Installing and Operating the Avaya G860 Media Gateway
# Contents

## Installing and Operating the Avaya G860 Media Gateway

1. **Introduction to the Avaya G860 Media Gateway**
   
   1.1 Media Gateway Block Diagrams

   1.1.1 Avaya G860 Board Configuration
   
   1.1.2 Avaya G860 Accessory Kit

   1.2 Front and Back Views of the Avaya G860

   1.3 The Chassis

   1.3.1 Earthing Requirements
   
   1.3.2 Power Requirements

   1.3.2.1 Power Consumption
   
   1.3.2.2 Electro Magnetic Compatibility (EMC) Features

   1.3.3 Midplane Keying

   1.4 Cooling System

   1.4.1 FML-5/Left Fan Tray - Fan Tray Unit

   1.4.2 FMR/5K - Fan Tray Unit

   1.4.3 FPM/5K - Advanced Fan Power Module

   1.4.4 Alarm Indicators

   1.5 Avaya G860 Boards

   1.5.1 The TP-6310 Media Gateway Board

   1.5.1.1 T3 6310 Board Panel T3 LED Indicators

   1.5.1.2 6310/RTM - Rear Transition Module

   1.5.2 SC (System Controller) Board

   1.5.2.1 Front Panel Mini DIN 8 COM Serial Port

   1.5.2.2 System Controller Panel Indicators & Controls

   1.5.3 SA Synchronization and Alarm RTM

   1.5.3.1 SA/RTM Overview

   1.5.3.2 Chassis Management

   1.5.3.3 Chassis Temperature Control

   1.5.3.4 Synchronization

   1.5.3.5 SA/RTM Card and Panel

   1.5.3.6 RS-232 Console Pin Signal Interface

   1.5.3.7 LED Interface

   1.5.3.8 Terminal Block Connector

   1.5.3.9 RJ48-c Pin Signal Interface (Optional)

   1.6 Ethernet Switch Boards

   1.6.1 ES/6600 - Used in Avaya G860 Configurations

   1.6.1.1 ES/6600 Panel Indicators

   1.6.1.2 ES/6600 Physical Slots to Ethernet Port Correlation - Avaya G860 Configuration

   1.6.1.3 ES/6600/RTM

   1.7 Board Assembly Order

2. **Getting Started with the Avaya G860**

   2.1 Installation Process Flow

   2.2 Site Preparation

   2.2.1 Physical Requirements

   2.2.1.1 Equipment
2.2.1.2 Electrical ................................................................. 54
2.2.1.3 Cables ........................................................................ 55
2.2.2 Defining IP Parameters .................................................. 56
2.2.2.1 Gateway Addresses ...................................................... 57
2.2.2.2 Boards' IP Addresses for Avaya G860 Configuration ....... 57
2.2.2.3 Network Servers' IP Addresses ...................................... 57
2.2.2.4 VLANs Configuration .................................................. 58
2.2.2.5 DiffServ Priorities ....................................................... 58
2.2.2.6 IEEE 802.1p QoS/CoS Layer 2 Traffic Prioritization ....... 58
2.2.2.7 IPSEC Configuration ................................................... 59
2.2.3 Environmental Requirements .......................................... 60
2.2.3.1 Environmental Conditions ............................................ 60
2.2.3.2 Temperature ............................................................... 60
2.2.3.3 Humidity ..................................................................... 60
2.2.3.4 Lightning Protection .................................................... 60
2.2.3.5 Altitude ....................................................................... 60
2.2.3.6 Earthquake ................................................................. 61
2.2.3.7 Rack Requirements ...................................................... 61
2.3 Preparing the IP Network Connectivity ................................. 61
2.3.1 Preparing the PSTN Network Connectivity ......................... 62
2.3.1.1 SDH/SONET Network Connections .............................. 62
2.3.1.2 T3 Network Connections ............................................. 62
2.3.2 Clock Synchronization ..................................................... 63
2.4 Unpacking/Checking Contents .............................................. 63
2.5 Mounting the Chassis on a Rack .......................................... 65
2.6 Earthing ............................................................................ 68
2.6.1 Earthing the Gateway ..................................................... 68
2.7 Powering Up ...................................................................... 69
2.7.1 Connecting System Power ................................................. 70
2.7.1.1 Connecting DC Power ................................................ 70
2.7.1.2 Connecting AC Power .................................................. 72
2.7.1.3 Connecting Power - 6310 System Configuration ............. 74
2.7.2 Post-Power Connection Test Procedures Checklist ............. 76
2.8 Configuring the Basic IP Network Parameters of SC Boards .... 78
2.8.1 Connecting to the SC Board's RS-232 Console ..................... 78
2.9 Cabling the Avaya G860 ....................................................... 81
2.9.1 Connecting the ES/6600 IP Network CAT 5 Copper Cabling ...... 82
2.9.2 Connecting the PSTN Interface - STM-1/OC-3 Configurations .... 83
2.9.2.1 Connecting Fiber Optic Cables to the SFP Trunk Interfaces ... 83
2.9.2.2 Fiber Optic Connections ............................................. 83
2.9.2.3 SFP Modules ............................................................... 83
2.9.2.4 Connecting the PSTN Interface .................................... 84
2.9.3 Connecting the T3 PSTN Interfaces .................................... 86
2.9.4 External Alarm Indicator Connections ............................... 86
2.10 Changing the Basic Configuration of the SC Boards .......... 88
2.10.1 Connecting to the SC Board's Terminal ............................. 89
2.10.1.1 Connecting to the SC Board's Terminal via Telnet ............ 89
2.10.1.2 Connecting to the SC Board's Terminal via SSH ............. 90
2.10.1.3 Connecting to the SC Board's Terminal via RS-232 Console .. 92
2.10.2 Users on SC Board's Terminal ......................................... 92
2.10.2.1 Logging in as a ROOT User ........................................ 92
2.10.2.2 Logging in as a CLI User ............................................. 93
2.10.3 Changing the Basic SC Configuration of the 1st SC Board .... 93
4.15 Configuring Clock Synchronization ..................................................... 252
  4.15.1 Standalone Board Sync Clock Mode for TP-6310 Configurations .... 252
  4.15.2 Timing Module BITS Sync Clock Mode for TP-6310 Configurations ... 254
4.16 Performance Monitoring .................................................................... 257
  4.16.1 Real-Time Performance Measurements ........................................ 258
  4.16.2 History Performance Measurements ............................................ 260
4.17 Media Gateway Inventory ................................................................. 265
4.18 Checking the Fan Speeds ................................................................. 266
4.19 Media Gateway Boards' Configuration Backdoor ......................... 266
  4.19.1 Supported Actions ...................................................................... 269
  4.19.2 Usage Tips ................................................................................. 269
4.20 Using Auxiliary Files ........................................................................ 270
  4.20.1 Auxiliary Files Repository ......................................................... 270
  4.20.2 Call Progress Tones (CPT) Files ................................................ 271
    4.20.2.1 Modifying the "Source" Call Progress Tones (CPT) File ...... 272
  4.20.3 Pre-Recorded Tones (PRT) Files ................................................ 278
    4.20.3.1 Creating a Pre-Recorder Tones File .................................... 278
  4.20.4 Voice Prompts Files .................................................................... 280
    4.20.4.1 Creating a Voice Prompts File ............................................ 281
  4.20.5 External Coders Files .................................................................. 284
    4.20.5.1 Modifying the "Source" External Coders File ...................... 284
    4.20.5.2 Converting External Coders File to Binary Format .............. 285
# Table of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-1</td>
<td>Block Diagram</td>
<td>20</td>
</tr>
<tr>
<td>1-2</td>
<td>Avaya G860 Board Configuration</td>
<td>21</td>
</tr>
<tr>
<td>1-3</td>
<td>Avaya G860 Configuration - Front View</td>
<td>22</td>
</tr>
<tr>
<td>1-4</td>
<td>Avaya G860 DC Power - Back View</td>
<td>23</td>
</tr>
<tr>
<td>1-5</td>
<td>FML-5/Left Fan Tray - Fan Tray Unit</td>
<td>27</td>
</tr>
<tr>
<td>1-6</td>
<td>FMR/5K - Fan Tray Unit</td>
<td>28</td>
</tr>
<tr>
<td>1-7</td>
<td>FPM/DC/5K - Avaya G860 System Configurations</td>
<td>28</td>
</tr>
<tr>
<td>1-8</td>
<td>FML-5/Left Fan Tray Fan Tray Unit Panel and Alarm Indicators</td>
<td>29</td>
</tr>
<tr>
<td>1-9</td>
<td>6310 Board Panel</td>
<td>31</td>
</tr>
<tr>
<td>1-10</td>
<td>6310/RTM</td>
<td>34</td>
</tr>
<tr>
<td>1-11</td>
<td>SC Panel</td>
<td>36</td>
</tr>
<tr>
<td>1-12</td>
<td>SC Front Panel Mini DIN 8 Serial Port Connector</td>
<td>37</td>
</tr>
<tr>
<td>1-13</td>
<td>Synchronization &amp; Alarm (SA) RTM</td>
<td>40</td>
</tr>
<tr>
<td>1-14</td>
<td>SA/RTM Panel</td>
<td>41</td>
</tr>
<tr>
<td>1-15</td>
<td>RJ-48c Trunk Connectors</td>
<td>43</td>
</tr>
<tr>
<td>1-16</td>
<td>ES/6600 Panel</td>
<td>46</td>
</tr>
<tr>
<td>1-17</td>
<td>ES/6600/RTM</td>
<td>50</td>
</tr>
<tr>
<td>2-1</td>
<td>Installation Process Flow</td>
<td>53</td>
</tr>
<tr>
<td>2-2</td>
<td>Initial Unpacking of the Carton</td>
<td>63</td>
</tr>
<tr>
<td>2-3</td>
<td>Removing Top of Carton</td>
<td>64</td>
</tr>
<tr>
<td>2-4</td>
<td>Accessory kit at the top of the Carton</td>
<td>64</td>
</tr>
<tr>
<td>2-5</td>
<td>Opening the Plastic Covering</td>
<td>65</td>
</tr>
<tr>
<td>2-6</td>
<td>Attaching the Chassis to the Rack</td>
<td>67</td>
</tr>
<tr>
<td>2-7</td>
<td>Chassis on the Rack - Front View</td>
<td>67</td>
</tr>
<tr>
<td>2-8</td>
<td>Installing Rack Using Pre-Installed Support Studs</td>
<td>68</td>
</tr>
<tr>
<td>2-9</td>
<td>Earthing Connections Chassis Rear - PEM/DC/5K - 6310 Configuration</td>
<td>69</td>
</tr>
<tr>
<td>2-10</td>
<td>Earthing Connections Chassis Rear - PEM/AC/5K</td>
<td>69</td>
</tr>
<tr>
<td>2-11</td>
<td>DC Power Connections Redundant Pairs</td>
<td>71</td>
</tr>
<tr>
<td>2-12</td>
<td>Connecting the DC Power</td>
<td>72</td>
</tr>
<tr>
<td>2-13</td>
<td>PS/DC/5K Power Supply - 6310 System Configuration</td>
<td>74</td>
</tr>
<tr>
<td>2-14</td>
<td>DC Power Connections Redundant Pair</td>
<td>75</td>
</tr>
<tr>
<td>2-15</td>
<td>Input Terminal Wiring</td>
<td>75</td>
</tr>
<tr>
<td>2-16</td>
<td>SFP Modules and Their Locks</td>
<td>84</td>
</tr>
<tr>
<td>2-17</td>
<td>Redundancy Connection Scheme for the 6310 RTM</td>
<td>85</td>
</tr>
<tr>
<td>2-18</td>
<td>T3 - Male Connector MOLEX PN: 73100-0255</td>
<td>86</td>
</tr>
<tr>
<td>2-19</td>
<td>Normal Logic Alarm Connection Diagram</td>
<td>87</td>
</tr>
<tr>
<td>2-20</td>
<td>Inverse Logic Alarm Connection Diagram</td>
<td>87</td>
</tr>
<tr>
<td>2-21</td>
<td>Opening the Telnet Session</td>
<td>89</td>
</tr>
<tr>
<td>2-22</td>
<td>An Example of a Telnet Session</td>
<td>90</td>
</tr>
<tr>
<td>2-23</td>
<td>Putty Configuration</td>
<td>91</td>
</tr>
<tr>
<td>2-24</td>
<td>An example of an SSH Session</td>
<td>91</td>
</tr>
<tr>
<td>2-25</td>
<td>Pinging the SC Board</td>
<td>100</td>
</tr>
<tr>
<td>4-1</td>
<td>Clustering of Two L-3 Switches</td>
<td>125</td>
</tr>
<tr>
<td>4-2</td>
<td>Separate Networks</td>
<td>127</td>
</tr>
<tr>
<td>4-3</td>
<td>IPSec Encryption</td>
<td>224</td>
</tr>
<tr>
<td>4-4</td>
<td>Standalone Board Sync Clock Mode for TP-6310 Configurations</td>
<td>253</td>
</tr>
<tr>
<td>4-5</td>
<td>Timing Module BITS Sync Clock Mode for TP-6310 Configurations</td>
<td>255</td>
</tr>
<tr>
<td>4-6</td>
<td>Display Real-Time PMS</td>
<td>258</td>
</tr>
<tr>
<td>4-7</td>
<td>Select Screen</td>
<td>258</td>
</tr>
<tr>
<td>4-8</td>
<td>Real-Time Performance Measurement Display</td>
<td>259</td>
</tr>
<tr>
<td>4-9</td>
<td>MG Monitoring</td>
<td>259</td>
</tr>
<tr>
<td>4-10</td>
<td>Real Time Performance Measurements Display</td>
<td>260</td>
</tr>
<tr>
<td>4-11</td>
<td>Configure MG PM Profile</td>
<td>261</td>
</tr>
<tr>
<td>4-12</td>
<td>MG Background Monitoring</td>
<td>261</td>
</tr>
<tr>
<td>4-13</td>
<td>Question</td>
<td>262</td>
</tr>
<tr>
<td>4-14</td>
<td>Start_Polling</td>
<td>262</td>
</tr>
<tr>
<td>4-15</td>
<td>Display Historical PMs</td>
<td>263</td>
</tr>
</tbody>
</table>
Figure 4-16: Select Screen .................................................................................................................. 263
Figure 4-17: History Performance Measurements Display ............................................................. 264
Figure 4-18: Historical Performance Measurements Display ....................................................... 265
Figure 4-19: MG Inventory .............................................................................................................. 266
Figure 4-20: Prerecorded Tones File(s) Screen with wav Files ...................................................... 279
Figure 4-21: File Data Dialog Box ................................................................................................. 279
Figure 4-22: Voice Prompts Screen ............................................................................................... 281
Figure 4-23: Select Files Window .................................................................................................. 282
Figure 4-24: Voice Prompts Window with wav Files ..................................................................... 283
Figure 4-25: File Data Window ....................................................................................................... 283
Figure 4-26: Coders Window ......................................................................................................... 286
Figure 5-1: Baffled Blank Panel for Front Slots ............................................................................ 290
Figure 5-2: Blank Panel for Rear Slots ......................................................................................... 290
Figure 5-3: Red Ejector Buttons on a Board ................................................................................. 291
Figure 5-4: SC Software Package Upload Using FTP ..................................................................... 293
Figure 5-5: SC Software Package Upload Using FTP ..................................................................... 294
Figure 5-6: EMS Avaya G860 Status screen-Power Supply Status .............................................. 313
Figure 5-7: EMS Avaya G860 Status screen-PEM Status ............................................................... 314
Figure 5-8: Replacing the Fan Tray Unit ....................................................................................... 315
Figure 5-9: EMS Avaya G860 Status screen-Fan Status ................................................................ 316
Figure 5-10: EMS Avaya G860 Status screen-Fan Status .............................................................. 317
Figure 5-11: Air Filter .................................................................................................................. 318
Figure 5-12: EMS Avaya G860 Status screen-Fan Status .............................................................. 319
Figure 6-1: MG Information ........................................................................................................... 330
Figure 6-2: Maintenance Actions Icon and Popup Menu ........................................................... 331
Figure 6-3: Files Manager Screen ............................................................................................... 331
Figure 6-4: Welcome Questionnaire ............................................................................................ 334
Figure 6-5: EMS Online Software Upgrade Workaround .......................................................... 335
Figure 6-6: Software Upgrade in Process, Managed by the SC Board ......................................... 336
Figure 6-7: Software Upgrade in Process, Abort Screen .............................................................. 339
Figure 7-1: Viewing an 'SNMP Trap' Log ..................................................................................... 362
## List of Tables

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-1</td>
<td>Components of the Avaya G860 Board Configuration</td>
<td>21</td>
</tr>
<tr>
<td>1-2</td>
<td>Avaya G860 Front View Component Descriptions</td>
<td>22</td>
</tr>
<tr>
<td>1-3</td>
<td>Avaya G860 Back View Component Descriptions</td>
<td>23</td>
</tr>
<tr>
<td>1-4</td>
<td>Avaya G860 Version Chassis Dimensions</td>
<td>24</td>
</tr>
<tr>
<td>1-5</td>
<td>Avaya G860 Chassis Configuration Power Requirements</td>
<td>25</td>
</tr>
<tr>
<td>1-6</td>
<td>Chassis Front Panel Alarm Indicators and Buttons</td>
<td>29</td>
</tr>
<tr>
<td>1-7</td>
<td>TP-6310 Board Panel STM-1/OC-3 Version LED Indicators</td>
<td>32</td>
</tr>
<tr>
<td>1-8</td>
<td>TP-6310 Board Panel LED Alarm Signals for SDH or SONET Terminology</td>
<td>32</td>
</tr>
<tr>
<td>1-9</td>
<td>TP-6310/T3 Board Panel LED Indicators</td>
<td>33</td>
</tr>
<tr>
<td>1-10</td>
<td>Mini DIN 8 Pin Signal Interface</td>
<td>37</td>
</tr>
<tr>
<td>1-11</td>
<td>SC Board Indicators</td>
<td>37</td>
</tr>
<tr>
<td>1-12</td>
<td>SA/RTM RS-232 Console Pin Signal Interface</td>
<td>42</td>
</tr>
<tr>
<td>1-13</td>
<td>SA/RTM LED Indicators</td>
<td>42</td>
</tr>
<tr>
<td>1-14</td>
<td>Terminal Block</td>
<td>43</td>
</tr>
<tr>
<td>1-15</td>
<td>SA/RTM BITS (RJ48-c) Pin Signal Interface</td>
<td>43</td>
</tr>
<tr>
<td>1-16</td>
<td>SA/RTM BITS LEDs</td>
<td>44</td>
</tr>
<tr>
<td>1-17</td>
<td>Port/Link Activity Indicators</td>
<td>47</td>
</tr>
<tr>
<td>1-18</td>
<td>Port Speed Indicators</td>
<td>47</td>
</tr>
<tr>
<td>1-19</td>
<td>System Indicator</td>
<td>47</td>
</tr>
<tr>
<td>1-20</td>
<td>Fault Indicator</td>
<td>47</td>
</tr>
<tr>
<td>1-21</td>
<td>Ethernet Switch Hot-Swap Indicator</td>
<td>48</td>
</tr>
<tr>
<td>1-22</td>
<td>ES/6600 Physical Slots to Ethernet Port Correlation</td>
<td>48</td>
</tr>
<tr>
<td>1-23</td>
<td>ES/6600/RTM Port Pin Outs</td>
<td>51</td>
</tr>
<tr>
<td>1-24</td>
<td>Board Assembly Order for 6310 System Configuration - View 1</td>
<td>51</td>
</tr>
<tr>
<td>1-25</td>
<td>6310 System Configuration Board Assembly - View 2</td>
<td>52</td>
</tr>
<tr>
<td>2-1</td>
<td>Equipment Requirements</td>
<td>54</td>
</tr>
<tr>
<td>2-2</td>
<td>6310 System Configuration Electrical Requirements</td>
<td>54</td>
</tr>
<tr>
<td>2-3</td>
<td>Cabling Requirements</td>
<td>56</td>
</tr>
<tr>
<td>2-4</td>
<td>Gateway Addresses</td>
<td>57</td>
</tr>
<tr>
<td>2-5</td>
<td>Boards’ IP Addresses for Avaya G860 Configuration</td>
<td>57</td>
</tr>
<tr>
<td>2-6</td>
<td>Network Servers’ IP Addresses</td>
<td>57</td>
</tr>
<tr>
<td>2-7</td>
<td>VLANs Configuration</td>
<td>58</td>
</tr>
<tr>
<td>2-8</td>
<td>DiffServ Priority Parameters</td>
<td>58</td>
</tr>
<tr>
<td>2-9</td>
<td>IEEE 802.1p Service Priority Classes</td>
<td>58</td>
</tr>
<tr>
<td>2-10</td>
<td>Security Profiles</td>
<td>59</td>
</tr>
<tr>
<td>2-11</td>
<td>NEBS Requirements</td>
<td>59</td>
</tr>
<tr>
<td>2-12</td>
<td>Temperature Range</td>
<td>60</td>
</tr>
<tr>
<td>2-13</td>
<td>Humidity Range</td>
<td>60</td>
</tr>
<tr>
<td>2-14</td>
<td>Altitude Range</td>
<td>60</td>
</tr>
<tr>
<td>2-15</td>
<td>Earthquake Requirements</td>
<td>61</td>
</tr>
<tr>
<td>2-16</td>
<td>Rack Requirements</td>
<td>61</td>
</tr>
<tr>
<td>2-17</td>
<td>AC Power Cable Types</td>
<td>72</td>
</tr>
<tr>
<td>2-18</td>
<td>Power Requirements</td>
<td>74</td>
</tr>
<tr>
<td>2-19</td>
<td>AC Power Cable Types</td>
<td>76</td>
</tr>
<tr>
<td>2-20</td>
<td>Functional Checks on Component Indicators - 6310 System Configuration</td>
<td>77</td>
</tr>
<tr>
<td>2-21</td>
<td>IP Separation and ES/6600 Port Allotment</td>
<td>82</td>
</tr>
<tr>
<td>3-1</td>
<td>Automatic Backup Parameters</td>
<td>107</td>
</tr>
<tr>
<td>4-1</td>
<td>Provisioning Types</td>
<td>111</td>
</tr>
<tr>
<td>4-2</td>
<td>IP Parameters of the Media Gateway</td>
<td>113</td>
</tr>
<tr>
<td>4-3</td>
<td>IP Parameters of the Media Gateway Board</td>
<td>114</td>
</tr>
<tr>
<td>4-4</td>
<td>Hardware and Application Types</td>
<td>117</td>
</tr>
<tr>
<td>4-5</td>
<td>Redundancy Group Parameters</td>
<td>120</td>
</tr>
<tr>
<td>4-6</td>
<td>NTP Server Configuration and Status</td>
<td>124</td>
</tr>
<tr>
<td>4-7</td>
<td>Aggregated Links and Least Significant Bits</td>
<td>132</td>
</tr>
</tbody>
</table>
Table 4-8: Aggregation Distribution Policy-Recommended .......................................................... 132
Table 4-9: Aggregation Distribution Policy-Not Recommended IPs ........................................ 133
Table 4-10: Interfaces and VLAN 802.1 p/q Tab Parameters ........................................................ 136
Table 4-11: Subnet Separation Tab Parameters ........................................................................ 141
Table 4-12: Static Route Table Tab Parameters ....................................................................... 141
Table 4-13: Subnet Settings ....................................................................................................... 142
Table 4-14: VLANs Settings ..................................................................................................... 143
Table 4-15: QoS Premium Services .......................................................................................... 143
Table 4-16: DiffServ Class Name and Protocol Group Assignments ......................................... 144
Table 4-17: One Interface ........................................................................................................ 145
Table 4-18: Two Interfaces (interface1 = OAM + Control; interface2 = Media) ...................... 146
Table 4-19: Two Interfaces (interface1 = OAM; interface2 = Control + Media) ..................... 147
Table 4-20: Three Interfaces .................................................................................................. 147
Table 4-21: Port allocation in accordance with ES type, Aggregation and Number of Interfaces .. 148
Table 4-22: Trunk Properties ................................................................................................... 159
Table 4-23: Fiber Group Properties ........................................................................................ 160
Table 4-24: NFAS Parameters of the Trunk .............................................................................. 162
Table 4-25: Media Gateway Board's Voice Settings ................................................................. 163
Table 4-26: SIP Proxy Server Parameters ............................................................................... 168
Table 4-27: SIP Proxy Settings ................................................................................................ 168
Table 4-28: SIP Registration Parameter .................................................................................. 173
Table 4-29: Number Manipulation Table ............................................................................... 175
Table 4-30: Number Manipulation Table Parameters .............................................................. 176
Table 4-31: NPI/TON Values for ISDN ETSI ......................................................................... 179
Table 4-32: SIP Routing Table ............................................................................................... 179
Table 4-33: Telephone to IP Routing Table Parameters ........................................................... 182
Table 4-34: IP to Telephone Routing Parameters ................................................................... 185
Table 4-35: Internal DNS Table Parameters .......................................................................... 186
Table 4-36: Alternative Routing Table .................................................................................... 186
Table 4-37: Alternative Routing Parameters .......................................................................... 187
Table 4-38: SIP / ISDN Cause Mapping Tables ..................................................................... 188
Table 4-39: SIP to ISDN Cause Mapping Parameters .............................................................. 189
Table 4-40: ISDN to SIP Cause Mapping Parameters .............................................................. 189
Table 4-41: Coder Parameters ................................................................................................ 190
Table 4-42: Trunk Group Parameters ...................................................................................... 192
Table 4-43: Trunk Group Settings Parameters ....................................................................... 194
Table 4-44: SIP Profiles Tables .............................................................................................. 196
Table 4-45: Coder Parameters ................................................................................................ 197
Table 4-46: Tel Profile Parameters .......................................................................................... 199
Table 4-47: IP Profiles Parameters ........................................................................................ 203
Table 4-48: Security Features .................................................................................................. 209
Table 4-49: X.509 Files Parameters of the Media Gateway ..................................................... 220
Table 4-50: X.509 Files Status Parameters of the Media Gateway ........................................ 221
Table 4-51: OAM Security Profile Parameters ....................................................................... 225
Table 4-52: MGC Security Profile Parameters ...................................................................... 227
Table 4-53: Firewall Rule Parameters ..................................................................................... 232
Table 4-54: Filesystem Integrity of the SC Board ................................................................... 236
Table 4-55: Filesystem Integrity Parameters of the Media Gateway ........................................ 237
Table 4-56: Centralized User Authentication Parameters ......................................................... 251
Table 4-57: Timing Module BITS Sync Clock Mode Parameters .............................................. 256
Table 4-58: Configuration Backdoor Parameters .................................................................... 267
Table 4-59: Supported Auxiliary Files ................................................................................... 270
Table 4-60: Default Call Progress Tones ................................................................................ 275
Table 5-1: Software Installation Failure Scenarios .................................................................. 292
Table 5-2: SC Installation Package Files ............................................................................... 293
Table 6-1: New Features of ver.5.2 Software that must be Manually Activated after Upgrading From an Earlier Version .............................................................................................................. 338
Table 7-1: Troubleshooting Faults in the Media Gateway .......................................................... 344
Table 7-2: Debug Recording Rule Properties ........................................................................... 356
Introductory Notes

Tip: When viewing this manual on CD, Web site or on any other electronic copy, all cross-references are hyperlinked. Click on the page or section numbers (shown in blue) to reach the individual cross-referenced item directly. To return back to the point from where you accessed the cross-reference, press the alt and ⌘ keys.

Notice

This manual describes the installation, operation and maintenance of the Avaya G860 Media Gateway.

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, Avaya cannot guarantee the 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 Technical Support customers at www.avaya.com under Support / Product Documentation.

