 - **Non-Interactive** - the upgrade process moves to the next Media Gateway board without any user interaction; user is informed when all Media Gateway boards complete the upgrade.
 - **Pause after the first Media Gateway board** – the upgrade pauses after the first Media Gateway board is upgraded; the user may test the system to ensure that the first Media Gateway board's upgrade was successful before upgrading the remaining Media Gateway boards.
 - **Pause after each Media Gateway board**—the upgrade pauses after each Media Gateway board is upgraded.; the user controls the start time for each of the Media Gateway board upgrades and thus may further minimize the amount of calls affected by the upgrade process.
- **Graceful Shutdown Period (sec)** - the amount of time allowed for calls to end before upgrading each Media Gateway board via the Graceful Shutdown mechanism. This parameter has no affect when the Media Gateway board is upgraded via the Hitless Upgrade mechanism. During the Graceful Shutdown Period (if it is used), the Media Gateway board accepts no new calls, and at the end of this period all remaining calls are dropped.
- **Graceful Shutdown Period for Abort (sec)** – graceful shutdown period that is used during rollback sequence when user presses the Abort button.



Notes:

- Set **Graceful Shutdown Period** parameter to the smallest applicable time, since it directly affects the total time of the upgrade process and new calls are not established on the specific Media Gateway board during this time.
- Even when you choose Hitless Upgrade as a preferred upgrade mechanism, some Media Gateway boards may be upgraded via Graceful Shutdown mechanism (for more information, see Section 'Overview' on page 811). Therefore, set proper value of **Graceful Shutdown Period** and estimate required worst-case upgrade maintenance time.
- Rollback sequence always uses the Graceful Shutdown mechanism. Therefore always set proper value for **Graceful Shutdown Period for Abort** parameter.

46.4.3 Transferring the SC Software Package to the SC Boards

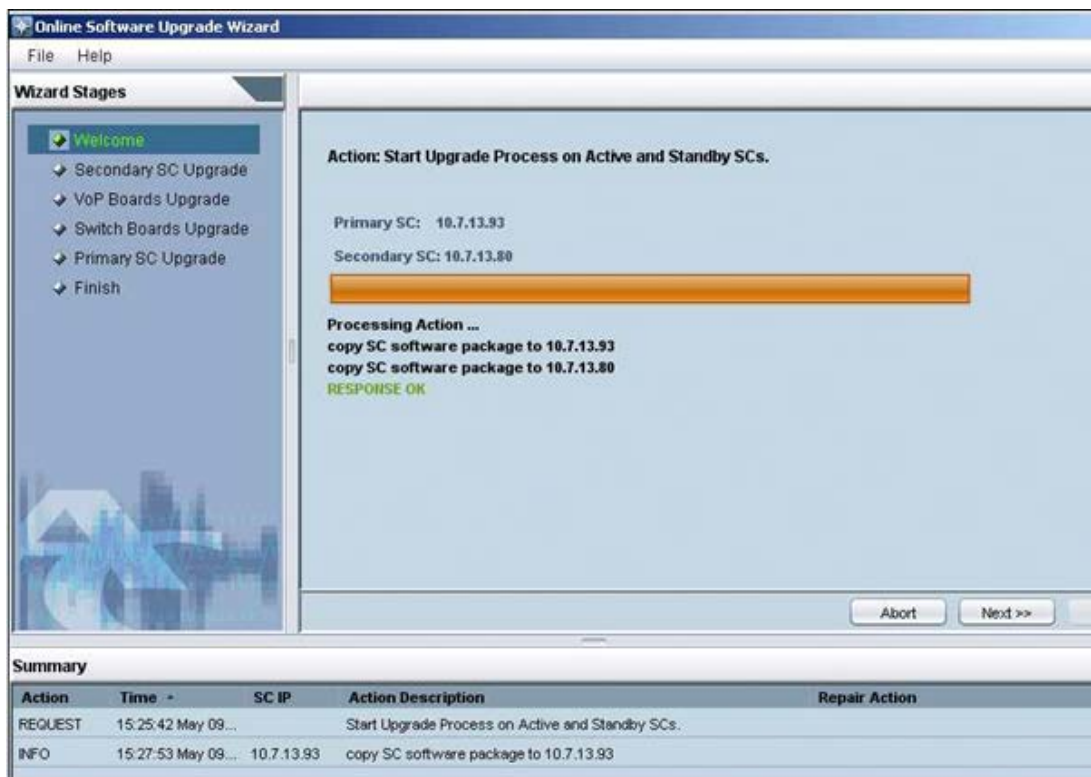
After clicking the **Next** button in the Welcome Questionnaire screen, the SC software package is transferred from the EMS server to both SC boards. This operation takes a few minutes in a typical IP network environment (with 10 Mbps or better bandwidth). However, it may take much longer if the IP network connection between the EMS server and the SC boards has limited bandwidth.

If IP network connection between EMS server and the SC boards has limited bandwidth, you may perform the following workaround to reduce the time of the Online Software Upgrade within the *upgrade maintenance time period*.

➤ **To reduce the time of the Online Software Upgrade within the maintenance time period, perform this workaround:**

1. Well in advance of the *upgrade maintenance time period*, activate the Upgrade Wizard.
2. Follow the wizards screen up to the stage where the Media Gateway software package has been transferred to the SC boards (during that stage the Media Gateway operation is not affected). The position of the Wizard screens to watch out for is shown below.

Figure 46-4: Start Upgrade Process



3. When the software package transfer is complete, the Next button is activated.



WARNING

DO NOT click **Next**. Instead, proceed with the steps below.

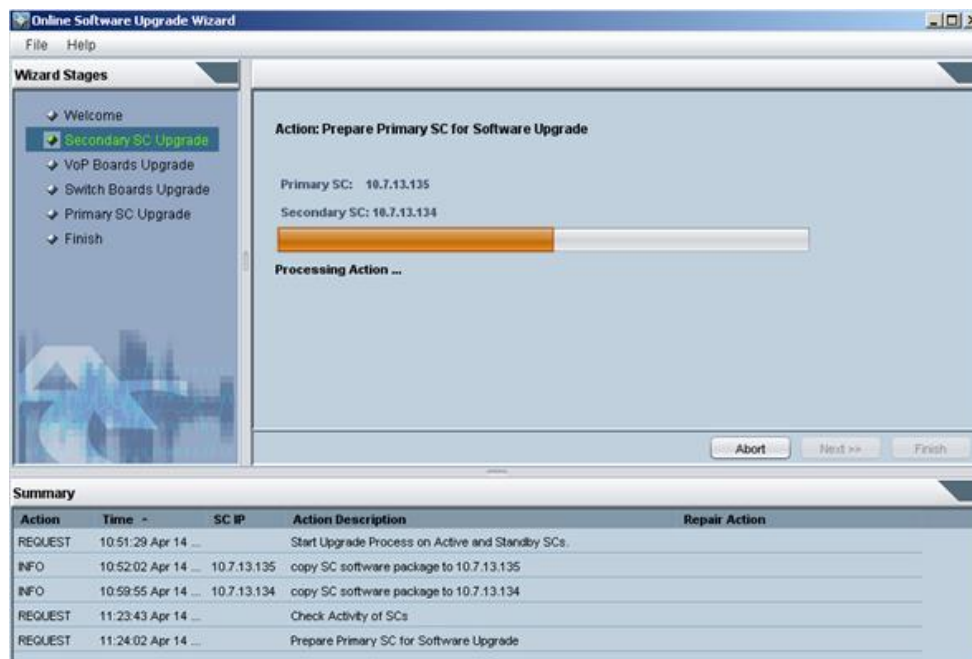
4. To close the Upgrade Wizard, click the  button (in the top-right corner). Now you are ready for the commencement of the *upgrade maintenance time period*.
5. When the *upgrade maintenance time period* begins, re-open the Upgrade Wizard as described in 'Starting the Online Software Upgrade Wizard' on page 820.
6. The upgrade process continues from the step at which it left off earlier.

46.4.4 Upgrading the 2nd SC Board

In the first stage, the 2nd (initially Standby) SC board's software is upgraded. When upgrade on this board is completed, a switchover action occurs which exchanges Active/Standby status between the SC boards. The 2nd SC board becomes the Active board and the 1st SC board becomes the Standby SC board. Thereafter, the 2nd SC board (now the Active SC board) manages the upgrade process of the Media Gateway boards and Ethernet Switch (ES) boards.

Following the upgrade of the Media Gateway boards' software, the software upgrade is then performed on the 1st SC board which is now the Standby SC board.

Figure 46-5: Upgrading the 2nd SC Board



When you upgrade between major software versions, a large number of OS patches are installed on the SC boards during the "SC board upgrade" stage. These OS patches provide better security and overall system stability. For SC Rev.1 boards (using the Solaris OS), the OS patches installation may take up to 1 hour to complete on each SC board. No user interaction is required. For SC Rev.2 boards (using the Linux OS), the OS patches installation typically takes less than 5 minutes.

For subsequent minor upgrades (between maintenance releases), the "SC board upgrade" phase is considerably faster because all required OS patches are already installed.



Note: An upgrade between major software versions on a chassis that uses SC Rev.1 boards (using the Solaris OS) may take more than 3 hours due to the OS patches installation. Plan your upgrade maintenance time period accordingly or pre-install OS patches as described in 'Pre-installing OS Patches' on page [817](#).

After the 2nd SC board is upgraded, you can open the EMS and inspect the new Media Gateway configuration and the status of the Media Gateways components. The following statuses should be displayed at this stage of the upgrade; they do not indicate any malfunction:

- The Media Gateway is marked as "Upgrade In Progress".
- 1st SC board (initially Active) is marked as failed (Unlocked/Disabled).
- 2nd SC board (initially Standby) is marked as Active (Unlocked/Enabled).
- Both ES boards are marked as failed (Unlocked/Disabled).

46.4.5 Upgrading the Media Gateway Boards

The Media Gateway boards are upgraded one after another starting from the lowest slot number. Redundant boards are last to be upgraded.

The affect on the active calls that are handled by the specific Media Gateway board depends on the upgrade mechanism – Hitless Upgrade or Graceful Shutdown. For more information, see Section 'Online Software Upgrade-Overview' on page 811 and 'Starting the Online Software Upgrade Wizard' on page 820.

Depending on the options you chose in the Welcome Questionnaire (see 'Welcome Questionnaire' on page 821) the upgrade process may pause after upgrading the first or every Media Gateway board. If you choose to do so, you may perform some tests to verify that the upgrade of a specific Media Gateway board succeeded prior to continuing with the next board.



Note : Media Gateway boards in a locked state are skipped by the Online Software Upgrade Wizard. They will be automatically loaded with a new software version as soon as they are unlocked (even after the Upgrade Wizard is no longer running).

46.4.6 Upgrading the ES Boards

The Ethernet Switch boards are upgraded one after another starting from the standby ES board (the ES board that functions as a standby board when the Online Software Upgrade is started).

After the "ES Board Upgrade" stage is completed, it is recommended to perform basic tests to verify that the new software version, that is currently applied to all boards, except the 1st SC board (which was initially Active, however is currently Standby), functions correctly. After completing these tests decide whether to proceed with the Upgrade or to Rollback to the previous software configuration.

46.4.7 Upgrading the 1st SC Board

Finally the 1st SC board (initially Active, however currently Standby) is upgraded to the new version. The upgrade may take considerable time if OS patches need to be installed on the SC board and the board is of the SC Rev.1 hardware type (using the Solaris OS). Use the same workaround as described in "Upgrading the 2nd SC Board" on page 824 to minimize this time.

When upgrade of the 1st SC board is completed, SC activity switchover is performed to return the system to its initial configuration – i.e. the 1st SC board is Active and 2nd SC board is Standby.

46.4.8 Finish

Click **Finish** to close the Software Upgrade Wizard.

46.5 After Completing the Online Software Upgrade



Note: After completing the Online Software Upgrade, perform software backup as described in 'SC Software Backup/Restore Procedures' on page [774](#) to assure backup availability should it be required later.

After you complete the Online Software Upgrade Wizard, the Media Gateway software and all of its components are upgraded to the new software version. However, some new features of the software may not be automatically activated.

The following table lists the most important features of the Version 6.6 software that are not automatically activated when you upgrade from earlier major versions. You should manually activate these features as described in the relevant section.

Table 46-1: New Features of Version 6.6 Software that must be Manually Activated after Upgrading from an Earlier Version

Feature Name	Detailed Description
Remote access by root user	Remote access by root user is disabled on newly installed Version 6.6 software. However, when you perform upgrade from an earlier software version where remote root access was enabled, the configuration remains unchanged to simplify the transition to the new software. After completing the Online Software upgrade, you must manually disable remote access by root user as it poses a severe security risk. For more information, see Section 'Disabling a Direct Remote Login' on page 311. Ensure that at least one CLI user is defined on both SC boards and provisioned with a known password. Otherwise, you will be unable to establish connection with the SC board's terminal over the IP network. For more information, see Section 'Command Line Interface' on page 107.

46.6 Rollback

At any time during an upgrade process, you can perform a rollback to the previous software configuration by pressing the **Abort** button in the Online Software Upgrade Wizard. In addition to that, the EMS automatically triggers a rollback in case of abnormal upgrade process failure.



Note: Rollback is triggered by pressing the **Abort** button and not the  button (in the top-right window corner).

Rollback is graceful at **any** stage. Only those Media Gateway boards that were upgraded to the new software version are reset. The reset is done gracefully – similar to the way the upgrade is performed via Graceful Shutdown mechanism. The ES boards are downgraded to the previous version automatically one by one – without any affect on the service (for more information, see Section 'Overview' on page [811](#)).



Note: The **Hitless Upgrade** mechanism is not supported for rollback. Rollback is always performed via the **Graceful Shutdown** mechanism.

46.7 Software Upgrade/Rollback Troubleshooting

If you experience an unexpected software or hardware problem during online software upgrade (e.g., if the PC on which the EMS client runs, crashes, or the network connection to the media Gateway is lost) and because of the failure you can neither complete nor abort the online software upgrade, you must perform a manual rollback to the previous software configuration.



Note: Prior to starting the Manual Rollback, verify if upgrade can be recovered from the specific scenario as described in the previous section.

46.7.1 Performing a Manual Rollback to the Previous Software Configuration

This section describes how to perform a manual rollback to the previous software configuration.

➤ **To perform a manual rollback to the previous software configuration:**

1. Close the EMS Upgrade Wizard screen.
2. Connect to *both* SC boards via Telnet, SSH or Console (see 'Command Line Interface' on page 107)
3. Login as **root** user. If you are performing Online Software Upgrade from Version 6.2 or an earlier software version, you may directly login as **root** user over the remote IP connection (Telnet or SSH). Otherwise, see 'Command Line Interface Users' on page 113.
4. To stop the Media Gateway software on *both* SC boards, type **tools sc dn** and press **Enter**.

```
client208::~~# tools sc dn
```



Note: Stop the Media Gateway software on both SC boards as described above.

5. If you can not connect via Telnet/SSH to some SC board, take these 3 steps:
 - a. Reboot the SC board by pressing **RESET** button on its front panel or pulling it out of the chassis and re-inserting it back in.
 - b. Wait for 5 minutes until SC board completes the reboot.
 - c. Login to the board via Telnet/SSH as **root** user and stop the Media Gateway software on it as described in step 4.
6. If you still cannot connect to a specific SC board via Telnet/SSH after completing the previous step, then it's highly likely that there is a hardware failure on the board or a severely incorrect software configuration. Remove the failed SC board from the chassis. For details on replacing a failed SC board, see 'SC Board Replacement Procedure' on page 793.



Note: It is important to stop the Media Gateway software on *both* of the SC boards and remove the failed SC boards from the chassis prior to proceeding to the next step.

7. Rollback the 1st SC board.

To restore the Media Gateway software from the pre-upgrade backup image, at the prompt change directory to the place where backup file is stored (if it's not in your home directory) and execute the backup file.

```
client208:~# ./backup.bk
```

8. To start the Media Gateway software, type **reboot**. Press **Enter**.

```
client208:~# reboot
```

9. Rollback the 2nd SC board (if it exists).
 - Rollback of the 2nd SC board is similar to the rollback of the 1st SC board described above. However, it is important to rollback a 1st SC board first, which minimizes the downtime frame when the Mediant Media Gateway is not functioning. If the 1st SC board has been removed, media gateway service is not restored until the rollback of the 2nd SC board is completed.
10. Rollback the Media Gateway boards.
 - The Media Gateway boards are automatically reset by the Media Gateway software and rolled back to the previous software version. You are not required to take any additional measures to accomplish this.
11. Rollback the Ethernet Switch boards.
 - Lock/unlock the Ethernet Switch boards one after another, to roll them back to the previous software version.

46.7.2 Recovery from a Network Failure or EMS Server/Client Crash

The following abnormal Online Software Upgrade process scenarios during can interfere with a regular workflow:

- Network disconnects
 - Between EMS client and EMS server
 - Between EMS server and SC boards
- EMS client crash
- EMS server crash

For all of the above scenarios, you may recover and proceed with the Online Software Upgrade from the same point where it was interrupted.

➤ **To recover the Online Software Upgrade from a network failure or EMS server/client crash:**

1. Close and re-open the EMS client.
2. Restart the Upgrade Wizard on the specific Mediant 8000 system.
3. When prompted to resume the currently running Upgrade session, click **Next** to continue the upgrade from the same point where it was interrupted.



Note: In certain network failures, The **Connect** button may be displayed on the Upgrade Wizard screen. If the directions above do not help perform the recovery, click the **Connect** button to recover from the network failure.

This page is intentionally left blank.

Part VII

Diagnostics and Troubleshooting

This section describes the recommended method for maintaining AudioCodes' Mediant 8000 Media Gateway's. AudioCodes provides a wide range of diagnostic tools to enable users to easily identify an error condition and to provide a consequent solution or work around.

47 Troubleshooting Strategy

The goal of the maintenance procedures described in this section is, in the even of a component failure, to return the Media Gateway to full capacity as rapidly as possible. The maintenance philosophy is focused on locating the faulty component and replacing it. The Media Gateway's components are not normally repaired at the Customer's site. The following principles have been formulated to guide you in troubleshooting the system:

- Try connecting to the Media Gateway's management interface (SNMP or CLI) via the IP network. Use the appropriate management tools (e.g., the EMS GUI or CLI commands) to inspect the current Media Gateway status and locate the fault. Locating the fault this way could save you a visit to the site or save you time when you arrive there.
- Use a systematic process of elimination to try and identify the source of the problem. Ask the users of the Media Gateway to describe the nature of the problem they have encountered. Ask yourself questions such as these:
 - What is the scope of the problem?
 - Does it affect one particular interface, a group of interfaces, or the entire Media Gateway?
 - What capabilities are affected?
 - Does the problem occur during daytime hours only, or also during the night?
 - Did the problem(s) start after any configuration changes or other operator activities were made?
 - What is the likely source of the problem? A faulty interface or board? Loose or incorrect cabling? A problem in the common equipment or configuration definition?
- Perform the simplest test first. For example, if a particular interface does not work, check that the junction box cord is properly inserted and swap the interface cable to another working interface to see if the fault lies in the interface, before checking the wiring or the Media Gateway configuration.