© 2008 Avaya Ltd. All rights reserved.
This document is subject to change without notice.

Trademarks

Avaya and Avaya logo are trademarks or registered trademarks of Avaya Inc. All other products or trademarks are property of their respective owners.

Customer Support

Customer technical support and service are provided by Avaya Inc. Distributors, Partners, and Resellers from whom the product was purchased. For Customer support for products purchased directly from Avaya, contact support@avaya.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. Hexadecimal notation is indicated by 0x preceding the number.
Related Documentation

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

- **Mediant 5000 Product Description** - contains the description of the product features, components, standard control protocols and management protocols (Document # LTRT-925xx).
- **Installing and Operating the Avaya G860 Media Gateway** (this 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-907xx).
- **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 Media Gateway (Document # LTRT-914xx).
- **Mediant 5000/8000 Command Line Interface (CLI) Reference Guide** – (Document # LTRT- 892xx)
- **Mediant 5000/8000 Media Gateway Release Notes** - Document # LTRT-909xx
- **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 5000 to send all alarms set as they are to be handled according to manual or automatic 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-910xx).
- **EMS Product Description** – Document # LTRT-940xx
- **EMS OAM Guide for 5000/8000** - Document # LTRT-942xx
- **EMS OAM Integration Guide for 5000/8000** - Document # LTRT-192xx
- **EMS Release Notes** - Document # LTRT-905xx
1 Introduction to the Avaya G860 Media Gateway

The Avaya G860 Media Gateway is a high channel density, standards-compliant, VoIP, wireless, cables and wireline media gateway system. The Avaya G860 incorporates Avaya's 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 Avaya G860 is a robust, scalable and modular solution, designed for the carrier environment, matching the density requirements for medium deployments, while meeting Network Service Providers' demands for high availability, reliable new voice infrastructure networks. For maximum reliability, the Avaya G860 features protection switching and full redundancy of all common equipment.
1.1 Media Gateway Block Diagrams

The block diagram of the Avaya G860 is shown below.

Figure 1-1: Block Diagram

[Block diagram image of the Avaya G860 Media Gateway block diagrams]
1.1.1 Avaya G860 Board Configuration

The table below details the components of the Avaya G860 board configuration.

Table 1-1: Components of the Avaya G860 Board Configuration

<table>
<thead>
<tr>
<th>Component</th>
<th>Redundant Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chassis</td>
<td>1</td>
</tr>
<tr>
<td>SC (System Controller)</td>
<td>2</td>
</tr>
<tr>
<td>SA/RTM (Synchronization and Alarm Rear Transition Module)</td>
<td>2</td>
</tr>
<tr>
<td>ES/6600 (Ethernet Switch Board - 24 Gigabit Ethernet)</td>
<td>2</td>
</tr>
<tr>
<td>ES/6600/RTM (Ethernet Switch 7 I/O Rear Transition Module)</td>
<td>2</td>
</tr>
<tr>
<td>TP-6310 Media Gateway Boards</td>
<td>Up to 4</td>
</tr>
<tr>
<td>6310/RTM (TP-6310 I/O Rear Transition Module)</td>
<td>Up To 3</td>
</tr>
<tr>
<td>6310/RTM/Redundant (TP-6310 I/O Rear Transition Module – Redundant)</td>
<td>1</td>
</tr>
<tr>
<td>PS/DC/5K or PS/AC/5K (AC or DC Power Supply Modules)</td>
<td>3</td>
</tr>
<tr>
<td>PEM/DC/5K or PEM/AC/5K (AC or DC Power Entry Modules)</td>
<td>1 AC/2 DC</td>
</tr>
<tr>
<td>FML-5 (Fan Tray Module)</td>
<td>1</td>
</tr>
<tr>
<td>AF/5K (Air Filter)</td>
<td>1</td>
</tr>
<tr>
<td>FMR/5K (Auxiliary Fan Tray Module)</td>
<td>1</td>
</tr>
<tr>
<td>FPM/5K (AC or DC Fan Tray Power Supply Module)</td>
<td>2</td>
</tr>
<tr>
<td>Blank panels (Full configuration):</td>
<td></td>
</tr>
<tr>
<td>Blank panel - Panel only</td>
<td>1</td>
</tr>
<tr>
<td>Blank panel - Baffled filler panel</td>
<td>1</td>
</tr>
</tbody>
</table>
In the Avaya G860 configuration, slots 5 and 6 require blank Baffled filler panels as part of the temperature control system.

1.1.2 Avaya G860 Accessory Kit

Each Avaya G860 is accompanied by an accessory kit, which includes:

- RS-232 Straight Cable for System Controller Console Terminal (not crossed-over)
- RS-232 Straight Cable for Ethernet Switch Console Terminal (not crossed-over)
- AC Power Cable (as per configuration)
- CD containing Avaya G860 system software and system documentation
- CDs containing the EMS software (Optional)

1.2 Front and Back Views of the Avaya G860

Table 1-2: Avaya G860 Front View Component Descriptions

<table>
<thead>
<tr>
<th>Item #</th>
<th>Component Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>TP-6310 Boards</td>
</tr>
<tr>
<td>2</td>
<td>Blank and Baffled Panels</td>
</tr>
<tr>
<td>3</td>
<td>ESD Connectors on the Attachment Brackets</td>
</tr>
<tr>
<td>4</td>
<td>Fan Tray Module with Alarm LEDs</td>
</tr>
<tr>
<td>5</td>
<td>ES 6600 Ethernet Switch Boards</td>
</tr>
</tbody>
</table>
1. Introduction to the Avaya G860 Media Gateway

<table>
<thead>
<tr>
<th>Item #</th>
<th>Component Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>System Controller (SC) Boards</td>
</tr>
<tr>
<td>7</td>
<td>FMR/5K Fan Module</td>
</tr>
<tr>
<td>8</td>
<td>Power Supplies</td>
</tr>
</tbody>
</table>

![Figure 1-4: Avaya G860 DC Power - Back View](image)

Table 1-3: Avaya G860 Back View Component Descriptions

<table>
<thead>
<tr>
<th>Item #</th>
<th>Component Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>6310/RTM/ Redundant</td>
</tr>
<tr>
<td>2</td>
<td>6310/RTM</td>
</tr>
<tr>
<td>3</td>
<td>ES/6600/RTM</td>
</tr>
<tr>
<td>4</td>
<td>SA/RTM/Timing</td>
</tr>
<tr>
<td>5</td>
<td>PEM units</td>
</tr>
<tr>
<td>6</td>
<td>FPM Advanced Fan Module</td>
</tr>
<tr>
<td>7</td>
<td>ESD Connections</td>
</tr>
</tbody>
</table>

1.3 The Chassis

The Avaya G860 chassis complies with NEBS Level 3 requirements and conforms to CompactPCI PICMG 2.0 standards. It contains a 10-slot card cage. All component boards have a sturdy, hot-swap cPCI 6U form factor. Boards are inserted from the front and the back and engage the midplane on either side inside the card cage. Slots for the boards are numbered from one to ten on the left of the card cage in the front,
The midplane contains slot keys to match the appropriate board. This prevents insertion of a board in a wrong location.

The Avaya G860 chassis configuration also houses two fan tray units, facing the front of the chassis, one is to the left of the card cage and another is in the upper right-hand corner of the chassis. The fan tray unit to the left of the card cage also houses an air filter. The chassis also holds three Power Supply modules to the right of the card cage (under the second fan tray unit).

<table>
<thead>
<tr>
<th>Dimension</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Width</td>
<td>48.3 cm (19 inches)</td>
</tr>
<tr>
<td>Height</td>
<td>22.2 cm (8.75 inches)</td>
</tr>
<tr>
<td>Depth</td>
<td></td>
</tr>
<tr>
<td>With projections</td>
<td>36.5 cm (13.7 inch)</td>
</tr>
<tr>
<td>Without projections</td>
<td>30 cm (11.8 inch)</td>
</tr>
<tr>
<td>Weight (Fully loaded)</td>
<td>20.45 kg (45.1 lb)</td>
</tr>
</tbody>
</table>

1.3.1 Earthing Requirements

Earthing and Bonding

Connect the equipment enclosure via the provided stud to Protective earth using No. 6 AWG copper grounding conductor from an approved earthing electrode.

Metallic parts of network equipment installed in the outside plant shall be grounded in accordance with Rule 99 of the most recent edition of the National Electrical Safety Code (NESC), ANSI/IEEE C2.[36]

Safety Earth

Intrinsically, the Avaya G860 chassis must be safety-earthed using an equipment-earthing conductor. Do not depend on locknut-bushings and double-locknuts for bonding purposes. Use the earthing hardware provided with the chassis.

Earthing Electrode

The gateway must be earthed to a stable local earth reference. The gateway's earth terminal should be connected thought a separate earth wire (6 recommended) to the rack's earthing. The earth connection's resistance must not be greater than 0.1 ohm. Verify that the rack's earthing is properly performed.

1.3.2 Power Requirements

The Avaya G860 chassis configuration is powered from either AC or DC sources.
1. Introduction to the Avaya G860 Media Gateway

Table 1-5: Avaya G860 Chassis Configuration Power Requirements

<table>
<thead>
<tr>
<th>Type</th>
<th>Power Requirements</th>
<th>Connection Provisions</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC</td>
<td>100 to 240 V AC, nominal 50/60 Hz</td>
<td>PEMs (Power Entry Modules) with Standard 3-prong quick connect socket</td>
</tr>
<tr>
<td>DC</td>
<td>-40.5 to -60 V DC</td>
<td>PEMs with Input terminals</td>
</tr>
</tbody>
</table>

- The AC power cable should be connected to power sockets that are protected by a protection device providing a maximum of 16A protection capacity.
- The AC inlet contains two fuses, one for each pole. To replace a fuse, use only Littelfuse P/N 215010 (10A 250V).

1.3.2.1 Power Consumption

DC Input Power

For Avaya G860 configurations, the average power consumption for a full complement of boards is approximately:

- 600 watts - 5.3 A at 115 VAC
- 600 watts - 2.7 A at 230 VAC
- 640 watts - 13.4 A at 48 VDC

Two Power Entry Modules (PEM), are provided for DC connections on the rear of the chassis. Power is required to be between -40.5 and -60 VDC. Each PEM unit contains one input terminal. Each of the DC input terminals is reverse current protected. The input terminals on each of the PEM units provide redundancy protection for the power entry circuitry.

Recommendations for DC Power input:

- When using DC power as the primary input, ensure that the power supply complies with the safety requirements of Call Agent CAN/CSA-C22.2 No. 60950-00 and UL 60950, and EN 60950.
- For High Availability, connect two separate DC power sources to avoid total power failure if one of the DC power sources fails.

1.3.2.2 Electro Magnetic Compatibility (EMC) Features

The chassis is designed to comply with known EMC/RFI standards, including FCC Part 15, Class B; ICES-003, Class A; EN 55022, Class B; EN 300 386.

Compliance measures include:

- **Venting holes** - for air intake and exhaust, sized to provide for blockage of frequencies within the specified range
- **Blank panels with contact fingers** - used for covering empty slots when a configuration requires such
- **RFI filters** - built-in to the DC power inputs, assuring that conductive interference does not reach the Power Supply Modules, or that switching signals generated by
the Power Supply Modules do not propagate over the main feed.

- **Air filters** - integrates a honeycomb EMI shield in its assembly. The honeycomb structure consists of "cells" that are engineered to trap and absorb EMI noise while maintaining 95% to 99% aperture for minimal airflow impedance. A gasket installed around the frame makes sure there is conductivity of the frame to the enclosure.

### 1.3.3 Midplane Keying

Each slot is equipped with a key on the midplane to match the appropriate board type in order to prevent inserting a wrong 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, be sure NOT to force a board into a slot to avoid damaging either the board or the midplane.

### 1.4 Cooling System

The cooling system of the Avaya G860 includes the following hardware components:

- FML-5/Left Fan Tray - Fan Tray Unit
- FMR/5K - Fan Tray Unit
- FPM/5K - Advanced Fan Power Module

#### 1.4.1 FML-5/Left Fan Tray - Fan Tray Unit

The Avaya G860 components are cooled by a fan tray unit FML-5 located at the left of the card cage. The fan tray unit draws cool air in through a perforated grill on the left side of the chassis. The incoming air passes through a removable filter (located within the fan assembly, immediately inside the perforated grill), whose honeycombed design prevents RF interference. The air flows over the boards, cooling them and sends the warmed air out the perforated grill on the right side of the chassis.
1. Introduction to the Avaya G860 Media Gateway

Refer to the figure below and for additional information, refer to Alarm Indicators on page 29.

**Figure 1-5: FML-5/Left Fan Tray - Fan Tray Unit**

![FML-5/Left Fan Tray - Fan Tray Unit](image)

**WARNING**
The FML-5/Left Fan Tray Fan Tray Unit is hot-swappable. However its presence is imperative for maintaining normal temperature inside the chassis. Therefore, when replacing it, carry out the replacement procedure in a prompt and efficient manner.

1.4.2 **FMR/5K - Fan Tray Unit**

For Avaya G860 board configurations, an auxiliary fan tray unit (FMR/5K) is located in the top right-hand corner of the chassis, above the power supply units. In addition to the FML-5/Left Fan Tray, the FMR/5K draws the warmed air out of the card cage. The warmed air passes through the FMR/5K's temperature sensors and flows out the air vents on right side of the chassis. The FMR/5K's temperature sensors detect any overheating that may occur inside the card cage and triggers the appropriate alarm whose LED indicator is on the FML-5/Left Fan Tray fan tray unit (on the left side).

The FML-5/Left Fan Tray contains 5 fans, providing required airflow for each board in the card cage, even if one of the fans stops working.
The FMR/5K fan tray unit contains three LEDs:

- **HSR (Hot Swap Request)** - for future implementation
- **Hot Swap**
- **Power**

The clean air is drawn 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 Avaya G860 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 especially constructed to allow optimal air flow within the chassis.

The FML-5/Left Fan Tray Fan Tray Module is easily removed and is hot-swappable.

The FML-5/Left Fan Tray contains 5 fans, providing required airflow for each board in the card cage, even if one of the fans stops working.

### 1.4.3 FPM/5K - Advanced Fan Power Module

In the Avaya G860 system configuration, the Advanced Fan Power Module (FPM/5K) is the power supply for the fan tray unit. It is provided in either a DC or AC version according to the main power configuration. Two FPM/5K units are provided for redundant protection. The FPM/5K are hot-swappable. (The AC version is not shown.)

LEDs on the FPM/5K indicate power status. In a future version LEDs are to indicate Swap Ready and HSR status.
1.4.4 Alarm Indicators

The FML-5/Left Fan Tray fan tray unit panel contains the system's alarm indicators (LEDs) Alarm Cutoff and Reset buttons.

The alarm indicators are connected to the fault detection and alarm system provided with the Avaya G860. As needed, LEDs indicate critical, major or minor system faults as well as system and system alarms.

Figure 1-8: FML-5/Left Fan Tray Fan Tray Unit Panel and Alarm Indicators

1.4.4.1 Alarm Indicators

The table below describes the chassis’ front panel alarm indicators.

Table 1-6: Chassis Front Panel Alarm Indicators and Buttons

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
<th>Color Code</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYSTEM LED</td>
<td>Indicates that the System Controller board is properly functioning</td>
<td>Green</td>
<td>Steady Green indicates proper SC board functioning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Red</td>
<td>Default</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Steady Red during initialization of active SC</td>
</tr>
<tr>
<td>CRITICAL LED</td>
<td>Indicates the detection of a fault (or faults) - categorized as 'Critical'</td>
<td>Green</td>
<td>Green when no critical alarms</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Red</td>
<td>Default</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Red when critical alarm is set. When This LED is on, all other Major and Minor severity LED are also lit</td>
</tr>
<tr>
<td>MAJOR LED</td>
<td>Indicates the detection of a fault</td>
<td>Green</td>
<td>Green when no Major alarms</td>
</tr>
</tbody>
</table>
### Component Description

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
<th>Color Code</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>(or faults) - categorized as 'Major'</td>
<td>Orange</td>
<td>Default</td>
<td>Orange when Major alarm is set. When this LED is on, the Minor severity LED is also lit</td>
</tr>
<tr>
<td>MINOR LED</td>
<td>Indicates the detection of a fault (or faults) - categorized as 'Minor'</td>
<td>Green</td>
<td>Green when no Minor alarms</td>
</tr>
<tr>
<td></td>
<td>Orange</td>
<td>Default</td>
<td>Orange when minor alarm is set</td>
</tr>
<tr>
<td>SHELF LED</td>
<td>Indicates the health or failure of the chassis' hardware as detected by the alarm module</td>
<td>Green</td>
<td>Green when initialization is completed</td>
</tr>
<tr>
<td></td>
<td>Red</td>
<td>Default</td>
<td>Red during initialization process</td>
</tr>
<tr>
<td>ACO Pushbutton</td>
<td>Alarm Cut Off</td>
<td>---</td>
<td>Used to mute the Telco alarm relay devices attached to the SA/RTM. Returns all of the alarm relays to normal position, deactivating the alarm relay devices. The chassis LEDs and other gateway alarm signals are NOT affected. Accessed with finger</td>
</tr>
<tr>
<td>Pushbutton</td>
<td>For future use</td>
<td>---</td>
<td></td>
</tr>
</tbody>
</table>

### 1.5 Avaya G860 Boards

#### 1.5.1 The TP-6310 Media Gateway Board

The TP-6310 board is a high-density, hot-swappable, compactPCI resource board with a capacity of 2016 DS0 channels, supporting all necessary functions for voice, data and fax streaming over IP networks. This board operates as a stand-alone SIP media gateway. The TP-6310 board provides STM-1/OC-3, PSTN and T3 interfaces via its Rear Transition Module (RTM).

The TP-6310 board and RTMs are shown below. The 6310/RTM panel contains Tx and Rx transceivers for:

- 1+1 (total 2) PSTN STM-1/OC-3 interfaces
- 3 T3 (DS-3) PSTN interfaces (6 connectors – 3 RX and 3 TX)

**Note:** The TP-6310 supports either a single OC-3 interface or three DS-3 interfaces.

Each OC-3 PSTN connection is a cage provided with a slim form pluggable SFP 155 Mbps optical module to connect to an optical fiber with an STM-1/Dual-LC optical connector. The SFP module complies with the INF-8074i - Small Form-factor Pluggable (SFP) Transceiver MultiSource Agreement (MSA).
To ensure full integrated Automatic Protection Switching (APS) for the PSTN interface, the fiber optic cables must be connected to corresponding PSTN connectors on the 6310/RTM. The PSTN interface is provided with 1+1 protection.

- Each STM-1/OC-3 PSTN I/O connection is a cage provided with a slim form pluggable SFP 155 Mbps optical module with Tx and Rx transceivers to connect to an optical fiber with a dual-LC optical connector.
- Each T3 PSTN interface port is a mini-SMB connector with Tx and Rx transceivers.

The 6310/RTM is designed for protection capabilities and provides a unique Redundant protection functionality. The 6310/RTM/Redundant itself does not provide any PSTN ports. The same redundant RTM should be used for both STM-1 and T3 versions.

Slots 7 to 10 are used for up to 4 TP-6310 boards (including the redundant TP-6310 board) according to the customer’s requirements. The appropriate rear RTMs are located in the rear cage of the Avaya G860 Media Gateway in the corresponding slot. The figures below display the panels of the TP-6310 board and 6310/RTM.

For redundant N+1 protection, the 6310/RTM/Redundant Standby board is provided. It contains no port connections and occupies slot 10.

**Figure 1-9: 6310 Board Panel**
### Table 1-7: TP-6310 Board Panel STM-1/OC-3 Version LED Indicators

<table>
<thead>
<tr>
<th>Group</th>
<th>LED #</th>
<th>LED Label</th>
<th>Color</th>
<th>States</th>
</tr>
</thead>
<tbody>
<tr>
<td>FAIL</td>
<td>Off</td>
<td></td>
<td>Red</td>
<td>Normal Operation</td>
</tr>
<tr>
<td>ACT</td>
<td>Off</td>
<td></td>
<td>Blinking Yellow</td>
<td>Stand alone board (non HA system)</td>
</tr>
<tr>
<td>PSTN</td>
<td>A; B</td>
<td>Link</td>
<td>Green</td>
<td>Working Link OK</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Yellow</td>
<td>Protection Link OK</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Red</td>
<td>Refer to TP-6310 Board Panel LED Alarm</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Signals for SDH or SONET Terminology</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>C</td>
<td>Link</td>
<td>Off</td>
<td>No Link</td>
</tr>
<tr>
<td></td>
<td>Alrm</td>
<td></td>
<td>Off</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PWR</td>
<td></td>
<td>Off</td>
<td>Board Power is down</td>
</tr>
<tr>
<td></td>
<td>SWAP</td>
<td>READY</td>
<td>Off</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Blue</td>
<td>Normal Operation (see Note)</td>
</tr>
</tbody>
</table>

### Table 1-8: TP-6310 Board Panel LED Alarm Signals for SDH or SONET Terminology

Meaning of Alarm Signals for SDH or SONET (next applicable release)

<table>
<thead>
<tr>
<th>Alarm (Red)</th>
<th>SDH Name</th>
<th>Status</th>
<th>SONET Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>For Alarm LEDs Alrm1-A, 2-A, 3-A, Alrm 1-B, 2-B, 3-B</td>
<td>LOS</td>
<td>Loss of Signal</td>
<td>LOS</td>
</tr>
<tr>
<td></td>
<td>RS-LOF (RS = Regenerator Section)</td>
<td>Loss of Frame</td>
<td>LOF</td>
</tr>
<tr>
<td></td>
<td>MS-AIS (MS = Multiplex Section)</td>
<td>Alarm Indication Signal</td>
<td>AIS-L (L = Line)</td>
</tr>
<tr>
<td></td>
<td>MS-RDI (MS = Multiplex Section)</td>
<td>Remote Defect Indication</td>
<td>RDI-L (L = Line)</td>
</tr>
<tr>
<td>Off</td>
<td>-</td>
<td>Normal Operation</td>
<td>-</td>
</tr>
</tbody>
</table>
1.5.1.1 T3 6310 Board Panel T3 LED Indicators

Table 1-9: TP-6310/T3 Board Panel LED Indicators

<table>
<thead>
<tr>
<th>Group</th>
<th>LED #</th>
<th>LED Label</th>
<th>Color</th>
<th>States</th>
</tr>
</thead>
<tbody>
<tr>
<td>FAIL</td>
<td>Off</td>
<td>Normal Operation</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Red</td>
<td>Failure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ACT</td>
<td>Off</td>
<td>Stand alone board (non HA system)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Blinking Yellow</td>
<td>Redundant board in standby mode</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Green</td>
<td>Working board</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PSTN</td>
<td>A; B; C</td>
<td>Link</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td>No Link</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Green</td>
<td>T3 Synchronized</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Yellow</td>
<td>RAI</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Remote Alarm Indication (The yellow alarm)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ALRM</td>
<td>Off</td>
<td>No Near End Alarms</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Red</td>
<td>Traffic loss due to one of the following 3 signals:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>LOS</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Loss of Signal</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>LFA</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Loss of Frame Alignment</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AIS</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Alarm Indication Signal (The blue alarm)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PWR</td>
<td>Off</td>
<td>Board Power is down</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Green</td>
<td>Normal Operation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SWAP READY</td>
<td>Off</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Blue</td>
<td>Normal Operation (see Note)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1.5.1.2 6310/RTM - Rear Transition Module

The TP-6310 Rear Transition Module (RTM) board (6310/RTM) provides the fiber optic I/O connections for the following interfaces:

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

Each I/O connection is an SFP (Small Form-factor Pluggable) module with hot-insertion capabilities provided with a 155 Mbps optical SFP Module for a fiber optic OC-3/STM-1 interface.

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.
**Note:** The unused SFP receptacles are covered with dust covers as shown in the figure, above.

All of the boards are hot-swappable - the boards can be removed or inserted when the system is under power.
1. Introduction to the Avaya G860 Media Gateway

1.5.2 SC (System Controller) Board

The System Controller (SC) is a Sun™ CompactPCI™ Single Board Computer (SBC). Solaris™ operating system and Media Gateway control software are preinstalled on the SC board's on-board hard disk, which is designed for the 7/24 carrier grade operation.

The SC board provides PCI Industrial Computers Manufacturers' Group (PICMG) CompactPCI Packet Switched Backplane compliance and is NEBS Level 3 certified to meet the requirements of the communications and service provider environments. The SC board provides one vacant PCI mezzanine card (PMC) slot, which allows expanding its functionality in the future.

The SC boards are located in the first two slots 1 and 2 (color coded red in the chassis card cage).

The front panel Mini DIN 8 COM serial port provides RS-232 console connection.

Note: The RS-232 console connection can be made via the SC front panel Mini DIN 8 COM serial port or via the RS-232 serial port on the SA/RTM.
Figure 1-11: SC Panel
Front Panel Mini DIN 8 COM Serial Port

The front panel Mini DIN 8 COM serial port provides RS-232 console connection to the SC board.

The figure below displays the pin assignments for the front panel Mini DIN 8 COM serial port.

Figure 1-12: SC Front Panel Mini DIN 8 Serial Port Connector

```
7 DCD
8 Shield GND
5 RXD
2 CTS
6 RTS
4 GND
3 TXD
1 DTR
```

The signal interface of the Mini DIN 8 connector is according to the table below:

<table>
<thead>
<tr>
<th>Pin #</th>
<th>Signal Name</th>
<th>Pin #</th>
<th>Signal Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DTR</td>
<td>5</td>
<td>RXD</td>
</tr>
<tr>
<td>2</td>
<td>CTS</td>
<td>6</td>
<td>RTS</td>
</tr>
<tr>
<td>3</td>
<td>TXD</td>
<td>7</td>
<td>DCD</td>
</tr>
<tr>
<td>4</td>
<td>GND</td>
<td>8</td>
<td>Shield GND</td>
</tr>
</tbody>
</table>

System Controller Panel Indicators & Controls

Several indicators are located on the SC (refer to the table below).

Table 1-11: SC Board Indicators

<table>
<thead>
<tr>
<th>Label</th>
<th>Color</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activity</td>
<td>Green</td>
<td>Located on the PMC hard disk PMC module</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lit each time the SC software accesses the hard disk</td>
</tr>
<tr>
<td></td>
<td></td>
<td>During normal operation, it blinks</td>
</tr>
<tr>
<td>ALARM/USER</td>
<td>Blinking Green</td>
<td>Blinking Green indicates that the SC board is functioning properly</td>
</tr>
<tr>
<td></td>
<td>Yellow</td>
<td>Yellow indicates Ethernet Switch board status, communicated from the EMS</td>
</tr>
<tr>
<td>Label</td>
<td>Color</td>
<td>Function</td>
</tr>
<tr>
<td>-------------</td>
<td>-------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>READY</td>
<td>Green</td>
<td>Green power indicator; the board is properly powered.</td>
</tr>
<tr>
<td>HOT-SWAP</td>
<td>Blue</td>
<td>Indicates that the board can be extracted from the chassis. When a board is inserted into a system, the LED is lit automatically until the hardware connection process is completed. The LED then remains off until the extraction is once again enabled when opening the extractors.</td>
</tr>
</tbody>
</table>

There are two recessed pushbutton switches on the front-panel of the SC:

**WARNING**

DO NOT use these pushbuttons to shutdown or reset the Sun™ Solaris™ operating system. Doing so can cause file corruption and loss of system serviceability. Use the correct shutdown procedure described in Shutdown Procedures. These pushbuttons are for use by Avaya Technical Support personnel only.

**ABORT** - Pressing the ABORT pushbutton halts the normal operation of the Solaris OS (and Media Gateway software); the board is dropped to the OpenBoot level and OK prompt is displayed.