The table below presents possible courses of action to remedy faults arising in the Mediant 8000 Media Gateway.

Table 47-1: Troubleshooting Faults in the Media Gateway

Problem	Possible Cause(s)	Actions to Take	See:
Media Gateway is "dead". All LEDs (on boards and power supply modules) are off or red and there is no sound from the ventilation fans.	Power supply problem	Check the DC power connection and voltage. Connect all the power wires and turn on the appropriate switches.	DC Power System

Problem	Possible Cause(s)	Actions to Take	See:
Media Gateway operation is silent	Fans problem	Check the airflow from the ventilation holes on the chassis sides. Verify that the fan units are inserted properly.	'Cooling System' on page 43
No Console communication to the SC board.	Console settings	Check the communication port settings to verify: 9600, 8, N, 1	'Connecting to the CLI via an RS-232 Serial Console' on page 109
	Cable connection	Verify that the Console cable is connected to the appropriate console connection (on SC board's front or on the SA/RTM module)	'Connecting to the CLI via an RS-232 Serial Console' on page 109
	Incorrect cable pinout	Verify that console cable pinout is correct.	'SC Rev.1 board (Solaris OS)' on page 64 'SC Rev.2 Board (Linux OS)' on page 66 'SA Synchronization and Alarm RTM' on page 69
	Cable problem	Replace the cable	
No communication with the Media Gateway (ping to the private SC's IP doesn't work)	Chassis is disconnected from the network	Check that the ES boards' uplinks are properly connected to the external IP network.	'Connecting to the IP Network' on page 116
	External network problems	Connect to the 1 st SC board's CLI interface via the RS-232 serial console and check the ping to the 2 nd SC board. If it works, but the ping from the external equipment (e.g., EMS server or PC) does not – verify the configuration of IP switches and routers that interconnect the external equipment with the Media Gateway chassis.	External Layer 3 Ethernet Switches or Routers in Section 'Connecting the Mediant 8000 to the IP Network' on page 217 .

Problem	Possible Cause(s)	Actions to Take	See:
	VLAN configuration mismatch – for ES/6600.	Verify that the VLAN configuration of the OAM subnet on the Media Gateway matches the VLAN configuration of the external IP network. Re-configure VLAN configuration if needed.	'Working with VLANs' on page 188
	Wrong basic IP configuration of SC boards (e.g. subnet mask or default router)	Connect to the CLI interface of the SC board via RS-232 serial console. Run install command and re-configure the SC board's basic network configuration.	'Configuring the Basic IP Network Parameters of SC Boards' on page 117
	ES board malfunction	Reset both ES boards by extracting them from the chassis and re-inserting them. It may take up to 10 minutes for the ES boards to complete the "reset procedure".	'Working with the ES boards' on page 261
No communication with the Media Gateway (ping to the private SC's IP works; however, ping to Telnet does not)	Media Gateway is in Secure Mode	Use SSH to connect to the Media Gateway's CLI interface on the SC boards in Secure Configuration Mode.	'Connecting to the CLI via the IP Network' on page 111
	SC board is at the OpenBoot level (ok prompt)	Connect to the SC board's CLI interface via RS-232 serial console. Press Enter . If you see the ok prompt – type go to continue normal board's operation. If this does not help – reset the board by pressing the RESET button. Wait up to 3 minutes until the SC board completes the reboot. If this does not help – extract the board from the chassis and re-insert it.	'Working with System Controller Boards' on page 223

Problem	Possible Cause(s)	Actions to Take	See:
	Duplicate IP address	Verify that no other equipment uses the same IP address as the one assigned to the SC board. Connect to the SC board's CLI interface via the RS-232 serial console and check for "duplicate IP address" messages (wait a few minutes to see if the messages are recorded). If the "duplicate IP address" problem exists, do one of the following: - locate and reconfigure/remove the faulty external equipment - update the basic SC's network configuration (redefine the IP addresses).	'Configuring the Basic IP Network Parameters of SC Boards' on page 117
No communication with the Media Gateway (ping to the Global SC's IP does not work)	Media Gateway software is not running on either SC board	Media Gateway software starts automatically after the SC board is rebooted. If this does not help – one of the following scenarios must have occurred: - Media Gateway software is not installed on the SC board – install it - Basic IP network parameters of SC board were altered (option 1 in install command), but the system configuration (options 3 or 4) were not run – run the missing options.	'Installing the Media Gateway software on the SC Board' on page 795 'Configuring the Basic IP Network Parameters of SC Boards' on page 117
No communication with the Media Gateway (The CLI connection to the Global SC's IP address works; however the connection to SNMP does not)	Wrong SNMP manager settings	Ensure that the SNMP protocol configuration on the SNMP manager matches the Mediant 8000 configuration. For the SNMP v2 protocol, ensure that the correct SNMP community strings are configured. For the SNMP v3 protocol, ensure that the correct privacy and security settings are configured.	'Configuring Connectivity with EMS Server' on page 153

Problem	Possible Cause(s)	Actions to Take	See:
	Media Gateway software is not running on both SC boards	Start the Media Gateway software on both SC boards by rebooting them.	'Working with System Controller Boards' on page 223
	External firewall blocks communication with the Mediant 8000.	Verify that the SNMP communication with the Media Gateway is not blocked by a firewall or other 3 rd party network equipment.	'Network Services on SC Boards' on page 357
No communication with the Media Gateway (ping to the SC's Global IP is unstable; occasionally does not succeed)	Wrong external IP network configuration	The Mediant 8000 must be connected to two external Layer 3 switches or routers, that must be configured for fully redundant operation via the use of VRRP/HSRP protocols. Improper configuration of external switches may lead to unstable IP network connectivity. Make sure that the external switches/routers have the "spanning tree" feature enabled.	'External Layer 3 Ethernet Switches or Routers' in Section 'Connecting the Mediant 8000 to the IP Network' on page 217
No communication with the Media Gateway (after ES board failure/switchover, there is no ping to SC's Global IP).	Two external Layer 3 switches or routers, to which the Mediant 8000 is connected, are not properly configured for redundant operation.	The Mediant 8000 must be connected to two external Layer 3 switches or routers, which must be configured for fully redundant operation via the use of VRRP/HSRP protocols. Improper configuration of external switches may lead to connectivity loss in case of ES board switchover.	External Layer 3 Ethernet Switches or Routers in Section 'Connecting the Mediant 8000 to the IP Network' on page 217 .
Problems with ES boards			
ES board is Disabled (colored <i>red</i> in the EMS)	Ethernet Switch board is completing the Unlock action	It may take up to 10 minutes for the ES board to complete the reboot that accompanies the Unlock action. Wait patiently. Note: while one ES board reboots, another ES board takes activity and provides IP connectivity to the rest of the boards in the chassis.	'Working with the ES boards' on page 261
	Ethernet Switch board malfunctions	Try to repeat lock/unlock action on the ES board.	'Working with the ES boards' on page 261

Problem	Possible Cause(s)	Actions to Take	See:
ES board is Disabled (colored <i>red</i> in the EMS) and all it's LEDs are turned off.	The uplink of the Ethernet Switch board is disconnected.	Connect the uplink to the ES board. If the ES board doesn't become Enabled (colored <i>green</i> in the EMS) – reset it by performing <i>Lock/Unlock</i> actions.	'Working with the ES boards' on page 261
Problems with Media Gateway boards			
Media Gateway board is Disabled (colored <i>red</i> in the EMS)	Media Gateway board is completing the Unlock action	It may take up to 3 minutes for the Media Gateway board to complete the reboot that accompanies the Unlock action. Wait patiently.	'Working with the Media Gateway Boards' on page 245
	Duplicate IP address	Verify that no other equipment uses the same IP addresses as the ones configured for the Media Gateway board. If the "duplicate IP address" problem exists do one of the following: locate and reconfigure/remove the faulty external equipment update Media Gateway board's configuration (redefine IP addresses)	'Working with the Media Gateway Boards' on page 245

Problem	Possible Cause(s)	Actions to Take	See:
	Media Gateway board malfunction	Try to repeat lock/unlock action on the Media Gateway board. Wait up to 3 minutes for the board to complete the reboot. If this does not help, alter the <i>BoardProvisioningMode</i> parameter in Media Gateway properties screen to "MAC Address", set the correct MAC addresses, and repeat lock/unlock sequence on the Media Gateway board. Do not forget to restore the BoardProvisioningMode parameter in the Media Gateway to "Geographical Address" value after finishing the troubleshooting. Even if this troubleshooting helped, there is no need to keep it permanently as the Media Gateway board typically works in "Geographical Address" mode for the consequent lock/unlock cycles.	'Working with the Media Gateway Boards' on page 245 'Troubleshooting the Newly Installed Media Gateway Board' on page 799
	"Diagnostics on Reset" parameter is enabled	In the EMS, open Media Gateway board's Provisioning screen. Go to the "Diagnostics" tab and set the "Diagnostics on Reset" parameter to "Disable" or set the "Diagnostics Startup Level" to a lower value.	
Active calls are dropped during the switchover from a failed Media Gateway board to the redundant board.	Configuration of the Media Gateway boards prevents hot redundancy	Verify configuration of the Redundancy Group and current "redundancy status" of all the Media Gateway boards.	'The Redundancy Model' on page 249
Media Gateway board is not reset upon <i>Lock</i> action	A problem with the Media Gateway board's RTM (Rear Transition Module)	Make sure that the Media Gateway board's RTM is inserted properly Gateway rear slot and that its latches are firmly closed.	'6310 Rear Transition' on page 51 '8410/RTM Rear Transition Module' on page 55

Problem	Possible Cause(s)	Actions to Take	See:
	A problem with SC board's SA/RTM	Make sure that the SA/RTM modules of both SC boards are inserted properly in the rear slots and that their latches are firmly closed. Perform <i>Lock</i> action on another Media Gateway board. If the problem occurs on it too – reset the SA/RTM module by extracting it from the chassis and re-inserting it back.	'SA/RTM Synchronization and Alarm Rear Transition Module' on page 69
Problems with Voice Quality			
G.711 voice quality is bad (clicks)	Wrong codec definition in the remote Media Gateway	In the remote Media Gateway, check that packetization time period (Ptime) is 20 msec and the correct μ -law or A-law compression is in use.	'Configuring the Voice Settings' on page 527
	Silence Suppression is not compatible with the remote Media Gateway (when remote Media Gateway is not an AudioCodes Media Gateway)	Disable Silence Suppression and check if quality is improved.	'Configuring the Voice Settings' on page 527
No voice	There is no common codec with the remote Media Gateway	Change voice codec definitions on the SoftSwitch.	See documentation provided by the relevant Softswitch vendor.
Echo on the PSTN terminations	Clock Synchronization	Check and validate the clock synchronization of the PSTN network and update the Media Gateway's configuration.	'Configuring TDM Synchronization' on page 516

48 Recovering the OAM VLAN Settings

The **tools vlan** command allows you to configure the Media Gateway's OAM VLAN tag to match the setting in the site IP network. This may be needed to re-establish connectivity with the Mediant 8000 in one of the following cases:

- The VLAN configuration of the OAM subnet to which the Media Gateway is connected was changed.
- The Backup file was restored on the Mediant 8000 with the OAM VLAN settings that differ from the current network configuration.

The procedures described below, are provided mostly for backward-compatibility (if you have configured the IP Network in a previous version). This procedure is not relevant if you have configured the IP Network according to the section 'Connecting to IP Network' on page 116.

➤ **To recover the OAM VLAN settings:**

1. Connect to the CLI interface on the Active SC board (typically located in Slot 1) via RS-232 serial console. For more information, see Section 'Connecting to the CLI via an RS-232 Serial Console' on page 109.
2. Login as **root** user. For more information, see Section 'Logging in as a Root User' on page 115.
3. At the prompt, type **tools vlan** and press **Enter**.

```
client238::~~# tools vlan
CONFIGURE OAM VLAN TAG
```

4. You are prompted to enter the OAM VLAN tag, type the appropriate number and press **Enter**.
 - To disable the VLAN configuration - enter **0**
 - To enable the VLAN configuration - enter the **OAM VLAN tag ID**
5. Confirm the action.

```
Enter OAM VLAN tag (0-no VLAN / 2-3999) : 4
Configure OAM VLAN tag 4
Are you sure? (y/[n]) : y
```

The ES boards are reset and the new OAM VLAN settings are applied to the Media Gateway. As soon as the ES boards return to service (it may take up to 10 min), you can connect to the management interfaces on the SC board (SNMP or CLI) via the IP network.

This page is intentionally left blank.

49 Collecting Advanced Media Gateway Board Logs

Media Gateway boards are constantly monitored by the Media Gateway software running on the SC boards and events/alarms are reported via the appropriate management interface (SNMP, Syslog or CLI).

In addition to the above monitors, when Media Gateway Board behaves abnormally and regular events/alarms are not sufficient for problem analysis, Advanced Media Gateway Board Logs may be used for problem troubleshooting. This section describes how to collect and analyze these advanced logs.



Note: Advanced Media Gateway Board Logs constitute a debug interface. Consider using the Syslog Management Interface instead – as described in 'Syslog Management Interface' on page 175.

49.1 Syslog Protocol

Media Gateway boards use the Syslog protocol to generate log and error messages. The Syslog protocol is an event notification protocol that allows a device to send event notification messages across IP networks to event message collectors, also known as Syslog servers. Since each process, application and operating system was developed independently, there is little uniformity between the different Syslog messages. For this reason, no assumption is made regarding the contents of the messages other than the minimum requirements of its priority.

49.1.1 Configuring the Syslog Server

As an alternative to using the Syslog server on the active SC board (and viewing the logs via the **log** command), you can configure the system to forward Syslog messages from the Media Gateway boards to an external Syslog server. This action is controlled via the following parameters at the Media Gateway level:

- 'EnableBoardLoggingOnSC' - enable or disable logging of the Media Gateway board logs on SC board; default - *enable*
- 'EnableBoardLoggingOnExternalServer' - enable or disable logging of the Media Gateway board logs on external Syslog server; default - *disable*
- 'BoardLoggingExternalIP' - IP address of the external Syslog server

Board Logging (syslog) configuration may also be configured for a specific Media Gateway board (e.g., it is possible to send Syslog messages from different Media Gateway boards to different Syslog servers). To do this, at the Board level, set the **UseBoardLoggingGWLevelConfiguration** parameter to *no* and provision the following parameters at the Board level (similar to those at the Media Gateway level):

- 'EnableBoardLoggingOnSC'
- 'EnableBoardLoggingOnExternalServer'
- 'BoardLoggingExternalIP'

49.1.1.1 Displaying VoIP Board Log Files

In the default configuration, the Active SC board acts as a Syslog server. It intercepts all syslog messages generated by the Media Gateway boards and stores them in the log files.

The log files may be viewed via the following CLI command (available to all CLI users):

log [<options>] board# <slot number>

Without any options, the **log** command displays the new logs as they are generated by the Media Gateway boards. For example, to display the logs of Media Gateway board in slot 8, use the **log board#8** command.

With option **-<number>**, the **log** command displays the last <number> of log messages. For example to see the last 100 log messages from Media Gateway board in slot 6, use the **log -100 board#6** command.

With option **-f**, the **log** command displays the complete log file. For example, **log -f board#10** command displays the full log of Media Gateway board in slot 10.

Option **-h** allows viewing the history of the log files (10 last log files are stored in the history).

49.1.2 SIP Board Syslog Level

Media Gateway boards use the Syslog protocol to generate log and error messages. The Syslog protocol is an event notification protocol which allows a device to send event notification messages across IP networks to event message collectors, also known as Syslog servers. Since each process, application and operating system is unique, there is minimal uniformity for Syslog messages. For this reason, no assumption is made regarding the contents of the messages other than the minimum requirements of its priority.

Media Gateway SIP boards act as a Syslog client and are capable of generating the following message levels:

- Only Emergency level Errors and Warning messages are enabled (debug disable).
- Warning level-Flow debugging is enabled (debug level 1).
- Debug level-Flow, device interface, stack interface, session manager, and device interface expanded debugging are enabled (debug level 5).

- Advanced Debug level -This option is recommended when the device runs under "heavy" traffic (debug level 7). In this mode:
 - The Syslog debug level automatically changes between Debug level, and Warning level and Emergency level, depending on the device's CPU consumption so that VoIP traffic isn't affected.
 - Syslog messages are bundled into a single UDP packet, after which they are sent to a Syslog server (bundling size is determined by the 'MaxBundleSyslogLength' parameter). Bundling reduces the number of UDP Syslog packets, thereby improving CPU utilization.

You can configure these Debug levels for SIP messages globally for all SIP boards (by setting 'SIP Logging Level' in the gateway level Troubleshooting screen) or disable the sending of SIP messages to the Syslog server entirely by setting the parameter 'Apply SIP Logging Level' to 'Disable'.

Alternatively, you can configure the Debug level for each individual board by setting 'SIP Syslog Logging Level' (in the board level Troubleshooting screen) or disable the sending of SIP messages entirely by configuring the same parameter 'SIP Syslog Logging Level' to 'DebugDisable'.



Note: If you configure the debug level globally after you have already configured the debug level for a specific board or you later configure it, then the board configuration applies.

49.2 Filtering Syslog Messages and Debug Recordings

The device can filter Syslog messages and debug recording (DR) packets, sent by a designated SIP board to a Syslog server with a packet capturing application (such as Wireshark) respectively. This feature ensures that CPU consumption is reduced and an adverse impact upon VoIP performance is minimized.

You can configure up to thirty filtering rules, each based on a selected filtering criteria (e.g., an IP Group). Each filtering criteria can be configured with a range. For example, you can filter Syslog messages for IP Groups 1 through 4.

Once you have configured the filters, you can in addition choose to capture specific Debug recording packets for the filter criteria. For example, you can capture SIP signaling or signaling and media for IP Groups 1 through 4.

49.2.1 Configuring Filter Rules

The configuration of SIP logging rules is enabled at the Media Gateway level. This to enable logging filters for the entire Media Gateway. However, a customer can also specify a VoP board or a number of VoP boards that will be configured with the current filter rule.



Note: If you set the 'Enable Syslog' parameter to disable, then no filtering is performed and therefore all messages are sent to the Syslog server.