**RESET** - Pressing the RESET pushbutton resets the board and causes reboot. Note that some hardware components (e.g., hard disk) are not fully reset via the RESET pushbutton. Therefore, to properly reset the boards, extract them from the chassis and re-insert them.

### 1.5.3 SA Synchronization and Alarm RTM

This section describes the Synchronization and Alarm (SA) rear transition module (RTM).

#### 1.5.3.1 SA/RTM Overview

The Synchronization and Alarm (SA) RTM (rear transition module) is designed to be plugged into the rear slots 1 or 2, behind the SC boards. This module controlled by the SC and provides the chassis management capabilities. It also optionally provides the system synchronization between the Media Gateway and the BITS (Building Integrated Timing Supply).

The chassis management capabilities include: controlling the fans’ operation, monitoring the proper operation of the power supply modules, monitoring the midplane voltages, controlling the chassis temperature, chassis LEDs, pushbutton and the alarm dry contact relay functions.

The synchronization capabilities include: Synchronizing the IO cards in the chassis to BITS equipment and to any available system line clocks. This complies with the GR-1244 Stratum-3 and G.813 requirements. The system has a full redundant mechanism with no single point of failure.

Each SA board is hot swappable, allowing replacement while the system is active. In addition to the chassis control functionality, it provides an RS-232 and terminal block...
connectors for connecting to a Telco alarm unit and support two RJ-48 T1/E1 line interface for the BITS interface on each SA/RTM module.

The Media Gateway software uses the Synchronization and Alarm module to monitor and to control the chassis operation. The gateway reports any abnormal conditions as they occur in the form of managed alarms. Each alarm includes an indicator to correspond to the severity. In addition, the Synchronization and Alarm module is able to control three dry-contact relays to replicate the gateway’s status for minor, major and critical alarms. When the reported alarm is resolved, the gateway detects that the alarm has been cleared and reports as appropriate. The connections are made using terminal block connector on the front of the SA/RTM (gateway’s rear side).

The three alarm LEDs on the chassis label panel function in a similar way. In the event of a fault condition or an alarm condition, the appropriate chassis LED is activated and the alarm trap is sent over the SNMP protocol.

The system status can be monitored via the Element Management System (EMS) for, or via the gateway SNMP interface. For more information, refer to the EMS User’s Manual (Document # LTRT-963xx).

1.5.3.2 Chassis Management

The following summarizes the SA chassis management functionality:

- Monitoring all midplane voltages
- Monitoring proper operation of all power supplies
- Monitoring and controlling chassis temperature by changing the fans’ speed as a function of chassis temperature
- Monitoring the speed of all chassis fans
- Monitoring the temperature of boards
- Controlling the state of alarm relays
- Controlling the front panel chassis LEDs
- Detecting the state of front chassis push-buttons

1.5.3.3 Chassis Temperature Control

One of the important chassis management functions facilitated by the SA/RTM is to control the gateway temperature. This temperature control is accomplished by adjusting the rotational speed of the fans, thereby keeping the internal temperature at acceptable levels for proper gateway operation. In addition, reducing the fan rotational speed significantly reduces the level of generated acoustic noise.

1.5.3.4 Synchronization

The following summarizes the Synchronization functionality that is provided with the optional SA-1/RTM module:

- Integrates two SA/RTM cards to support 1+1 redundancy capability
- Provides Stratum 3 synchronization clock to all Media Gateway synchronous interfaces.
  - Complying with Telecordia GR-1244-CORE and GR-253-CORE Stratum 3.
  - Complying with ITU-T G.813.
  - Free Run accuracy of 4.6ppm.
  - Fully HA with no single point of failure.

- External Clock Synchronization (MG equipped with 6310 boards):
  - Supporting ITU G.813 options 1 and 2, ETSI EN 300-462-5-1, ANSI SMC T1.105.09 and Bellcore GR-1244-core stratum 3.
  - Supporting the following External Reference input:
    - G.703 E1/T1 External Clock Port (SSM isn’t supported);
    - 2048 kHz synchronization signal according to clause 13/G.703 (T12).
    - Output synchronization signals on STM-1/OC3 PSTN lines.

- In board 1+1 T1/E1/T12 redundancy with no single point of failure.
  - In System 1+1 SA redundancy with no single point of failure.
  - Synchronization links alarm processing

- Provides Line timing synchronization from any PSTN STM1/OC3 interface of the TP-6310 board.
- Two RJ-48c connectors (BITS1 & BITS2) on the SA/RTMs. Each RJ-48c connector includes two built-in LEDs.

To configure clock synchronization for your site, see section Configuring Clock Synchronization.

### 1.5.3.5 SA/RTM Card and Panel

The following figure illustrates the SA/RTM card including the optional Timing module.

![Figure 1-13: Synchronization & Alarm (SA) RTM](image)

**Note:** The SA/RTMs with resident Timing module is not supplied with this release and must be ordered separately. Consult with an Avaya representative on how to order this module.
The following figure illustrates the SA/RTM front panel:

**Figure 1-14: SA/RTM Panel**
The SA/RTMs are located in the rear cage of the Avaya G860, in the respective slots 1 and 2, behind the SC boards in the front cage. These RTMs contain an RS-232 console port 9-pin female D-type connector (P2). The corresponding cable is a straight cable with a 9-pin male D-type connector (P1).

### 1.5.3.6 RS-232 Console Pin Signal Interface

The following table describes the signal interface of the connector.

<table>
<thead>
<tr>
<th>P1 Pin #</th>
<th>Signal Name</th>
<th>P2 Pin #</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>-</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>RX (Receive Data)</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>TX (Transmit Data)</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>-</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>GND (Ground)</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>-</td>
<td>6</td>
</tr>
<tr>
<td>7</td>
<td>-</td>
<td>7</td>
</tr>
<tr>
<td>8</td>
<td>-</td>
<td>8</td>
</tr>
<tr>
<td>9</td>
<td>-</td>
<td>9</td>
</tr>
</tbody>
</table>

### 1.5.3.7 LED Interface

The following table describes the SA/RTM LED interface.

<table>
<thead>
<tr>
<th>Label</th>
<th>Color</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>FAIL</td>
<td>Red</td>
<td>Board failure (fatal error)</td>
</tr>
<tr>
<td>ACT</td>
<td>Green</td>
<td>Board initialization sequence terminated OK</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Indicates the Active board</td>
</tr>
<tr>
<td></td>
<td>Yellow</td>
<td>Board initialization sequence terminated OK</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Yellow on indicates Standby board</td>
</tr>
<tr>
<td>HOT-SWAP</td>
<td>Blue</td>
<td>Board can be removed or inserted</td>
</tr>
<tr>
<td>PWR</td>
<td>Green</td>
<td>Power is supplied to the board</td>
</tr>
</tbody>
</table>
1.5.3.8 Terminal Block Connector

The following table describes the terminal block.

<table>
<thead>
<tr>
<th>Alarm Type</th>
<th>Description</th>
<th>Connector Types</th>
<th>Number of Connectors</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRT</td>
<td>Critical</td>
<td>COM, NC, NO</td>
<td>3</td>
</tr>
<tr>
<td>MJR</td>
<td>Major</td>
<td>COM, NC, NO</td>
<td>3</td>
</tr>
<tr>
<td>MNR</td>
<td>Minor</td>
<td>COM, NC, NO</td>
<td>3</td>
</tr>
<tr>
<td>USR</td>
<td>User Defined</td>
<td>COM (x2)*, NC, NO, *IN 1, *IN 2</td>
<td>6</td>
</tr>
</tbody>
</table>

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

1.5.3.9 RJ48-c Pin Signal Interface (Optional)

The following table describes the signal interface of the connector.

<table>
<thead>
<tr>
<th>P1 Pin #</th>
<th>Signal Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Receive-Negative</td>
</tr>
<tr>
<td>2</td>
<td>Receive-Positive</td>
</tr>
<tr>
<td>3</td>
<td>-</td>
</tr>
<tr>
<td>4</td>
<td>Transmit-Negative</td>
</tr>
<tr>
<td>5</td>
<td>Transmit-Positive</td>
</tr>
<tr>
<td>6</td>
<td>-</td>
</tr>
<tr>
<td>7</td>
<td>-</td>
</tr>
<tr>
<td>8</td>
<td>-</td>
</tr>
</tbody>
</table>

Figure 1-15: RJ-48c Trunk Connectors
1.5.3.9.1 Built-In LED Interface

The following table describes the SA/RTM BITS (built-in) LEDs.

<table>
<thead>
<tr>
<th>Label</th>
<th>Color</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>LED#1</td>
<td>Gray</td>
<td>No Signal</td>
</tr>
<tr>
<td></td>
<td>Green</td>
<td>BITS signal – synchronized</td>
</tr>
<tr>
<td>LED#2</td>
<td>Gray</td>
<td>Not in use</td>
</tr>
</tbody>
</table>

1.6 Ethernet Switch Boards

1.6.1 ES/6600 - Used in Avaya G860 Configurations

The ES/6600 Ethernet Switch board, based on CPC6600, is a full wire-speed Layer2 10/100/1000 24 port Gigabit Ethernet switch that is compatible with both PICMG 2.16 CompactPCI® backplanes. The ES/6600 board is accompanied by a corresponding RTM, which provides up to 7 copper-based Ethernet ports. In the Avaya G860 configuration, the ES/6600 board provides 18 Gigabit port connections via the midplane and 6 1000Base-T ports via a Rear Transition Module. The 6600 ES boards have an internal interlink connection. There is an F-Link between the two ES boards using one of the RTM ports. For more details on the ES/6600/RTM, refer to ES/6600/RTM on page 50.

The ES/6600 Ethernet Switch board provides the following features:

- 24 10/100/1000Mbps cPSB-compliant Ethernet ports (11 are connected to the Avaya G860 midplane slots, the remainder are for future use)
- An RS-232 console port 6-pin female RJ-11 connector. This port is used for maintenance only.

**Note:** The 10/100 Base-TX management port on the front panel is not used in the Avaya G860 configuration. Use the RS-232 console port instead.

- Dual 44Gbs switched fabrics
- Advanced Fast Filter Processor for wire speed Layer2-7 packet classification and filtering
- Support for hardware connection layer of PICMG 2.1 Hot Swap, enhanced with Performance Technologies' exclusive Auto Configuration Replication.
- Full duplex 802.3x Flow Control
- 16K MAC addresses (Layer2)
- Managed learning of attached devices on a per-port basis for enhanced network security
1. Introduction to the Avaya G860 Media Gateway

- 802.3ac tagged packet support
- Jumbo packet (9KB) support
- 802.1p priority queuing (8 classes of service).
- 802.1Q VLAN support (16 VLANs)
- 802.3-2000 Link Aggregation (up to 12 groups, 8 ports per group)
- Broadcast storm detection and suppression
- Multi-Port Mirroring
- Power-On diagnostics
- Single-slot Rear Transition Module supports up to 6 1000BaseT ports, plus console.

The figure below shows the front panel view of the ES/6600 Ethernet Switch board.
Figure 1-16: ES/6600 Panel
1.6.1.1 ES/6600 Panel Indicators

The status of all Ethernet ports is shown by LED indicators on the front panel.

Table 1-17: Port/Link Activity Indicators

<table>
<thead>
<tr>
<th>Indicator Status</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>Link exists</td>
</tr>
<tr>
<td>Off</td>
<td>No Link exists</td>
</tr>
<tr>
<td>Flashing Green</td>
<td>Activity (transmit or receive)</td>
</tr>
</tbody>
</table>

Note 1: The 10/100 Base-TX ports flash the Activity indicator when there is transmit or receive activity.

Note 2: The Gigabit (SX) ports flash the Activity indicator when there is receive activity only.

Table 1-18: Port Speed Indicators

<table>
<thead>
<tr>
<th>Indicator Status</th>
<th>Switched Ports</th>
<th>Management Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yellow</td>
<td>1000 Mbps</td>
<td>100 Mbps</td>
</tr>
<tr>
<td>OFF</td>
<td>10 or 100 Mbps</td>
<td>10 Mbps</td>
</tr>
</tbody>
</table>

Table 1-19: System Indicator

<table>
<thead>
<tr>
<th>Indicator Status</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>Board is operational</td>
</tr>
<tr>
<td>Yellow</td>
<td>Board is booting</td>
</tr>
<tr>
<td>OFF</td>
<td>No power or serious fault</td>
</tr>
</tbody>
</table>

Table 1-20: Fault Indicator

<table>
<thead>
<tr>
<th>Indicator Status</th>
<th>State Indication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red</td>
<td>Fault</td>
</tr>
<tr>
<td>OFF</td>
<td>No fault or no power</td>
</tr>
</tbody>
</table>
Note: The FAULT indicator is off unless a serious internal error is detected.

Table 1-21: Ethernet Switch Hot-Swap Indicator

<table>
<thead>
<tr>
<th>Indicator Status</th>
<th>State Indication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blue</td>
<td>Board can be removed or inserted</td>
</tr>
</tbody>
</table>

1.6.1.2 ES/6600 Physical Slots to Ethernet Port Correlation - Avaya G860 Configuration

Note 1: The Ethernet Switches are interconnected internal Ethernet links.

Note 2: Occupied in terms of the Ethernet Switch and reflected by the indicators.

Table 1-22: ES/6600 Physical Slots to Ethernet Port Correlation

<table>
<thead>
<tr>
<th>Slot Number</th>
<th>Slot 3 Ethernet Switch Port</th>
<th>Slot 4 Ethernet Switch Port</th>
<th>Dedicated to Board Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>SC</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>2</td>
<td>SC</td>
</tr>
<tr>
<td>3</td>
<td>-</td>
<td>24</td>
<td>Ethernet Switch</td>
</tr>
<tr>
<td>4</td>
<td>24</td>
<td>-</td>
<td>Ethernet Switch</td>
</tr>
<tr>
<td>5</td>
<td>3</td>
<td>3</td>
<td>N/A</td>
</tr>
<tr>
<td>6</td>
<td>4</td>
<td>4</td>
<td>N/A</td>
</tr>
<tr>
<td>7</td>
<td>5</td>
<td>5</td>
<td>TP-6310</td>
</tr>
<tr>
<td>8</td>
<td>6</td>
<td>6</td>
<td>TP-6310</td>
</tr>
<tr>
<td>9</td>
<td>13</td>
<td>13</td>
<td>TP-6310</td>
</tr>
<tr>
<td>10</td>
<td>14</td>
<td>14</td>
<td>TP-6310</td>
</tr>
<tr>
<td>-</td>
<td>18</td>
<td>18</td>
<td>GbE port used for O&amp;M or Control traffic when Interface Separation is enabled</td>
</tr>
<tr>
<td>-</td>
<td>19</td>
<td>19</td>
<td>GbE port used for Control traffic when Interface Separation is enabled</td>
</tr>
<tr>
<td>-</td>
<td>20</td>
<td>20</td>
<td>GbE port that can be aggregated with port 21 and 22</td>
</tr>
</tbody>
</table>
## 1. Introduction to the Avaya G860 Media Gateway

<table>
<thead>
<tr>
<th>Slot Number</th>
<th>Slot 3 Ethernet Switch Port</th>
<th>Slot 4 Ethernet Switch Port</th>
<th>Dedicated to Board Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>21</td>
<td>21</td>
<td>GbE port used aggregated with port 20</td>
</tr>
<tr>
<td>-</td>
<td>22</td>
<td>22</td>
<td>GbE port used aggregated with port 20 when Media Aggregation Enabled</td>
</tr>
<tr>
<td>-</td>
<td>23</td>
<td>23</td>
<td>GbE port used as mirror port for Maintenance purposes</td>
</tr>
</tbody>
</table>
1.6.1.3  **ES/6600/RTM**

The ES/6600/RTM is supplied with the ES/6600 Ethernet Switch board and allows connection from the Avaya G860 to 10/100/1000Base-T external Ethernet equipment. The ES/6600/RTM also contains an RS-232 console port, which is used for configuration or debugging.

*Figure 1-17: ES/6600/RTM*
1.7 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. Any slot with no board assigned to it must be covered with a blank panel.

Slot 10 contains the Redundant TP-6310 board and the order for inserting the rest of the TP-6310 boards begins in Slot 9. The fourth (final) TP-6310 board is inserted in slot 7.

**Note 1:** For all TP-6310 system configuration board assembly options, Slot 5 must retain the blank panel with air baffle and Slot 6 must retain the blank panel.

**Note 2:** The Redundant TP-6310 board requires the 6310/RTM/Redundant.

### Table 1-23: ES/6600/RTM Port Pin Outs

<table>
<thead>
<tr>
<th>Pin Number</th>
<th>Signal Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Rx+</td>
</tr>
<tr>
<td>2</td>
<td>Rx-</td>
</tr>
<tr>
<td>3</td>
<td>Tx+</td>
</tr>
<tr>
<td>4</td>
<td>-</td>
</tr>
<tr>
<td>5</td>
<td>-</td>
</tr>
<tr>
<td>6</td>
<td>Tx-</td>
</tr>
<tr>
<td>7</td>
<td>-</td>
</tr>
<tr>
<td>8</td>
<td>-</td>
</tr>
</tbody>
</table>

### Table 1-24: Board Assembly Order for 6310 System Configuration - View 1

<table>
<thead>
<tr>
<th>Slot #</th>
<th>Front Board</th>
<th>Rear Board</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slot 1</td>
<td>SC</td>
<td>SA/RTM/TIMING</td>
</tr>
<tr>
<td>Slot 2</td>
<td>SC</td>
<td>SA/RTM/TIMING</td>
</tr>
<tr>
<td>Slot 3</td>
<td>ES/6600</td>
<td>ES/6600/RTM</td>
</tr>
<tr>
<td>Slot 4</td>
<td>ES/6600</td>
<td>ES/6600/RTM</td>
</tr>
<tr>
<td>Slot 5</td>
<td>Blank Panel – Air Baffle</td>
<td>Blank Panel</td>
</tr>
<tr>
<td>Slot 6</td>
<td>Blank Panel</td>
<td>Blank Panel</td>
</tr>
<tr>
<td>Slot 7</td>
<td>TP-6310 #3</td>
<td>6310/RTM</td>
</tr>
<tr>
<td>Slot 8</td>
<td>TP-6310 #2</td>
<td>6310/RTM</td>
</tr>
<tr>
<td>Slot 9</td>
<td>TP-6310 #1</td>
<td>6310/RTM</td>
</tr>
</tbody>
</table>
For ventilation purposes, blank panels are always inserted in slot 6 and underneath the lowest TP-6310 number. For example, if there are two TP-6310s inserted in slots 9 and 10, blank panels are inserted in slots 6 and 8 and air baffles are inserted in slots 5 and 7.

**Table 1-25: 6310 System Configuration Board Assembly - View 2**

<table>
<thead>
<tr>
<th>Slot #</th>
<th>Front Board</th>
<th>Rear Board</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slot 1</td>
<td>SC</td>
<td>SA/RTM/TIMING</td>
</tr>
<tr>
<td>Slot 2</td>
<td>SC</td>
<td>SA/RTM/TIMING</td>
</tr>
<tr>
<td>Slot 3</td>
<td>ES/6600</td>
<td>ES/RTM</td>
</tr>
<tr>
<td>Slot 4</td>
<td>ES/6600</td>
<td>ES/RTM</td>
</tr>
<tr>
<td>Slot 5</td>
<td>Blank Panel – Air Baffle</td>
<td>Blank Panel</td>
</tr>
<tr>
<td>Slot 6</td>
<td>Blank Panel</td>
<td>Blank Panel</td>
</tr>
<tr>
<td>Slot 7</td>
<td>Blank Panel – Air Baffle</td>
<td>Blank Panel</td>
</tr>
<tr>
<td>Slot 8</td>
<td>Blank Panel</td>
<td>6310/RTM</td>
</tr>
<tr>
<td>Slot 9</td>
<td>TP-6310 #1</td>
<td>6310/RTM</td>
</tr>
<tr>
<td>Slot 10</td>
<td>TP-6310 Redundant (Redundant Configuration)</td>
<td>6310/RTM/Redundant</td>
</tr>
</tbody>
</table>
2. Getting Started with the Avaya G860

2.1 Installation Process Flow

The installation process flow depicted in the figure below illustrates the steps involved in the installation process.

Figure 2-1: Installation Process Flow
2.2 Site Preparation

2.2.1 Physical Requirements

The following describes the equipment that must be prepared on site before the Avaya G860 can be installed.

2.2.1.1 Equipment

<table>
<thead>
<tr>
<th>Item</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>L2/L3 Switch or Routers</td>
<td>Two are required for High Availability. They must have 1 Gbps optical ports, refer to Interfacing with the IP Networks on page 61.</td>
</tr>
<tr>
<td>NTP Server</td>
<td>Server platform for the Network Time Protocol (a redundant platform is recommended). For simple configurations, the EMS server may be used as the NTP server. However it does not have redundant protection and its internal clock accuracy is low.</td>
</tr>
<tr>
<td>SNMP Management Station</td>
<td>Avaya EMS (Element Management System) or Customer EMS. Alternatively, a MIB Browser can be used for minimal management operations</td>
</tr>
<tr>
<td>PC Terminal Console</td>
<td>The PC with RS-232 COM port or a dedicated RS-232 Terminal Console is used to install and configure the SC board software</td>
</tr>
<tr>
<td>Telco Rack</td>
<td>19-inch rack can support up to 6 Avaya G860s</td>
</tr>
<tr>
<td>Screws and Washers</td>
<td>Appropriate for installing Avaya G860 chassis on rack</td>
</tr>
<tr>
<td>Wrist Strap and banana plug or alligator clip</td>
<td>For electrostatic discharge (ESD) connection</td>
</tr>
<tr>
<td>Lugs and screws</td>
<td>Appropriate for earthing</td>
</tr>
</tbody>
</table>

2.2.1.2 Electrical

<table>
<thead>
<tr>
<th>Item</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outlets</td>
<td>Suitable for above equipment and AC or DC inputs as appropriate to Customer requirements for the Avaya G860.</td>
</tr>
<tr>
<td>Circuit breaker</td>
<td>A 25A max double pole circuit breaker to act also as a disconnect device. The capacity of the circuit breaker in the electrical cabinet must be sufficient to handle the power requirements described in this document</td>
</tr>
</tbody>
</table>
2. Getting Started with the Avaya G860

<table>
<thead>
<tr>
<th>Item</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power consumption</td>
<td>Provide sufficient capacity for the average power consumption for a full complement of boards:</td>
</tr>
<tr>
<td></td>
<td>Power consumption:</td>
</tr>
<tr>
<td></td>
<td>• Avaya G860 chassis with maximum TP-6310 boards:</td>
</tr>
<tr>
<td></td>
<td>600 watts - 5.3 A at 115 VAC</td>
</tr>
<tr>
<td></td>
<td>600 watts - 2.7 A at 230 VAC</td>
</tr>
<tr>
<td></td>
<td>640 watts - 13.4 A at 48 VDC</td>
</tr>
<tr>
<td>For AC power only</td>
<td>UPS backup</td>
</tr>
</tbody>
</table>

2.2.1.3 Cables

**Note 1:** Be sure to prepare the interface connections before beginning the Avaya G860 installation.

**Note 2:** For Cable pin out information, refer to the pin out tables in Avaya G860 Boards on page 30.
### Table 2-3: Cabling Requirements

<table>
<thead>
<tr>
<th>Item</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>RS-232 Cables</td>
<td>For SC and ES Console Terminals (provided with the product)</td>
</tr>
<tr>
<td>Fiber Optic Cables</td>
<td>The customer is responsible for providing:</td>
</tr>
<tr>
<td>For Avaya G860 Configuration</td>
<td><strong>STM-1/OC-3 cables:</strong></td>
</tr>
<tr>
<td></td>
<td>Twin fiber optic cable to each STM-1/OC-3 interface using with Dual-LC optical connectors for connection to dual (Tx and Rx) 155 Mbps Optical transceivers. These cables should be as specified in GR-253-CORE. Length is determined by the customer.</td>
</tr>
<tr>
<td></td>
<td>Quantity: 1 fiber pair for each utilized interface on a TP-6310 board</td>
</tr>
<tr>
<td></td>
<td>Small Factor Optical transceivers (SFP) modules are supplied as part of the Media Gateway board.</td>
</tr>
<tr>
<td></td>
<td>(Refer to Connecting the PSTN Interface on page 83.)</td>
</tr>
<tr>
<td></td>
<td><strong>PSTN T3 cables:</strong></td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Quantity: up to 3 cable pairs for each TP-6310 board.</td>
</tr>
<tr>
<td></td>
<td>(Refer to Connecting the T3 PSTN Interfaces on page 86.)</td>
</tr>
<tr>
<td></td>
<td><strong>Ethernet 1000 Base-T links:</strong></td>
</tr>
<tr>
<td></td>
<td>For ES/6600/RTM: One CAT 5 cable for each GbE port connection.</td>
</tr>
<tr>
<td></td>
<td>Quantity: Up to 5 CAT-5 cables for each ES/6600 board.</td>
</tr>
<tr>
<td></td>
<td>(Refer and Connecting the ES/6600 IP Network CAT 5 Copper Cabling on page 82.)</td>
</tr>
<tr>
<td>Earthing Cables</td>
<td>Refer to Earthing Requirements on page 24.</td>
</tr>
<tr>
<td>Power Cables</td>
<td>Use 14 AWG stranded wiring for hook up to local power source</td>
</tr>
<tr>
<td></td>
<td>(Refer to Connecting System Power on page 70.)</td>
</tr>
</tbody>
</table>

### 2.2.2 Defining IP Parameters

The tables below detail the parameters that the customer must allocate and provide as preparation for the installation procedures.

If the Avaya G860 is to be connected to the IP network with Interface Separation, separate IP addresses for OAM, Media and Control Networks must be allocated for Media Gateway and Media Gateway boards. Otherwise, a single IP address must be allocated for each component;

In the tables below, use OAM Network column only if Interface Separation is not available. Otherwise, use relevant columns, according to the specific IP network separation topology.
2. Getting Started with the Avaya G860

For more information, refer to Configuring the Media Gateway for IP Connectivity on page 127.

### 2.2.2.1 Gateway Addresses

If the network has a single subnet, use the Single Subnet Configuration column in the table below. If the network includes 3 subnets, use the 3 Subnets - OAM, Media and Control Network columns in the table below:

<table>
<thead>
<tr>
<th>OAM Network</th>
<th>Media Network</th>
<th>Control Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subnet Mask</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Default Gateway Router</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 2.2.2.2 Boards' IP Addresses for Avaya G860 Configuration

#### Table 2-5: Boards' IP Addresses for Avaya G860 Configuration

<table>
<thead>
<tr>
<th>Slot No.</th>
<th>Element</th>
<th>IP Address</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>TP-6310</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>TP-6310</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>TP-6310</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>TP-6310</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 2.2.2.3 Network Servers' IP Addresses

For the relevant Network Servers, prepare the IP addresses according to the table below.

#### Table 2-6: Network Servers' IP Addresses

<table>
<thead>
<tr>
<th>Network Server</th>
<th>IP Addresses</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EMS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NMS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OSS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>APS</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
2.2.2.4 **VLANs Configuration**

If VLANs are used in the network, prepare the VLANs configuration information using the table below.

<table>
<thead>
<tr>
<th>VLAN ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>OAM Network</td>
</tr>
<tr>
<td>Media Network</td>
</tr>
<tr>
<td>Control Network</td>
</tr>
</tbody>
</table>

2.2.2.5 **DiffServ Priorities**

Use the following table for specifying the DiffServ priority settings. Take them from the Network configuration.

<table>
<thead>
<tr>
<th>DiffServ Class Name</th>
<th>Protocol Group</th>
<th>DiffServ Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>Communications between network devices within one administrative domain like ICMP, COPS, RSVP, DNS, DHCP, BootP, high priority OAM</td>
<td></td>
</tr>
<tr>
<td>Premium Media</td>
<td>Telephony service like RTP media, T.38 Fax over IP, Lawful Intercept or Control protocols</td>
<td></td>
</tr>
<tr>
<td>Premium Control</td>
<td>Signaling protocols like MEGACO, MGCP, TGCP.</td>
<td></td>
</tr>
<tr>
<td>Gold</td>
<td>Used for Voice Streaming, Video on demand Broadcast TV, Video surveillance</td>
<td></td>
</tr>
<tr>
<td>Bronze</td>
<td>Used for long-lived TCP, and HTTP flows, such as Non time-critical OAM&amp;P, Email, Instant Messaging</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** The priority settings assigned to a DiffServ Class name is assigned per Protocol group. The same assignment is relevant to all of the protocols in the Protocol group.

2.2.2.6 **IEEE 802.1p QoS/CoS Layer 2 Traffic Prioritization**

If IEEE 802.1p is specified, prepare the Service Priority Class information according to the table below.

<table>
<thead>
<tr>
<th>Service Priority Classes</th>
<th>Tag</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Service Class DiffServ</td>
<td></td>
</tr>
<tr>
<td>Premium Media DiffServ</td>
<td></td>
</tr>
</tbody>
</table>
2. Getting Started with the Avaya G860

## Service Priority Classes

<table>
<thead>
<tr>
<th>Tag</th>
</tr>
</thead>
<tbody>
<tr>
<td>Premium Control DiffServ</td>
</tr>
<tr>
<td>Gold Service Class DiffServ</td>
</tr>
<tr>
<td>Bronze Service Class DiffServ</td>
</tr>
</tbody>
</table>

### 2.2.2.7 IPSEC Configuration

If IPSEC is used to establish secure communication between the Avaya G860 Media Gateway and OAM servers, prepare Security Profile configuration information according to the table below.

<table>
<thead>
<tr>
<th>Server</th>
<th>IKE Pre-Shared Key</th>
<th>IKE Encryption (DES/3DES)</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NMS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OSS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>APS</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 2.2.3 Environmental Requirements

The Avaya G860 chassis mechanical envelope complies with the requirements of NEBS GR-63-CORE, Issue 2.

The table below provides a list of the mechanical requirements which were imposed on the chassis design.

<table>
<thead>
<tr>
<th>Physical Protection Requirements</th>
<th>Test level</th>
<th>Reference (GR-63 para.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Humidity</td>
<td>5 to 90%</td>
<td>4.1.2</td>
</tr>
<tr>
<td>Altitude</td>
<td>-60 to 3048 m (10,000 ft)</td>
<td>4.1.3</td>
</tr>
<tr>
<td>Fire Resistance</td>
<td></td>
<td>4.2.3</td>
</tr>
<tr>
<td>Drop Test, Packaged</td>
<td>Drop height: 600 mm</td>
<td>4.3.1 (10-25 kg, one person carrying)</td>
</tr>
<tr>
<td>Drop Test, Unpackaged</td>
<td>Drop height: 75 mm</td>
<td>4.3.2 (10-25 kg, one person carrying)</td>
</tr>
<tr>
<td>Earthquake</td>
<td>Zone 4</td>
<td>4.4.1</td>
</tr>
<tr>
<td>Office Vibration</td>
<td>5-100-5 Hz/0.1g, 0.1 oct/minute; 3 axes</td>
<td>4.4.3</td>
</tr>
<tr>
<td>Transportation Vibration</td>
<td>5-100 Hz, 0.1 oct/min; 100-500 Hz, 0.25 oct/min</td>
<td>4.4.4</td>
</tr>
</tbody>
</table>
Presently, the system operation is guaranteed under the following conditions:

### 2.2.3.1 Environmental Conditions

### 2.2.3.2 Temperature

#### Table 2-12: Temperature Range

<table>
<thead>
<tr>
<th>Extended Short-term Temperature Range for Operation</th>
<th>-5°C to +55°C / 23°F to +131°F</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recommended Ambient Temperature</td>
<td>+5°C to +40°C / 41°F to +104°F</td>
</tr>
</tbody>
</table>

### 2.2.3.3 Humidity

#### Table 2-13: Humidity Range

<table>
<thead>
<tr>
<th>Relative Humidity Range for Operation</th>
<th>5 to 90%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nominal Relative Humidity</td>
<td>70% (wet bulb)</td>
</tr>
</tbody>
</table>

### 2.2.3.4 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, where the surge level may not exceed 2kV.

### 2.2.3.5 Altitude

#### Table 2-14: Altitude Range

| Altitude | Up to 3048 m (10,000 ft) |
2.2.3.6 Earthquake

Table 2-15: Earthquake Requirements

| Earthquake Zone | 4 |

2.2.3.7 Rack Requirements

Table 2-16: Rack Requirements

| Telco Rack | 19-inch |
| Space | As per GR-63-CORE
         | Maintenance access 762 mm (2' 6") |
         | Wiring access 610 mm (2') |

2.3 Preparing the IP Network Connectivity

The Avaya G860 Gateway must be connected to the IP network for proper operation. The Avaya G860 may operate in different IP network topologies, including networks with multiple VLANs and subnets. Refer to Connecting the Media Gateway to the IP Network on page 157 and Use Cases for IP Network Connectivity Configuration on page 148.

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

- Two Layer 2 or Layer 3 Ethernet Switches are available (to be connected to the two ES boards).
- 1GB Ethernet interfaces are used (for IP network topologies with separate OAM, Media and Control networks – 1GB interface should be used for Media network);

**Note:** For ES/6600 switch boards up to 3GB copper aggregated links may be used for connecting the to the media network.

- Switches are interconnected by at least 1GB Ethernet interface (for ES/6600, 3GB interconnection may be required if media traffic is aggregated).
- If Layer 2 switches are used, ensure that the spanning tree algorithm is activated on them to prevent network loops.
- If Layer 3 switches are used, ensure that VRRP is properly configured on them and enables Layer 2 interconnectivity between the switches.
2.3.1 Preparing the PSTN Network Connectivity

Prepare the PSTN Network connections that will be used for connecting the Avaya G860 Gateway to the other PSTN equipment. The PSTN network connection type depends on the type of the Media Gateway boards installed in the Avaya G860 Gateway:

- TP-6310 STM-1/OC-3 – STM-1/OC-3 fiber links
- TP-6310 T3 – T3 trunks

2.3.1.1 SDH/SONET Network Connections

For the Avaya G860 STM-1/OC-3 configuration, to prepare for connecting the gateway to the PSTN network, be sure to investigate the type and the topology of the provided links and follow the checks listed below.

1. Check that the SDH/SONET interface bit-rate for the TP-6310 boards’ is 155Mbps.
2. Verify that the provided link is behind the Add-Drop Multiplexer (ADM). The SONET/SDH links are design to support point-to-point topology only. They cannot be part of the SONET/SDH ring.
3. Investigate SONET/SDH configuration parameters.
4. Investigate the multiplexing hierarchy of the provided PSTN links. It should be configured the same as the gateway’s links. The Avaya G860 provides two types of multiplexing hierarchies (or multiplexing method) each for SONET and SDH. You can choose VC12 for SDH or VT1.5 for OC3, one of them without changing the multiplexing
5. Investigate APS (Automatic Protection Switching) capabilities of the connected STM-1/OC-3 PSTN equipment. Check the:
   - Topology - linear or ring
   - 1+1 or 1:N
   - Transmission direction - uni-directional or bi-directional
   - If the traffic switching is revertive or not
   - Protection channel function - permanent carrier or not, shared among working channels
6. Check the clock synchronization plan of the site.

2.3.1.2 T3 Network Connections

For the Avaya G860 T3 configuration, before connecting the Avaya G860 to the PSTN network, be sure to investigate the following:

1. Check the framing method of the connected interface.
2. Investigate the clock synchronization plan of the site and supported methods on the connected equipment.
3. Check the transmission characteristics of the connected interface.
4. Check the connector types of the T3 wires. The Avaya G860 requires mini-SMB connectors.
2. Getting Started with the Avaya G860

5. Check the cable type. The Avaya G860 uses twin T3 cables to the T3 Tx and Rx connectors.

2.3.2 Clock Synchronization

Verify the clock synchronization configuration of the site. For more information, refer to section Configuring Clock Synchronization on page 252.

2.4 Unpacking/Checking Contents

The Avaya G860 (configured and populated as per the customer’s order) is shipped in a heavy-duty corrugated cardboard container. Two people are required to lift the Avaya G860 Media Gateway from its packing container. A third person is needed to fasten the chassis to the rack while two people are holding the chassis in place.

➢ To unpack the Avaya G860 Gateway, take these 10 steps:

1. Transport the Avaya G860 to the installation location using an appropriate conveyor.

   ![Note: Do not cut the straps.](image)

2. Open the top flaps of the packing box.

3. Detach the straps from the top flaps and lay them on the floor. (Refer to the figure below.)

![Figure 2-2: Initial Unpacking of the Carton](image)
4. Lift the box frame up and off of the gateway unit. (Refer to the figure below.)

**Figure 2-3: Removing Top of Carton**

5. Remove the insulation material and accessory kit that is on top and around the gateway unit. (Refer to the figure below.)

**Figure 2-4: Accessory kit at the top of the Carton**
6. Open the protective plastic covering and pull it down around the chassis, taking care to free it from the terminal block covers (refer to the figure below).

Figure 2-5: Opening the Plastic Covering

7. Grasp the Avaya G860 handles on either side of the chassis (this requires two people, one on each side of the carton, grasping the handle on that side) and lift it from the carton.

8. Place the Avaya G860 chassis upright on a stable surface.

9. Save the packaging material in case the equipment needs to be transported at a future time.

10. Check the contents of the shipment against the delivery documents. Report any discrepancy regarding the contents or apparent damage to Avaya headquarters or your local Avaya representative, as soon as possible.

2.5 Mounting the Chassis on a Rack

Note 1: The Avaya G860 complies with Network Equipment Building System (NEBS) requirements for racks.

Note 2: The Avaya G860 must be installed only in restricted access locations with ambient temperature not exceeding 40 deg C.

The Avaya G860 is provided with mounting flanges on either side of the front of the chassis, appropriate for standard 19-inch racks (provided by Customers). 23-inch racks are not supported by the Avaya G860.
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.)

**Tip:** A chassis pre-installed in the rack can assist in the installation by placing the chassis on it while fastening the chassis to the rack.

➢ **To mount the chassis on a rack, take these 2 steps:**

1. Grasp the handles on either side of the chassis as well as on the base of the chassis. Lift it and fit it onto the rack.
2. While a technician is holding the chassis in place; a second person fastens the chassis to the rack rails using four screws (not provided), two on each side of the chassis or as appropriate for your rack type. Refer to the figure below.

Figure 2-6: Attaching the Chassis to the Rack

Figure 2-7: Chassis on the Rack - Front View
2.6 Earthing

2.6.1 Earthing the Gateway

The gateway must be earthed to a stable local earth reference. The gateway's earth terminal should be connected through a separate earth wire (6 AWG recommended) to the rack's earthing. The earthing connection's resistance must not be greater than 0.1 ohm. Verify that the rack's earthing is properly done.

Earthing provisions for the Avaya G860 are located on the Power Entry Module (PEM) panel, as shown in the figure below. There are two earth connectors situated immediately to the right of each DC power connector or to the left of the AC power connector. The chassis is supplied with earth lugs and screws.

The screw size is ¼ inch. The lug diameter is 0.63 inches.

To connect the earthing, take this step:

- On the rear panel of the chassis, for DC, there are two pairs of earthing screws (refer the figure below showing the DC version); for AC there is one pair of earthing screws (refer the figure below showing the AC version). To each of these pairs, connect a two-hole standard barrel type copper lug attached to earthing wire. An example of an appropriate two-hole standard barrel copper lug is Molex heavy duty terminal connector #19221-0168.

Earthing - 5000-DC-6310.
2. Getting Started with the Avaya G860

2.7 Powering Up

After mounting the chassis and connecting the earth, the Avaya G860 is ready to power up. Before powering up, the following verification procedure must be carried out.

- **Verify that the following 4 items are correct:**
  1. Check that an earthing lug is present and that the hardware connections at both ends of the cable are tight.
  2. Check that all front slots are occupied, either by a board or by an appropriate front blank panel.
  3. Check that all rear slots are occupied, either by a board or by a blank panel.
  4. Verify that all boards are installed in their dedicated slots (refer to Front and Back Views of the Avaya G860 on page 22).
2.7.1 Connecting System Power

Power connections to the Avaya G860 must comply with local safety codes. Power connections must be performed by qualified personnel only.

Caution

Be sure to make the earth connection before connecting the power. Refer to Earthing on page 68.

2.7.1.1 Connecting DC Power

The PEMs on the rear of the chassis are provided with redundant pairs of power inputs for DC. These pairs are marked J1 and J2. The two PEMs provide 1+1 module redundancy.

Each pair (the two input terminals marked J1 and the two input terminals marked J2) must be connected to a separate power source for the redundancy configuration to function correctly.

For minimum power (with no redundant protection) only one or the four total power inputs terminals must be connected.

For one power source with redundant protection, power must be connected to either the two input terminals marked J1 and the two input terminals marked J2, on each of the PEM modules.

For two power supplies with single wiring, connect one J1 and one J2 power input terminals.
For full redundancy protection, for power feed protection, as well as PEM module protection, connect power to both the J1 and J2 power inputs terminals on both PEM modules.

Figure 2-11: DC Power Connections Redundant Pairs

![DC Power Connections Redundant Pairs](image)

**WARNING**
Make sure that the power connections are according to the indicated polarity.

➢ To connect the DC power to the terminals on each terminal block, take these 5 steps:

1. Remove input terminals from the PEM.
2. Connect two 14 AWG stranded wiring to the inputs, paying attention to the polarity, and tightening the upper screws.
3. Reinsert the input terminal pins into the power input terminals, and fasten the screws on the left and right sides. Refer to the figure below.
4. Check the LED indicators of the various boards are lit according to the table below.
5. Repeat these steps for the connections on the second PEM.
2.7.1.2 Connecting AC Power

A standard, properly earthed, socket and associated circuit breaker is provided on the rear of the chassis. A power cable is provided according to the customer’s local standard.

Table 2-17: AC Power Cable Types

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RACT00001</td>
<td>POWER CORD AC 3 WIRE MEMA 5-15P AMERICAN TYPE</td>
</tr>
<tr>
<td>RACR00006</td>
<td>POWER CORD AC 3 WIRE 2.5m AUSTRALIAN TYPE</td>
</tr>
<tr>
<td>RACR00001</td>
<td>POWER CORD AC 3 WIRE 1.8m CONTINENTAL EUROPE TYPE</td>
</tr>
<tr>
<td>RACR00003</td>
<td>POWER CORD AC 3 WIRE 2.5m CHINESE TYPE</td>
</tr>
<tr>
<td>RACR00004</td>
<td>POWER CORD AC 3 WIRE 2.5m BRITISH TYPE WITH 3A FUSE</td>
</tr>
<tr>
<td>RACR00005</td>
<td>POWER CORD AC 3 WIRE 2.5m ARGENTINEAN TYPE</td>
</tr>
</tbody>
</table>
2. Getting Started with the Avaya G860

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RACR00002</td>
<td>POWER CORD AC 3 WIRE 1.8m ISRAELI TYPE</td>
</tr>
</tbody>
</table>

**Note 1:** Using an AC power source with UPS is recommended to avoid total power failure if the AC power source fails. For redundant system configurations the UPS is required to assure continuous system functionality, in the event that a component failure occurs.

**Note 2:** The AC power cable should be connected to power sockets that are protected by a protection device providing a maximum of 16A protection capacity.

➢ **To connect the AC power to the terminals, take the next 9 steps:**

1. If a UPS is included, verify that an AC power source with UPS is to be used (required for redundant system configurations).
2. Verify that the circuit breaker in the electrical cabinet is sufficient to handle the power requirements.
3. Verify that the PEM is set to either 115VAC (for the range of 90 to 135 VAC) or 230 VAC (for the range of 190 to 264 VAC) as your standards require. If not, use a screwdriver to open the fuse cavity cap, remove and rotate the red fuse so that the type you require is displayed through the cap’s opening. (Refer to the figure above.)
4. Close the cap. (there should be a click).
5. Check that the switch is set to the off position (O).
6. Connect the standard power cable to the 3-prong socket on the rear panel.
7. Plug in the power cable into an earthed power outlet.
8. Turn the switch to the on position (I).
9. Check that the LED indicators of the various boards are lit according to Avaya G860 Boards on page 30.
2.7.1.3 Connecting Power - 6310 System Configuration

Figure 2-13: PS/DC/5K Power Supply - 6310 System Configuration

The Avaya G860 chassis with 6310 system configuration is powered from AC or DC sources. (The AC version is not shown.)

Caution
Use Avaya approved Power Supply units ONLY.

<table>
<thead>
<tr>
<th>Type</th>
<th>Power Requirements</th>
<th>Connection Provisions</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC</td>
<td>100 to 240 V AC, nominal 50/60 Hz</td>
<td>Standard 3-prong sockets</td>
</tr>
<tr>
<td>DC</td>
<td>-40.5 to -60 V DC</td>
<td>Input terminals</td>
</tr>
</tbody>
</table>

2.7.1.3.1 Connecting DC Power

The rear of the chassis (refer to the figure below) is provided with redundant power inputs for DC, each located on a PEM module. For redundant protection, each input terminals must be connected to a separate power source.
Each power entry port of the Avaya G860 must be connected to DC mains through a 25A max double pole circuit breaker, which acts also as a disconnect device.

**WARNING**
Make sure that the power connections are according to the indicated polarity.

➢ **To connect the DC power to the terminals on each terminal block, take these 5 steps:**

1. Remove input terminal from the PEM.
2. Connect two 14 AWG stranded wiring to the input, paying attention to the polarity, and tightening the upper screws.
3. Reinsert the input terminal pin into the power input terminal, and fasten the screws on the left and right sides. Refer to the figure below.
4. Check the LED indicators of the various boards are lit according to the table below.
5. Repeat these steps for the connections on the second PEM.

**Figure 2-15: Input Terminal Wiring**
2.7.1.3.2 Connecting AC Power

A standard, properly earthed, socket and associated circuit breaker is provided on the rear of the chassis. A power cable is provided according to the customer’s local standard.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RACR00024</td>
<td>POWER CORD AC 3 WIRE 1.8m IEC-320 AMERICAN TYPE 16AWG</td>
</tr>
<tr>
<td>RACR00030</td>
<td>POWER CORD AC 3 WIRE IEC-320 AUSTRALIAN TYPE 16AWG</td>
</tr>
<tr>
<td>RACR00025</td>
<td>POWER CORD AC 3 WIRE IEC-320 EUROPEAN TYPE 16AWG</td>
</tr>
<tr>
<td>RACR00028</td>
<td>POWER CORD AC 3 WIRE IEC-320 CHINESE TYPE 16AWG</td>
</tr>
<tr>
<td>RACR00026</td>
<td>POWER CORD AC 3 WIRE IEC-320 BRITAIN TYPE 16AWG w/13A FUSE</td>
</tr>
<tr>
<td>RACR00029</td>
<td>POWER CORD AC 3 WIRE IEC-320 ARGENTINEAN TYPE 16AWG</td>
</tr>
<tr>
<td>RACR00027</td>
<td>POWER CORD AC 3 WIRE IEC-320 ISRAELI TYPE 16AWG</td>
</tr>
</tbody>
</table>

Note 1: Using an AC power source with UPS is recommended to avoid total power failure if the AC power source fails. For redundant system configurations the UPS is required to assure continuous system functionality, in the event that a component failure occurs.

Note 2: The AC power cable should be connected to power sockets that are protected by a protection device providing a maximum of 16A protection capacity.

2.7.2 Post-Power Connection Test Procedures Checklist

➢ To complete the installation up to this point, verify the next 6 items are correct:

1. Check the electrical connections:
   - For DC power: Verify that the power connections to the DC power inputs on the PEMs have been made according to the desired configuration.
     - For the 6310 system configuration, two DC power inputs for full redundant protection.
   - For DC power: Verify the polarity of the connected cables to the DC inputs.

2. Verify that air is flowing out the air vents of the chassis by feeling the air flow at the vents.

3. Check that there is communication via the console connected to the SA/RTM that is associated to the initial active SC board. Perform this check on both of the SC boards and SA/RTM pairs.
4. Using the Ethernet Switch RS-232 cable, connect to the Ethernet Switch board’s console port and verify that communication is established.

5. Verify that the external Ethernet equipment recognizes the Ethernet activity.

6. Check the LED indicators of the various boards are lit according to the table below.

<table>
<thead>
<tr>
<th>Functional Unit</th>
<th>Indicator</th>
<th>Indicator Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ES/6600 boards</td>
<td>SYSTEM</td>
<td>Yellow</td>
<td>Basic board integrity checks were completed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Green</td>
<td>Awaiting BootP response</td>
</tr>
<tr>
<td></td>
<td>FAULT</td>
<td>OFF</td>
<td>Normally OFF</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>LED is Red if the board fails</td>
</tr>
<tr>
<td></td>
<td>Hot Swap</td>
<td>OFF</td>
<td>Normally OFF</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>LED is Blue during Hot Swap</td>
</tr>
<tr>
<td>SC boards</td>
<td>READY</td>
<td>Green</td>
<td>The board’s power module is operational</td>
</tr>
<tr>
<td></td>
<td>ALARM/USER</td>
<td>Flashing Green</td>
<td>Indicates correct operation of processor</td>
</tr>
<tr>
<td></td>
<td>Hot Swap</td>
<td>OFF</td>
<td>Normally OFF</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>LED is Blue during Hot Swap</td>
</tr>
<tr>
<td>Media Gateway boards</td>
<td>PWR</td>
<td>Green</td>
<td>The board is correctly powered</td>
</tr>
<tr>
<td></td>
<td>ACT</td>
<td>OFF</td>
<td>At initial power the Green ACT LED is OFF for all boards. After software is installed on the SC board, this LED on the boards is lit, except for the redundant, standby board, for which it is OFF.</td>
</tr>
<tr>
<td></td>
<td>Hot Swap</td>
<td>OFF</td>
<td>Normally OFF</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>LED is Blue during Hot Swap</td>
</tr>
<tr>
<td>Fan Tray Module FML-5/Left Fan Tray</td>
<td>-</td>
<td></td>
<td>All LEDs on Refer to Alarm Indicators on page 29</td>
</tr>
<tr>
<td>Fan Tray Module FMR/5K</td>
<td>PWR</td>
<td>Green</td>
<td>Normally ON</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Power input received</td>
</tr>
<tr>
<td></td>
<td>Hot Swap</td>
<td>OFF</td>
<td>Normally OFF</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>LED is Blue during Hot Swap</td>
</tr>
<tr>
<td></td>
<td>HRS</td>
<td></td>
<td>Not implemented in this version</td>
</tr>
<tr>
<td></td>
<td>Push-button</td>
<td>-</td>
<td></td>
</tr>
</tbody>
</table>
### 2.8 Configuring the Basic IP Network Parameters of SC Boards

The IP network parameters of SC boards (IP address, subnet mask and default gateway), which allow basic connectivity between the SC boards and external servers and machines (e.g., EMS server), must be configured prior to connecting the chassis to the external IP network.

**Note:** Failure to do carry out this configuration prior to connecting the Avaya G860 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.

#### 2.8.1 Connecting to the SC Board's RS-232 Console

An RS-232 Console Terminal must be connected to both SC boards for configuring the basic IP network parameters. A regular PC with terminal client software (e.g., HyperTerminal or TeraTerm) may be used as a Console Terminal.

The Console Terminal must be connected to either the SC board's Mini DIN 8 COM serial port or the serial port on the SA/RTM.

The pin assignments for the SC’s Mini DIN 8 Com serial port are detailed in Front Panel Mini DIN 8 COM Serial Port on page 37.

The SA/RTM has a serial port with stacked DB-9 connectors. The RS-232 Console Port 9-pin female D-type connector on the SA/RTM and its pin assignments are

---

<table>
<thead>
<tr>
<th>Functional Unit</th>
<th>Indicator</th>
<th>Indicator Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Fan Power Module FPM/5K</td>
<td>Power</td>
<td>Green</td>
<td>Normally OFF&lt;br&gt;LED is Red if voltage to the fans is improper</td>
</tr>
<tr>
<td></td>
<td>Hot Swap</td>
<td>OFF</td>
<td>Normally OFF&lt;br&gt;LED is Blue during Hot Swap</td>
</tr>
<tr>
<td>Power Supply Module</td>
<td>Power</td>
<td>Green</td>
<td>Indicates ON&lt;br&gt;Power input is within specified limits</td>
</tr>
<tr>
<td></td>
<td>FAULT</td>
<td>OFF</td>
<td>Normally OFF&lt;br&gt;Red LED is ON&lt;br&gt;Power input voltage is not within specified limits, over-temperature or input failure</td>
</tr>
<tr>
<td>Power Entry Module</td>
<td>Power</td>
<td>Green</td>
<td>Normally ON&lt;br&gt;Power input received</td>
</tr>
<tr>
<td></td>
<td>Swap Ready</td>
<td>OFF</td>
<td>Normally OFF&lt;br&gt;LED is Blue during Hot Swap</td>
</tr>
</tbody>
</table>
To connect the console terminal, take these 3 steps:

1. Connect the Console Terminal via the RS232 cable to either the SC’s Mini DIN 8 COM serial port or the serial port on the SA/RTM.
2. If you are using a PC, run the terminal client software (e.g., HyperTerminal).
3. Configure the terminal connection properties as follows:
   - Bits per second: 9600
   - Data bits: 8
   - Parity: none
   - Stop bits: 1
   - Flow control: none

The procedures for configuring the SC board's IP connectivity must be performed on both of the SC boards residing in Slots 1 and 2.

Note 1: All IP addresses and unique names in the following examples are for demonstration purposes only and must be designated by the customer according to his system requirements.

Note 2: Be sure to enter the IP addresses carefully. Errors can prevent the system from connecting to the IP network.

To update the Basic SC Network parameters, take these 10 steps:

1. Connect to the SC board's RS-232 console. For more information, refer to Connecting to the SC Board's Terminal on page 89.
2. Login as root user. For more information, refer to Users on SC Board's Terminal on page 92.
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.pl and press Enter.
5. Choose option 1.
client238:~# /install.pl
Found uncompressed Avaya installation package...
Verify installation package integrity...

-------------------------------------------------
SC Software Installation & Basic Configuration
-------------------------------------------------
1 - Update SC network parameters.
2 - Install and configure.
3 - Change installed configuration.
4 - Copy configuration from Active SC.
5 - Uninstall the software.
0 - Quit.

Choose (0-5) : 1

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

6. At the SC name prompt, enter the unique name you designate for the SC board. Press Enter.
   When configuring the 2nd SC board, make sure to provide a different name from the 1st SC board.

   SC name (node name)                   [clientxx]: SC1

7. Enter the correct IP address for the SC board and press Enter.
   The provisioned address is an "internal IP address" of the SC board that may be used to connecting to it even when the Media Gateway software is not running or not installed.

   IP address                      [10.6.8.33]: 10.7.13.91

8. Enter the correct IP address for the Default router and press Enter.

   Default router                     [10.6.0.1]: 10.7.0.1

9. To start the configuration, type y and press Enter.

   According to IP and mask, network is 10.7.0.0.
   Start configuring (y/n) ?              [n]: y

   >>> Updated /etc/hosts ...
2. Getting Started with the Avaya G860

>>> Updated /etc/nodename ...
>>> Updated /etc/defaultrouter ...
>>> Updated /etc/hostname.dmfe0 ...
>>> Updated /etc/netmasks ...
>>> Updated hostname ...