➤ To configure SIP Logging Filter rules:

1. Click  to access the Media Gateway status screen.
2. In the Navigation pane, select **Troubleshooting** ➤ **SIP Logging**.
3. Use the  or  buttons to add or remove entries.
4. Select a specific row, and then in the Configuration pane, click **SIP Logging Filter**; the SIP Logging Filter Settings screen is displayed.
5. Configure SIP Logging Filter parameters according to the table SIP Logging Filter Properties below.
6. Configure a Debug Capture filter if desired (to start the Debug Capture for a specific board, in the board Troubleshooting screen, from the Status drop-down list, select **Start**).

7. Click the Maintenance icon , and then select **Unlock** to activate the configuration.

Table 49-1: SIP Logging Filter Properties

Parameter Name	Type	Provisioning Type	Description
Filter Type	Enum Any TrunkID TrunkGroup Bchannel TeltolP IPtoTel IP Group SRD Classification IPtoIP routing User IP Trace	Instant	Defines the filter criteria: - Any (default) - TrunkID = Filters according to a specified Trunk ID (applicable only to the Gateway application). - Trunk Group ID = Filters according to a specified Trunk Group ID (Applicable only to the Gateway/IP-to-IP application). - B-channel = Filters according to a specified Trunk and B-channel (applicable only to the Gateway/IP-to-IP application). - Tel-to-IP = Filters according to a specified Tel-to-IP routing rule listed in the Outbound IP Routing table (applicable only to the Gateway/IP-to-IP application). - IP-to-Tel = Filters according to a specified IP-to-Tel routing rule listed in the Inbound IP Routing table (applicable only to the Gateway/IP-to-IP application). - IP Group = Filters according to a specified IP Group ID listed in the IP Group table. - SRD = Filters according to a specified SRD ID listed in the SRD table. - Classification = Filters according to a specified Classification rule listed in the Classification table (applicable only to the SBC and application). - IP-to-IP Routing = Filters according to a specified SBC IP-to-IP routing rule listed in the IP-to-IP Routing table (applicable only to the SBC application). - User = Filters according to a specified user defined by username or user@host.

Parameter Name	Type	Provisioning Type	Description
			IP Trace = Filters according to a specified IP network trace wireshark-like expression.

49.3 Media Gateway Board's Debug Recording Traces and Logging

Media Gateway Board Debug Recording Traces is a powerful debugging tool that provides ability to capture traffic being handled by the specific Media Gateway board. It may be used for analyzing different inter-op scenarios or specific Media Gateway board malfunctions.

The tool enables forwarding of the specific packets being handled by the Media Gateway board to the user-specified remote IP address. The remote IP address may belong to one of the following:

- External PC
- Standby SC board

Flexible user-defined filtering rules may be applied to select traffic to be forwarded. For example, it is possible to select traffic between the Media Gateway board and specific remote Media Gateway. Or, alternatively, select traffic that belongs to the specific call. Multiple filtering rules may be applied simultaneously.

Forwarded traffic may be recorded on the External PC or Standby SC board via any network sniffer application.

When Debug Recording Traces are forwarded to the External PC, the WireShark application is recommended both for the trace collection and analysis. It may be downloaded from '<http://www.wireshark.org>.' '<http://www.wireshark.org>.' AudioCodes proprietary plugin, provided on the Media Gateway Installation CD. It must be placed in the plugins folder (typically **C:\Program Files\Wireshark\Plugins\X.X.X.X**), where X.X.X.X is the number of the installed version). This plugin dissects all packets on port 925 as Debug Recording Traces.



Note: The WireShark plugins are not backward compatible. Loading incompatible plugins may cause the application to crash.

When Debug Recording Traces are forwarded to the Standby SC board, the standard UNIX **snoop** utility is recommended for trace collection. Collected data may be stored in files that may be transferred to the external PC with WireShark application for analysis.



Note: The **snoop** utility is not available on the SC boards when Media Gateway is configured for Secure Operation Mode. In this case, use an external PC to collect Media Gateway board's debug recording traces.

49.3.1 Collecting Debug Recording Traces on the Standby SC board

Debug Recording Traces may be collected on the Standby SC board and captured to the local files. These files may be later transferred via FTP/SFTP/SCP protocols to the external PC with the WireShark application and analyzed. Alternatively, these files may be sent to the AudioCodes Technical Support for further analysis.



Note: Debug Recording Traces should never be collected on the Active SC board, since this may cause Media Gateway service interruption. Always use Standby SC board or external PC to collect Debug Recording Traces.

➤ To collect Debug Recording Traces on the Standby SC board:

1. Connect to the Standby board via Console, Telnet or SSH. For more information, see Section 'Command Line Interface' on page 107. Use the internal (not Global) SC IP addresses if you connect via Telnet or SSH.
2. Login as the **root** user. For more information, see Section 'Logging in as a Root User' on page 115.
3. To start capturing the Debug Recording Traces, at the prompt, type
 - For SC Rev.1 boards (using Solaris OS), type: **snoop -o <file name> port 925**
 - For SC Rev.2 boards (using Linux OS), type **tcpdump -w <file name> -s 0 port 925**

Replace **<file name>** with the name of the file to be created.

```
client238:./# snoop -o debug.snoop port 925
Using device /dev/dmfe1 (promiscuous mode)
0
```

4. To stop capturing the Debug Recording Traces, press **Ctrl-C** key sequence.



Note: The **snoop** utility is not available on the SC Rev.1 boards (using Solaris OS) when Media Gateway is configured for Secure Operation Mode. In this case, use an external PC to collect Media Gateway board's debug recording traces.

49.4 Collecting Call Data Records (CDRs)

In addition to the Advanced Media Gateway board logs, Call Data Records (CDRs) may be collected from the Media Gateway board and used for analyzing its operation.

CDR data is collected on the Media Gateway board and may be forwarded to the active SC board or any other NFS server via the NFS protocol. The CDR storage is limited to 1000 CDRs; therefore, on a system with a high amount of traffic, the CDR data is overwritten relatively quickly.

49.4.1 Collecting Call Data Records on SIP Boards

You can collect Call Data Records on SIP boards and forward them to a Syslog server or to a predefined CDR server.

➤ **To collect CDRs from the SIP board:**

1. Click  to access the Media Gateway status screen.
2. Select the desired SIP board.
3. In the Navigation pane, select **Troubleshooting** and in the Configuration pane, click **Troubleshooting Settings**; the Troubleshooting Settings screen is displayed.
4. Configure the parameter **CDR Report Level** to forward CDRs to a the Syslog Server (see below). For example, you can configure this parameter with a CDR level twice per call; once at the beginning of the call and once at the end of the call.
5. (Optional) Set the parameter **SIP CDR Server** to a dedicated CDR Server IP address.

This enables CDR records to be distinguished from regular syslog messages.

Table 49-2: CDR Report Level

Parameter Name	Type	Provisioning Type	Description
CDR Report Level	Enum None, EndCall, StartAndEndCall, ConnectAndEndCall, StartAndEndConnectAndCall	Instant	Determines whether CDRs are sent to the Syslog server. When enabled, indicates upon events they are sent. Valid options include: ▪ 0 = Call Detail Record (CDR) is not used (default). ▪ 1 = CDR is sent to the Syslog server at the end of each call. ▪ 2 = CDR report is sent to Syslog at the start and end of each call. ▪ 3 = CDR report is sent to Syslog at connection and at the end of each call. ▪ 4 = Start and Connect and End Call = CDR report is sent to Syslog at the start, at connection, and at the end of each call.

49.4.2 Collecting Call Data Records (CDRs) on MEGACO Boards

This section describes how to collect Call Data Records (CDRs) on MEGACO boards.

➤ To collect CDRs from the MEGACO board:

1. Click  to access the Media Gateway status screen.
2. In the Navigation pane, select **Media** and then in the configuration pane, click **Media Server Settings**; the Media Server Settings screen is displayed.
3. Set **Enable NFS Server On SC Board** parameter to *Enable*.
4. Connect to the CLI interface on the Active SC board. For more information, see Section 'Command Line Interface' on page 107.
5. Login as a CLI user with administrative privileges (e.g. *acladmin*). For more information, see Section 'Logging into Command Line Interface' on page 115.
6. To start CDR recording, at the prompt, type **tpCmd moBoard#X /cp/cdr start** and press **Enter**. Replace X with the number of the Media Gateway board for which you want to record CDRs.

```
client238::~~# tpCmd moBoard#7 /cp/cdr start
```

7. To stop CDR recording, at the prompt, type **tpCmd moBoard#X /cp/cdr stop** and press **Enter**.

```
client238::~~# tpCmd moBoard#7 /cp/cdr stop
```

8. To send recorded CDR data to the Active SC board via NFS protocol, at the prompt, type **tpCmd moBoard#X /cp/cdr send file://sc-ip-address/filename**. Replace **sc-ip-address** with the Global IP address of the Active SC board and **filename** with the full name of the CDR file to be created.

```
client238::~~# tpCmd moBoard#7 /cp/cdr send
file://10.7.9.245/Project/bin/log/cdr /cdr.txt
```



Note: It is also possible to directly transmit CDR data to any NFS server instead of the Active SC board. To do so, use IP address of the NFS server and corresponding directory in the above command.

9. To view recorded CDR data, at the prompt, type **more <filename>**.

```
client238::~~# more /Project/bin/log/cdr/cdr.txt
```

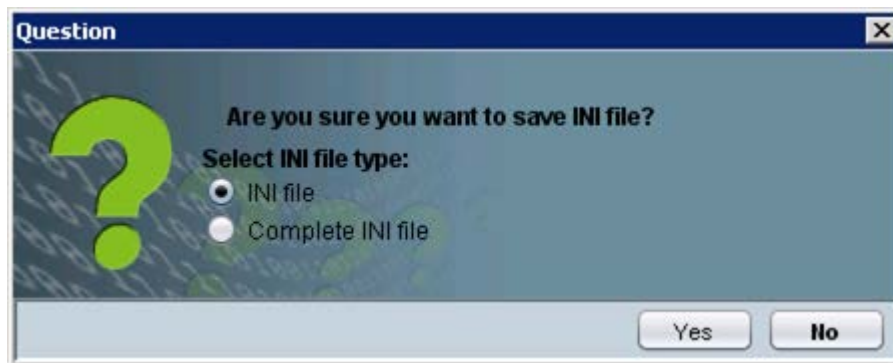
10. After you complete the CDR recording, open the Media Settings screen as described in step 2 and set **Enable NFS Server On SC Board** parameter to *Disable*.

49.5 Collecting the Media Gateway Board's INI File

The INI file contains the configuration data of the Media Gateway board. It may be used together with Advanced Media Gateway board logs to perform advanced troubleshooting.

➤ **To collect the INI File from the Media Gateway board:**

1. Click  to access the Media Gateway status screen.
2. Select the desired Media Gateway board.
3. Right-click the selected Media Gateway board and from the pop-up menu, select **Maintenance ► Save INI File**; the Save INI File dialog is displayed.



4. Choose a location on your PC or on the file server to save the **INI** file using one of the following options:
 - INI file – includes only those parameters with changed values (not including those with default values).
 - Complete INI file– includes all parameters (including those with default values).

This page is intentionally left blank.

50 Accessing Advanced Status- Media Gateway Board via WEB

The Media Gateway board's status is typically examined via the EMS GUI or via CLI commands. The latter contain all required information for detailed operation, configuration and maintenance of the Media Gateway board (for more information, see Section 'Working with the Media Gateway Boards' on page 245).

However in certain scenarios, you may be asked by AudioCodes technical support to collect some advanced status data of the specific Media Gateway board. In this case, the WEB interface of the Media Gateway board may be used for collecting this data.



Note: The WEB interface of the Media Gateway board should only be used for collecting debug data upon explicit request from the AudioCodes technical support. It is not officially supported for any other use.

Access to the WEB interface of the Media Gateway board is disabled by default.

➤ **To enable access to the Media Gateway board's WEB interface:**

1. Click  to access the Media Gateway status screen.
2. In the Navigation pane, select **Troubleshooting** and then in the configuration pane, click **Troubleshooting Settings**; the Troubleshooting Settings screen is displayed.
3. Configure the following parameters:
 - Set **Enable Web Access** parameter to *Enable*.
 - Set **Web Access IP 1** parameter to the IP address of the PC that will be used to access the Media Gateway board's WEB interface
 - Set **Web Access Password** parameter to the password to be used when accessing the Media Gateway board's WEB interface

Once access to the WEB interface of the Media Gateway board is enabled, access it via the regular web browser (e.g., Internet Explorer) from the PC that was granted access to the WEB interface as described above.

➤ **To access Media Gateway board's WEB interface:**

1. On the PC, whose IP address you previously provisioned, open web browser (e.g., Internet Explorer).
2. Enter the following URL: Error! Hyperlink reference not valid. **address>**, where **<IP address>** is the OAM IP address of the Media Gateway board.



Note: Use https:// and not http:// in the URL when accessing the Media Gateway board's WEB interface.

3. When prompted to enter username and password, enter the following:
 - username: **monitor_user**
 - password: password, configured as described above.

51 Collecting Traces from the Ethernet Switch Board's Mirror Port

Ethernet Switch Boards provide the ability to mirror selective IP traffic that is passed through the ES boards. Mirrored packets may be duplicated on ES board's mirror port and recorded on the external equipment (e.g. PC) connected to this port. Alternatively, mirrored packets may be sent to the standby SC board and recorded via a standard network capture utility. Recorded data may be analyzed via regular network analysis tools – e.g. Wireshark ('<http://www.wireshark.org>.' '<http://www.wireshark.org>.').

Different user-defined Mirror Filters may be specified to select packets that will be mirrored. Multiple filters may be used to capture different kinds of traffic (e.g. call control and media). Mirror Filters may be activated for the active ES.

Debugging data, captured on the ES board's mirroring port may be used to troubleshoot different network-related problems on the Media Gateway, as well as to validate interoperability between the Media Gateway and 3rd party equipment.

➤ **To configure Media Gateway to mirror IP traffic, the following tasks must be performed:**

- Configure ES Mirror Filters to select IP packets that will be mirrored by each ES board. Alternatively you may configure ES board to mirror all traffic from the specific internal IP port (i.e. SC or Media Gateway board).
- Configure ES board to record mirrored traffic on Mirror Port or on Standby SC board.
- Start mirroring on ES board.

51.1 Configuring ES Mirror Filters

Mirror filters define which of the IP packets that pass through the specific ES board, are mirrored by it. Multiple and different mirror filters may be defined on each ES board.

51.1.1 ES/6600

Mirror filters may be specified either in a “free text” format, where the user explicitly specifies a range of the bits in the IP packet and the hexadecimal value (e.g. “1-16=33 134-137=a”), or in a more user-friendly format, where the user may enter the value of each IP packet's header element. Header elements, presented to user, belong to Ethernet, IP, TCP, UDP or ICMP headers. Choose header elements that are relevant for the specific packets that you are verifying by referring to the figures below.

51.1.2 ES-2

Mirror filters may be specified either by a physical ingress port of ES ,or by IP packet's header element. Header elements, presented to user, belong to Ethernet, IP, TCP, UDP or ICMP headers. Choose header elements that are relevant for the specific packets that you are verifying by referring to the figures below.

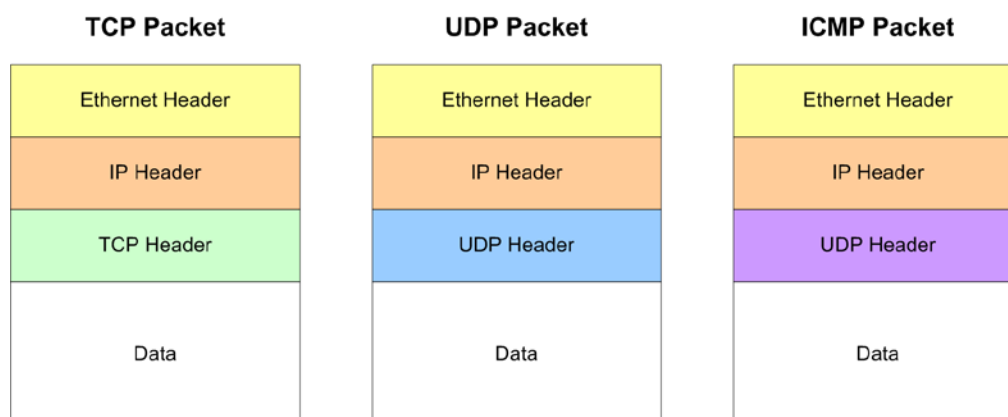
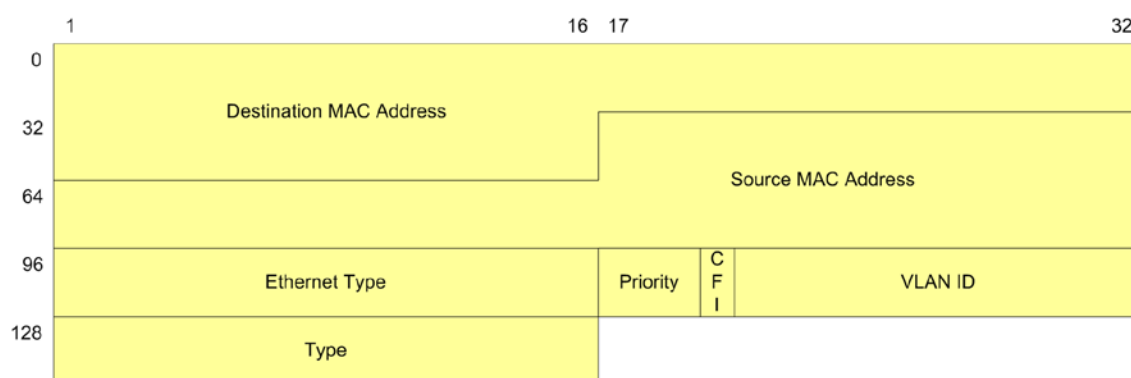
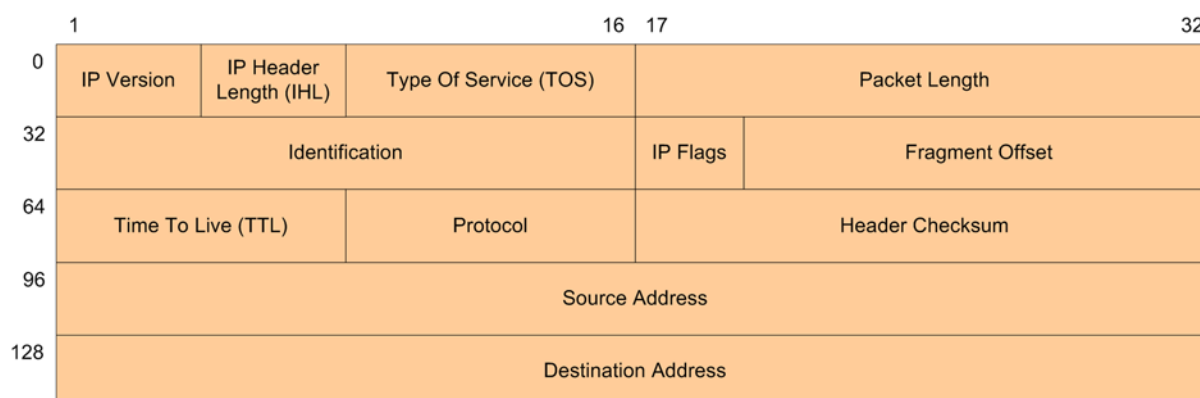
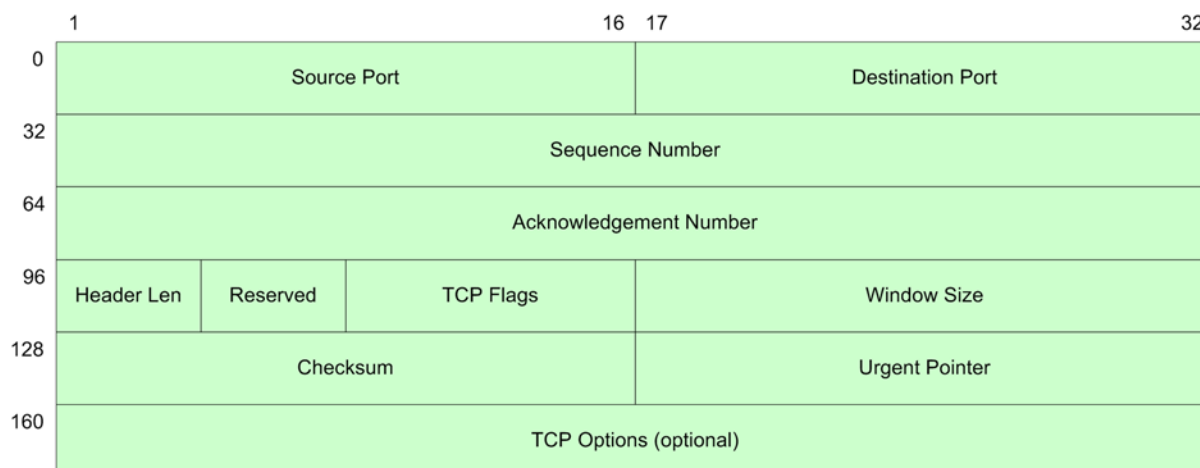
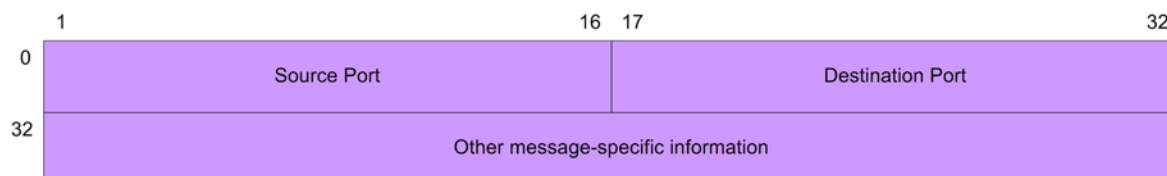
Figure 51-1: IP Packets