Done
***********************************************************************

10. The SC board must be rebooted after updating it's Basic IP Network Parameters.
To reboot the SC board, type y and press Enter.

**
** After reboot you MUST choose option 2 (if **
** not installed yet) or option 3 of this script. **
**
***********************************************************************

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

Note: The Media Gateway software does not run automatically after configuring Basic SC Network parameters and rebooting the SC board. To complete the software configuration, perform the "Basic SC Configuration" as described in Changing the basic Configuration of the SC Boards on page 88 for details.

It is mandatory to perform the "Basic SC Configuration" even for insignificant changes to the IP network configuration (e.g., change of the hostname). When such changes to the configuration are needed, run the "Basic SC Configuration" script and at the prompts, accept the existing values provided by the script, except for the modification you are required to make.

2.9 Cabling the Avaya G860

For configurations with TP-6310 + STM-1/OC-3 boards:

- ES/6600 IP Network Cabling - Connecting the ES/6600 IP Network CAT 5 Copper Cabling on page 82
- 6310/RTM/STM1-OC3 PSTN Cabling - TP-6310 Configuration - Connecting the PSTN Interface on page 83

For configurations with TP-6310 + T3 boards:

- ES/6600 IP Network Cabling - Connecting the ES/6600 IP Network CAT 5 Copper Cabling on page 82
- 6310/RTM/T3 Cabling - Connecting the T3 PSTN Interfaces on page 86

For all configurations:

- SA/RTM External Alarm Indicator Connections - External Alarm Indicator Connections on page 86
Caution Laser
Note that the TP-6310 and Ethernet Switch board contains 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.

Care in Handling Fiber Optic Cabling
When handling the fiber optic cables, be sure to implement the following points:

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

Incoming optic cabling from the network infrastructure can originate from the top of the rack or from another chassis within the rack. Preserve the minimum-bending ratio indicated by the cable manufacturer.

To assure full high-availability capabilities, the configuration of the interface to the IP backbone must include certain redundant features from which two separate fiber optic cables are incoming to the Avaya G860 Media Gateway. For more information on, refer to the section below.

2.9.1 Connecting the ES/6600 IP Network CAT 5 Copper Cabling

Note 1: The CAT 5 inputs of the ES/6600 boards are connected to a 1 Gigabit copper interface.

Note 2: When planning the connection, ensure that there is no closed loop in the network.

➢ To connect the CAT 5 copper cables, take this step:

1. Connect to the ports on the ES/6000/RTM according to your OAM, Control and Management IP Separation configuration. (Refer to the table below.)
2. While connecting the CAT 5 Copper cables, be sure to thread them using the customers’ exterior cable management guides.

Connection to the IP network is established.

Table 2-21: IP Separation and ES/6600 Port Allotment

<table>
<thead>
<tr>
<th>IP Interface Separation</th>
<th>Port Allotment</th>
</tr>
</thead>
<tbody>
<tr>
<td>One IP Interface</td>
<td>OAM/Control/Media</td>
</tr>
</tbody>
</table>
### 2. Getting Started with the Avaya G860

#### 2.9.2 Connecting the PSTN Interface - STM-1/OC-3 Configurations

**Note:** OC-3 is typically used where DS1/DS3 is available, and STM-1 is typically used where E1 is available.

#### 2.9.2.1 Connecting Fiber Optic Cables to the SFP Trunk Interfaces

To ensure full 1+1 redundancy protection, the fiber optic cables must be connected to corresponding PSTN connectors in the 6310/RTM/STM1-OC3.

#### 2.9.2.2 Fiber Optic Connections

Avaya provides 155 Mbps Optical SFP modules for OC-3/STM-1 links. To interface with these connectors, the customer provides incoming twin fiber optic cable with Dual-LC plug.

#### 2.9.2.3 SFP Modules

The SFP modules contain a locking mechanism that insures 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 are supplied already inserted into the 6310/RTM/STM1-OC3. If an SFP module is removed from the RTM, be sure to set the SFP module to the Lock position **BEFORE** inserting it into the RTM port.

---

<table>
<thead>
<tr>
<th>IP Interface Separation</th>
<th>Port Allotment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Two IP Interfaces</td>
<td>18</td>
</tr>
<tr>
<td>Three IP Interfaces</td>
<td>18</td>
</tr>
</tbody>
</table>
2.9.2.4 Connecting the PSTN Interface

To connect the PSTN interface, take these 2 steps:

1. On a 6310/RTM/STM1-OC3, connect twin single-mode fiber optic cable with Dual-LC plugs to the PSTN transceivers marked 1A in the PSTN Group.

2. Connect twin fiber optic cable with Dual-LC plugs to the PSTN transceivers marked 1B in the PSTN Group.
2. Getting Started with the Avaya G860

Figure 2-17: Redundancy Connection Scheme for the 6310 RTM

ATM
1+1 Redundancy
1A and 1B
Make a redundant pair

PSTN – STM-1/OC-3
1+1 Redundancy
A and B
Make a redundant pair

Dust covers
cover the unused
receptacles

PSTN – T3
A – TX, RX
B – TX, RX
C – TX, RX
2.9.3 Connecting the T3 PSTN Interfaces

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.

![T3 - Male Connector MOLEX PN: 73100-0255](image)

➢ To connect the PSTN T3 interface, take this step:
   - On each of the 6310/RTM, connect a cable with mini-SMB male connector to each of the T3 mini-SMB female connectors.

2.9.4 External Alarm Indicator Connections

External alarm indicators can be connected to the SA/RTM. Use the green Terminal Block Connector to connect external devices according to the Critical, Major, and Minor severities as indicated. Devices can be controlled using Common, Normally Open or Normally Closed methods. See the diagram of the SA/RTM in SA/RTM Panel on page 41.

The SA/RTM provides two connectors – one is soldered on the SA PCB and the second is a terminal block. The Terminal block contains 3 dry contact relays for connecting to Telco alarm equipment. This connection method is recommended for providing a high availability solution.

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, take these 6 steps:
   1. Check the equipment to be connected.
   2. Open the screws that connect the terminal block to the PCB’s connector.
   3. Unplug the terminal block.
   4. Select one of these two methods to connect the relays of both SA/RTMs 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
5. Make connections according to the appropriate diagram below.

Figure 2-19: Normal Logic Alarm Connection Diagram

Normal Logic Connection

Figure 2-20: Inverse Logic Alarm Connection Diagram
6. Plug-in the terminal block into the PCB connector.

2.10 Changing the Basic Configuration of the SC Boards

The Media Gateway software is typically pre-installed on the SC boards. Therefore, you do not need to install it on a newly received chassis. However, you must perform the Basic Configuration of the SC board to match its configuration settings to your working network environment.

Note: If you are explicitly instructed by Avaya Tech Support to install a new software version on the SC boards, refer to the SC Board Replacement Procedure on page 290.

Two SC boards reside in Slot 1 and Slot 2. Software configuration procedures detailed in the following sections are relevant to both SC boards.

In the initial configuration, for the SC board in Slot 1, the software is configured so that it initially functions as the Active board, while for the SC board in Slot 2, the software is configured so that it initially functions as the Standby or Redundant board.

The SC boards' configuration procedure consists of the following parts:

- Changing the Basic SC Configuration on the 1st SC Board on page 93
- Changing the Basic SC Configuration on the 2nd SC Board on page 98
- Rebooting both boards to complete the configuration change.
2. Getting Started with the Avaya G860

Note 1: All IP addresses and unique names in the following examples are for demonstration purposes only and must be designated by the customer according to customer system requirements.

Note 2: When the Avaya G860 Media Gateway is connected to the IP network with configured VLAN tagging, IP connectivity to the Media Gateway chassis may not be available during the "Basic Configuration" of SC boards. If this occurs, use the RS-232 console to connect to the SC boards.

2.10.1 Connecting to the SC Board's Terminal

The following management interfaces may be used to connect to the SC board's terminal (CLI interface):

- Telnet
- SSH
- RS-232 console

2.10.1.1 Connecting to the SC Board's Terminal via Telnet

This section describes how to connect to the SC board's terminal (CLI interface).

➢ To connect to the SC board's terminal from a Windows-based PC via Telnet, take the following 3 steps:

1. From the Start menu, select Run. The Run dialog box appears.
2. In the Open field, type `telnet <ip>` (<ip> is the IP address of the specific SC board) and press Enter. A Telnet session is opened.

Figure 2-21: Opening the Telnet Session
3. At the prompt, type a username and password.

![Figure 2-22: An Example of a Telnet Session](image)

When IP connectivity is not available, you can use the RS-232 console to establish connection with an SC board. Refer to Connecting to the SC Board's RS-232 Console on page 78 for details.

**Note 1:** If the Media Gateway is configured for Secure Operation mode and you wish to connect to the SC board's terminal (CLI interface), you must connect using SSH. For more information, refer to 'Connecting to the SC Board's Terminal via SSH' below and Secure Operation Mode on page 212.

**Note 2:** The standard Windows XP Telnet client provides a limited support of VT-100 control characters. For a better CLI experience, use one of the following Telnet/SSH clients instead:

- TeraTerm v2.3 - http://hp.vector.co.jp/authors/VA002416/teraterm.html
- PuTTY - http://www.putty.nl (http://www.freeradius.org)

### 2.10.1.2 Connecting to the SC Board's Terminal via SSH

The SSH client software is not available on Windows XP by default. Install one of the following SSH clients to connect to the SC board's terminal via SSH:

- TeraTerm Pro v4.x (see note above)
- PuTTY

➢ **To connect to the SC board’s terminal from a Windows-based PC via SSH using PuTTY, take the following 3 steps:**

1. Start PuTTY. The PuTTY Configuration dialog appears.
2. In the Host Name (or IP Address) field, type the IP address of the specific SC board.
2. Getting Started with the Avaya G860

3. In the Protocol field choose SSH. Click the Open button. An SSH session is opened.

![Figure 2-23: Putty Configuration]

4. At the prompt, type a username and password.

![Figure 2-24: An example of an SSH Session]
2.10.1.3 Connecting to the SC Board's Terminal via RS-232 Console

When IP connectivity is not available, you can use the RS-232 console to establish connection with an SC board. For more information, refer to Connecting to the SC Board's RS-232 Console on page 78.

2.10.2 Users on SC Board's Terminal

There are 3 types of users available on the SC board's terminal:

- **root** – superuser; should be used for re-installation and OS-related maintenance tasks only; the superuser is unique and always available; default password – root.

- **CLI users with administrator privileges** – users that may be used for accessing Media Gateway's CLI with administrative privileges; i.e. may both view Media Gateway status and configuration and modify it (e.g., they may define new applications or stop Media Gateway service); the software installation creates a sample CLI administrator user named cli (default password – cli, which must be modified upon initial login).

- **CLI users with monitor privileges** – users that may be used for accessing Media Gateway CLI; however may only view Media Gateway status and configuration. A CLI user with monitor privileges cannot modify configuration or affect Media Gateway service.

Additional CLI users may be created on the SC board. It is recommended to create a separate CLI user for each operator working with the Media Gateway. For more information, refer to CLI User Administration on page 243.

2.10.2.1 Logging in as a ROOT User

For security reasons, Media Gateway software ver. 2 or later doesn't enable you to directly login as root user over a remote terminal connection (over either a Telnet and SSH connection) to the SC board. Instead, if you need to perform actions with root permissions, you must do one of the following:

2.10.2.1.1 Option 1

Connect via an RS-232 console and login as root user.

2.10.2.1.2 Option 2

Perform the following actions:

1. **Connect via Telnet or SSH and login as a regular CLI user (e.g., user cli).**
   Provide password of the CLI user (e.g., cli_12345).

2. **At the prompt, specify the following command:**
   su – root

3. **Enter the root password when prompted for it (e.g., root) to become root user.**
2. Getting Started with the Avaya G860

2.10.2.2 Logging in as a CLI User

CLI users may log in when connected via any available management interface – Telnet, SSH or RS-232. Provide CLI user name at the prompt (e.g., cli) and later on appropriate password (e.g., cli_12345).

When you login as CLI user for the first time, you will be asked to change the CLI user password. Note that the CLI user password is stored independently on each SC board. Therefore, if you modify the CLI user password on one SC board, repeat the same operation on another SC board (by connecting to its private IP address).

In the following examples, it will be assumed that CLI user password was changed to cli_12345.

2.10.3 Changing the Basic SC Configuration of the 1st SC Board

To change the basic SC configuration of the 1st SC board, take these 15 steps:

1. Connect to the SC board via Telnet, SSH, or RS-232 console. For more information, refer to Connecting to the SC Board's Terminal on page 89.
2. Log in as the root user (default password is root). For more information, refer to Users on SC Board’s Terminal on page 92.
3. At the prompt, type /install.pl and press Enter.
4. Choose option 3.

The text that a user enters is shown in bold and the IP addresses are assumed for the purposes of this example. Note the keyboard shortcuts detailed in the middle of the Example below.

client238:~# /install.pl
Found uncompressed Avaya installation package...
Verify installation package integrity...
SC Software Installation & Basic Configuration

1 - Update SC network parameters.
2 - Install and configure.
3 - Change installed configuration.
4 - Copy 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 the Media Gateway OAM interface with external entities (e.g., the EMS).

   Global SC IP address [0.0.0.0]: 10.7.13.90

6. 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

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

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

8. At the **EMS server** prompt, enter the IP address of the EMS server.

   EMS Server IP Address [0.0.0.0]: 10.7.6.7

9. 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 |

**Note 1:** Time zone names are specified in a standard UNIX tz/zoneinfo format. 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).

Refer to the http://www.timezoneconverter.com for a complete list of supported time zone names, their DST settings and current time in each time zone.

**Note 2:** For major US and European cities, short time zone name (without continent name) is supported as well – e.g. Paris instead of Europe/Paris.

**Note 3:** Complete list of supported time zone names may also be viewed by issuing the following command on the SC board:

```
```

10. At the **Enable Security** prompt, to enable Security, type 1. To disable Security, type 0. For more information refer to Secure Operation Mode on page 212.

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

11. If you have enabled Security, you are prompted to enter the **EMS IKE Pre-Shared Key**. We recommend you type in an IKE Pre-Shared Key consisting of at least 10 characters (no spaces among them).

| EMS IKE Pre-Shared Key | [leave unchanged]: ********** |

**Note:** The Media Gateway with enabled Security must be defined accordingly in the EMS. The same IKE Pre-Shared Key must be entered in the MG Information screen. Refer to Secure Operation Mode on page 212.

12. You are prompted to enter the SC Root Password and the SNMP Read and Write Community strings. To leave a password unchanged, press **Enter**. To change a password, enter the new password. It must be at least 8 characters. Re-enter the new password when prompted.

13. The default password and SNMP community strings are:

- SC Root Password - root
- SNMP Read Community - **public**
- SNMP Write Community - **private**

**Note:** For security reasons, it is recommended to change **root** password and SNMP community strings. Make a note of the new passwords you enter and keep it in a secure location for future reference.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SC Root Password</td>
<td>[leave unchanged]: ******</td>
</tr>
<tr>
<td>SNMP Read Community</td>
<td>[leave unchanged]: ******</td>
</tr>
<tr>
<td>SNMP Write Community</td>
<td>[leave unchanged]: ******</td>
</tr>
</tbody>
</table>

A summary of the settings is displayed.

---

**Configuration Summary:**

---

- **Global SC IP Address:** 10.7.9.245
- **1st SC IP Address:** 10.7.13.104
- **2nd SC IP Address (or 1.1.1.1 if none):** 10.7.13.91
- **EMS Server IP Address:** 10.7.6.21
- **Enable Security:** 0 (no)
- **SC Root Password:** ******
- **SNMP Read Community:** ******
- **SNMP Write Community:** ******

---

14. 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 ...
   >>> Restore file /etc/inet/services from the backup ...
   >>> refresh INET daemon ...
   >>> Update root password ...
   >>> Disable IPSEC configuration ...
   >>> Configure Timer Resolution ...
   >>> Make backup of modified file /etc/system ...

(This sequence is abbreviated)

*************************************************************
2. Getting Started with the Avaya G860

* NOTE: To configure the OAM VLAN, run 'tools vlan' script * 
* on the Active SC (usually the 1st SC) after reboot. * 
******************************************************************

******************************************************************
* IF THE CONFIGURATION IS SUCCESSFUL *
* YOU MUST REBOOT THE SC!!!!!!!!!! *
******************************************************************

Note: If the Avaya G860 Media Gateway is connected to the IP network with 
configured VLAN tagging, IP connectivity does not immediately become 
available after the "Basic Configuration" of the SC board. To make it 
available, after reboot, on the Active SC board, use the tools vlan 
command to configure OAM VLAN configuration. For more information 
refer to Recovering the Basic Interface Separation, VLANs & Link 
Aggregation Default Settings on page 350

15. Complete the configuration of the 2nd SC board before Rebooting the 1st SC Board. Proceed with 'Changing the SC Software Configuration on the 2nd SC Board' below. Although the SC board must be rebooted to complete the configuration, if you are configuring the 1st SC board do not reboot it until you complete the configuration of the 2nd SC board in the procedure below. Reboot both SC boards simultaneously.

Note: DO NOT reboot the 1st SC board until you complete configuration of the 2nd SC board in the procedure below. Reboot both SC boards simultaneously.

IMPORTANT: If the system configuration includes a 2nd SC, 
DONOT REBOOT the 1st SC until the installation 
of the 2nd SC is complete.

Reboot both SCs at the same time.

16. When the configuration of both SC boards is complete, to commence reboot, 
type y and press Enter.

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

The SC board reboots. The software files on the SC board are updated and 
commence operating automatically using the new software configuration.
2.10.4 Changing the Basic SC Configuration on the 2nd SC Board

To change the basic SC configuration on the 2nd SC board, take these 7 steps:

1. Connect to the SC board via Telnet, SSH, or RS-232 console. For more information, refer to Connecting to the SC Board's Terminal on page 89.
2. Login as the root user. For more information, refer to Users on SC Board's Terminal on page 92.
3. At the prompt, type `/install.pl` and press Enter.

Entered text is shown in bold and the IP addresses are assumed for the purposes of this example. Note the keyboard shortcuts detailed in the middle of the Example below.

```
client238:~# /install.pl
Found uncompressed Avaya installation package...
Verify installation package integrity...

SC Software Installation & Basic Configuration

1 - Update SC network parameters.
2 - Install and configure.
3 - Change installed configuration.
4 - Copy configuration from Active SC.
5 - Uninstall the software.
0 - Quit.

Choose (0-5) : 4
```

5. At the CLI user name prompt, enter the name of a CLI user on the 1st SC board (e.g., cli). For more information, refer to 'Users on SC board's Terminal'.

```
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.

Please provide the following credentials:
CLI user name [cli]: cli
```

Note: You can use any CLI user defined on the 1st SC board.
2. Getting Started with the Avaya G860

6. At the CLI user password prompt, enter the password of the specific CLI user on the 1st SC board (e.g., cli_12345).

   CLI user password:

7. At the ROOT password prompt, enter the password of root user on the 1st SC board (e.g., root).

   ROOT user password:

8. Configuration is copied from the 1st SC board and a summary of the settings is displayed.

   Logging into other SC...cli...root...Success!
   Copying Files...Done!

   Configuration Summary:

   Global SC IP Address            : 10.7.9.245
   1st SC IP Address               : 10.7.13.104
   2nd SC IP Address (or 1.1.1.1 if none)  : 10.7.13.91
   EMS Server IP Address           : 10.7.6.21
   Enable Security                 : 0 (no)
   SC Root Password                : ******
   SNMP Read Community             : ******
   SNMP Write Community            : ******

8.5 Configuration Summary:

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

   Start configuring (y/n) [y]: y

   >>> 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 ...
   >>> refresh INET daemon ...
   >>> Update root password ...
   >>> Disable IPSEC configuration ...
   >>> Configure Timer Resolution ...
   >>> Make backup of modified file /etc/system ...

   (This sequence is abbreviated)

   *************************************************
   * IF THE CONFIGURATION IS SUCCESSFUL *
10. Now that the configuration of both the 1st and 2nd SC boards is complete, both SC boards are to be rebooted. To reboot both SC boards, at the Reboot prompt, type y or accept the default.

**IMPORTANT:** If the system configuration includes a 2nd SC, DO NOT REBOOT the 1st SC until the installation of the 2nd SC is complete.

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

The SC boards reboot. The software files on the SC boards are updated and commence operating automatically using the new software configuration.

### 2.11 Testing the Configured System

➢ To verify that the SC software has been properly configured, perform the following tests:

1. Ping the Global IP address of the SC boards from another machine (e.g., PC or EMS).
   
   a. To open the Command Prompt, from the Start menu, select Run> Accessories> Command Prompt. The Command Prompt screen appears.
   
   b. At the command prompt, type ping <Global SC IP Address> and press Enter. A reply should be received.

**Figure 2-25: Pinging the SC Board**
2. Using Telnet or SSH, access each SC board using the internal (not Global) SC IP addresses. Login as any CLI user (e.g., user cli, password cli_12345). For more information, refer to Users on SC Board's Terminal on page 92.

3. At the prompt, type **tools scp** and press **Enter**.

4. Verify that SC software is running.

```
client238:~# tools sc p
```

**LIST OF SC SOFTWARE PROCESSES**

```
27184  tg_syslo  tg_syslog
27181  tg_core   tg_core
27180  tg_bootp  tg_bootp
27179  tg_tpncp  tg_tpncpif
27178  tg_sat    tg_sat
27177  tg_hbg    tg_hbg
27176  tg_hbm    tg_hbm
27154  tg_watch  /Project/bin/exe/tg_watchdog
```

5. In the EMS application, open the Media Gateway Status screen and check the status of the system elements. For more information, refer to the *Element Management System User's Manual, Document #: LTRT-910xx*. 

---

**Note:** If the Ping has not received the proper response, check the physical connections to the network and/or VLAN configuration.
3 Media Gateway Software Backup/Restore Procedures

3.1 Creating the SC Software Backup

A backup of the Media Gateway software should be made at the following times:

- After completing the initial installation and configuration
- After making any change in the Media Gateway configuration
- Before performing a Online Software Upgrade (this is to be sure that an up-to-date backup is indeed available, in the unlikely event of a problem occurring as the result of the software upgrade)
- After completing Online Software Upgrade

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.

Backup Components

The following components of Media Gateway software are to be backed up:

- Software binaries for all Avaya G860 Media Gateway components, including:
  - SC boards' software
  - Media Gateway boards' software (CMP files)
  - ES boards' software
- Configuration database (MOs)
- Configuration files
- Auxiliary Files

Note: The Solaris OS image is not part of the Media Gateway software backup. Therefore you must ensure that correct Solaris OS version is installed on the SC board prior to restoring the backup on it.

➢ To create a backup for the Media Gateway software, take these 7 steps:

1. Connect to the Active SC board via Telnet, SSH or RS232 Console. For more information, refer to Connecting to the SC Board's Terminal on page 89.
2. Login as a CLI user with administrative privileges (e.g., user cli, password cli_12345). For more information, refer to Users on SC Board's Terminal on page 92.

Note: Backup may also be performed from the ROOT account.

3. At the prompt, type `tools bk` and press `Enter`.

```
sc1::~# 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 SC software, including executable files and configuration database.
**********
IMPORTANT: you must run this tool only on ACTIVE SC board!!

Make a backup? ([y]/n) : y
```

4. You are prompted to accept the default backup file name (backup.bk) or type in a new name for the backup file.

In the example below, the file name is `backup_12jun2006.bk`. The backup file is created in the home directory of the active user (e.g., /data/cli directory for cli user) unless you specify a complete file name starting with the symbol, "/" (e.g., /data/shared/12_jun2006.bk).

It is recommended to end the backup file name with the extension ".bk".

5. Press `Enter`. The backup file is created.

```
Backup file name [backup.bk] : backup_12jun2006.bk

---------------------------------------------
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 /backup.bk was successfully created.
```
The backup process may take up to 10 minutes. Wait patiently till it completes.

6. For safekeeping, use \texttt{ftp} or \texttt{scp/sftp} to copy the backup file to a location external to the SC board.

### 3.2 Restoring 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 \textit{both} of the SC boards, and, therefore, the entire system must be non-operational for this process.

\begin{itemize}
  \item \textbf{Note 1}: The Restore procedure must be performed on both of the SC boards.
  \item \textbf{Note 2}: 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. Refer to Configuring the Basic IP Network Parameters of SC Boards on page 78 for details.
  \item \textbf{Note 3}: The Solaris OS image is not part of the Software Backup. Therefore, you must ensure that the correct version of the Solaris OS is installed on both SC boards prior to running the Restore procedure described below. Refer to the Appendix, Installing the Solaris™ 9 OS on page 375 for details.
\end{itemize}

To restore the Media Gateway software from the backup file, take these 8 steps:

1. Connect to \textit{both} SC boards via Console, Telnet or SSH. Use the internal (not Global) SC IP addresses if you connect via Telnet or SSH. For more information, refer to Connecting to the SC Board's Terminal on page 89.

2. Login as the \texttt{root} user. For more information, refer to Users on SC Board's Terminal on page 92.

3. To shutdown \textit{both} of the SC boards, on each SC board, at the prompt, type the command, \texttt{tools sc dn}. You are prompted to confirm this command.

\begin{verbatim}
client238:~:# tools sc dn
STOP SC SOFTWARE
--------------
Stop SC software? ([y]/n) : y

>>> Stop watchdog process...
>>> Wait for application to stop...
\end{verbatim}

\begin{itemize}
  \item \textbf{Note}: Both SC boards must be shut down (via the \texttt{tools sc dn} command) prior to proceeding to the next step.
  \item \textbf{DO NOT} restore the backup on the Standby SC board while the Active SC is still operating, since the restored configuration database is destroyed by the replication mechanism.
\end{itemize}
4. Use **ftp** or **scp/sftp** to copy the **backup** file from its safekeeping location to **both** of the SC boards.

5. On the **1st** SC board (in Slot 1), change current directory to the place where backup file is stored. Type ```./<backup_file_name>``` and press Enter.

```
client238:~# cd /data/cli
client238:~# ./backup_12jun2006.bk
```

**RESTORE**

```
This backup contains the following data:
Product type     : Mediant 5000
Software version : 5.2.11
Created at       : Sun Jan  7 18:20:10 2007
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.

```
Restore? ([y]/n) : y
```

6. Type **y** and press Enter. The restore process begins.