Figure 51-2: Ethernet Header

Figure 51-3: IP Header


Figure 51-4: TCP Header**Figure 51-5: UDP Header****Figure 51-6: ICMP Header**

➤ To configure ES mirror filters:

1. Click  to access the Media Gateway status screen.
2. In the Navigation pane, select **Troubleshooting** ➤ **ES Mirror Filters**; the ES Mirror Filters list is displayed.
3. Use the  or  buttons to add or remove entries.
4. Select a specific row and then in the configuration pane, click **ES Mirror Filter Settings**; the ES Mirror Filter Settings screen is displayed.
5. Configure the ES Mirror Filter parameters according to the table 'ES Mirror Filter Properties' below.
6. Click the Maintenance icon  and select **Unlock** to activate the configuration.

Table 51-1: ES/6600 and ES-2 Mirror Filter Properties

Parameter Name	Type	Provisioning Type	Description
Name	String	Instant	The textual, user-defined name for the ES Mirror Filter, enabling it to be identified intuitively and easily.
Free User Text	String	Online	Mirror filter description according to the ES board's internal filter syntax. The syntax consists of one or more "filter blocks"; each block consisting of the bits range and a hexadecimal value. For example filter "1-16=33 134-137=a" matches IP packets that have 16 bits, starting from bit 1, with hexadecimal value 33 (equivalent decimal value 51) and 4 bits, starting from bit 134, with hexadecimal value A (equivalent decimal value 10).
Dest MAC	String	Online	Defines the value of the "Destination MAC Address" element in the packet's Ethernet header (bits 1-48). The value must be specified in hexadecimal format. When set to 'n' matches all element values.

Parameter Name	Type	Provisioning Type	Description
Src MAC	String	Online	Defines the value of the "Source MAC Address" element in the packet's Ethernet header (bits 49-96). The value must be specified in hexadecimal format. When set to 'n' matches all element values.
VLAN Tag	Integer -1 to 4095	Online	Defines the value of the "VLAN Tag and Priority" element in the packet's Ethernet header (bits 117-128). The value must be specified in decimal format. When set to -1 matches all element values.
Protocol	Integer -1 to 255	Online	Defines the value of the "Protocol" element in the packet's IP header (bits 217-224). The value must be specified in decimal format. When set to -1 matches all element values.
Src IP	String	Online	Defines the value of the "Source IP Address" element in the packet's IP header (bits 241-272). The value must be specified in hexadecimal or string format. When set to 'n' matches all element values.
Dst IP	String	Online	Defines the value of the "Destination IP Address" element in the packet's IP header (bits 273-304). The value must be specified in hexadecimal or string format. When set to 'n' matches all element values.
Src Port	-1 to 65535	Online	Defines the value of the "Source Port" element in the packet's TCP, UDP or ICMP header (bits 305-320). The value must be specified in decimal format. When set to -1 matches all element values.
Dst Port	String	Online	Defines the value of the "Destination Port" element in the packet's TCP, UDP or ICMP header (bits 321-336). The value must be specified in decimal format. When set to -1 matches all element values.

Table 51-2: Additional ES/6600 Mirror Filter Properties

Parameter Name	Type	Provisioning Type	Description
Egress Port	Integer 0-26	Online	Egress (outgoing) ES board port where the filter is applied. Value of 0 means that filter is applied to all ports.
Use Free User Text	Enum False, True	Online	Defines whether the filter is specified as a free user text, according to the ES board internal filter syntax, or via the explicit fields and their values. Note that the explicit fields match the structure of the normal IP packet. For filtering other communication protocols (e.g. SCTP) you may use the free user text format.
Free User Text	String	Online	Mirror filter description according to the ES board's internal filter syntax. The syntax consists of one or more "filter blocks"; each block consisting of the bits range and a hexadecimal value. For example filter "1-16=33 134-137=a" matches IP packets that have 16 bits, starting from bit 1, with hexadecimal value 33 (equivalent decimal value 51) and 4 bits, starting from bit 134, with hexadecimal value A (equivalent decimal value 10).
Class of Service	Integer -1 to 7	Online	Defines the value of the "Class Of Service" element in the packet's Ethernet header (bits 113-115). The value must be specified in decimal format. When set to -1 matches all element values.
Type	Integer -1 to 65535	Online	Defines the value of the "Type" element in the packet's Ethernet header (bits 129-144). The value must be specified in decimal format. When set to -1, matches all element values.
IP Version	Integer -1 to 15	Online	Defines the value of the "IP Version" element in the packet's IP header (bits 145-148). The value must be specified in decimal format. When set to -1, matches all element values.

Parameter Name	Type	Provisioning Type	Description
TOS	Integer -1 to 63	Online	Defines the value of the "Type Of Service" element in the packet's IP header (bits 153-160). The value must be specified in decimal format. When set to 'n', matches all element values.
Packet Length	Integer -1 to 65535	Online	Defines the value of the "Packet Length" element in the packet's IP header (bits 161-176). The value must be specified in decimal format. When set to -1, matches all element values.
ID Number	Integer -1 to 65535	Online	Defines the value of the "Identification" element in the packet's IP header (bits 177-192). The value must be specified in decimal format. When set to -1, matches all element values.
Fragment Flag	Integer -1 to 7	Online	Defines the value of the "Fragment Flag" element in the packet's IP header (bits 193-195). The value must be specified in decimal format. When set to -1, matches all element values.
Fragment Offset	Integer -1 to 8191	Online	Defines the value of the "Fragment Offset" element in the packet's IP header (bits 196-208). The value must be specified in decimal format. When set to -1, matches all element values.
Flags		Online	Defines the value of the "Flags" element in the packet's IP header (bits 193-208). The value must be specified in decimal format. When set to -1, matches all element values.
TTL	Integer -1 to 255	Online	Defines the value of the "Time To Live" element in the packet's IP header (bits 209-216). The value must be specified in decimal format. When set to -1, matches all element values.

Parameter Name	Type	Provisioning Type	Description
Header Checksum	Integer -1 to 65535	Online	Defines the value of the "IP Header Checksum" element in the packet's IP header (bits 225-240). The value must be specified in decimal format. When set to -1, matches all element values.
Seq Num	Integer -1 to MAXINT	Online	Defines the value of the "Sequence Number" element in the packet's TCP header (bits 337-368). The value must be specified in decimal format. When set to -1, matches all element values.
AckNum	Integer -1 to MAXINT	Online	Defines the value of the "Acknowledgement Number" element in the packet's TCP header (bits 369-400). The value must be specified in decimal format. When set to -1, matches all element values.
TCP Header Len	Integer -1 to 15	Online	Defines the value of the "TCP Header Length" element in the packet's TCP header (bits 401-404). The value must be specified in decimal format. When set to -1, matches all element values.
Reserved	Integer -1 to 15	Online	Defines the value of the "Reserved" element in the packet's TCP header (bits 405-408). The value must be specified in decimal format. When set to -1, matches all element values.
Flag	Integer -1 to 255	Online	Defines the value of the "TCP Flags" element in the packet's TCP header (bits 409-416). The value must be specified in decimal format. When set to -1, matches all element values.
Window Size	Integer -1 to 65535	Online	Defines the value of the "Window Size" element in the packet's TCP header (bits 417-432). The value must be specified in decimal format. When set to -1, matches all element values.

Parameter Name	Type	Provisioning Type	Description
Other	String	Online	Defines the value of the "Checksum", "Urgent Pointer" and "TCP Options" elements in the packet's TCP header (bits 433-511). The value must be specified in hexadecimal format. When set to 'n' ,matches all element values.

51.2 Configuring Mirroring on ES boards' Port

As an alternative to configure ES Mirror Filters, you may configure ES board to mirror all traffic from/to the specific port (either internal or external). This effectively mirrors all traffic of the specific SC or Media Gateway board. Note, however, that capacity of the mirror port is limited therefore you may not be able to mirror traffic from more than a few internal ES board's ports. Also note that capture files, produced by mirroring all traffic on the specific port, may be very large and therefore their analysis may be very time-consuming.

➤ To configure ES boards to mirror all traffic on the specific port:

1. Click  to access the Media Gateway status screen.
2. Select the active Ethernet Switch (ES) board.
3. In the Navigation Pane, select **Switch Ports**; the ES Board Ports list is displayed.
4. Select the relevant ES board Port from the list. Use the Name column to determine which SC or Media Gateway board is connected to each ES board's port.
5. Right-click the selected ES Board Port and choose **Change Mirror Mode > Ingress / Egress / Both** to *enable mirroring of ingress (incoming), egress (outgoing)* or all traffic from the specific port.
6. Repeat steps 2-4 on the standby Ethernet Switch board (if needed).

51.3 Configuring Mirror Destination

Each ES board may be configured to forward mirrored traffic either on it's mirror port (port 23 for ES/6600 or port 10 for ES-2) or to the Standby SC board.

When the ES board mirrors traffic to the mirror port, external equipment (e.g. PC) should be connected to this port and some network capture software (e.g. Wireshark) must be run to capture and analyze the data.



Note: When ES board is configured to mirror traffic from one of its ports, only mirroring to the mirror port is supported (due to the potentially large amount of mirrored traffic).

When the ES board mirrors the traffic to the Standby SC board, mirrored packets must be recorded on the Standby SC via a network capture utility. Media Gateway software may be configured to perform this recording automatically via the standard **snoop** or **tcpdump** utility (on SC Rev.1 and SC Rev.2 boards respectively), or alternatively the user may perform manual recording via the alternative software (e.g. WireShark).

When mirrored traffic is sent to the Standby SC and recording is performed via the standard network capture utilities, the captured files are stored in the */Project/bin/log/capture* directory on the Standby SC board. These files may be later transferred to external PC (via FTP/SCP/SFTP) and analyzed in a network analyzer (e.g. Wireshark).



Note: When the Media Gateway using SC Rev.1 (using the Solaris OS) boards is configured in Secure Operation Mode, the **snoop** utility is removed from SC boards for security purposes, and therefore automatic recording of the mirrored data is not available. Use mirroring to the mirror port instead; or manually install a network capture utility on the Standby SC board and manually run it.

➤ To configure ES board's mirroring destination:

1. Click  to access the Media Gateway status screen.
2. Select the active Ethernet Switch board.
3. Right-Click the selected ES board and choose **Maintenance > Mirror to ES Eth default mirror port (Port#23 for CPC600 or Port#10 for ES-2) or Mirror to Redundant SC Eth Port**.
4. Repeat steps 2-3 on the Standby Ethernet Switch board (if required).

- To configure the Media Gateway software to automatically capture data mirrored to the Standby SC board via snoop utility (for ES/6600 switch only):

1. Click  to access the Media Gateway status screen.
2. In the Navigation pane, select **Troubleshooting** ➤ **ES Mirror Filter**; the ES Mirror Filters list is displayed.
3. Use the  or  buttons to add or remove entries.
4. Select a specific row and then in the configuration pane, click **ES Mirror Filter Settings**; the ES Mirror Filter Settings screen is displayed.
5. Set the **Capture On Red SC When Mirror** parameter to *Enable*.
6. Click the Maintenance icon  and select **Unlock** to activate the configuration.

51.4 Starting Mirroring on ES Board

After you completed all above-described configuration steps, you must start mirroring on each applicable ES board. Note that normally all IP traffic passes through the Active ES board. However, in some scenarios, certain IP traffic may pass through the Standby ES board as well.

- To start mirroring on ES boards:

1. Click  to access the Media Gateway status screen.
2. Select the active Ethernet Switch board.
3. Right-Click the selected ES board and choose **Maintenance > Enable Mirror Port**.

51.5 Stopping Mirroring on ES Board

After you collected all required information, stop mirroring on all ES boards.



Note: IP Traffic mirroring produces extra load on the Media Gateway and ES boards in particular. Stop mirroring as soon as you have completed collection of the required data.

- To stop mirroring on ES boards:

1. Click  to access the Media Gateway status screen.
2. Select the active Ethernet Switch board.
3. Right-click the selected ES board and choose **Maintenance > Disable Mirror Port**.

This page is intentionally left blank.

52 Internal System Controller (SC) Software Logs

The Mediant 8000 reports all alarms and events and that require the user's attention via the SNMP traps mechanism. You can view these events/alarms using the standard management interfaces - SNMP or CLI.

In addition, the Media Gateway software produces internal logs that may be used for advanced troubleshooting. These logs are instrumental for AudioCodes technical support and field engineers and should not be used by customers, unless explicitly directed to by AudioCodes technical support.

52.1 Log Areas

All of the Mediant 8000 logs are stored locally on the System Controller (SC) board's hard disk. There are logs collected for the redundant SC board as well. The logs are active by default (there is no need to activate them manually).

Logs from different software modules are stored in separate directories. Most of these directories should not be directly accessed by customers. The following sections describe all available log directories in each of the available Log Areas:

- Customer's Log Area - logs that may be directly accessed by the customer
- AudioCodes Technical Support Log Area - logs intended for AudioCodes Technical Support and Field Engineers.

52.2 Customer's Log Area

- **/Project/bin/log/trap** –the directory that logs all events and alarms provided via SNMP traps. It includes the information about system's maintenance activity, changes in certain components state, chassis activities and health (e.g., chassis over-heating, Media Gateway board switch-over, trunks or other system's elements failure, etc.).
- **/Project/bin/log/activity** - the directory that logs all CLI users' activity.



Note: These are the only logs that should be directly accessed by the customer under normal conditions.

52.2.1 AudioCodes Technical Support Log Areas

- **/Project/bin/log/alarm** – the directory that logs all of the activities at the chassis hardware management level (e.g., power supplier, fans, etc.)
- **/Project/bin/log/boardsLog** - this directory includes sub-directories for each Media Gateway board in the Mediant 8000 chassis. It includes all internal software logs reported by a specific Media Gateway board via the Syslog interface.
- **/Project/bin/log/bootp** – the directory that logs information regarding the BootP server process at the SC board (the BootP server is used for uploading software

and configuration file to the Media Gateway board during the **Unlock** action)

- **/Project/bin/log/core** – the directory that logs information regarding the Media Gateway configuration activities and status updates. The log is produced by the main software management module and typically represents the most valuable log file for troubleshooting the Media Gateway problems.
- **/Project/bin/log/hbg** – the directory that logs information regarding the Heartbeat generator activities (heartbeats are constantly exchanged between the SC boards and are used for the SC switchover when the active SC board fails)
- **/Project/bin/log/hbm** – the directory that logs information regarding the Heartbeat monitor activities (heartbeats are received by Active SC board from all other boards in the chassis and are used for triggering SC and Media Gateway switchover mechanisms)
- **/Project/bin/log/PSTNTrace** - the directory that logs recorded PSTN traces for certain calls
- **Project/bin/log/tpncpif** - the directory that logs information regarding TPNCIP Infrastructure activities against the chassis resident boards
- **/Project/bin/log/watchdog** - the directory that logs information of the watchdog activities (the watchdog constantly monitors state of all of the active Media Gateway software processes and restarts them if needed)
- **/Upgrade/log** – the directory that contains information about the Online Software Upgrade process and related activities

52.3 Log Files Storage

In the log information storage directory, '**Project/bin/log**' (located in both the active and standby SC boards) log files are retained and overwritten according to specific limitations. The oldest file (per item) is deleted automatically either upon disk space concerns or upon reaching the maximum number of files per subject.

The file names in the directory are:

- '**current**' – the current opened log file
- '@[serial number of the file]' – the older closed log file

The following Log file management options can be configured by AudioCodes technical support only: ('**Project/bin/SystemParams.ini**' file, '**logger**' section):

- "**num_of_files**" - the number of log files to keep per subject (the default is 10)
- "**max_file_size**" – the maximum size of each file (the default is 10 MB)
- "**disk_full_threshold**" – the disk usage threshold that causes forced cleanup of old log files (the default is 90%)

52.4 Viewing Log Files

All of the Log files including both the current and the closed (old) files of each subject can be seen or called upon using the following command:

log [<options>] <logfile>

Supported log files are: **core, bootp, cli, hbg, hbm, tpncp, sat, trap, upgrade, watchdog, syslog, activity**

The **log** command may also be used for viewing Media Gateway board logs by specifying **board # <slot number>** instead of the logfile. For more information, see Section 'Collecting Advanced Media Gateway Board Logs' on page 843.

Without any options, the log command displays the new logs as they are generated by the Media Gateway boards. With option **-<number>**, it displays the last <number> of lines from the logfile (e.g., **log -100 trap** displays the last 100 logs from the trap log file). With option **-f**, it displays the complete log file. Option **-h** allows viewing the history of the log files (10 last log files are stored in the history).

The example below demonstrates how the current **SNMP trap** logs can be viewed:

Figure 52-1: Viewing an 'SNMP Trap' Log

```

Telnet 10.7.13.104

+-----+
| Welcome to Media Gateway |
+-----+

Short help:
  tools sc p           see list of SC processes
  tools sc dn          stop SC software
  tools sc up           start SC software

client251:~# log trap
- Type: equipmentAlarm, Probable Cause: powerProblem, Id: 26
- AdditionalInfo: Measured fans speed, Top-Rear=3300, Top-Front=3375, Bottom-
Rear=0, Bottom-Middle=4963, Bottom-Front=4963
07/09 06:47:19.639 moGW 2_1 () sent alarm:
- Name: Operational Info, Severity: cleared, Source:
- TextualDescription: Finish ENABLE action
- Type: other, Probable Cause: other, Id: 5
07/09 07:07:59.039 moCPUBoard 19_2 (Board#2) sent alarm:
- Name: Operative State Change, Severity: indeterminate, Source: Board#2
- TextualDescription: SC enabled
- Type: other, Probable Cause: other, Id: 27
  
```

52.5 Operating System Logs

Operating System (OS) logs are stored on each SC board in the **/var/adm/messages** or **/var/log/messages** file (on SC Rev.1 and SC Rev.2 boards correspondingly). The file is rotated on a daily basis. Up to 4 backup versions are preserved.

Use the **log [<options>] messages** command or standard UNIX utilities (e.g., **more** or **less**) to view the file content.

52.6 Collecting the Report File

The Media Gateway software provides a special command for collecting a Report file, that contains all relevant log and configuration files and must be submitted to AudioCodes Technical Support as part of any problem report. The Report file should be collected independently from each SC board and contains enough data to analyze common issues with Media Gateway software.

Report file may be collected via EMS GUI or, alternatively, via command-line interface (CLI).

➤ To collect the Report file via the EMS GUI:

1. Click  to access the Media Gateway status screen.
2. In the Actions bar, click **Collect Logs**; the Collect Log Files screen is displayed.
3. Select the SC board from which you wish to collect the log files and select the specific files that should be collected.
4. Wait patiently while the logs are collected (this may take up to 10 minutes, depending on the selected options).
5. When collection completes, you are prompted to store the file on the EMS client PC or on a network file server.

➤ To collect the Report file via the CLI:

1. Connect to the CLI interface on both SC boards. For more information, see Section 'Command Line Interface' on page [107](#).
2. Login as a CLI user with administrative privileges (e.g. **acladmin**). For more information, see Section 'Logging into Command Line Interface' on page [115](#).
3. At the prompt, type **tools report** and press **Enter**.
4. Enter the name of the report file and press **Enter**.
5. Wait patiently till report file is generated.

```
• client238::~~# tools report  
GENERATE BUG REPORT
```

```
Enter bug report file name [report.tar] :report.tar  
Include VoP board logs? ([y]/n) : y  
>>> Collect some summary data...  
>>> Pack data into the //report.tar...  
>>> Compress report file...
```

```
Please deliver file //report.tar.gz to Tech Support.
```

6. Download file from the SC board via or SCP/SFTP/FTP to your PC and send it as part of the problem report.

This page is intentionally left blank.

53 Information Needed when Contacting Technical Support

When contacting AudioCodes Technical Support (see the title page or last page of this manual for detailed contact information), send the following information:

1. A description of the Media Gateway configuration - including the number and type of Media Gateway boards, network configuration, signaling protocols being used the exact software version.
2. A detailed description of the problem.
3. Any information obtained from the troubleshooting process, suspected components, captured network traces etc.
4. Information about any changes made to the system and its environment recently, i.e. configuration changes, networking setup changes, etc.
5. Report File collected from both SC boards. See 'Collecting Report File' on page 874.

This page is intentionally left blank.

Part VIII

Appendices

This part describes additional Mediant 8000 configuration procedures.

A Examples of IP Network Connectivity Configuration

This section provides examples of how to configure IP Network Connectivity on the Mediant 8000. The CLI commands are used to perform the network configuration, thus enabling such configuration even via a RS-232 serial console (e.g. when the EMS server is not available or there is no connectivity with it).

The following configuration scenarios are described:

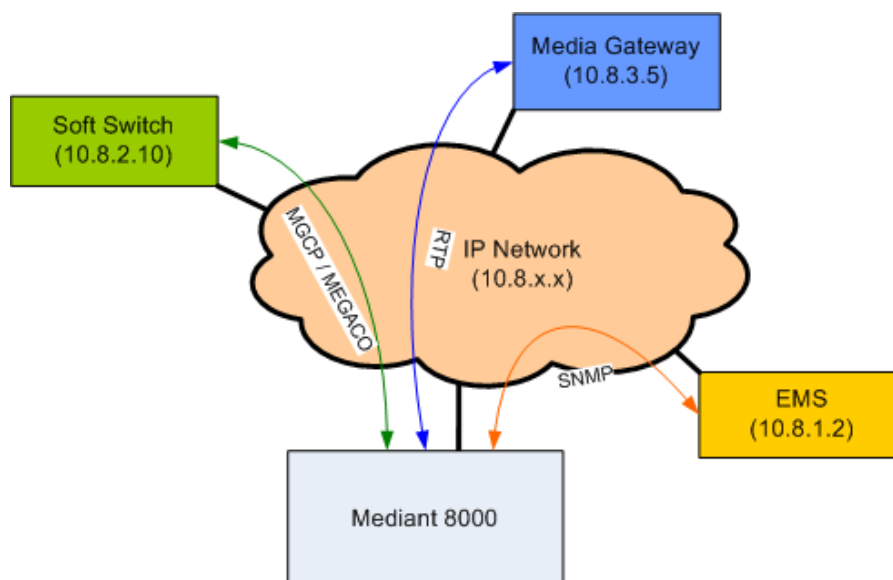
- One Subnet is used for all IP traffic – management (OAM), call control and media; VLAN tagging is not used
- Three Subnets are used – for management (OAM), call control and media traffic; subnets are separated via the use of tagged VLANs and a single physical interface is used for connecting to the IP network.

See 'Connecting the Media Gateway to the IP Network' on page 178 , for a generic description of the Mediant 8000 IP Network Connectivity.

A.1 Example 1: One Subnet, One Physical Interface, No VLAN Tags

This example describes the most common (default) configuration of the IP networking subsystem, where a single IP network (without subnet separation) is used for transmitting all types of IP traffic – management (OAM), call control and media. This configuration is deployed by many customers due to its simplicity and high interoperability.

Figure A-1: Network Example 1: One Subnet, No VLANs



➤ **To configure the Mediant 8000 for a specific network setup:**

1. Configure the basic IP network parameters of the SC boards as described in 'Configuring the Basic IP Network Parameters of SC Boards' on page 117. You will be asked for the following parameters:
 - IP Address – enter the IP address allocated for the specific SC board, e.g. 10.8.1.11 for SC board in Slot 1 and 10.8.1.12 for the SC board in Slot 2
 - Subnet Mask – enter the Subnet Mask of the IP Network, e.g. 255.255.0.0
 - Default Gateway – enter the IP address of the Default Gateway, e.g. 10.8.0.1

Perform the basic IP network configuration on both SC boards located in slots 1 and 2 respectively. Ensure that you configure the same Subnet Mask and Default Gateway on both SC boards.
2. Configure the Global IP address to be used by the active SC board as described in 'Performing Basic Configuration of the Mediant 8000 Software' on page 146. When prompted, provide the allocated IP address – e.g. 10.8.1.10.
3. Connect to the CLI interface on the Active SC board (typically located in Slot 1). Use the Global IP Address, if you establish a connection via SSH/Telnet. Use the RS-232 serial console, if IP connectivity with the Mediant 8000 is unavailable. For more information, see 'Connecting to the CLI via an RS-232 Serial Console' on page 109.
4. Login as a CLI user with administrative privileges (e.g. **acladmin**). For more information, see 'Logging into the Command Line Interface' on page 115.
5. Lock the Media Gateway via the following command (note that this command will stop all services provided by the Media Gateway):

```
SC-1 -- ~ -- /moGw
• lock
```

```
Do you really want to lock /moGw [y/n] y
Performing lock action on /moGw - OK!
```



Note: If the Media Gateway's current network separation configuration matches the target one, this step is not required.

6. Configure the Gateway's interface separation settings (single interface, no VLANs in use):

```
modify Interfaces=0
modify MediaAggregationEnable=0
modify OAMTagId=0
```

7. Configure the Media Gateway's board's IP Addresses:

```
modify moBoard#11/moBoardIPAddress#1=10.8.1.20
modify moBoard#12/moBoardIPAddress#1=10.8.1.21
modify moBoard#13/moBoardIPAddress#1=10.8.1.22
modify moBoard#14/moBoardIPAddress#1=10.8.1.23
```

8. Activate the new network configuration by unlocking the Media Gateway:

```
SC-1 -- ~ -- /moGW
• unlock
```

```
Performing unlock action on /moGW - OK!
```

The new network configuration will be activated. The Media Gateway boards will be reset and their **Operational State** will be changed to *Disabled* (boards will be displayed as Red in the EMS GUI).

It may take up to 5 minutes for all Media Gateway boards to complete the restart. When the Media Gateway board returns to service, its **Operational State** will be changed to *Enabled* and the board's color will be displayed as Green in the EMS GUI.

9. If interface separation of VLAN Tags configuration was changed, you will be asked to reset (lock/unlock) the ES boards prior to performing the unlock action on the Media Gateway. In such case, do the following:

a. Lock both ES boards:

```
SC-1 -- ~ -- /moGW
• lock esboard#9
```

```
Do you really want to lock /moGW/moSwitchBoard#9? [y/n] y
Performing lock action on /moGW/moSwitchBoard#9 - OK!
```

```
• lock esboard#19
```

```
Do you really want to lock /moGW/moSwitchBoard#19? [y/n] y
Performing lock action on /moGW/moSwitchBoard#19 - OK!
```

b. Unlock the ES board in slot 9:

```
SC-1 -- ~ -- /moGW
• unlock esboard#9
```

```
Performing unlock action on /moGW/moSwitchBoard#9 - OK!
```

- c. Wait up to 10 minutes until the ES board in slot 9 completes the restart operation and returns to service. Use the following command to determine whether the ES board has completed the restart operation. Value Enabled(1) indicates that the board is back in service:

```
SC-1 -- ~ -- /moGW
• show esboard#9 param OperationalState
OperationalState=Enabled(1)
```

- d. Unlock the ES board in slot 19:

```
SC-1 -- ~ -- /moGW
• unlock esboard#19
Performing unlock action on /moGW/moSwitchBoard#19 - OK!
```

- e. Wait up to 10 minutes until the ES board in slot 19 completes the restart and returns to service. Use the following command to determine whether the ES board has completed the restart operation. Value Enabled(1) indicates that the board is back to service:

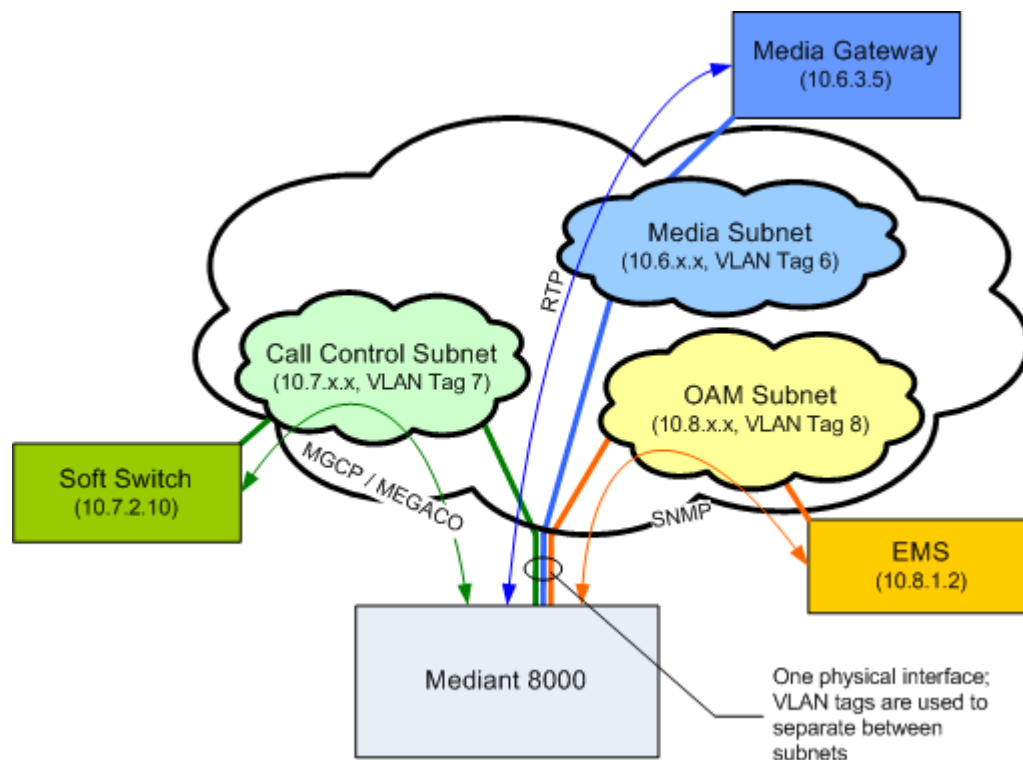
```
SC-1 -- ~ -- /moGW
• show esboard#19 param OperationalState
OperationalState=Enabled(1)
```

10. Connect network cables to port 20 on both ES boards (located in slots 9 and 19).

A.2 Example 2: Three Subnets, VLAN Tags, One Physical Interface

This example describes a complex configuration of an IP networking subsystem, where the dedicated IP network segment (subnets) are used for transmitting management (OAM), call control and media traffic. Subnets are separated via the use of tagged VLANs and the Mediant 8000 is connected to all of them via a single physical interface.

Figure A-2: Network Example 2 : Three Subnets, VLAN Tags, One Physical Interface



➤ To configure the Mediant 8000 for a specific network setup:

1. Configure the basic IP network parameters of the SC boards as described in 'Configuring the Basic IP Network Parameters of the SC Boards' on page 117. You will be prompted for the following parameters:
 - IP Address – enter the IP address allocated for the specific SC board in the OAM subnet, e.g. 10.8.1.11 for the SC board in Slot 1 and 10.8.1.12 for the SC board in Slot 2
 - Subnet Mask – enter the Subnet Mask of the OAM Subnet, e.g. 255.255.0.0
 - Default Gateway – enter the IP address of the Default Gateway in the OAM Subnet, e.g. 10.8.0.1

Perform the basic IP network configuration on both SC boards located in slots 1 and 2 respectively. Ensure to provide the same Subnet Mask and Default Gateway on both SC boards.

2. Configure the Global IP address to be used by the active SC board as described in 'Performing Basic Configuration of the Mediant 8000 Software' on page 146 . When prompted, provide the allocated IP address in OAM subnet – e.g. 10.8.1.10.
3. Connect to the CLI interface on the Active SC board (typically located in Slot 1). Use Global IP Address if you establish connection via SSH/Telnet. Use the RS-232 serial console if IP connectivity with the Mediant 8000 is unavailable. For more information, see 'Connecting to the CLI via an RS-232 Serial Console' on page 109.
4. Login as a CLI user with administrative privileges (e.g. **acladmin**). For more information, see 'Logging into the Command Line Interface' on page 115.
5. Lock the Media Gateway via the following command (note that this will stop all services provided by the Media Gateway):

```
SC-1 -- ~ -- /moGW
```

```
• lock
```

```
Do you really want to lock /moGW [y/n] y
Performing lock action on /moGW - OK!
```

6. **For the ES/6600 switch only:** Configure the Media Gateway's interface separation settings (single interface, three VLANs in use):

```
modify Interfaces=0
modify MediaAggregationEnable=0
modify OAMTagId=8

add moVlanTag#1
modify moVlanTag#1 VLANTagID=6

add moVlanTag#2
modify moVlanTag#2 VLANTagID=7
```

7. Configure three IP subnets available on site:

```

add moSubnet#2
modify moSubnet#2 SubnetIP=10.6.0.0
modify moSubnet#2 SubnetPrefixBitsLength=16
modify moSubnet#2 DefaultGW=10.6.0.1
modify moSubnet#2 VLANTagID=6

add moSubnet#3
modify moSubnet#3 SubnetIP=10.7.0.0
modify moSubnet#3 SubnetPrefixBitsLength=16
modify moSubnet#3 DefaultGW=10.7.0.1
modify moSubnet#3 VLANTagID=7

add moNetworkProfile#1/moNetworkSubnet#2
modify moNetworkProfile#1/moNetworkSubnet#2 SubnetIndex=2
add moNetworkProfile#1/moNetworkSubnet#3
modify moNetworkProfile#1/moNetworkSubnet#3 SubnetIndex=3

```

8. Configure the Media Gateway board's IP Addresses:

```

modify moBoard#11/moBoardIPAddress#1=10.6.1.20
modify moBoard#11/moBoardIPAddress#2=10.7.1.20
modify moBoard#11/moBoardIPAddress#3=10.8.1.20

modify moBoard#12/moBoardIPAddress#1=10.6.1.21
modify moBoard#13/moBoardIPAddress#2=10.7.1.21

modify moBoard#14/moBoardIPAddress#3=10.8.1.21

```

9. Activate new network configuration by unlocking the Media Gateway :

```

SC-1 -- ~ -- /moGW
•   unlock

```

```

Performing unlock action on /moGW - OK!

```

10. The new network configuration will be activated. Media Gateway boards will be reset and their **Operational State** will be changed to *Disabled* (boards will be displayed as Red in the EMS GUI).

It may take up to 5 minutes for all Media Gateway boards to complete the restart. When the Media Gateway board returns to service, its **Operational State** will be changed to *Enabled* and the board's color will be displayed as Green in the EMS GUI.