```
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.
```

The restore process may take up to 10 minutes. Wait patiently till it completes.

7. On the second SC board (typically in Slot 2), repeat steps 5 to 6.

8. To reboot **both** of the SC boards, type **reboot**. The restored software is automatically initialized after the reboot has taken place.

### 3.3 Automatic Backups

In addition to user-initiated backups described in Creating the SC Software Backup on page 103 and Restoring Media Gateway Software from Backup on page 105, Media Gateway software periodically performs an Automatic Backup procedure.

Automatic backups are performed on a 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 backup versions are created in the /backup directory on
3. Media Gateway Software Backup/Restore Procedures

the Active SC board. Up to 5 backups are preserved, allowing restore of the Media Gateway configuration to one of the 5 specific past states.

**Note:** Automatic backups are created on Active SC board. There is no replication of backup files between the Active and Standby SC boards. Therefore, when you need to restore Media Gateway from the automatic backup, it is recommended to check the content of /backup directory on both SC boards.

Automatic backups may be used to restore Media Gateway configuration in case of severe malfunction or misconfiguration. The procedure for restoring the automatic backup is identical to the one described above for user-initiated backup. For more information, refer to Restoring Media Gateway Software from Backup on page 105.

➢ **To customize Automatic Backup configuration, take these 4 steps:**

1. Access the **MG Status** screen.
2. Click **Clock**. The Media Gateway Parameters Provisioning screen appears.
3. Select the **Automatic Backup Settings** tab.
4. Configure the Automatic Backup settings according to the table below.

<table>
<thead>
<tr>
<th>Table 3-1: Automatic Backup Parameters</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Automatic Backup</td>
<td>Yes, No</td>
<td>Instant</td>
<td>Enables or disables Automatic Backup functionality. Default: Enabled</td>
</tr>
<tr>
<td>Automatic Backup Day</td>
<td>Enum</td>
<td>Instant</td>
<td>Defines the day of the week when Automatic Backup is performed. Default: Sunday</td>
</tr>
<tr>
<td>Automatic Backup Hour</td>
<td>Integer</td>
<td>Instant</td>
<td>Defines the hour when Automatic Backup is performed. Default: 2 (corresponds to 2:00 AM)</td>
</tr>
<tr>
<td>Automatic Backup Minute</td>
<td>Integer</td>
<td>Instant</td>
<td>Defines the minute when Automatic Backup is performed. Default: 0 (corresponds to 2:00 AM)</td>
</tr>
<tr>
<td>Parameter Name</td>
<td>Type</td>
<td>Provisioning Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------</td>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Automatic Backup History Size</td>
<td>Integer</td>
<td>Online</td>
<td>Defines how many “history” backup files are stored in the /backup directory on the Active SC board. Default: 4</td>
</tr>
</tbody>
</table>
4 Configuring & Operating the Media Gateway

4.1 Overview

The Avaya G860 configuration consists of 2 parts:

- Basic configuration – a minimal number of configuration parameters that must be configured during the initial installation or via CLI. These are typically not altered unless Media Gateway is physically moved from one IP network to another. (Refer to Changing the Basic SC Network Configuration on page 88 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 the Avaya G860 is described in this section.

Management Interfaces

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

- SNMP interface
- CLI interface

Avaya Element Management System (EMS)

The Avaya G860 is typically accompanied by the Avaya Element Management System (EMS) that is used for managing the Media Gateway via an SNMP interface. The EMS is a universal standards-compliant feature-rich solution that provides management capability for the full line of Avaya 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.

For detailed information on using the EMS refer to:

- Element Management System User’s Manual, Document # LTRT 910xx
- EMS Alarm Guide - Document # LTRT 946xx
- EMS Parameter Guide for 5000/8000 - Document # LTRT 942xx
- EMS Release Notes - Document # LTRT-912xx

3rd-Party SNMP Managers

The Avaya G860 may also be managed by a standards-compliant 3rd party SNMP manager. For detailed information on using an SNMP interface, refer to:

- Programmer’s User Manual - Document # LTRT-914xx
CLI Management Interface

In addition, a CLI interface may be used for management, configuration and status monitoring. For detailed information, refer to:

- CLI Reference - Document # LTRT-892xx

4.1.1 Managed Objects, Administrative and Operational State

The operational configuration of the Avaya G860 Media Gateway uses an ITU-T X.730/731 compatible data model.

The operational configuration of Avaya G860 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 Trunk.

An example of an MO that represents logical resources is: Firewall Profile.

The 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.

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.

Lock/Unlock Actions

The Operational State of the MO can not 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, but the Operational State of the MO is disabled. As soon as the Media Gateway returns to service its Operational State is changed to enabled.
4. Configuring & Operating the Media Gateway

4.1.2 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 provisioning type that indicates under what conditions specific attribute may be modified. The following provisioning types are supported:

<table>
<thead>
<tr>
<th>Provisioning Types</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instant</td>
<td>The attribute may be configured at any time. No specific state of the corresponding MO is enforced.</td>
</tr>
<tr>
<td>Online</td>
<td>The corresponding MO must be locked prior to altering the specific attribute.</td>
</tr>
<tr>
<td>Offline</td>
<td>The corresponding MO and its &quot;father&quot; (hierarchical superior) must be locked prior to altering the specific attribute (e.g., an Offline attribute in an MO Trunk requires the corresponding Media Gateway Board to be locked – The Media Gateway Board containing the MO trunk must be locked.)</td>
</tr>
<tr>
<td>Offline_create</td>
<td>The attribute behaves as an Instant attribute after the MO is initially created. However, the attribute turns into an offline attribute as soon as the MO is unlocked.</td>
</tr>
<tr>
<td>Instant_apply</td>
<td>The attribute may be configured at any time, but is updated only when the apply action is performed. The EMS automatically performs an apply action when the user presses the corresponding Apply button in the Provisioning screen – therefore for EMS users, these attributes are identical to the Instant attributes. CLI users must explicitly issue the apply command after altering MO's configuration.</td>
</tr>
</tbody>
</table>

NOTE: The currently instant_apply type is used for SIP-related MOs only.

4.1.3 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 fault alarms issued by the Media Gateway

Fault alarms 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. Alarms are sent as traps to the SNMP managers (e.g., EMS) and recorded in the alarm log file accessible via CLI interface.

Refer to the Appendix, List of Alarms on page 379 for a full list of alarms supported by the Avaya G860 Media Gateway.
4.2 Carrier Grade Alarms

The Carrier Grade Alarms feature enables reliable delivery of the fault alarms to the SNMP manager in case of network outages or SNMP manager failures. It implements Active Alarms and Alarms History table that may be used by the SNMP manager to retrieve updates on missed alarms. EMS fully supports the Carrier Grade Alarms feature. For more information refer to the LTRT-XXXX Programmers Guide.

The Avaya G860's basic alarm system has been extended to a carrier-grade alarm system. A carrier-grade alarm system provides a reliable alarm reporting mechanism that takes into account EMS outages, network outages, and transport mechanism, such as SNMP over UDP.

The Avaya G860's carrier-grade alarm system is characterized by the following:

- **Active Alarm Table** - The SC MIB maintains an active alarm table to allow a manager to determine which alarms are currently active in the Avaya G860 system.

- **Alarm History** - The SC MIB maintains the history of the alarms that have been raised and traps cleared to allow a manager to recover any lost, raised or cleared traps.

This allows the EMS to synchronize its view of the Avaya G860's active alarms.

4.3 Configuring the IP Addresses of Media Gateway Boards and Network Servers

The Avaya G860 Media Gateway is typically shipped to the customer in a state where the Media Gateway MO is **locked** (and therefore all other MOs are **locked** as well). Setting the Avaya G860 to the **locked** state prevents the Media Gateway from automatically using the default IP addresses configured in the factory production environment, before you can configure the IP addresses appropriate for your network environment.

IP addresses of all of the Avaya G860 Media Gateway components, and of all of the network servers with which the Media Gateway works, should be updated prior to unlocking the Avaya G860 Media Gateway for the first time.

➢ To update the IP addresses of the Media Gateway, take these 8 steps:

1. Access the **MG Status** screen.

2. Click **Properties**. The Media Gateway Parameters Provisioning screen appears.

3. In the **Network Services** tab, update the following parameters (if applicable):
   - Main DNS Server IP Address
   - DNS Server 2 IP Address
   - DNS Server 3 IP Address
   - NTP Server
   Refer to the IP Parameters of the Media Gateway Table on page 113 for more details.

4. For each configured Media Gateway board:
4. Configuring & Operating the Media Gateway

Right-click on the desired Media Gateway board and from the popup menus, select **Configuration > Properties**.

5. In the **Network Services** tab, update the following parameters (if applicable):
   - IP Address 1
   - IP Address 2

Refer to IP Parameters of the Media Gateway Board Table on page 114 for more details.

6. Click the **MGCs** button. The MGCs List screen appears.

7. For each configured MGC:
   
   Click the corresponding row and from the popup menus, select **Properties**. The Provisioning screen is displayed.

8. In the **MGC Addressing** tab, update the following parameters (if applicable):
   - Primary Call Agent IP
   - 1st Redundant Agent IP
   - 2nd Redundant Agent IP
   - 3rd Redundant Agent IP
   - 4th Redundant Agent IP
   - 5th Redundant Agent IP
   - 6th Redundant Agent IP
   - 7th Redundant Agent IP

Refer to IP Parameters of the Media Gateway Controller Table on page 114 for more details.

### 4.3.1 IP Parameters of the Media Gateway Table

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Main DNS Server IP Address</td>
<td>IP Address</td>
<td>Instant</td>
<td>The IP address of the main (primary) DNS server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The value 0.0.0.0 means that the DNS server is not available.</td>
</tr>
<tr>
<td>DNS Server 2 IP Address</td>
<td>IP Address</td>
<td>Instant</td>
<td>The IP address of the second (redundant) DNS server.</td>
</tr>
<tr>
<td>DNS Server 3 IP Address</td>
<td>IP Address</td>
<td>Instant</td>
<td>The IP address of the third (redundant) DNS server.</td>
</tr>
</tbody>
</table>
### Parameter Name | Type | Provisioning Type | Description
--- | --- | --- | ---
NTP Server | IP Address | Instant | The IP address of the Network Time Protocol (NTP) server. The NTP server is used for synchronizing the clocks of the computers of the network. When defined, the clock of all the Media Gateway boards are synchronized to the NTP servers’ reference clock.  
- The value 0.0.0.0 means that the EMS server is used as the NTP server.  
- The value 1.1.1.1 means that the NTP server is not available.

### 4.3.2 IP Parameters of the Media Gateway Board Table

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| IP Address 1 | IP Address | Online | The IP address of the 1st CPU module of the Media Gateway board.  
- The TP-6310 Media Gateway boards have 1 CPU module. |
| IP Address 2 | IP Address | Online | The IP address of the 2nd CPU module of the Media Gateway board.  
For TP-6310 Media Gateway boards leave it as 0.0.0.0. |

### 4.4 Working with System Controller Boards

The System Controller (SC) board provides chassis management functionality and a "single management point of contact" to the Media Gateway. All management operations (configuration, fault and status monitoring) are performed through the SC board.

**Redundancy Mode**

There are two SC boards in the chassis. Each board has a local IP address. The two SC boards operate in an asymmetric 1+1 redundant mode. At any time, one of the SC boards is Active and performs chassis management, while the other SC board is Standby. A Global OAM IP address 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 OAM IP address is moved to the new Active SC board during activity switchover.
4. Configuring & Operating the Media Gateway

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.

The status of the SC boards is represented by a standard **Operational State** attribute. The **Administrative State** of the SC board is not supported:

- When the SC board is functioning properly, its **Operational State** is set to **Enabled** and in the EMS, the SC board is colored **green**.
- 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**.

4.4.1 SC Board Actions

The following action can be performed on an SC board:

- **Switchover** – relevant for the Standby SC only. The activity of the SC boards is switched, making the Standby SC the Active one. The initially Active SC is restarted during the **switchover** action and it may take up to 2 minutes before it returns back to service (as a Standby SC).

4.5 Working with the Media Gateway Boards

The Media Gateway boards provide VoIP functionality and manage both signaling and media streams. Each Media Gateway board operates as a standalone Media Gateway. It has its own IP address and manages communication with Media Gateway Controller or SIP agents.

**Redundancy Mode**

The Media Gateway boards operate in an asymmetric N+1 redundant mode. One of the Media Gateway boards 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 in the shortest possible time. As soon as the problem is fixed (replacing the failed board with a functional Media Gateway board) 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 Avaya G860 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). Proper ways to simulate Media Gateway board switchover are:

- Perform switchover via EMS GUI (or CLI)
- Extract Media Gateway board from the chassis.

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-gray**.

The status of the Media Gateway boards is represented by standard **Operational State** and **Administrative State** attributes.

- When the Media Gateway board is functioning properly, its **Operational State** is set to **Enabled** and in the EMS, the board is colored **green**.
- 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**.

4.5.1 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 board is added to the Media Gateway (via **AddBoard** action):

- Hardware Type – defines the type of the Media Gateway board's hardware:
  - TP-6310 OC-3/STM-1
  - TP-6310 T3

- Application Type – defines the type of the software application that runs on the Media Gateway board:
  - Gateway
  - SIP Gateway
  - Media Server
  - SIP Media Server

Note: Avaya uses the G860 as a SIP gateway.
The following combinations of Hardware and Application Types are supported:

### Table 4-4: Hardware and Application Types

<table>
<thead>
<tr>
<th>Hardware Type</th>
<th>Application Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>TP-6310 OC-3/STM-1</td>
<td>Gateway</td>
</tr>
<tr>
<td></td>
<td>SIP Gateway</td>
</tr>
<tr>
<td></td>
<td>Media Server</td>
</tr>
<tr>
<td></td>
<td>SIP Media Server</td>
</tr>
<tr>
<td>TP-6310 T3</td>
<td>Gateway</td>
</tr>
<tr>
<td></td>
<td>SIP Gateway</td>
</tr>
<tr>
<td></td>
<td>Media Server</td>
</tr>
<tr>
<td></td>
<td>SIP Media Server</td>
</tr>
</tbody>
</table>

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 OC-3/STM-1 and T3 boards are supported. However, only boards that match the hardware type of the redundant board are protected by the redundancy mechanism.

### 4.5.2 Media Gateway Board Actions

The following actions can be performed to add/remove Media Gateway board:

- **Add Board** (on the empty slot) – add Media Gateway board. The user is prompted to choose the Hardware Type and Application Type of the Media Gateway board. Make sure to configure the hardware type to match the type of the board that is actually inserted into the slot.

  The General IPM and SIP IPM application types are available for IP Media OC-3/STM-1 or T3 hardware types only.

- **Remove** (on the Media Gateway board) – removes a Media Gateway board. The board must be **locked** prior to performing this action.

### Media Gateway Board Actions

The following actions are available on the Media Gateway boards:

- **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, but 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. The user is prompted to choose a regular board from which the Redundant configuration is copied (refer to Configuring Media Gateway Board Redundancy on page 119 for more details)

- **Switchover** – is available on the Redundant board only. It forces an activity switchover to the Redundant board. The regular board is not automatically reset after a manual *switchover* action. The user must attend to its *lock/unlock* state.

- **Switchback** – available on regular boards after switchover only. It forces activity switchback to the regular board.

### 4.5.3 Redundancy Modes

The Redundant Media Gateway board may provide the following *redundancy modes* for each of the Media Gateway boards in the chassis:

- **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, but active calls are dropped. Service may be interrupted for a few minutes after the switchover.

### Redundancy Mode Availability

Redundancy mode availability for specific Media Gateway board depends on the following factors:

- Configuration of the specific Media Gateway board
- Configuration of the Redundant board (and Redundancy Group)

Configuration of the Media Gateway board consists of a number of configuration parameters. Each parameter has a Redundancy Type that determines whether or not it affects redundancy mode. The following Redundancy Types are available:

- **Hot** – parameter does not affect the redundancy mode availability; even when its value differs between normal and redundant boards, Hot Redundancy mode is available; most of the configuration parameters belong to this type;

- **Warm** – parameter affects redundancy mode availability; when its value in configuration of normal and redundant board matches, Hot redundancy mode is available; otherwise Warm redundancy mode is forced;

Redundancy mode availability is determined by comparing configuration of normal and redundant Media Gateway boards:

- Verifying whether respective parameter values for each board are different
- Verifying the Redundancy Type of the respective parameters of each board
At any time, the Redundant board may provide Hot Redundancy for some Media Gateway boards and Warm Redundancy for other Media Gateway boards. A summary screen is available in the EMS that summarizes the current redundancy mode for all Media Gateway boards.

To view the redundancy mode for all Media Gateway boards, take these 3 steps:

1. Access the **MG Status** screen.
2. Click **Redundancy**. The Redundancy Group Provisioning screen is displayed.
3. To view the list of all Media Gateway boards and their redundancy mode settings, click the **Redundancy TP List** tab.

The following columns are displayed:

- **Protection Required**
  
  The "Best possible" redundancy mode according to the current configuration. The redundancy mode may be downgraded to "warm" because of the mismatch in the configuration of specific parameters of the regular and the Redundant Media Gateway boards. If this occurs, the Weak HA Params column contains the detailed description of the problem. This field is updated even when Media Gateway board is not enabled or the Redundant board is not available and represents the configuration status only.

- **Redundant Mode**
  
  The actual redundancy mode of the specific Media Gateway board. It may be less than the "best possible" mode due to any of the following reasons:
  
  - The Media Gateway board is out of service
  - The Redundant board is out of service
  - The Redundant board is currently replacing a Media Gateway board (switchover occurred) and, therefore, can not provide redundancy for an additional Media Gateway board

Media Gateway Redundancy configuration consists of 2 major parts:

- Configuring the Redundancy Group
- Configuring the Redundant Media Gateway Board

To configure Redundancy Group, take these 3 steps:

1. Access the **MG Status** screen.
2. Click **Redundancy**. The Redundancy Group Provisioning screen is displayed.
3. Configure redundancy group parameters according to the table, Redundancy Group Parameters Table on page 120.
### Table 4-5: Redundancy Group Parameters

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failed Board Automatic Switchover</td>
<td>Enum</td>
<td>Online</td>
<td>Enables or enables automatic switchover upon failure of the specific Media Gateway board. When set to <em>disabled</em>, the redundancy mechanism of the Media Gateway boards is disabled.</td>
</tr>
<tr>
<td>Failed Board Automatic Restart</td>
<td>Enum</td>
<td>Online</td>
<td>Enables or enables automatic restart of a failed Media Gateway board when switchover is impossible (the Redundant Board is not ready, or is currently backing up some other board). When set to <em>disabled</em>, the failed board remains <em>disabled</em> until the user manually locks/unlocks it.</td>
</tr>
<tr>
<td>Force Warm Redundancy</td>
<td>Enum</td>
<td>Online</td>
<td>Forces <em>warm</em> redundancy mode on all of the Media Gateway boards, including those boards that have a configuration that allows <em>hot redundancy</em> mode. This option is to be used for rare scenarios where <em>hot</em> redundancy is inapplicable or does not work properly.</td>
</tr>
</tbody>
</table>

➢ **To configure a Redundant Media Gateway board, take these 5 steps:**

1. Access the [MG Status] screen.
2. Add a new Media Gateway board (if it does not already exist). Refer to Adding Media Gateway Boards to an Avaya G860 System on page 307 for detailed instructions.
3. Select a Media Gateway board to be configured as the Redundant board.
4. Right-click on the selected Media Gateway board and, from the popup menu, select Maintenance> Make Board Redundant. The Board Redundancy dialog box appears.
5. From the Select Board dropdown list, select the regular board from which the configuration is to be copied.

The configuration of the Redundant Media Gateway board is copied from the regular board specified as part of the Make Board Redundant action. The redundancy mode of the board from which the configuration is copied is *hot*.

If another Media Gateway board has a different configuration that is not supported by the redundancy mechanism (the parameters that differ have Warm redundancy type), its redundancy mode is *warm*.

A similar phenomenon may occur if the configuration of the board (from which the Redundant configuration is copied) is altered. You can repeat the Make Board Redundant action at any time (even when the board is already configured as redundant) to copy the configuration from a specific Media Gateway board and make its redundancy mode *hot*. Alternatively, you can alter the configuration of the Redundant board via the same Provisioning Screens that are used for configuring a regular Media Gateway board.
4. Configuring & Operating the Media Gateway

4.5.4 Updating License Key

The License Key defines a list of features and applications available on the Media Gateway board (e.g., 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 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.

To upgrade the License Key, customers receive a License Key file that contains licenses for one or more Media Gateway boards from the Avaya Tech Support. You must apply these licenses to Media Gateway boards via the Update License Key action. To apply the updated license key, the Media Gateway board must be restarted (locked/unlocked).

➤ To update License Key of specific Media Gateway board, take these 6 steps:

1. Upload the License Key file to the EMS Software Manager:
   a. From the Tools menu, select Software Manager. The Software Manager screen appears.
   b. In the upper left corner, click . The add Files screen appears.
   c. In Auxiliary tab, click and navigate to the desired License Key file.
   d. Click OK. The file name appears 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. Access the screen.

3. Right-click on 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 / Unlock 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 all of the Media Gateway boards in the chassis require updating, you can use the Gateway-level License Keys Update action instead:

   Click the Maintenance Action button located at the top-right of the screen and from the popup menu, select License Keys Update.

4.6 Working with the Ethernet Switch Boards

The Ethernet Switch (ES) board provides IP network connectivity for all of the boards inside the Avaya G860 chassis (i.e., the SC and Media Gateway boards.)
**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.

**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 3 is initially the Active ES board (upon chassis power up) and the ES board in slot 4 is initially the Standby ES board.

The status of the ES boards is represented by a standard **Operational State** and **Administrative State**, as well as **Severity** attributes. The **Severity** attributes are updated as follows:

- When the ES board is functioning properly and all of its configured uplinks are connected, the status attributes are set to **Clear** and in the EMS, the ES board is colored **green**.
- When the ES board is functioning properly, but one of its configured uplinks is disconnected, the **Severity** attribute is set to **Warning** and in the EMS, the ES board is colored **blue**.
- When the ES board is functioning properly, but the internal link (F-Link) is disconnected, the **Severity** attribute is set to **Major** and in the EMS, the ES board is colored **orange**.

**Note:** The internal link is temporarily disconnected when one of the ES boards is rebooted or removed from the chassis.

- When ES board is functioning properly, but it behaves suspiciously (e.g., for any reason, some of the other boards in the chassis can not communicate with it) the **Severity** attribute is set to **Minor** and in the EMS, the ES board is colored **yellow**.

**Note:** **Minor** severity is not cleared automatically. You must make a **Clear Severity** action instead.

- When ES board is not functioning properly, 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**.
4.6.1 ES Board Actions

The following actions can be performed on an ES board:

- **Lock** – stops service on the ES board. The locked board can not be used for providing network connectivity to the chassis, therefore if both ES boards are locked simultaneously, the Media Gateway boards loose 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 is 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 to use 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., for any reason, some of the other boards in the chassis can not communicate with it.)

4.7 Configuring NTP Server

An NTP server is used to synchronize the time of all of the computers across the IP network. The Avaya G860 requires an NTP server for a normal operation because it lacks a hardware clock that survives a chassis power down/up cycle.

For simple configurations, the EMS server can be used as the NTP server. However, it does not have redundant protection and its internal clock accuracy is low.

**Synchronization**

The Media Gateway synchronizes with NTP server periodically (every 15 minutes) and updates the NTP Server Status attribute accordingly. When three consequent synchronization attempts against NTP server fail, the NTP Server Status is changed to “NTP Connection Lost”. When a synchronization attempt succeeds, the NTP Server Status is changed to “NTP Connection Restored”.

According to this synchronization behavior, the Media Gateway “reacts” to the change in the NTP server presence as follows (the 5 min internal polling interval is taken into account in the following numbers):

- When the NTP server is disconnected, the NTP Server Status is updated to “NTP Connection Lost” within 50 minutes.
- When the NTP server is re-connected, the NTP Server Status is updated to “NTP Connection Restored” within 20 minutes.

➢ To configure NTP server, take these 3 steps:

1. Access the MG Status screen.

2. Click Properties. The Media Gateway Parameters Provisioning screen appears.
3. In the Network Services tab, update the parameters according to the table below.

**Table 4-6: NTP Server Configuration and Status**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| NTP Server IP Address | IP Address   | Instant           | Defines the IP address of the Network Time Protocol (NTP) server. NTP server is used to synchronize the time of all computers across the IP network. Media Gateway requires NTP server for a normal operation, because it lacks hardware clock that survives chassis power down/up cycle. The following "special values" are supported:  
  - 0.0.0.0 = use EMS server as the NTP server  
  - 1.1.1.1 = no NTP server is available |
| NTP Server Status Enum Read-Only | Indicates the status of the connectivity between Media Gateway and the NTP server. The following values are supported:  
  - NTPConnectionLost – there is no connection between Media Gateway and NTP server  
  - NTPConnectionRestored – connection between Media Gateway and NTP server is restored |

4.8 Connecting the Media Gateway to the IP Network

To ensure full high availability capabilities, one of the methods illustrated below may be incorporated into the IP Network Infrastructure. (fix structure with "Network" topic below).

4.8.1 Networks

The OAM VLAN and subnet is common for the entire Avaya G860 Media Gateway. Contrarily, more than one VLAN and subnets is allowed for the Media and Control.

The entity Network includes the Media and Control, subnets, VLAN and QoS. Networks are added dynamically and, in the current version, the number of networks is limited to two.

When a Network is provisioned, each Media Gateway board must be attached to one of the Networks.
4. Configuring & Operating the Media Gateway

Note: In the current version, the Control is part of the network. However, its VLAN, subnet and QoS can not differ between the networks. In future versions, this limitation is intended to be removed.

4.8.2 Example 1: Without Physical Separation