11. If interface separation of VLAN Tags configuration was changed, you will be asked to reset (lock/unlock) ES boards prior to performing the unlock action on Media Gateway . In such case, do the following:

- a. Lock both ES boards:

```
SC-1 -- ~ -- /moGW
```

- **lock esboard#9**

```
Do you really want to lock /moGW/moSwitchBoard#9? [y/n] y
```

```
Performing lock action on /moGW/moSwitchBoard#9 - OK!
```

- **lock esboard#19**

```
Do you really want to lock /moGW/moSwitchBoard#19? [y/n] y
```

```
Performing lock action on /moGW/moSwitchBoard#19 - OK!
```

- b. Unlock the ES board in slot 9:

```
SC-1 -- ~ -- /moGW
```

- **unlock esboard#9**

```
Performing unlock action on /moGW/moSwitchBoard#9 - OK!
```

- c. Wait up to 10 minutes until the ES board in slot 9 completes the restart operation and returns to service. Use the following command to determine whether the ES board has completed the restart operation or not. Value Enabled(1) indicates that board is back in service:

```
SC-1 -- ~ -- /moGW
```

- **show esboard#9 param OperationalState**

```
OperationalState=Enabled(1)
```

- d. Unlock the ES board in slot 19:

```
SC-1 -- ~ -- /moGW
```

- **unlock esboard#19**

```
Performing unlock action on /moGW/moSwitchBoard#19 - OK!
```

- e. Wait up to 10 minutes until the ES board in slot 19 completes the restart and returns to service. Use the following command to determine whether the ES board has completed the restart operation. Value Enabled(1) indicates that the board is back to service:

```
SC-1 -- ~ -- /moGW
```

- **show esboard#19 param OperationalState**

```
OperationalState=Enabled(1)
```

12. Connect the network cables to port 20 on both ES boards (located in slots 9 and 19).

B Appendix - Configuring HSRP/VRRP

This appendix describes how to configure the Media Gateway to operate with the Cisco Hot Standby Routing Protocol (HSRP).

B.1 Overview

The appendix describes example procedures for configuring the Media Gateway and the Cisco L3 switch network. The appendix also describes test failure scenarios. The procedures described in section 'Configuring the User Environment (Cisco L3 switch)' on page 893 are based on HSRP; however the same principals can also be applied to VRRP.

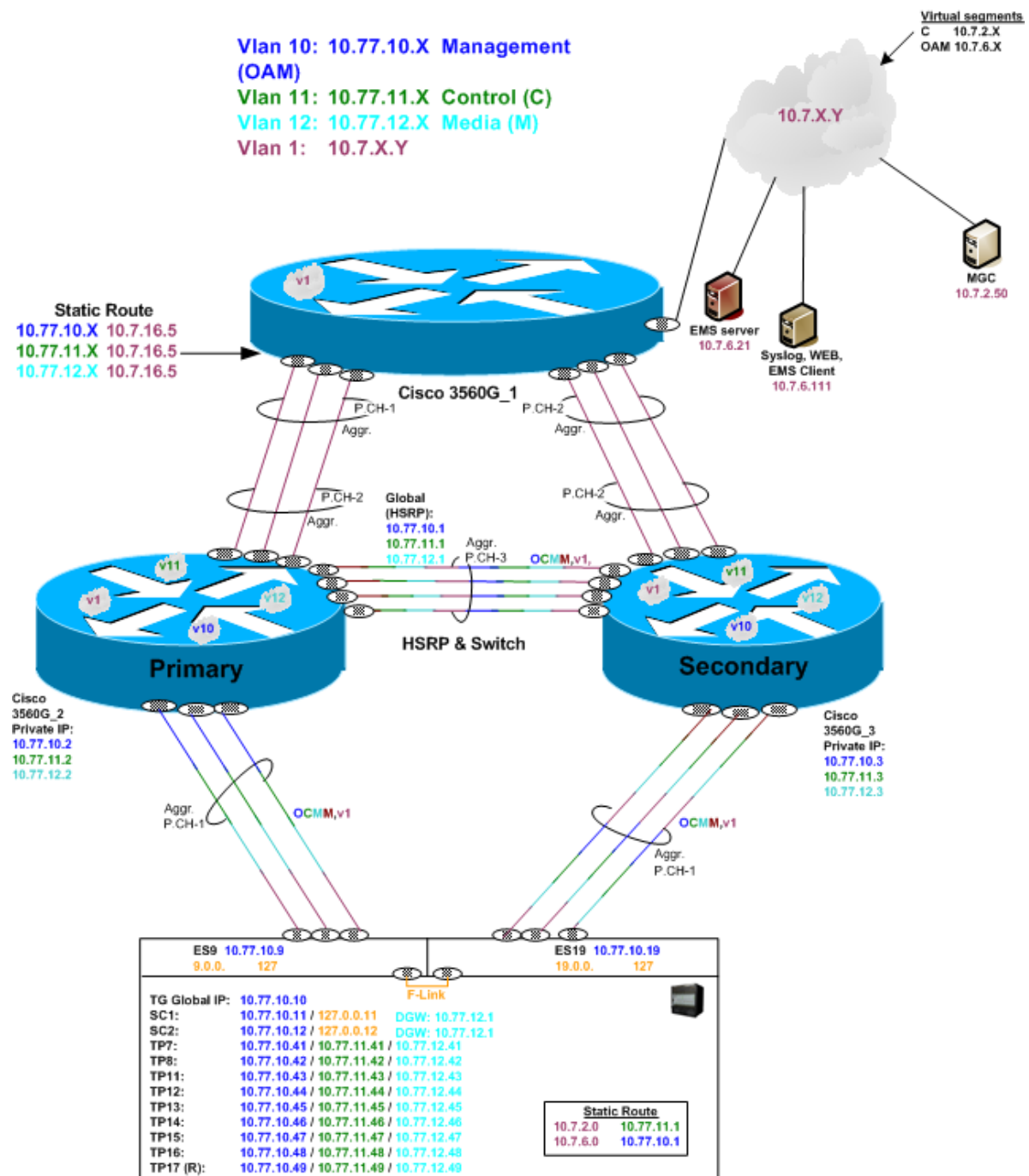
The example described in this appendix is based on the following data:

- 1 Mediant 8000
- 3 Cisco L3 switch (3560)
- 3 Subnets
- 3 VLANs
- No Physical Separation
- Link Aggregation



Note: The above data represents an example configuration. Modify configuration data according to your environment.

Figure B-1: HSRP/VRP Configuration



B.2 Configuring the Mediant 8000 Subnets

This section describes the CLI configuration actions required on the Media Gateway. The Media Gateway CLI configuration is based on the following example data:

B.2.1 Subnet Configuration

- OAM Subnet = 10.77.10.0/24
- CONTROL Subnet = 10.77.11.0/24
- MEDIA Subnet = 10.77.12.0/24

B.2.2 VLAN Configuration

- OAM VLAN ID = 10
- CONTROL VLAN ID = 11
- MEDIA VLAN ID = 12

B.2.3 OAM Subnet Settings

It is presumed that the SC boards are already configured with the correct IP addresses that belong to the OAM Subnet (10.77.10.0/24). If this is not the case, update the configuration as described in 'Configuring IP Network Connectivity on SC Boards' on page 195.

B.2.4 Interface Separation Settings

In the Media Gateway CLI, specify the following commands to configure the interface mode:

```
modify Interfaces=0
```

B.2.5 VLAN Settings

- In the Media Gateway CLI, specify the following commands to configure the Media Gateway to work with three VLANs:



Note: moVlanTag is relevant only for the ES/6600 switch only.

```
modify OAMTagID=10
add moVlanTag#1modify moVlanTag#1 VLANTagID=11
add moVlanTag#2
modify moVlanTag#2 VLANTagID=12
```

B.2.6 Subnets and Network Profiles Settings

- In the Media Gateway CLI, specify the following commands to configure the corresponding Subnets and Network Profiles:

```
add moSubnet#2
modify moSubnet#2 SubnetIP=10.77.11.0
modify moSubnet#2 SubnetPrefixBitsLength=24
modify moSubnet#2 DefaultGW=10.77.11.1
modify moSubnet#2 VLANTagID=11

add moSubnet#3
modify moSubnet#3 SubnetIP=10.77.12.0
modify moSubnet#3 SubnetPrefixBitsLength=24
modify moSubnet#3 DefaultGW=10.77.12.1
modify moSubnet#3 VLANTagID=12

add moNetworkProfile#1/moNetworkSubnet#2
modify moNetworkProfile#1/moNetworkSubnet#2 SubnetIndex=2
add moNetworkProfile#1/moNetworkSubnet#3
modify moNetworkProfile#1/moNetworkSubnet#3 SubnetIndex=3
```

B.2.7 Media Gateway Board's IP Addresses

In the Media Gateway CLI, specify the following commands to set the IP addresses of Media Gateway boards:

```
modify moBoard#7/moBoardIPAddress#1=10.77.10.100
modify moBoard#7/moBoardIPAddress#2=10.77.11.100
modify moBoard#7/moBoardIPAddress#3=10.77.12.100
```


B.2.8 Gateway Parameters Provisioning

When the Gateway requests (by ARP packet) the default gateway's MAC address, the virtual MAC address is received from the default gateway. When the RTP packets are received by the default gateway from the WAN, the private MAC is sent by the default gateway to the Gateway. Therefore, each time packets are sent and received to and from the WAN via the default gateway, the Gateway ARP table is updated. This update utilizes CPU resources.

To avoid excessive CPU utilization, the **MediaARPCacheoverride** parameter should be set to **2** (EnableGARP). When this value is set, the Gateway's ARP table is only updated when the GARP value is received. For example, when there is Gateway ES failover and another router becomes the default gateway.

```
modify /moGW/moBoard#7 MediaARPCacheoverride=EnableGARP(2)
```

B.3 Configuring the User Environment (Cisco L3 switch)

This section describes the CLI configuration actions required on the Cisco L3 switch.

B.3.1 IP Address

Set IP Address of Cisco L3 switch to VLAN interface and not to a physical interface.

```
ip address 10.77.10.3 255.255.255.0
```

B.3.2 Link Aggregation

In the Cisco CLI, perform the following link aggregation actions:

- Set the load distribution method among the ports in the EtherChannel. It's recommended to set the method to **dst-ip**, in case the TP IP address is consecutively allocated.

```
port-channel load-balance dst-ip
```



Note: If you retain the default value of the Cisco (src-mac), this leads to minimal distribution. Since the L3 switch replaces the source MAC-address (src-mac) of the packet frame with its MAC-address, the entire traffic will be transferred via only a single link.

- Verify for any IP address, which physical interface will be selected to communicate packets. To perform this action, specify the following command:

```
test etherchannel load-balance
```

- Assign a Cisco L3 switch port to a channel group and specify the LACP mode.
- **For ES/6600:** Configure a port into an active negotiating state in which the port starts negotiations with the Media Gateway ES port by sending LACP packets.

```
channel-group 1 mode active
```

- **For ES-2:** Configure a port into an “on” negotiating state in which no LACP is supported.

```
channel-group 1 mode on
```

B.3.3 Cisco L3 Switch-HSRP

In the Cisco CLI, specify the following commands:

- Set a hot standby priority value to choose the active router.

In the example described in this appendix, priority **105** is set for all VLAN interfaces for **3560_G2**. On the other L3 switch (**3560_G3**), the priority of all VLAN interfaces is 100 (default values). In the example, by default (if there is no failure) the active L3 switch is **3560_G2**.

```
standby 10 priority 105
```

- Configure an interface to track other interfaces so that if one of the other interfaces fails, the device's Hot Standby priority is lowered. In the example described in this appendix, all VLAN interfaces are configured to track the physical interfaces that are linked to **3560_G1** (GigabitEthernet0/20-0/22). When one of these links fails, the hot standby priority of all **3560_G1** interfaces VLAN decreases by 10, and **3560_G3** becomes the active switch.

There is no need to track the physical interfaces that are linked to the Media Gateway Ethernet Switch because the Media Gateway has a similar failover mechanism to switch from the Media Gateway Ethernet Switch with the link failure to the Media GatewayStandby Ethernet Switch.

```
standby 10 track GigabitEthernet0/20
```

B.3.4 Example Configuration Output

This section illustrates example command line output for the Cisco CLI commands specified in this section. Separate examples are illustrated for configuring the **3560_G1**, **3560_G2** and **3560_G3** Cisco switches.

The following data illustrates example output for the Cisco command **show running-config** for the **3560_G1** switch:



Note: For ES-2 switch, use command “channel-group XXX mode on”.

```
port-channel load-balance dst-ip
!
interface Port-channel1
!
interface Port-channel2
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
channel-group 1 mode active
!
interface GigabitEthernet0/3
channel-group 1 mode active
!
interface GigabitEthernet0/4
channel-group 1 mode active
!
interface GigabitEthernet0/5
channel-group 2 mode active
!
interface GigabitEthernet0/6
channel-group 2 mode active
!
interface GigabitEthernet0/7
channel-group 2 mode active
!
interface Vlan1
ip address 10.7.16.10 255.255.0.0
!
ip route 10.77.10.0 255.255.255.0 10.7.16.5
ip route 10.77.11.0 255.255.255.0 10.7.16.5
ip route 10.77.12.0 255.255.255.0 10.7.16.5
```

The following data illustrates example output for the Cisco command **show running-config** for the **3560_G2** switch:

```
port-channel load-balance dst-ip
!
interface Port-channel1
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 10-12
switchport mode trunk
!
interface Port-channel2
!
interface Port-channel3
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 10-12
switchport mode trunk
!
interface GigabitEthernet0/1
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 10-12
switchport mode trunk
channel-group 3 mode active
!
interface GigabitEthernet0/2
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 10-12
switchport mode trunk
channel-group 3 mode active
!
interface GigabitEthernet0/3
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 10-12
switchport mode trunk
channel-group 3 mode active
!
interface GigabitEthernet0/4
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 10-12
switchport mode trunk
channel-group 3 mode active
!
interface GigabitEthernet0/10
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 10-12
switchport mode trunk
channel-group 1 mode active
!
interface GigabitEthernet0/11
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 10-12
```

```
switchport mode trunk
channel-group 1 mode active
!
interface GigabitEthernet0/12
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 10-12
switchport mode trunk
channel-group 1 mode active
!
interface GigabitEthernet0/20
channel-group 2 mode active
!
interface GigabitEthernet0/21
channel-group 2 mode active
!
interface GigabitEthernet0/22
channel-group 2 mode active
!
interface Vlan1
ip address 10.7.16.4 255.255.0.0
standby 1 ip 10.7.16.5
standby 1 timers msec 330 msec 990
standby 1 priority 105
standby 1 preempt
standby 1 authentication HSRP1
standby 1 track GigabitEthernet0/20
standby 1 track GigabitEthernet0/21
standby 1 track GigabitEthernet0/22
!
interface Vlan10
ip address 10.77.10.2 255.255.255.0
standby 10 ip 10.77.10.1
standby 10 timers msec 330 msec 990
standby 10 priority 105
standby 10 preempt
standby 10 authentication HSRP10
standby 10 track GigabitEthernet0/20
standby 10 track GigabitEthernet0/21
standby 10 track GigabitEthernet0/22
!
interface Vlan11
ip address 10.77.11.2 255.255.255.0
standby 11 ip 10.77.11.1
standby 11 timers msec 330 msec 990
standby 11 priority 105
standby 11 preempt
standby 11 authentication HSRP11
standby 11 track GigabitEthernet0/20
standby 11 track GigabitEthernet0/21
standby 11 track GigabitEthernet0/22
!
```

```
interface Vlan12
ip address 10.77.12.2 255.255.255.0
standby 12 ip 10.77.12.1
standby 12 timers msec 330 msec 990
standby 12 priority 105
standby 12 preempt
standby 12 authentication HSRP12
standby 12 track GigabitEthernet0/20
standby 12 track GigabitEthernet0/21
standby 12 track GigabitEthernet0/22
```

B.3.5 “show running-config” of 3560_G3

The 3560_G3 output is identical to the **3560_G2** output, with the exception of the HSRP private IP addresses and the priority for **3560_G3 (default 100)**.

B.4 HSRP/VRRP Quality Testing

This section describes the quality tests that are recommended to be performed on the Cisco L3 switch. These tests are used to verify a smooth transition between states. There are 4 valid states (illustrated below).

The active Media Gateway Ethernet Switch is chosen by the Media Gateway according to the number of failed links between the Media Gateway Ethernet Switch, **3560_G2** and **3560_G2G3**.

On the other hand, the active L3 switch is chosen according to the failed link between **3560_G2** and **3560_G3** and between **3560_G2** and **3560_G1**.

In the EMS, the active Ethernet Switch is displayed.

To verify the L3 switch HSRP state, specify the following command:

```
show standby brief
```

B.4.1 Test Procedure

For each state, perform the following tests:

1. Check connectivity with the Media Gateway via the EMS.
2. Perform SC switch over and switch back.
3. Perform a call between a Mediant 8000 managed board and another endpoint in 10.7.0.0 / 16 network.
4. Perform TP switch over
5. Make sure that voice is heard on this call.
6. Perform TP switch back.
7. Make sure that voice is heard on this call.

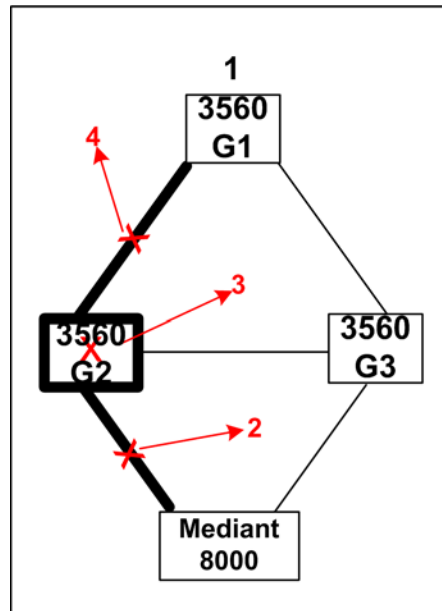
For each failure, perform the following tests:

8. Cause a failure
9. Check the existence of a call.
10. Close the call, and reestablish it.
11. Make sure that voice is heard on this new call.
12. Return the system to the Initial State.

B.4.1.1 Initial State: 1 (default state)

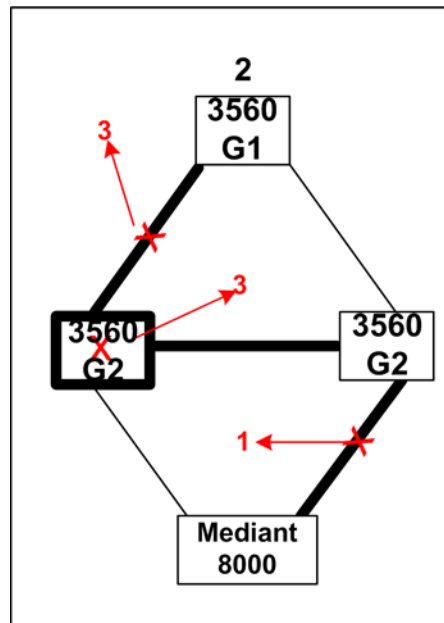
- In the EMS, right-click board 19 and select **Maintenance -> Align All Boards To Me -> state 2**
- Shut down 1 link from channel-group 1 on 3550_G2 Cisco ->state 2
- Shut down 1 link from channel-group 2 on 3550_G2 Cisco-> state 4
- Shut down 3550_G2 Cisco->state 3

Figure B-2: HSRP/VRPP Test State 1



B.4.1.2 Initial State: 2

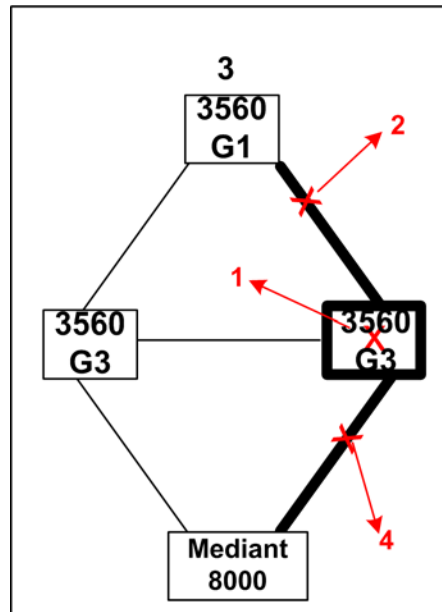
- In the EMS, right-click board 9 and select **Maintenance -> Align All Boards To Me -> state 1**
- Shut down 1 link from channel-group 1 on 550_G3 Cisco->state 1
- Shut down 1 link from channel-group 2 on 3550_G2 Cisco->state 3
- Shut down 3550_G2 Cisco ->state 3

Figure B-3: HSRP/VRPP Test State 2

B.4.1.3 Initial State: 3

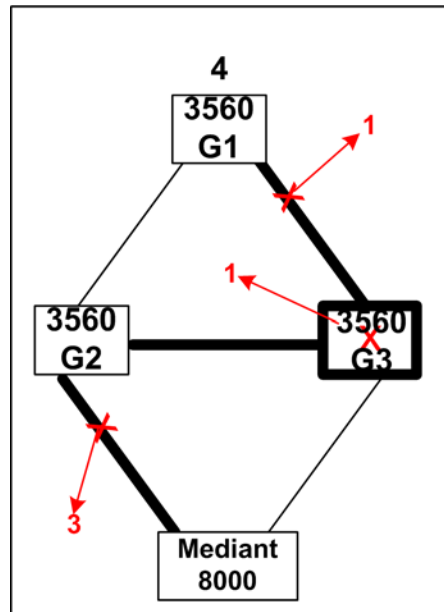
- In EMS, right-click board 9 and select **Maintenance -> Align All Boards To Me -> state 4**
- Shut down 1 link from channel-group 1 on 3550_G3 Cisco->state 4
- Shut down 1 link from channel-group 2 on 3550_G3 Cisco->state 2
- Shut down 3550_G3 Cisco->state 1

Figure B-4: HSRP/VRPP Test State 3



B.4.1.4 Initial State: 4

- In EMS, right-click board 19 and select **Maintenance -> Align All Boards To Me** -> state 3
- Shut down 1 link from channel-group 1 on 3550_G2 Cisco->state 3
- Shut down 1 link from channel-group 2 on 3550_G3 Cisco->state 1
- Shut down 3550_G2 Cisco->state 1

Figure B-5: HSRP/VRPP Test State 4

This page is intentionally left blank.

C Appendix: Testing Installation and Basic Configuration

The below test plan should be used after installing a new Media Gateway to assure the following:

- Media Gateway hardware is OK and was installed properly
- Media Gateway's basic configuration was successfully completed

It is recommended to integrate the below test plan as a component of the Acceptance Test Plan (ATP). The Media Gateway is a component of the complete ATP solution. The ATP is typically developed by the solution integrator and covers all solution components (e.g. Softswitch, Media Gateway, IP routers etc). The ATP typically verifies “end to end” functionality, for example, the calls running through the solution. The below test plan should be integrated in the ATP as part of this “end to end” functionality testing (e.g. you may send and receive calls through the Media Gateway, perform Media Gateway board switchover and then verify that calls are recovered on the redundant board).

Prior to running the tests described below, the tester should have a basic understanding of how to operate the product. Adjacent to each test case there is a reference to the relevant chapter in the documentation. The tester should read these chapters to acquire the required tools to run this test. Running this test can also be considered as an excellent initial hand's-on training session.

Table C-1: Test Procedures

#	Test Title	Test Description	Reference
1	Verify the connectivity between the EMS and the Media Gateway.	Open EMS client. Select Media Gateway in the MG Tree. Verify that Media Gateway status screen is displayed. Lock and Unlock Media Gateway. Verify that the appropriate changes to Administrative State alarms are displayed in the EMS alarms screen.	'Configuring Connectivity between Media Gateway and EMS Server' on page 171
2	Verify the NTP server configuration.	Verify that all provisioned NTP servers are <i>Unlocked</i> and <i>Enabled</i> . Open “NTP Server” status screen. Verify that at least one NTP server is provisioned (for simple installations EMS server may be used as NTP Server).	'Time and Date Configuration' on page 262
3	Verify the timezone configuration.	Connect to the CLI interface on both Active and Standby SC boards. Run date command. When both NTP Server and Timezone are properly configured, the date command should output correct time and date.	'Time and Date Configuration' on page 262

#	Test Title	Test Description	Reference
4	Verify the state of the Media Gateway	Open Media Gateways status screen. In the Information Pane, verify the following: Administrative State is <i>Unlocked</i> Operational State is <i>Enabled</i>	'Configuring & Operating the Media Gateway' on page 155
5	Verify the state of the SC boards.	Select 1 st SC board in the Media Gateway's status screen. In the Information Panel, verify the following: Administrative State is <i>Unlocked</i> Operational State is <i>Enabled</i> Repeat the above steps for the 2 nd SC board.	'Working with the SC Boards' on page 223
6	Verify the SC board switchover	Perform "Switch Over" maintenance action on the active SC board (the one with the grey background in the EMS GUI). Verify that SC switchover has successfully completed (another SC board should become active). Wait till the initially-active SC board returns to service (it's state changed to Unlocked/Enabled). Perform "Switch Back" maintenance action. Verify that activity switches back to initially-active SC board.	'Working with the SC Boards' on page 223
7	Verify the state of the ES boards	Select 1 st ES board in the Media Gateway's status screen. In the Information Panel, verify the following: Administrative State is <i>Unlocked</i> Operational State is <i>Enabled</i> Verify that the status of all uplinks, connected to the 1 st ES board, is <i>Unlocked / Enabled</i> with no alarms (uplink are displayed on the ES board's panel in the EMS status screen; uplinks in correct state are color-coded "green") Repeat the above steps for the 2 nd ES board.	'Working with the ES Boards' on page 261

#	Test Title	Test Description	Reference
8	Verify the ES board switchover	Disconnect uplink on the active ES board (the one with grey background in the EMS GUI). Verify connectivity between the EMS server and Media Gateway (Media Gateway is still visible in the EMS GUI). Verify that ES board's activity switchover is performed (another ES board should become active). Re-connect uplink to the ES board. Perform the "Align To Me" maintenance action on the "initially active" ES board. Verify that ES switchover is properly completed (initially-active ES board should become active).	'Working with the ES Boards' on page 261
9	Verify the state of the Media Gateway boards	Select 1st Media Gateway board in the Media Gateway's status screen. In the Information Panel, verify the following: Administrative State is <i>Unlocked</i> Operational State is <i>Enabled</i> Double-click the Media Gateway board and verify the state of it's PSTN links and trunks. All physically connected links and trunks should be <i>Unlocked/Enabled</i>. The rest of the links/trunks should be Locked. Repeat the above steps for all available Media Gateway boards.	'Working with the Media Gateway Boards' on page 245
10	Verify the state of the Media Gateway board's redundancy	Note: this test is applicable only to the configurations where redundant Media Gateway board is available. Open Redundancy provisioning screen. In the Redundancy TP List tab, verify that both Protection Required and Redundant Mode states for all non-redundant Media Gateway boards are hot.	'Working with the Media Gateway Boards' on page 245

#	Test Title	Test Description	Reference
11	Verify the Media Gateway board switchover	Note: this test is applicable only to configurations where the redundant Media Gateway board is available. Perform “Switch Over” maintenance action on one of the Media Gateway boards. Verify that switchover is performed (active Media Gateway board’s background is grey in the EMS; standby Media Gateway board’s background is blue; after switchover redundant board’s background color should be changed from blue to grey). Select redundant Media Gateway board. In the Information Panel, verify the following: Administrative State is <i>Unlocked</i> Operational State is <i>Enabled</i> Verify that all PSTN links/trunks are properly recovered on the redundant Media Gateway board. Lock and unlock the Media Gateway board, where you performed “Switch Over” maintenance action. Wait till its state is changed to <i>Unlocked/Enabled</i>. Perform “Switch Back” maintenance action on it. Verify that activity is switched back to it and its state is <i>Unlocked/Enabled</i>. Wait till the redundant Media Gateway returns to service (its state is changed to <i>Unlocked/Enabled</i>). Verify the state of Media Gateway board’s redundancy (as in the previous test).	'Working with the Media Gateway Boards' on page 245
12	Verify the state of the Media Gateway power supplies and FAN modules	Media Gateway power supplies and FAN modules are displayed on the EMS status screen. All physically-present elements should be color-coded <i>green</i> and have state <i>Unlocked/Enabled</i>.	'Configuring & Operating the Media Gateway' on page 155

#	Test Title	Test Description	Reference
13	Verify the state of the Media Gateway board's clock synchronization	Verify the status of the "System Clock" on the Media Gateway status screen. Normally-configured System Clock is color-coded <i>green</i>. Open the System Clock provisioning screen and verify that clock configuration matches your PSTN network setup.	Configuring TDM Synchronization (see page 265).

This page is intentionally left blank.

D Appendix - List of Notification Traps

The Media Gateway supports the generation of the following notification traps (alarms and events):

1. Board Failure Trap - failure of the specific board
2. Admin State Change - change of administrative state of specific entity
3. Operative State Change - change of operative state of specific entity
4. Trunk Alarm - trunk state change alarm
5. Configuration Error - configuration error
6. Operational Info - operational information
7. Voltage Alarm - voltage alarm
8. Fan Alarm - fan alarm
9. Temperature Alarm - temperature alarm
10. Ethernet External Link Alarm - ethernet external link alarm
11. Ethernet Internal Link Alarm - ethernet internal link alarm
12. Power Supply Alarm - power supply alarm
13. Push Button Alarm - push button alarm
14. Board Temperature Alarm - Media Gateway board temperature alarm
15. STM 1 Link Alarm - STM 1 link alarm
16. Board Diagnostics Alarm - board diagnostics alarmBoard Diagnostics Alarm - board diagnostics alarm
17. NTP Server Status Changed - NTP server status changed
18. GW Switchover Alarm - GW switchover alarm
19. Configuration Change - configuration change
20. SS7 Activity State Change - change of activity state of SS7 link or linkset
21. SS7 Local Inhibit State Change - change of local inhibit state of SS7 link
22. SS7 Remote Inhibit State Change - change of remote inhibit state of SS7 link
23. SS7 Congestion State Change - change of congestion state of SS7 link
24. Active Alarm Overflow Trap - overflow of Active Alarms table
25. Security Alarm – security alarm
26. Power Entry Module Alarm – alarm on the Power Entry Module (PEM)
27. Clock Synchronization Alarm – change in state of the PSTN clock synchronization
28. External Reference Clock Alarm – alarm on the external PSTN clock reference
29. Timing Module Alignment Alarm – change in the Media Gateway board's alignment to the Timing Module
30. Board Restart Alarm – indicates that specific Media Gateway board is being currently restarted
31. Hardware Error Alarm – hardware error alarm
32. High Availability Alarm – change in the HA status
33. Security Event – security event
34. Line Sync Reference Clock Alarm – alarm on the reference PSTN clock in Line Sync mode

- 35. DS3 Alarm – DS3 alarm
- 36. SIP Call Resource Alarm – SIP call resource outage alarm
- 37. SIP Proxy Failure Alarm – failure in communication between Media Gateway and SIP Proxy
- 38. SIP Overload Alarm – board is overloaded by SIP calls
- 39. D-Channel Status Alarm – D-channel status change
- 40. MGC Connection Alarm – failure in communication between Media Gateway and Media Gateway Controller (MGC)
- 41. Alarm Throttling Limit Exceeded Alarm – indicates that alarm throttling mechanism is activated and therefore some alarms are suppressed
- 42. Board CPU Overload Alarm – board CPU overload alarm
- 43. Trunk Activity State Change Alarm – change of trunk's activity status
- 44. V5.2 Port File Alarm – v5.2 port configuration change alarm
- 45. Switch Board Alarm – Ethernet Switch (ES) board alarm
- 46. License Key Alarm – license key mismatch alarm
- 47. AAA Alarm – centralized AAA server alarm
- 48. PM Threshold Alarm – PM threshold alarm for any History PM
- 49. Configuration Backdoor Event – Board is unlocked with Configuration Backdoor
- 50. B Channel Alarm – trunk sends B-channel alarm status
- 51. LDAP server alarm–connection with LDAP server is lost

For a detailed information on supported alarms, refer to the *LTRT-237xx* Mediant 5000 and Mediant 8000 Alarm and Performance Monitoring Guide.

54 Index

)

)OAM Subnet Settings 891

1

1.4.4.2Attaching IP Network Profile to the
Media Gateway Board 201, 210

6

6310/RTM - Rear Transition Module 49, 460,
463

6310/RTM Redundant 51, 841

8

8410/RTM E1/T1 Trunk Connectors 58, 93

8410/RTM Rear Transition Module 57, 841

8410/RTM Redundant 61

A

Accessing Advanced Status of Media Gateway
Board via WEB Interface.....857

Account Group.....622

Action/Event 446

Actions 438

Activating New Network Interfaces
Configuration.....187, 188, 214Activating Offline Network Configuration.....215,
216Activating the new X.509 Certificates on the
Media Gateway 329, 331, 337

Activity Switchover.....254

Actual Redundancy Mode 250, 252

Adding Certificates to the Auxiliary Files
Repository 331Adding Media Gateway Boards to a Mediant
8000 System 797Adding the Media Gateway Software to the
EMS Server 819

Additional Network Services and Settings .. 212

Additional Network Settings..... 203

Additional OAM Subnet Configuration 197

Administering Command Line Interface (CLI)
Users 115, 305, 361

Administering the EMS User..... 365

Administering the Local CLI User Database369

Administering the ROOT User 362

Advanced Configuration 90, 155, 483, 503, 507

After Completing the Online Software Upgrade
..... 827

Aggregated Link Failure Detection 193

Alarm Indicators 45

Allocating IP Addresses 97

Alternative Routing Provisioning Rules..... 670,
679

AMR Coder Policy..... 540

Appendix

Testing Installation and Basic Configuration
..... 905

Appendix

Examples of IP Network Connectivity
Configuration 96, 180

Appendix - Configuring HSRP/VRRP 889

Appendix - List of Notification Traps..... 911

Associating Media Gateway Controller with
Media Gateway Boards 285, 288Attaching an IP Network Profile to the Media
Gateway Board..... 202Attaching IP Network Profile to the Media
Gateway Board..... 198

AudioCodes Technical Support Log Areas .	871	Collecting Advanced Media Gateway Board Logs.....	845, 873
Automatic Backups.....	788	Collecting Call Data Records (CDRs).....	852
Automatic Switchback	258	Collecting Call Data Records (CDRs) on MEGACO Boards	854
Auxiliary Files Repository ...	295, 331, 422, 433, 453	Collecting Call Data Records on SIP Boards	852
B		Collecting Debug Recording Traces on the Standby SC board	851
Benefits.....	191	Collecting the Media Gateway Board's INI File	855
Board Assembly Order	47, 53, 87, 798, 799	Collecting the Report File	874, 878
Bringing V5.2 Interfaces	301	Collecting Traces from the Ethernet Switch Board's Mirror Port	859
C		Command Line Interface Users .	113, 142, 151, 829
Cables.....	92	Configuration Freeze and Configuration Change Event.....	399
Call Progress Tones (CPT) Files.....	422	Configuring & Operating the Media Gateway	156, 797, 908
CAS File Syntax	437	Configuring AD-Based Routing Rules	645
CAS Files.....	437	Configuring Additional MEGACO Settings .	289
Centralized AAA Servers.....	361, 375	Configuring Alternate Routing.....	679
Centralized RADIUS Servers	369, 384	Configuring an X.509 Certificate Expiration Date Reminder	336
Centralized TACACS+ Servers	375	Configuring Coder Groups.....	608
Centralized User Authentication via RADIUS Protocol	375	Configuring Coders Table	608
Changing Password of the CLI User	373	Configuring Connectivity between the Media Gateway and Additional SNMP Managers	175, 309
Changing the Password of the EMS User..	365, 818	Configuring Connectivity between the Media Gateway and EMS Server.....	341
Changing the ROOT User Password .	362, 365, 818	Configuring Connectivity between the Media Gateway and the EMS Server	154, 171, 180, 309, 341
Channelized T3	464		
Checking Certificate Revocation Status	338		
Cisco L3 Switch-HSRP	894		
CLI Interface Access Control.....	115, 389		
CLI Login Banner.....	360		
CLI Users Database and Operation Modes	361		
Coders Table	609		