In a configuration with the cluster of two interconnected L-3 switches, the Avaya G860 uplink is connected directly to L-3 switches.

Figure 4-1: Clustering of Two L-3 Switches

- The Media Gateway is connected to the IP backbone via '1+1' Ethernet Switches (ES).
- The two sets of aggregated uplinks of the Media Gateway should be connected to two different L2 networks.
- The L2 networks should have the same default Gateway (IP). Two L3 switches are clustered and recognize the same global IP.
- The L3 switches must be interconnected in layer 2 in order to allow connection between MGW boards and the SCs in the case that each is connected to a
different Ethernet switch.

- Normally, all the boards are aligned (by the SC SW) to the same ES; however, if due to a port failure, one of the boards (TP or SC) switches to the other ES, the connection with it is run through the external L3 switches.

- The two Ethernet switch boards must not be interconnected externally, as this, combined with the intercommunication between the L-3 switches (VRRP / HSRP) causes a closed loop in the network.

- The MGW Ethernet Switch boards are not running Spanning Tree Protocol, in order to allow fast ES switch over; however, the Media Gateway does not introduce loops in the L2 network due to the internal link.

- The L3 switches are clustered using VRRP / HSRP protocol. Since this connection is not High Availability, it is recommended to add an extra link to the aggregation.

- In a case of disconnection between the primary L3 switch and the WAN, all the MGW traffic (including the RTP) is routed to the secondary L3 switch via the VRRP / HSRP connection.

- The internal VLAN is used for connecting between the System controllers (Hart beats and replication) and the active System controller and the ESs for management.

- Both ESs are jumpered to use port 24 via internal BUS (F-link), and it is being used for the internal VLAN.

Note: For ES/6600, the interconnection between the Avaya G860 and external equipment can be aggregated for media traffic to achieve a maximum 3 Gigabit Ethernet bandwidth.

4.8.3 Example 2: With Physical Separation

In a configuration with physical separation, the Avaya G860 connects up to three networks. The duplicate ES connections provide High-Availability.

Note: For multiple networks, apply these methods to each of the networks in the network configuration.
4. Configuring & Operating the Media Gateway

4.9 Configuring the Media Gateway for IP Connectivity

IP Network Connectivity must be configured in the following categories:

- VLANs
- Interface Separation
- Link Aggregation (If applicable)
- DiffServ Priorities

Note 1: For ES/6600, the HA OAM Network and HA Control Network are GbE copper links and the HA Media Network is up to 3 GbE copper aggregated links.
4.9.1 Working with VRRP/HSRP Protocols

This section describes recommended and required actions when proprietary L3 switches use HSRP/VRRP protocols for failover capabilities.

4.9.1.1 In the User Environment

When proprietary L3 switches are clustered using the HSRP/VRRP protocols for failover capabilities, the following actions are recommended:

- The HSRP/VRRP routing between the proprietary L3 switches should be configured per VLANs and not per port.
- The proprietary L3 switches priorities should be configured with the outside network ports (to the WAN) and not with the Media Gateway. Setting this priority should result in all the VLANs switching to the redundant L3 switch in the event of a failover. When this priority is set and both proprietary L3 switches are up, the L3 switch with the higher priority becomes the active switch.

4.9.1.2 On the Media Gateway

1. Access the MG Status screen.
2. Click Properties. The Media Gateway Parameters Provisioning screen appears.
3. Choose a specific Gateway board (by clicking on it).
4. Click tab 'General Settings'.
5. In the ARP Table parameters pane, do the following:
   - Set parameter Media ARP Cache override to EnableGARP.
     where EnableGARP-the decision to change the Destination MAC address on the fly is based only on the Gratuitous ARP packets that are broadcast from the Media Gateway.
6. Click Apply.

Note: This setting ensures that the Media Gateway always sends data to the proprietary L3 switches using a global MAC address.

4.9.2 Working with VLANs

A VLAN is a logical grouping of nodes that reside in a common broadcast domain of the network, without any router hops. All the VLAN members can also be viewed as a group of devices on different physical LAN segments which can communicate with each other as if they were all on the same physical LAN segment. VLANs provide a number of benefits over the Typical Routed Network.

- VLANs control broadcast traffic. If a device in a particular VLAN transmits a broadcast frame, only devices in that VLAN receive the frame.
VLANs provide extra security. Devices in a VLAN can only communicate with devices on the same VLAN.

VLANs facilitates moves, additions, and changes for devices on networks. If a device in a VLAN is moved to a port in another part of the network, you can configure the new port to be in the VLAN of the moved device.

If the end node device is VLAN aware, the port automatically forwards the packets to the proper location. No reconfiguration is required.

When working within VLAN, each Ethernet frame in the VLAN is marked with VLAN ID (tag). The VLAN ID may be carried in the same frame itself when the frame has been tagged by the source station (or tagging switch), or the VLAN ID may be set to a default value assigned to the receiving port. Every switch port must be attached to at least one VLAN.

All frames that enter the switch are identified as to their VLAN membership. Once the frame is identified as belonging to a particular VLAN, it may only be forwarded to other ports that are members of that VLAN. VLAN membership is determined by a VLAN Identifier (VID). The VID may be carried in the frame itself when the frame has been tagged by the source station (or a tagging switch), or the VID may be set to a default value assigned to the receiving port. The default VID assigned to a frame by the receiving port, when the frame is not already tagged, is called the Port VID or PVID. This parameter is set by management action.

Once a frame has been identified as belonging to a VLAN, it can be transmitted only to those ports that are members of that VLAN.

### 4.9.2.1 VLAN Tagging

When no VLAN is defined, all the sent frames are not tagged. The frame structure does not include 802.1q and 802.1p fields. All untagged frames are received into the gateway, while all tagged frames are rejected.

When working with VLAN enabled, the Avaya G860 supports up to 4 different VLANs for the OAM, Control, and up to two for Media traffic. The user can independently enable/disable each VLAN and assign each of them with its VLAN ID (tag) or to operate in the untagged way.

Every packet that enters and leaves the switch must be attached to a VLAN. Every switch port must be attached to at least one VLAN. Therefore, at least one VLAN must be defined.

In "regular mode", with no VLANs defined for the switch, all in/out packets are attached to a default VLAN. Any packets with a tag are discarded. For each switch port, a default VLAN should be configured to which all untagged packets are attached.

The following rules should be applied when working with VLANs enabled:

- No more then one untagged VLAN on the same interface
- The number of interfaces <= the number of VLANs
- If number of interfaces equals the number of VLANs, all tagged / untagged permutations are valid
- The OAM VLAN ID must be different from the Media VLAN ID
- The same VLAN ID can not be used in more than one interface

For more information, see Interfaces, Subnets, VLANs & Tags on page 145
4.9.3 Link Aggregation in the Avaya G860

Link Aggregation allows up to three physical ports to be aggregated together forming a Link Aggregation Group, such that a MAC Client can treat the Link Aggregation Group as if it were a single link. Link Aggregation implementation fully conforms to the IEEE 802.3ad specification.

4.9.3.1 Benefits

By taking multiple LAN connections and treating them as a single, aggregated link, we can achieve several benefits:

- Increased link capacity. The total capacity of the aggregated link 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 links requiring high availability, this feature may be more important than the link capacity increase. The loss of link within the aggregation reduces the available capacity but does not disrupt the communication entirely.

4.9.3.2 Distribution Rules

The Avaya G860 Ethernet Switch allows for distributing the Ethernet traffic among the aggregated links based on the Source and Destination MAC address and the Source and Destination IP address.

Following are the six distribution rules:

1. **SrcMAC** - indicates that packets are distributed based on the last three bits of the Source MAC address.
   
   This rule is not recommended, since the user can't control the TP MAC addresses (half odd, half even)

2. **DestMAC** - indicates that the packets are distributed based on the last three bits of the Destination MAC address.
   
   This rule is not recommended, since usually the next network element (hop) is a router which is represented by a single MAC address. In such case, all traffic will be routed via one link only.

3. **SrcXORDestMAC** - indicates that the packets are distributed based on the last three bits of the XOR of the Source and Destination MAC address.

4. **SrcIP** - indicates that the packets are distributed based on the last three bits of the Source IP address.
   
   This is the recommended distribution policy; allocating the TP IP address sequentially.
   
   When using the **SrcIP** distribution policy and allocating the TP IP address sequentially, TPs with Odd IP addresses will be routed to one link and TPs with even IP addresses will be routed to another link.

**Note:** When the system distribution rule is configured by this recommended scheme, the next hop network element the L-3 switches should use the opposite distribution rule **DstIP**.
5. **DestIP** - indicates that the packets are distributed based on the last three bits of the Destination IP address.
   
   It is recommended only where the number of end points are large and IP addresses are statically allocated and there is an equal distribution between aggregated links.

6. **SrcXORDestIP** - indicates that the packets are distributed based on the last three bits of the XOR of the Source and Destination IP address.
   
   This mode is not recommended, due to difficulty to control.

Multiple packet items may be included as part of the packet distribution criteria. All packet items listed are included as part of the distribution criteria. The selected items are hashed to a port number within the aggregation. The hashing algorithm is proprietary and not configurable. Distribution rules are assigned to Trunk Groups rather than to ports or aggregators. When a group of aggregation ports select their aggregator, this aggregator becomes associated with a Trunk Group. The distribution rule assigned to the aggregator then becomes the Trunk Group’s distribution rule.

The default rule assigned to Ethernet Switch ports is SrcMAC.

It is recommended to allocate the Media Gateway boards’ IP addresses successively in order to assure an optimal distribution.

**LACPDU Transmission Interval (“timeout”)**

Link Aggregation Control Protocol (LACP) provides a standardized means for 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 that 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 Partner’s LACP_Timeout value.

The Avaya G860 ES LACP_Timeout default value is set to a Long Timeout (30 sec.) and configurable.

For more information, see Link Aggregation Options on page 139, Aggregation Switch-Over Logic on page 131 and Aggregation Distribution Rules on page 132.

**4.9.3.3 Aggregation Switch-Over Logic**

When a system is configured with 3 links aggregation, the following conditions determine when the MGW activates a switchover:

- Switch over from an ES where one or more links on an ES has the status **D**.
- Switch over to an ES with all the provisioned links with status **U**.

**Legend:**

- **A, B and C** – aggregated links
- **U** – Up port
- **D** – shut-Down port
4.9.3.4 Aggregation Link Distribution Policy-Example

Given the following data:

- The relevant data for the IP distribution decision are the three least significant bits of the MAC / IP address.
- 4 TPs
- Two aggregated links
- Distribution rule – source IP address (SrcIP).

The following data can be observed:

Table 4-7: Aggregated Links and Least Significant Bits

<table>
<thead>
<tr>
<th>3 – Least Significant Bits (LSB)</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>000</td>
<td>link-1</td>
</tr>
<tr>
<td>001</td>
<td>link-2</td>
</tr>
<tr>
<td>010</td>
<td>link-1</td>
</tr>
<tr>
<td>011</td>
<td>link-2</td>
</tr>
<tr>
<td>100</td>
<td>link-1</td>
</tr>
<tr>
<td>101</td>
<td>link-2</td>
</tr>
<tr>
<td>110</td>
<td>link-1</td>
</tr>
<tr>
<td>111</td>
<td>link-2</td>
</tr>
</tbody>
</table>

The following table describes the recommended aggregation distribution policy; two TPs per link, two even TPs on the 1st Link and two odd TPs on the 2nd link.

Table 4-8: Aggregation Distribution Policy-Recommended

<table>
<thead>
<tr>
<th>IP Addresses</th>
<th>3 Least Significant Bits</th>
<th>link</th>
</tr>
</thead>
<tbody>
<tr>
<td>TP1 – 192.168.10.8</td>
<td>000</td>
<td>1st link</td>
</tr>
<tr>
<td>TP2 – 192.168.10.1</td>
<td>001</td>
<td>2nd link</td>
</tr>
<tr>
<td>TP3 – 192.168.10.2</td>
<td>010</td>
<td>1st link</td>
</tr>
<tr>
<td>TP4 – 192.168.10.3</td>
<td>011</td>
<td>2nd link</td>
</tr>
</tbody>
</table>

The following table describes an aggregation distribution policy that is not recommended; all TPs on a single link.
### 4. Configuring & Operating the Media Gateway

#### 4.9.4 Interface Separation

The Avaya G860 framework allows the definition of a number of interfaces for connection to external equipment. Separate interfaces can be defined for each of the networks (OAM, Media and Control). This capability can be integrated with the definition of VLANs. For defining these separate interfaces, the following combinations can be configured:

- **One Interface four options:**
  - One VLAN for OAM, Control and Media*  
  - Two VLANs: One VLAN for Control and Media*, one VLAN for OAM  
  - Two VLANs: One VLAN for OAM and Control, one VLAN for Media*  
  - Three VLANs: One VLAN for OAM, one VLAN for Control, one VLAN for Media*

- **Two Interfaces four options:**
  - Option 1 (two VLANs):
    - Control + Media Interface with Control + Media* VLAN  
    - OAM Interface with OAM VLAN  
  - Option 2 (two VLANs):
    - OAM + Control Interface with OAM + Control VLAN  
    - Media Interface with Media* VLAN  
  - Option 3 (three VLANs):
    - OAM + Control Interface with OAM VLAN + Control VLAN  
    - Media Interface with Media* VLAN  
  - Option 4 (three VLANs):
    - OAM Interface with OAM VLAN  
    - Control + Media Interface with Control + Media* VLAN

- **Three Interfaces one option:**
  - OAM Interface with OAM VLAN  
  - Control Interface with Control VLAN  
  - Media Interface with Media* VLAN  

Media* - up to two Media VLANs

---

### Table 4-9: Aggregation Distribution Policy-Not Recommended IPs

<table>
<thead>
<tr>
<th>IP Addresses</th>
<th>3 Least Significant Bits</th>
<th>link</th>
</tr>
</thead>
<tbody>
<tr>
<td>TP1 – 192.168.10.1</td>
<td>001</td>
<td>2nd link</td>
</tr>
<tr>
<td>TP2 – 192.168.10.3</td>
<td>011</td>
<td>2nd link</td>
</tr>
<tr>
<td>TP3 – 192.168.10.5</td>
<td>101</td>
<td>2nd link</td>
</tr>
<tr>
<td>TP4 – 192.168.10.7</td>
<td>111</td>
<td>2nd link</td>
</tr>
</tbody>
</table>
4.9.5 Setting up the Physical Interfaces, VLANs & Subnet Separation

This section provides a general description for the various configuration options for setting up the Physical Interfaces, VLANs and Subnet Separation. For specific configuration options, see Use Cases for IP Network Connectivity Configuration on page 148.

**Note 1:** The options selected must match the interface setup of the counterpart Network components to which the Avaya G860 is connected.

**Note 2:** This operation must be performed on a locked Avaya G860 system. For more details, refer to the *Element Management System User's Manual, Document #: LTRT-910xx*.

➢ To set the Physical Interface, VLANs and Subnet Separation options, take these 4 steps:

1. Access the **MG Status** screen.
2. Click **Properties**. The Media Gateway Parameters Provisioning screen appears.
3. In the **Subnet & VLAN Settings, Interfaces Settings**, and **Static Route Table** tabs, set the options listed below.
4. Refer to the tables provided at the end of each section, which contain relevant parameters and their descriptions.

### 4.9.5.1 Subnet & VLAN Settings

**General Options**

- **Enable Separation Configuration**
  - For a system with no VLANs & Interface separation, retain the default **disable** option.
  - For a system with VLANs and or with Interface separation, select the **enable** option.

**OAM VLAN Options**

- **OAM Enable Tagging**
  - For OAM without VLAN tagging, retain the default **disable** option.
  - For OAM with VLAN tagging, select the **enable** option, and assign the OAM tag ID.

- **OAM tag ID**
  - Assign the **OAM** tag ID

- **OAM QoS Setting**
The following Service Class Priority groups are related to the OAM:

- For **Network Service Class Priority**:
  - For a system with no VLANs – irrelevant
  - For a system with VLANs – set a priority level.

- For **Gold Service Class Priority**:
  - For a system with no VLANs – irrelevant
  - For a system with VLANs – set a priority level.

- For **Bronze Service Class Priority**:
  - For a system with no VLANs – irrelevant
  - For a system with VLANs – set a priority level.

- For **Network DiffServ Priority**:
  - Set DiffServ Priority.

- For **Gold DiffServ Priority**:
  - Set DiffServ Priority.

- For **Bronze DiffServ Priority**:
  - Set DiffServ Priority.

**Control & Media VLAN lists - Relevant only for systems with VLANs**

The network VLAN tags for Media and Control must be chosen from these lists. Assign each of the VLAN tag ID (OAM, Control, Media1 and Media 2) the appropriate unique number.

- For **Media VLAN list first tag ID**:
  - Set the tag of the first Media VLAN

- For **Media VLAN list second tag ID**:
  - Set the tag of the second Media VLAN

- For **Control VLAN list first tag ID**:
  - Set the tag of the first Control VLAN

**Note:** The value range for each must be from 0, 2 to 3999 (The default is 0 = untagged).

Values 4000 to 4096 are for internal use only.
### Table 4-10: Interfaces and VLAN 802.1 p/q Tab Parameters

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| Interfaces              | Enum oneOCM, twoOCandM, twoOandCM, threeOandCandM | Online            | - System communications can be separated into up to three different VLANs:  
  - OAM  
  - Control  
  - Media  
  This parameter depends on the parameter tgMGInfoEnableVLANConfiguration, which if disables makes this parameter N/A. |
| Media Aggregation Enable| Enum disable, aggregate2, aggregate3 | Online            | Media communication physical interface aggregation. Up to three 1GB.  
**The options below follow Avaya recommendations.**  
- For a system with four 6310 boards or less, retain the default disable option. (One Link via ES port 20)  
- For a system with five to six 6310 boards, select the aggregate2 option. (Two Links via ES port 20 and 21)  
- For a system with seven to eight 6310 boards, select the aggregate3 option. (Three Links via ES port 20, 21 and 22) |
| Link Aggregation Timeout| Enum short, long      | Online            | Indicates the Link Aggregation Timeout. The periodic transmission of the ES LACP_Timeout may occur at a Long timeout (30 sec. - the default value) or Short timeout (1 sec.), which is determined by the Partner's LACP_Timeout value. |
### 4. Configuring & Operating the Media Gateway

#### Parameter Name

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Link Aggregation Distribution Rule</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enum srcMac, destMac, srcXorDestMac, srcIp, destIp, srcXorDestIp</td>
<td>Online</td>
<td>1. Defines the frame / packet distribution rule assigned to the group of aggregated external Ethernet links.</td>
<td></td>
</tr>
<tr>
<td>2. The six distribution rules are:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. SrcMAC - indicates that packets are distributed based on the last three bits of the Source MAC address.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. DestMAC - indicates that the packets are distributed based on the last three bits of the Destination MAC address.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. SrcXORDestMAC - indicates that the packets are distributed based on the last three bits of the XOR of the Source and Destination MAC address.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. SrcIP - (Default) indicates that the packets are distributed based on the last three bits of the Source IP address.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. DestIP - indicates that the packets are distributed based on the last three bits of the Destination IP address.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. SrcXORDestIP - indicates that the packets are distributed based on the last three bits of the XOR of the Source and Destination IP address. The last three bits of the Source IP Address are logically XORed with the last three bits of the Destination IP Address and used to index into the Trunk Group to get the destination port. This rule defines the distribution algorithm applied to the aggregated link. If no ‘rtag’ is provided, the current value for the specified ports is displayed.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Enable Separation Configuration | Enum disable, enable | Online | Enables separation of system communications into different VLANs and Interfaces.  |
| Network Service Class Priority | Integer 0-7 | Online | Layer two Class Of Service (according to 802.1p) represented by three bits. The network service class is applied to the DNS, DHCP, ICMP, etc.  |
| The range is 7 (highest) to 0 (lowest).  |
| The default value is 7.  |

Gold Service Class Priority | Integer 0-7 | Online | Layer two Class Of Service (according to 802.1p) represented by three bits. Gold service class is applied to voice streaming  |
<p>| The range is 7 (highest) to 0 (lowest).  |
| The default value is 4.  |</p>
<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bronze Service Class Priority</td>
<td>Integer</td>
<td>Online</td>
<td>Layer two Class Of Service (according to 802.1p) represented by three bits. Bronze service class is applied to management traffic. The range is 7 (highest) to 0 (lowest). The default value is 2.</td>
</tr>
<tr>
<td>OAM VLAN parameters</td>
<td></td>
<td></td>
<td>The VLAN parameters are enabled when the enable separation configuration is enabled.</td>
</tr>
<tr>
<td>OAM Enable Tagging</td>
<td>Enum</td>
<td>Online</td>
<td>Enables OAM communication VLAN tagging (according to 802.1.q)</td>
</tr>
<tr>
<td>OAM Tag ID</td>
<td>Integer</td>
<td>Online</td>
<td>OAM communication VLAN tag ID (according to 802.1.q). Valid only if parameter tgMGInfoOAMEnableTagging is enabled. The value range for each is 0 or from 2 to 3999 (The default is 0. 4000 to 4096 are for internal use only.)</td>
</tr>
<tr>
<td>OAM Priority</td>
<td>Integer</td>
<td>Online</td>
<td>System OAM communication priority (according to 802.1.p)</td>
</tr>
</tbody>
</table>

4.9.5.1.1 Interfaces Setting Options

Interfaces Options

- For **Interfaces**, select one of these options:
  - **oneOCM** - for one physical interface for all of the Operation Administration & Maintenance (OAM), Control (C), and Media (M) protocols
  - **twoOCandM** - for two physical interfaces divided between the three protocol groups:
    - Operation Administration & Maintenance (OAM) and Control (C)
    - Media (M)
  - **twoOandCM** - for two physical interfaces divided between the three protocol groups:
    - Operation Administration & Maintenance (OAM)
    - Control (C) and Media (M)
  - **threeOandCandM** - for three physical interfaces divided between the three protocol groups:
    - Operation Administration & Maintenance (OAM)
    - Control (C)
    - Media (M)
4. Configuring & Operating the Media Gateway

Note: If Enable Separation Configuration is disabled, the only optional interface is oneOCM.

For more information, see Interfaces, Subnets, VLANs & Tags on page 145.

4.9.5.1.2 Link Aggregation Options

For Media Aggregation Enable:

The options below follow Avaya recommendations.

- For a system with four 6310 boards or less, retain the default disable option. (One Link via ES port 20)
- For a system with five to six 6310 boards, select the aggregate2 option. (Two Links via ES port 20 and 21)
- For a system with seven to eight 6310 boards, select the aggregate3 option. (Three Links via ES port 20, 21 and 22)

For Link Aggregation Timeout:

This parameter is relevant only if Media Aggregation Enable is set to aggregate 2 or aggregate 3. If relevant, select one of the following:

- Long
- Short

For Link Aggregation Distribution Rule:

This parameter is relevant only if the Media Aggregation Enable is set to aggregate 2 or aggregate 3.

The Ethernet Switch allows for distributing the Ethernet traffic among the aggregated links based on the Source and Destination MAC address and the Source and Destination IP address.

It is recommended to allocate the Media Gateway boards’ IP addresses successively in order to assure an optimal distribution.

If relevant select one of the following:

- SrcMAC
- DestMAC
- SrcXORDestMAC
- SrcIP - (Default)
- DestIP
- SrcXORDestIP

For more information, see Link Aggregation Options on page 139, Aggregation Switch-Over Logic on page 131 and Aggregation Distribution Rules on page 132
4.9.5.1.3 Subnet Separation Options

Subnet Separation Tab

Multiple IP addresses for Subnet Separation can be enabled to match the system configuration.

Media®, Control and Management (OAM) traffic can be separated into three dedicated networks. Instead of a single IP address, three IP addresses and subnet masks can be assigned, each relating to a different traffic type. This architecture enables users to integrate a gateway into a three-network environment that is focused on security and segregation. Each entity in the gateway (e.g., RTP) is mapped to a single traffic type in which it operates.

Media® - up to two media subnets are allowed, one for each Network.

Configuration with no VLANs

For a configuration with no VLANs:
- It is recommended to set no Subnet Separation.
- Retain the default mark in the Multiple Subnet Configuration option checkbox (set to disabled).

Configuration with Multiple Subnets

The recommended rule is the number of Subnet Separations is equal to the number of VLANs.

For a Configuration with Multiple Subnets, select one of these options:
- oneOCM - for one subnet for all of the Operation Administration & Maintenance (OAM), Control (C), and Media (M) protocols
- twoOCandM - for two subnets divided between the three protocol groups:
  - Operation Administration & Maintenance (OAM) and Control (C)
  - Media (M)
- twoOandCM - for two subnets divided between the three protocol groups:
  - Operation Administration & Maintenance (OAM)
  - Control (C) and Media (M)
- threeOandCandM - for three subnets divided between the three protocol groups:
  - Operation Administration & Maintenance (OAM)
  - Control (C)
  - Media (M)

Note: If the Multiple Subnets Configuration is set to oneOCM, the provisioned Control and Media Subnet information is disregarded.
4. Configuring & Operating the Media Gateway

In the **Subnet & VLAN Tab**: The OAM subnet information displays the IP addresses as assigned to the OAM during the SC board installation process. These parameters are the Read Only and can be modified directly via the SC boards only. (When the **Multiple Subnets Configuration** is not set to oneOCM, the Default Gateway is relevant only for the SC board. For the Media Gateway boards, a related OAM network requires setting a static route.)

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global IP Address</td>
<td>IP Address</td>
<td>Read-Only</td>
<td>Global IP address for both SCs in the OAM Subnet</td>
</tr>
<tr>
<td>Default Gateway Address</td>
<td>IP Address</td>
<td>Read-Only</td>
<td>Default Gateway address for the OAM Subnet</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>IP Address</td>
<td>Read-Only</td>
<td>Subnet mask for the OAM network</td>
</tr>
<tr>
<td>Enable Multiple Subnet</td>
<td>Enum</td>
<td>Online</td>
<td>Enables / disables Multiple Subnet Configuration</td>
</tr>
<tr>
<td>Configuration</td>
<td>disable, enableTwoOCandM, enableTwoOandCM, enableThree</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

For more information, see Interfaces, Subnets, VLANs & Tags on page 145.

**4.9.5.2 Static Route Settings**

**Static Route Table** tab

You can set up to 25 static routes - one for each destination entity with which the Avaya G860 has regular communications.

➢ **To set a Static Route or an entity, take these 2 steps:**

  1. To add a row to the Static Route table, click ➔.
  2. Set the parameters according to the table below.

➢ **To modify a value in a Static Route row, take this step:**

  Double-click on value. The value can be modified.

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static Route number</td>
<td>Integer</td>
<td>Read-Only</td>
<td>Indicates the Call Agent Group number, defined by its row in the Call Agent Groups List.</td>
</tr>
</tbody>
</table>
### Parameter Name | Type | Provisioning Type | Description
--- | --- | --- | ---
Administrative State | Enum Locked, ShuttingDown, Unlocked | Read-Only | Administrative state of the Call Agent Group, managed by the User, who can manually lock it, unlock it, or shut it down.
Destination IP address | IP Address | Online | Defines the destination IP Address of the destination entity.
Destination Subnet Mask | IP Address | Online | Defines the destination Subnet Mask of the destination entity.
Gateway IP address | IP Address | Online | Defines the Remote Gateway IP Address of the destination entity.
Protocol Group Type (O,C,M) | Enum none, OAM, control, media | Online | Defines the Protocol Group type as none, OAM, Control or Media. Not relevant for a configuration with no Subnet Separation.
Hops Count to destination | Integer 0-256 | Online | Defines the hops count to the destination. The number of times a packet can be forwarded from one element to another in the network. (Typically up to 20)
Comment | String Up to 200 chars. | Instant | Enter an identification name to indicate for what destination entity this static route is set.

### 4.9.5.3 Setting Networks

- To set the Networks parameters, Media and Control VLANs and Subnet Separation options, take these 4 steps:
  1. Access the [MG Status] screen.
  2. Click [Networks]. The Networks list screen appears.
  3. To add a row to the Network table, click [+].
  4. Set the parameters according to the table below.

| Parameter Name | Type | Provisioning Type | Description |
|--- | --- | --- | ---
| Media Default GW | IP Address | Offline | Defines the Media default gateway |