Configuring Connectivity between the Media Gateway and the Syslog Server	178	Configuring MGCP/MEGACO Call Control Settings	277, 283
Configuring Connectivity with the EMS Server	154, 305, 838	Configuring Mirror Destination	868
Configuring ES Mirror Filters	859	Configuring Mirroring on ES boards' Port ...	867
Configuring Filter Rules	848	Configuring Network Topology ..	179, 183, 217, 304
Configuring IP Address on the Replaced SC Board.....	794	Configuring NTP Servers	271
Configuring IP Network Connectivity on Media Gateway Boards	179, 198	Configuring Query Attribute Key	644
Configuring IP Network Connectivity on SC Boards.....	179, 196, 199, 891	Configuring Redundant Media Gateway Board	248, 249, 254, 255
Configuring IP Network Interfaces.....	186	Configuring Security Settings	303
Configuring IP to Telephone/Inbound Routing	676	Configuring SIP / ISDN Cause Mapping.....	681
Configuring IPSEC/IKE for Call Control and Signaling Interfaces (on TP boards)	305, 346	Configuring STM-1/OC-3 Interfaces	460
Configuring IPSEC/IKE for Management Interfaces (on SC boards).....	172, 173, 177, 178, 309, 341	Configuring T3 Interfaces	463
Configuring IPSEC/IKE for MGCP/MEGACO Call Control Interfaces	346	Configuring TDM Clock Synchronization ...	516, 842
Configuring IPv6	210	Configuring Telephone to IP/Outbound Routing	671
Configuring LDAP server parameters .	640, 645	Configuring the Basic IP Network Parameters of SC Boards ..	118, 148, 196, 783, 795, 838, 882, 885
Configuring Media Gateway Board's IP Addresses	198, 202	Configuring the Calling Name Manipulation Table for Tel to IP Routing	661
Configuring Media Gateway Board's PSTN Settings	459	Configuring the CAS/ISDN Application	508, 513
Configuring Media Gateway board's PSTN parameters	296	Configuring the CAS/ISDN Subsystem.....	507
Configuring Media Gateway Controller	285	Configuring the E1/T1 Trunks.....	463, 465
Configuring Media Link Aggregation	194	Configuring the EMS and ROOT Passwords of the Mediant 8000 in the EMS.....	818
Configuring Media Realms	210, 739	Configuring the Internal DNS Table.....	625
Configuring MEGACO Virtual Gateways.....	283	Configuring the IUA/DUA Application .	513, 515
		Configuring the M2TN Application	504
		Configuring the M2UA (SG Side) Application	476, 482, 504
		Configuring the Media Settings.....	527, 842

Configuring the Mediant 8000 Subnets	891	Connecting IP Network Cables	121
Configuring the MGCP/MEGACO Protocols	277	Connecting Mediant 8000 to IP Network	185
Configuring the MTP3/M3UA Application...475, 485, 499, 504		Connecting STM-1/OC-3 PSTN Cables	123
Configuring the Number Manipulation Tables	658, 659	Connecting the Media Gateway to the IP Network	96, 117, 123, 179, 783, 881
Configuring the PSTN Subsystem.....	459	Connecting the Mediant 8000 to the IP Network	117, 185, 217, 839
Configuring the Redirect Number Manipulation IP to Tel Routing	662	Connecting the T3 PSTN Interfaces	125
Configuring the Redirect Number Manipulation Tel to IP Routing	663	Connecting to External Telco Alarm Equipment	127
Configuring the SBC Message Manipulation Table	763	Connecting to the CLI via an RS-232 Serial Console ..	109, 115, 118, 181, 364, 843, 882, 886
Configuring the SIP SRV to IP Table	626	Connecting to the CLI via the IP Internet Network	112, 115, 171, 779, 785
Configuring the SS7 Subsystem	472	Connecting to the IP Network	89, 117, 180, 843
Configuring the Syslog Server.....	845	Connecting to the PSTN Network.	89, 123, 467
Configuring the User Environment (Cisco L3 switch)	889, 893	Constraints for Adding Boards to the Mediant 8000 System	798
Configuring the V5.2 Access Gateway.....	296	Converting CAS File to Binary Format.....	451
Configuring Trunks for the V5.2 Access Gateway application.....	296	Converting External Coders File to Binary Format	453, 455
Configuring V5.2 Interfaces	297, 300, 301	Converting the Call Progress Tones File to Binary Format.....	423, 429
Configuring V5.2 Links	298	Cooling System.....	43
Configuring V5.2 User Ports.....	299	Creating a New CLI User	370
Configuring VLAN Tags.....	188	Creating a Pre-Recorder Tones File...	430, 431
Configuring VLAN Tags for Media and Control Subnets	189	Creating a Voice Prompts File	433
Configuring VLAN Tags for OAM Subnet...189, 196, 215		Creating IP Network Profile	201
Connecting Cables to Media Gateway's RTM Module	797	Creating the Media Gateway Software Backup	778, 788
Connecting E1/T1 PSTN Cables (TP-8410 Boards).....	125	Customer's Log Area	871
		D	
		Deleting a CLI User.....	372

Desired Redundancy Mode	251	ES-2 ES (Ethernet Switch) Board	80, 121
Determining Source and Destination URL ..	740	ES-2 Physical Slots to Ethernet Port Mapping	83
Diagnostics & Troubleshooting	796	ES-2 RTM Rear Transition Module	85
Dial Plan Prefix Tags for IP-to-Tel Routing .	456	ESD Requirements	791
Dialing Plan Notation	665, 666, 669, 676	Establishing Connectivity with the EMS Server	179, 180, 189
Disabled Remote Root Login	309	Ethernet ports allocation on ES-2-SINGLE boards	219
Disabling a Direct Remote Root Login 311, 827		Ethernet Ports Allocation on the ES/6600 Board	122, 187, 217, 221
Disabling Secure Operation Mode	308	Ethernet Switch Board	73, 802
Displaying VoIP Board Log Files	846	Ethernet Switch Board Replacement Procedure	801
Distribution Rules	191	Example 2	
Domain Name Provisioning	282	Three Subnets, VLAN Tags, One Physical Interface	885
DSP Templates	539	Example Configuration Output	895
E		Examples of IP Network Connectivity Configuration	881
Earthing the Chassis	102	External Coders Files	453
Electrical Requirements	42, 94	External Layer 3 Ethernet Switches or Routers	185, 221
EMS Verifications	817	F	
Empty Slots Cover Requirements	792	Faults and Alarms Monitoring	167, 471
Enabling a Direct Remote Root Login .310, 311		File System Integrity	226, 316
Enabling Secure Operation Mode	307, 308	Filtering Syslog Messages and Debug Recordings	848
Endpoint Name Provisioning	280	Finish	827
Environmental Requirements	95	Firewall Functionality on Media Gateway Boards	353
Ephemeral Terminations (for MEGACO only)	281	Function	449
Equipment Requirements	91	Functions	438
ES Board Actions – ES/6600	262		
ES Board Actions – ES-2	262		
ES/6600 ES (Ethernet Switch) Board	73		
ES/6600 Physical Slots to Ethernet Port Mapping	76		
ES/6600/RTM Rear Transition Module .78, 121			

G

Gateway Parameters Provisioning	893
General SIP Configuration.....	547
Generating a Certificate Signing Request (CSR)	329, 338
Generating a New Private Key	337
Graceful Shutdown Mode	812

H

Hardware and Application Types	247
Hardware Components.....	35
Hardware Installation.....	89, 99
Hardware Replacement.....	791
Hardware Replacement Preliminaries	791
History Performance Measurements	409
Hitless Upgrade Mode	812
HSRP/VRRP Quality Testing.....	899

I

Information Needed when Contacting Technical Support	877
INIT Variables.....	438
Initial Configuration.....	326
Installation Requirements	228
Installing from the USB Flash Drive	241
Installing OS Security Patches from a Latest Installation Package.....	313, 817
Installing the EMS Server and Client.....	98
Installing the Latest OS Security Patches from the	315
Installing the Linux OS from the USB CD/DVD Drive via the RS-232 Serial Console	244

Installing the Linux OS from the USB Flash Drive via the RS-232 Serial Console.....	238, 245
Installing the Linux OS on the SC Rev.2 Board	231
Installing the Mediant 8000 Software.....	64, 67, 129, 226, 266
Installing the Mediant 8000 Software on the SC Board to Operate as the Active board	133, 134, 362
Installing the Mediant 8000 Software on the SC Board to Operate as the Standby.....	134
Installing the Mediant 8000 Software on the SC Board to Operate as the Standby Board	134, 140
Installing the Operating System (OS) on the Replaced SC Board.....	794
Installing the Software on the Replaced SC Board	795, 838
Installing the Solaris 9 OS on the SC Board.....	229
Installing the Solaris OS on the SC Rev.1 Board	227
Interface Separation Settings	891
Internal NTP Implementation	270
Internal System Controller (SC) Software Logs	265, 871
Introduction	31
Intrusion Detection Events.....	398
IP Address	893
IP Groups Table.....	548, 611, 628
IP Network Interface Separation.....	188
IP Network Profiles	198, 200, 210
IP Profile Table	689
IP Subnets	198, 210

IP to Telephone/Inbound Routing Provisioning Rules	675	Media Gateway Board Replacement Procedure	795
IP to Telephone/Inbound Routing Table.....	666, 675, 679	Media Gateway Board's IP Addresses	892
IPSEC and IKE	339	Media Gateway Board's Debug Recording Traces and Logging.....	850
IP-to-IP Application	649	Media Gateway Boards in the EMS	246
ISDN Operational Status	515	Media Gateway Controller Addressing	279
L		Media Gateway Inventory	415
Least Cost Routing (LCR) Table	633	Media Gateway Software Backup/Restore Procedures	777
Lightning Protection	103	Media Link Aggregation	191
Link Aggregation.....	893	Media Security	305, 350
Link Aggregation Control Protocol.....	193	Megaco Control Protocol	278
Linux OS Installation Requirements	232	MEGACO Virtual Gateways.....	277, 282
Log Areas	871	MGCP Control Protocol	278
Log Files Storage	872	Modifying the.....	423, 453
Logging in as a Root User ..115, 118, 134, 140, 147, 150, 227, 231, 233, 237, 243, 307, 310, 313, 319, 358, 359, 360, 363, 365, 368, 370, 372, 373, 396, 785, 843, 851		Modifying the Media Gateway Configuration	165
Logging into the Command Line Interface .115, 129, 133, 153, 171, 181, 317, 779, 854, 874, 882, 886		Mounting the Chassis on a Rack	100
M		MTP3/M3UA Operational Status	498
M2UA (SG Side) Operational Status.....	482	Multiple Redundancy Groups	247, 255
Managed Objects (MOs) in the EMS.....	162	N	
Managed Objects, Administrative and Operational State	160	NAT Translation Table	632
Manipulation on all Inbound/Outbound SIP INVITE.....	658	NEBS Compliancy	40
Manipulation Tables	658	Network Services on the Mediant 8000	357, 839
Media Gateway Boards' Configuration Backdoor	417	Next State	451
Media Gateway Board Actions	247, 249, 797	NTP Synchronization and Status.....	269
		Numbering Plans and Type of Number	659, 666

O

One Subnet, One Physical Interface, No VLAN Tags	881
Online Provisioning.....	482, 498, 506, 515
Online Software Upgrade	226, 811
OpenBoot PROM on SC Rev.1 Boards.....	358
Operating System Logs	874
Operation Rules.....	665
OS Auditing on SC Boards	320
OS Auditing on the Mediant 8000 Media Gateway	321
OS Hardening.....	311
OS Security Patches (on SC boards).....	312
Overview....	159, 293, 715, 725, 811, 822, 826, 828

P

Packet Cable Security	350
Parameters	449
Password-less Access to the CLI Interface	115, 362, 390
Performing Basic Configuration of the Mediant 8000 Software	130, 196, 266, 882, 886
Performance Measurement Threshold Alarms	412
Performance Measurements	265, 401
Performance Monitoring Profiles	402
Performing a Manual Rollback to the Previous Software Configuration	829
Performing Basic Configuration of the Mediant 8000 Software on the SC board to Operate as the Active Board.....	147, 307, 362
Performing Basic Configuration of the Mediant 8000 Software on the SC Board to Operate as the Standby Board	150, 307

Performing the Online Software Upgrade...	820
Planning the Maintenance Time Period.....	815
Possible Uses for Telephone to IP/Outbound Routing	669
Possible Uses for the Number Manipulation Tables.....	658
Power Supply Modules Replacement.....	804
Power System.....	41
Powering Up	89, 103
Pre-installing OS Patches	816, 817
Preparing for the Mediant 8000 Software Installation	133
Preparing for the Online Software Upgrade	813
Preparing the E1/T1 PSTN Connections	98
Preparing the External Layer Switches or Routers.....	117
Preparing the 'Install Image' on the Install Server (EMS).....	228
Preparing the IP Network.....	814, 815
Preparing the IP Network Connectivity	96
Preparing the Media Gateway	813
Preparing the PSTN Network Connectivity...	98
Preparing the STM-1/OC-3 PSTN Connections	98
Preparing the T3 PSTN Connections	98
Pre-Recorded Tones (PRT) Files	430
Pre-Upgrade Configuration Backup.....	813
Profiles Tables	683
PSTN Gateway and IP-to-IP Applications ..	649
PSTN Gateway Application	649

Q

Quality of Service.....	197, 198, 201, 206

Querying the AD and Routing Priority 642

R

Real-Time Performance Measurements 405

Reasons for Alternative Routing..670, 675, 679

Recovering the OAM VLAN Settings...118, 843

Recovering the ROOT User Password 364

Recovery from a Network Failure or EMS
Server/Client Crash.....831

Redundancy Modes.....250

Redundant Configuration....482, 485, 499, 506,
515

Registration Refreshes 768

Registration Request Processing 765

Registrations Database 766

Re-installing the Linux OS via the Remote
Network Connection.....233

Re-installing the Linux OS via the RS-232
Serial Console.....235

Replacing Air Filters 808

Replacing the Failed Media Gateway Board
.....245, 795, 797

Replacing the Failed SC Board 793

Replacing the Fan Tray Modules 807

Replacing the Media Gateway Board's RTM
module 796

Reserved Words.....440

Restoring the Media Gateway Software from
Backup 783, 788

Rollback 828

Routing Based on LDAP Active Directory
Queries.....639

Routing using Registrations Database 767

S

SA/RTM Replacement Procedure 797, 800

SA/RTM Synchronization and Alarm Rear
Transition Module..... 69, 110, 519, 523, 842

SAS Modes 715

SAS Registration Manipulation 723

SBC Admission Control 768

SBC Condition Table 744

SBC Inbound and Outbound Manipulation . 754

SBC Media Handling..... 770

SBC Message Manipulation 658, 761

SBC Routing 628, 629, 745

SC Board Actions..... 225

SC Board Hardware Revisions 225

SC Board Replacement Procedure 793, 829

SC Rev.1 board (Solaris OS)..... 64

SC Rev.2 Board (Linux OS)..... 66, 110, 836

Secure Access to the CLI Interface 309

Secure Access to the SNMP Management
Interface 308

Secure Operation Mode..... 137, 149, 305, 306

Secure RTP 350

Securing the Syslog Management Interface178

Security Configuration Guidelines 305

Self-Signed Certificate 327

Session Border Controller (SBC) Application
..... 715, 725

SIP Board Syslog Level 846

SIP Dialog Initiation Process 739

SIP Interfaces Table 628, 630, 738

SIP Message Policy Table 637

SIP Network Definitions.....	737	STP Functionality (Alias Point Code).....	504
SIP over SSL/TLS (SIPS).....	305, 349	Subnets and Network Profiles Settings	892
SIP Protocol Settings.....	563	Supported Actions.....	420
SIP Proxy Sets	548	Supported SS7 Architectures	473
SIP Routing DNS Table.....	625	Synchronizing the CLI Users Database with the EMS Server	361, 367, 369
SIP SRV to IP Table	626	Syslog Management Interface	160, 177
SIP to ISDN and ISDN to Release Cause Mapping	681	Syslog Protocol	845
Site Preparation.....	89, 91	System Controller (SC) Board	63
Slot Assignment.....	791	T	
SNMP Management Interface	160, 171, 308	Tel Profile Table.....	684
Software Installation and Basic Configuration	89, 129	Telephone to IP/Outbound Routing Provisioning Rules.....	669
Software Upgrade/Rollback Troubleshooting	828	Telephone to IP/Outbound Routing Table .	666, 669, 679
Source IP Group Classification.....	740	Test Procedure	899
SRD Table	628, 737	The Chassis	39
SS7 M2TN Tunneling Architecture	475	The Command Line Interface (CLI)	89, 109, 129, 133, 134, 140, 147, 150, 153, 227, 229, 231, 233, 235, 237, 241, 243, 307, 310, 313, 318, 319, 358, 359, 360, 361, 363, 365, 368, 370, 372, 373, 393, 397, 829, 851, 854, 874
SS7 M2UA (SG Side) Architecture.....	474	The Mediant 8000 Installation Package	130
SS7 MTP3/M3UA Architecture	474	The Operating System on the SC Boards .	226, 795
Stand Alone Board Clock Mode	516	The Redundancy Model.....	249, 841
Stand-Alone Survivability (SAS) Application	715	The Routing Tables.....	668
Starting Mediant 8000 Software	153	The SAS Configuration	716
Starting Mirroring on ES Board.....	869	The SBC Configuration	716, 727
Starting the Online Software Upgrade Wizard	820, 824, 826	The SIP Proxy.....	547, 628, 670
States.....	438	The SIP Registrar	558
State's Line Structure	440	Time and Date Configuration.....	265
Static Routes	203	Time Zone Settings.....	265
Stopping Mirroring on ES Board.....	869		

Timing Module BITS Sync Clock Mode.....516, 519	Using Tagged VLANs for Subnet Separation 188
Timing Module Line Sync Clock Mode 516, 522	Using the EMS server as the NTP Server .. 266
TP-6310 Media Gateway Board 47, 463	V
TP-8410 Media Gateway Board 53, 465	V5.2 Access Gateway..... 293
Transferring the Mediant 8000 Installation Package to the SC Boards.....131, 313, 782, 785	V5.2 Interface Status and Maintenance Actions 294
Transferring the SC Software Package to the SC Boards.....815, 823	V5.2 Link Status and Maintenance Actions 295
Troubleshooting Strategy 835	V5.2 User Ports Status 295
Troubleshooting the ES/6600 Board Installation.....803	Verifying that the Online Software Upgrade is Supported..... 814
Troubleshooting the Newly installed Media Gateway Board 799, 841	Verifying the Current Version of the Linux OS on the SC Board..... 231
Trunk Group Settings Table 653, 675	Verifying the Current Version of the Solaris OS on the SC Board..... 227
Trunk Groups Table.....650	Viewing Log Files..... 873
Types of IP Network Traffic and Network Subnets 183	Viewing NTP Servers' Status..... 273
U	Viewing Trunk Channels Status..... 470
Unpacking/Checking Contents 99	VLAN Settings..... 891
Updating License Key.....259, 649	Voice Prompts Files 433
Upgrading the 1 st SC Board 826	W
Upgrading the 2 nd SC Board.....824, 826	Welcome Questionnaire 821, 826
Upgrading the ES Boards.....826	Working with the ES Boards 261, 801, 802, 803, 839, 840, 906, 907
Upgrading the Media Gateway Boards 826	Working with the Media Gateway Boards (TP- 6310 and TP-8410) 245, 795, 796, 840, 841, 857, 907, 908
Usage Tips.....420	Working with the SC Boards..... 223, 313, 315, 837, 839, 906
Use of OAM, Control and Media Subnets by Mediant 8000 Boards 185	Working with the V5.2 Access Gateway 294
User Registration 765	Working with VLANs 188
Using Auxiliary Files 421	X
Using External NTP Servers.....266	X.509 Public Key Infrastructure 265, 325

Mediant 8000™

Installation, Operation, Maintenance Manual