| Subnet Mask of Media | IP Address | Offline | Defines the subnet mask of the Media group |
### 4. Configuring & Operating the Media Gateway

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subnet Mask of Control</td>
<td>IP Address</td>
<td>Offline</td>
<td>Defines the subnet mask of Control group</td>
</tr>
<tr>
<td>Control Subnet IP</td>
<td>IP Address</td>
<td>Offline</td>
<td>Defines the IP of the Control group subnet</td>
</tr>
</tbody>
</table>

#### Table 4-14: VLANs Settings

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Media VLAN</td>
<td>Enum, enable, disable</td>
<td>Offline</td>
<td>Defines the Media VLAN tagging</td>
</tr>
<tr>
<td>Media VLAN tag ID</td>
<td>int</td>
<td>Online</td>
<td>Defines the Media VLAN tag ID</td>
</tr>
<tr>
<td>Enable Control VLAN</td>
<td>Enum, enable, disable</td>
<td>Offline</td>
<td>Defines the Control VLAN tagging</td>
</tr>
<tr>
<td>Control VLAN tag ID</td>
<td>int</td>
<td>Online</td>
<td>Defines the Control VLAN tag ID</td>
</tr>
</tbody>
</table>

#### Table 4-15: QoS Premium Services

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Premium Control Priority</td>
<td>Integer 0-7</td>
<td>Online</td>
<td>Defines the Premium Control Service Class Priority</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The range is 7 (highest) to 0 (lowest)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The default value is 6</td>
</tr>
<tr>
<td>Premium Control Diffserv</td>
<td>Integer 0-63</td>
<td>Online</td>
<td>Defines the Premium Control Diffserv Priority</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The range is 63 (highest) to 0 (lowest)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The default value is 55</td>
</tr>
<tr>
<td>Premium Media Priority</td>
<td>Integer 0-7</td>
<td>Online</td>
<td>Defines the Premium Media Service Class Priority</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The range is 7 (highest) to 0 (lowest)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The default value is 6</td>
</tr>
<tr>
<td>Premium Media Diffserv</td>
<td>Integer 0-63</td>
<td>Online</td>
<td>Defines the Premium Media Diffserv Priority</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The range is 63 (highest) to 0 (lowest)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The default value is 22</td>
</tr>
</tbody>
</table>
Note: The priority settings assigned to a DiffServ Class name is assigned per Protocol group. The same assignment is relevant to all of the protocols in the Protocol group.

Table 4-16: DiffServ Class Name and Protocol Group Assignments

<table>
<thead>
<tr>
<th>Protocol Group</th>
<th>Target Applications and Services</th>
<th>Tolerance to:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Loss</td>
</tr>
<tr>
<td>Premium</td>
<td>Telephony service like RTP media, T.38 Fax over IP, Lawful Intercept or Control protocols</td>
<td>Very Low</td>
</tr>
<tr>
<td>Platinum</td>
<td>Used for Video Conferencing, Interactive Gaming</td>
<td>Low</td>
</tr>
<tr>
<td>Network</td>
<td>Communications between network devices within one administrative domain like ICMP, COPS, RSVP, DNS, DHCP, BootP, high priority OAM</td>
<td>Low</td>
</tr>
<tr>
<td>Gold</td>
<td>Used for Voice Streaming, Video on demand Broadcast TV, Video surveillance</td>
<td>Med-Low</td>
</tr>
<tr>
<td>Bronze</td>
<td>Used for long-lived TCP, and HTTP flows like Non time-critical OAM&amp;P, Email, Instant Messaging</td>
<td>Low</td>
</tr>
</tbody>
</table>

4.9.5.4 Class of Service (COS)

This section describes the Quality/Class of Service (COS) for the ES 6600.

4.9.5.4.1 ES 6600-Class of Service (COS)

The CPC6600 supports eight traffic priority queues per egress port. Each queue provides a different class of service, i.e., those frames queued to the higher priority queues are transmitted ahead of those on the lower priority queues.

The CPC6600 assigns frames to the egress port queues on the basis of the priority field carried with the 802.1Q tag header, or based on packet filters. The 802.1Q specification allows for 8 traffic classes to be specified in the tag header field of the frame. The 8 traffic classes are mapped to the 8 available COS Queues. The mapping is programmable.

Once packets have been mapped to the eight COS queues, the queues are drained at the egress port based on a programmable scheduling algorithm. The possible scheduling algorithms include: Strict Priority, Weighted Round Robin, and Weighted Round Robin with Bounded Delay.

Note: Currently the COS queue mapping and the scheduling algorithms can’t be configured by the user.
4.9.5.5 COS Queue Configuration

ES6600
Queue Algorithm: strictPriority

Priority to Queue mappings:

<table>
<thead>
<tr>
<th>Priority</th>
<th>COS Queue</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
</tr>
</tbody>
</table>

4.9.5.6 Interfaces, Subnets, VLANs and Tags

4.9.5.6.1 Basic Rules

The following describes the basic rules for VLAN tagging:

1. Number of VLANs = Number of Subnets.
2. Number of Interfaces = Number of VLANs.
3. The OAM VLAN tag must be different from the Media VLAN tag.
4. The same VLAN tag is not allowed on different physical interfaces.

The following table describes the basic rules for a single interface.

<table>
<thead>
<tr>
<th>VLAN Status</th>
<th>Description</th>
<th>Tag Options</th>
</tr>
</thead>
</table>
| VLANs disabled. For an illustrated example, see Use Case: Connecting Using One Physical Interface, No VLANs and One Subnet. | • All system communication is untagged.  
• Multiple Subnets are disabled  
• Single IP subnet for OAM, Control and Media | |
| VLANs enabled-One VLAN Tag (T)       | • Single tag for OAM, Control and Media; CoS is not supported in this mode  
• Multiple Subnets are disabled;  
• Single IP subnet for OAM, Control and Media | |
<table>
<thead>
<tr>
<th>VLAN Status</th>
<th>Description</th>
<th>Tag Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Two VLANs (OC, M): Tags</td>
<td>Multiple Subnets are enabled; Two different IP subnets</td>
<td>OC&lt;sub&gt;T&lt;/sub&gt;; M&lt;sub&gt;T&lt;/sub&gt;</td>
</tr>
<tr>
<td></td>
<td>VLAN1 = OAM + Control</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VLAN2 = Media</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subnet1 = OAM + Control</td>
<td></td>
</tr>
<tr>
<td></td>
<td>subnet2 = Media</td>
<td></td>
</tr>
<tr>
<td>Two VLANs(O, CM): Tags</td>
<td>Multiple Subnets are enabled; Two different IP subnets</td>
<td>O&lt;sub&gt;U&lt;/sub&gt;; CM&lt;sub&gt;T&lt;/sub&gt;</td>
</tr>
<tr>
<td></td>
<td>VLAN1 = OAM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VLAN2 = Control + Media</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subnet1 = OAM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>subnet2 = Control + Media</td>
<td></td>
</tr>
<tr>
<td>Three VLAN Tags*</td>
<td>Multiple Subnets are enabled; three different IP subnets; OAM, Control and Media</td>
<td>O&lt;sub&gt;T&lt;/sub&gt;; C&lt;sub&gt;T&lt;/sub&gt;; M&lt;sub&gt;T&lt;/sub&gt;</td>
</tr>
</tbody>
</table>

The following table describes the basic rules for two interfaces.

**Table 4-18: Two Interfaces (interface1 = OAM + Control; interface2 = Media)**

<table>
<thead>
<tr>
<th>VLAN Status</th>
<th>Description</th>
<th>Tag Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Two VLANs (OC, M): Tags</td>
<td>Multiple Subnets enabled; Two different IP subnets</td>
<td>OC&lt;sub&gt;T or U&lt;/sub&gt;; M&lt;sub&gt;T or U&lt;/sub&gt;</td>
</tr>
<tr>
<td></td>
<td>VLAN1 = OAM + Control</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VLAN2 = Media</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subnet1 = OAM + Control</td>
<td></td>
</tr>
<tr>
<td></td>
<td>subnet2 = Media</td>
<td></td>
</tr>
<tr>
<td>Three VLAN Tags</td>
<td>Multiple Subnets enabled; three different IP subnets; OAM, Control and Media</td>
<td>O&lt;sub&gt;T&lt;/sub&gt;; C&lt;sub&gt;U&lt;/sub&gt;; M&lt;sub&gt;T or U&lt;/sub&gt;</td>
</tr>
<tr>
<td></td>
<td>O&lt;sub&gt;T&lt;/sub&gt;; C&lt;sub&gt;T&lt;/sub&gt;; M&lt;sub&gt;T or U&lt;/sub&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>O&lt;sub&gt;T&lt;/sub&gt;; C&lt;sub&gt;T&lt;/sub&gt;; M&lt;sub&gt;T or U&lt;/sub&gt;</td>
<td></td>
</tr>
</tbody>
</table>
Table 4-19: Two Interfaces (interface1 = OAM ; interface2 = Control + Media)

<table>
<thead>
<tr>
<th>VLAN Status</th>
<th>Description</th>
<th>Tag Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Two VLANs (O, CM): Tags</td>
<td>Multiple Subnets enabled; Two different IP subnets</td>
<td>O_T or U CM or U</td>
</tr>
<tr>
<td></td>
<td>VLAN1=OAM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VLAN2=Control + Media</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subnet1=OAM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>subnet2=Control + Media</td>
<td></td>
</tr>
<tr>
<td>Three VLAN Tags.</td>
<td>For an illustrated example, see Use Case: Connecting Using One Physical interface, Three VLANs and Three Subnets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Multiple Subnets enabled; three different IP subnets; OAM, Control and Media</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Any VLAN tagging combination can be formed</td>
<td></td>
</tr>
</tbody>
</table>

The following table describes the basic rules for three interfaces.

Table 4-20: Three Interfaces

<table>
<thead>
<tr>
<th>VLAN Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Three VLAN Tags</td>
<td>Multiple Subnets enabled; three different IP subnets; OAM, Control and Media</td>
</tr>
<tr>
<td></td>
<td>Any VLAN tagging combination can be formed</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tag options</td>
<td>T – tagged</td>
</tr>
<tr>
<td></td>
<td>U – untagged</td>
</tr>
<tr>
<td>O</td>
<td>OAM</td>
</tr>
<tr>
<td>C</td>
<td>Control</td>
</tr>
<tr>
<td>M</td>
<td>Media</td>
</tr>
<tr>
<td>U</td>
<td>Untagged</td>
</tr>
</tbody>
</table>

4.9.5.7 ES 6600 Ethernet Switch Port Allocation

4.9.5.7.1 Port Allocation

For ES/6600, the OAM Network and Control Network are GbE copper links and the Media Network is up to 3 GbE copper aggregated links.
The following table describes the interface types:

<table>
<thead>
<tr>
<th>Interface Types</th>
<th>ES/6600</th>
</tr>
</thead>
<tbody>
<tr>
<td>OAM</td>
<td>18</td>
</tr>
<tr>
<td>Control</td>
<td>19</td>
</tr>
<tr>
<td>Media</td>
<td>20, 21, 22 (aggregate-able)</td>
</tr>
<tr>
<td>Mirror</td>
<td>23</td>
</tr>
<tr>
<td>F-link</td>
<td>24</td>
</tr>
</tbody>
</table>

4.9.5.7.2 Port Aggregation

**ES/6600** – Three port for Media (enabled for aggregation fully conformance to IEEE-802.3ad, up to 3 ports). Allocated ports 20, 21, 22: three options (no aggregation, 20+21, and 20+21+22).

<table>
<thead>
<tr>
<th>Interfaces</th>
<th>Two interfaces:</th>
</tr>
</thead>
<tbody>
<tr>
<td>OCM – 20*</td>
<td>OC – 18, M – 20*</td>
</tr>
<tr>
<td></td>
<td>O – 18, CM – 20*</td>
</tr>
</tbody>
</table>

Table 4-21: Port allocation in accordance with ES type, Aggregation and Number of Interfaces

<table>
<thead>
<tr>
<th>Interfaces</th>
<th>Two interfaces: OC – M</th>
<th>Two interfaces: O – CM</th>
<th>Three interfaces O – C – M</th>
</tr>
</thead>
<tbody>
<tr>
<td>ES/6600</td>
<td>OCM – 20*</td>
<td>OC – 18, M – 20*</td>
<td>O – 18, CM – 20*</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>C – 19, M – 20*</td>
</tr>
</tbody>
</table>

Legend;

O – OAM
C – Control
M – Media

20*-If aggregation is enabled (including 21/22)

4.10 Use Cases for IP Network Connectivity Configuration

This section describes various user case scenarios for setting up the Physical Interfaces, VLANs and Subnet Separation. The following scenarios are described:

- Connecting using one physical interface, no VLANs and One subnet
- Connecting using one physical interfaces, three VLANs and three subnets
- Connecting using three physical interfaces, three VLANs and three Subnets

For additional information on the various configuration elements, see the previous section Setting up the Physical Interfaces, VLANs & Subnet Separation on page 134.
4. Configuring & Operating the Media Gateway

4.10.1 Use Case: Connecting Using One Physical interface, Three VLANs and Three Subnets

In this example, there is one physical interface separation and three logical separations.

4.10.1.1 Physical Interface Options

Subnet and VLAN Settings tab:
For Enable Separation Configuration, select enable.

Interfaces Settings tab:
For Interfaces, select oneOCM – for one physical interface for all of the Operation Administration & Maintenance (OAM), Control (C), and Media (M) protocols.

For more information, see Interfaces, Subnets, VLANs & Tags on page 145.

4.10.1.2 Link Aggregation Options

Interfaces Settings tab:
- For Media Aggregation Enable:
  The options below follow Avaya recommendations.
  - For a system with four 6310 boards or less, retain the default disable option.
    (One Link via ES port 20)
  - For a system with five to six 6310 boards, select the aggregate2 option.
    (Two Links via ES port 20 and 21)
  - For a system with seven to eight 6310 boards, select the aggregate3 option.
    (Three Links via ES port 20, 21 and 22)

- For Link Aggregation Timeout:
  Relevant only if the Media Aggregation Enable is set to aggregate 2 or aggregate 3.
  The periodic transmission of the ES LACP_Timeout may occur at a Long timeout (30 sec. – the default value) or Short timeout (1 sec.), which is determined by the Partner’s LACP_Timeout value.

- For Link Aggregation Distribution Rule:
  Relevant only if the Media Aggregation Enable is set to aggregate 2 or aggregate 3.
  The Ethernet Switch allows for distributing the Ethernet traffic among the aggregated links based on the Source and Destination MAC address and the Source and Destination IP address.
  The six distribution rules are:
  1. SrcMAC - indicates that packets are distributed based on the last three bits of the Source MAC address.
  2. DestMAC - indicates that the packets are distributed based on the last three bits of the Destination MAC address.
  3. SrcXORDestMAC - indicates that the packets are distributed based on the last three bits of the XOR of the Source and Destination MAC address.
4. **SrcIP** - indicates that the packets are distributed based on the last three bits of the Source IP address.

5. **DestIP** - indicates that the packets are distributed based on the last three bits of the Destination IP address.

6. **SrcXORDestIP** - indicates that the packets are distributed based on the last three bits of the XOR of the Source and Destination IP address.

The default rule assigned to Ethernet Switch ports is SrcIP.

It is recommended to allocate the Media Gateway boards’ IP addresses successively in order to assure an optimal distribution.

For more information, see Link Aggregation Options on page 139, Aggregation Switch-Over Logic on page 131 and Aggregation Distribution Rules on page 132.

### 4.10.1.1.3 VLAN Options

The following Service Class Priority groups are related to the OAM and not listed in the VLAN Setup table below.

### 4.10.1.1.4 OAM VLAN Tagging

- For **OAM enable Tagging** – set enable
- For **OAM Tag ID** – set the OAM VLAN tag ID.

### 4.10.1.1.5 OAM QoS Setting

The following Service Class Priority groups are related to the OAM:

- For **Network Service Class Priority** – set a priority level.
- For **Gold Service Class Priority** – set a priority level.
- For **Bronze Service Class Priority** – set a priority level.
- For **Network DiffServ Priority** – Set DiffServ Priority.
- For **Gold DiffServ Priority** – Set DiffServ Priority.
- For **Bronze DiffServ Priority** – Set DiffServ Priority.

### 4.10.1.1.6 Media & Control VLAN tagging

- Control & Media VLAN lists
  
  The network VLAN tags for Media and Control must be chosen from these lists. Assign each of the VLAN tag ID (OAM, Control, Media1 and Media 2) the appropriate unique number.

- For **Media VLAN list first tag ID**: Set the tag of the first Media VLAN
- For **Media VLAN list second tag ID**: Irrelevant for this example
- For **Control VLAN list first tag ID** Set the tag of the first Control VLAN
4. Configuring & Operating the Media Gateway

**Note:** The value range for each must be from 0, 2 to 3999 (The default is 0 = untagged). Values 4000 to 4096 are for internal use only.

➢ To set the Networks parameters, Media and Control VLANs and Subnet Separation options, take these 4 steps:

1. Access the **MG Status** screen.
2. Click **Networks**. The Networks list screen appears.
3. Double click on the row item.
   Or,
   If the Network Table is empty, to add a row, click **.**
   The Network properties dialog box appears.
4. Set the Network properties as follows:
   • For **Enable Control VLAN** – set enable for enable tagging
   • For **Control VLAN Tag ID** – set the Control VLAN tag ID
   • For **Enable Media VLAN** – set enable for enable tagging
   • For **Media VLAN Tag ID** – set the Media VLAN tag ID

**Control & Media QoS Setting**

- For **Network Service Class Priority**: set a priority level.
- For **Premium Control Priority** – set the Control Service class priority level
- For **Premium Control DiffServ**– set the Control DiffServ priority.
- For **Premium Media Priority** - Set the Media Service class Priority level.
- For **Premium Media DiffServ** - Set the Media DiffServ Priority.

4.10.1.1.7 Subnet Separation Options

Subnet Separation tab:

The recommended rule is the number of Subnet Separations is equal to the number of VLANs.

- For **Multiple Subnet Configuration** set to threeOandCandM

**Network Properties screen**

Use the directions above to access the **Network Properties** screen and set the properties as follows:

- For the **Media Default GW**, assign the correct IP address for the Default Gateway
- For the **Media Subnet Mask**, assign the correct Media subnet mask IP.
4.10.1.8 Static Route Settings

Static Route Table tab:
You can set up to 25 static routes - one for each destination entity with which the Avaya G860 has regular communications.

Use the icon to add a row to the Static Route table.
To modify a value, double-click on it.
Set the following parameters:

- **Destination IP Address** – The IP address of the destination entity.
- **Destination Subnet Mask** – The Subnet Mask of the destination entity
- **Gateway IP Address** – The Gateway IP address
- **Protocol Group Type (O,C,M)** – Set the O, C and M in accordance with the Route Protocol Group. This field is for information only and is non-operational.
- **Hops Count to Destination** – The number of times a packet can be forwarded from one element to another in the network. (Typically up to 20)
- **Comment** - enter an identification name to indicate for what destination entity this static route is set.

4.10.2 Use Case: Connecting Using One Physical Interface, No VLANs and One Subnet

In this example, there is no physical interface separation and no logical separation.

4.10.2.1.1 Physical Interface Options

Subnet and VLAN Settings tab:

For **Enable Separation Configuration**, select **Disable** – for one physical interface for all of the Operation Administration & Maintenance (OAM), Control (C), and Media (M) protocols.

For more information, see Interfaces, Subnets, VLANs & Tags on page 145.

4.10.2.1.2 Link Aggregation Options

Interfaces Settings tab:

- For **Media Aggregation Enable**:

  The options below follow Avaya recommendations.

  - For a system with four 6310 boards or less, retain the default disable option. (One Link via ES port 20)
For a system with five to six 6310 boards, select the **aggregate2** option.  
(Two Links via ES port 20 and 21)

For a system with seven to eight 6310 boards, select the **aggregate3** option.  
(Three Links via ES port 20, 21 and 22)

**For Link Aggregation Timeout:**

Relevant only if the Media Aggregation Enable is set to **aggregate 2** or **aggregate 3**.

The periodic transmission of the **ES LACP_Timeout** may occur at a Long timeout (30 sec. – the default value) or Short timeout (1 sec.), which is determined by the Partner’s **LACP_Timeout** value.

**For Link Aggregation Distribution Rule:**

Relevant only if the Media Aggregation Enable is set to **aggregate 2** or **aggregate 3**.

The Ethernet Switch allows for distributing the Ethernet traffic among the aggregated links based on the Source and Destination MAC address and the Source and Destination IP address.

The six distribution rules are:

1. **SrcMAC** - indicates that packets are distributed based on the last three bits of the Source MAC address.
2. **DestMAC** - indicates that the packets are distributed based on the last three bits of the Destination MAC address.
3. **SrcXORDestMAC** - indicates that the packets are distributed based on the last three bits of the XOR of the Source and Destination MAC address.
4. **SrcIP** - indicates that the packets are distributed based on the last three bits of the Source IP address.
5. **DestIP** - indicates that the packets are distributed based on the last three bits of the Destination IP address.
6. **SrcXORDestIP** - indicates that the packets are distributed based on the last three bits of the XOR of the Source and Destination IP address.

The default rule assigned to Ethernet Switch ports is **SrcIP**.

It is recommended to allocate the Media Gateway boards’ IP addresses successively in order to assure an optimal distribution.

For more information, see Link Aggregation Options on page 139, Aggregation Switch-Over Logic on page 131 and Aggregation Distribution Rules. on page 132

### 4.10.2.1.3 VLAN Options

Subnet and VLAN Settings tab:

- **For Enable Separation Configuration**, select **Disable** – for one physical interface for all of the Operation Administration & Maintenance (OAM), Control (C), and Media (M) protocols
- **For Network Service Class Priority** – irrelevant for no VLANs
- **For Gold Service Class Priority** – irrelevant for no VLANs
- **For Bronze Service Class Priority** – irrelevant for no VLANs
4.10.2.1.4 Subnet Separation Options

Subnet Separation tab:

For a configuration with no VLANs, it is recommended to set no Subnet Separation. The recommended rule is the number of Subnet Separations is equal to the number of VLANs.

- For Multiple Subnet Configuration set to oneO\(\text{CM}\)

4.10.2.1.5 Static Route Settings

Static Route Table tab:

You can set up to 25 static routes - one for each destination entity with which the Avaya G860 has regular communications.

Use the icon to add a row to the Static Route table.

To modify a value, double-click on it.

Set the following parameters:

- **Destination IP Address** – The IP address of the destination entity.
- **Destination Subnet Mask** – The Subnet Mask of the destination entity.
- **Gateway IP Address** – The Gateway IP address of the destination entity.
- **Protocol Group Type (O,C,M)** – Not relevant for a configuration with no Subnet Separation.
- **Hops Count to Destination** – The number of times a packet can be forwarded from one element to another in the network. (Typically up to 20)
- **Comment** – enter an identification name to indicate for what destination entity this static route is set.

4.10.3 Use Case: Connecting Using Three Physical interfaces, Three VLANs and Three Subnets

In this example, there are three physical interface separations and three logical separations.

4.10.3.1.1 Physical Interface Options

Subnet and VLAN Settings tab:

For Enable Separation Configuration, select **enable**.

Interfaces Settings tab:

For **Interfaces**, select **threeOandCandM** – for three physical interfaces divided between the three protocol groups:

- Operation Administration & Maintenance (OAM)
- Control (C)
- Media (M)
4. Configuring & Operating the Media Gateway

4.10.3.1.2 Link Aggregation Options

For Media Aggregation Enable:

The options below follow Avaya recommendations.

- For a system with four 6310 boards or less, retain the default disable option. (One Link via ES port 20)
- For a system with five to six 6310 boards, select the aggregate2 option. (Two Links via ES port 20 and 21)
- For a system with seven to eight 6310 boards, select the aggregate3 option. (Three Links via ES port 20, 21 and 22)

For Link Aggregation Timeout:

Relevant only if the Media Aggregation Enable is set to aggregate 2 or aggregate 3.

The periodic transmission of the ES LACP_Timeout may occur at a Long timeout (30 sec. – the default value) or Short timeout (1 sec.), which is determined by the Partner’s LACP_Timeout value.

For Link Aggregation Distribution Rule:

Relevant only if the Media Aggregation Enable is set to aggregate 2 or aggregate 3.

The Ethernet Switch allows for distributing the Ethernet traffic among the aggregated links based on the Source and Destination MAC address and the Source and Destination IP address.

The six distribution rules are:

1. SrcMAC - indicates that packets are distributed based on the last three bits of the Source MAC address.
2. DestMAC - indicates that the packets are distributed based on the last three bits of the Destination MAC address.
3. SrcXORDestMAC - indicates that the packets are distributed based on the last three bits of the XOR of the Source and Destination MAC address.
4. SrcIP - indicates that the packets are distributed based on the last three bits of the Source IP address.
5. DestIP - indicates that the packets are distributed based on the last three bits of the Destination IP address.
6. SrcXORDestIP - indicates that the packets are distributed based on the last three bits of the XOR of the Source and Destination IP address.

The default rule assigned to Ethernet Switch ports is SrcIP.

It is recommended to allocate the Media Gateway boards’ IP addresses successively in order to assure an optimal distribution.

For more information, see Link Aggregation Options on page 139, Aggregation Switch-Over Logic on page 131 and Aggregation Distribution Rules. on page 132

4.10.3.1.3 VLAN Options

OAM VLAN Tagging:

- For OAM enable Tagging – set enable
For OAM Tag ID – set the OAM VLAN tag ID.

OAM QoS Settings:

The following Service Class Priority groups are related to the OAM:

- For **Network Service** Class Priority: – set a priority level.
- For **Gold Service** Class Priority – set a priority level
- For **Bronze Service** Class Priority – set a priority level
- For **Network DiffServ** Priority - Set DiffServ Priority
- For **Gold DiffServ** Priority- Set DiffServ Priority
- For **Bronze DiffServ** Priority- Set DiffServ Priority

Media & Control VLAN Tagging:

**Control & Media VLAN lists**

The network VLAN tags for Media and Control must be chosen from these lists. Assign each of the VLAN tag ID (OAM, Control, Media1 and Media 2) the appropriate unique number.

- For **Media VLAN list first tag ID**: Set the tag of the first Media VLAN
- For **Media VLAN list second tag ID**: Irrelevant for this example
- For **Control VLAN list first tag ID** Set the tag of the first Control VLAN

**Note:** The value range for each must be from 0, 2 to 3999 (The default is 0 = untagged). Values 4000 to 4096 are for internal use only.

### 4.10.3.1.4 Subnet Separation Options

Subnet Separation tab:

Click a mark in the **3 Subnets per OAM, Media and Control** option checkbox. The Subnet Separation table at the bottom of the screen is enabled. The recommended rule is the number of Subnet Separations is equal to the number of VLANs.

- For **Multiple Subnet Configuration** set to three (OAM, Media 1, Media 2)

Network Properties screen:

Use the directions above to access the **Network Properties** screen and set the properties as follows:

- The **OAM** row displays the IP addresses as assigned to the OAM during the SC board installation process. These parameters are Read Only and can be modified directly via the SC boards only.

  - For the **Media Default GW** row, assign the correct IP address for the Default Gateway

  - For the **Media** and Subnet Mask, assign the correct Media subnet mask IP.

  - The **Media** Subnet IP address is the logical end determined accordingly.
For the **Control Subnet Mask**, assign row, Use the correct Control subnet mask IP.

For **Add Static Routes** button or the Control Subnet IP, assign the correct Control subnet IP **Static Route Table** tab. Refer to the **Static Route Table** tab section below.

Assign the Subnet Mask and Subnet IP address for the Control Protocol group.

### 4.10.3.1.5 Static Route Settings

Static Route Table tab:

You can set up to 25 static routes - one for each destination entity with which the Avaya G860 has regular communications.

Use the icon to add a row to the Static Route table.

To modify a value, double-click on it.

Set the following parameters:

- **Destination IP Address** – The IP address of the destination entity.
- **Destination Subnet Mask** – The Subnet Mask of the destination entity
- **Gateway IP Address** – The Gateway IP address
- **Protocol Group Type (O,C,M)** – Set the O, C and M in accordance with the Route Protocol Group. This field is for information only and is non-operational.
- **Hops Count to Destination** – The number of times a packet can be forwarded from one element to another in the network. (Typically up to 20)
- **Comment** - enter an identification name to indicate for what destination entity this static route is set.

### 4.11 Configuring PSTN Connectivity

PSTN Connectivity must be configured in the following categories as applicable:

- Trunks
- SDH/SONET
- ISDN

#### 4.11.1 Configuring the Trunks

**Trunk** defines a connection between switches within the PSTN exchange. It contains a certain number of **channels** that may carry voice or signaling messages (depending on the PSTN protocols being used).

**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.

### Supported Actions

The following actions are available on the Trunk:

- **Lock** – take trunk out-of-service; the synchronization with the remote PSTN side will be lost.
- **Unlock** – return trunk in-service.

**Note:** Whenever you need to lock or unlock a trunk which is a member of an NFAS group, you must lock and unlock in the following order:

Prior to provisioning, lock the trunks in the following order:

1. The NFAS bearer trunks.
2. The trunk serving as the backup D channel, if you defined a backup D-channel.
3. The trunk serving as the primary D channel.

When you finish configuring, unlock the trunks in the following order:

1. The trunk serving as the backup D channel, if you defined a backup D-channel.
2. The trunk serving as the primary D channel.
3. The NFAS bearer trunks.

▶ **To view status of the trunks on specific Media Gateway board, take these 4 steps:**

1. Access **MG Status** screen
2. Double-click on the specific Media Gateway board
3. For TP-6310 boards – double-click on the PSTN Fiber Group line item.
4. Click **DS1 Trunks**. The list of trunks appears.

To enable the basic connectivity of the Media Gateway board, set its trunks to match the configuration on the far side. Double-click on the trunk to open its Provisioning screen. Refer to the table below for details.

**Note:** Pay special attention to the **Framing Method Type** attribute in Trunk’s configuration – it must match the **Protocol Type** attribute.

After completing the configuration, unlock the trunk to bring it into service. Verify that the trunk synchronizes with the remote side by checking that its **Operational State** becomes **Enabled**. To minimize amount of irrelevant traps and notifications, keep the unsynchronized trunks locked.
### Table 4-22: Trunk Properties

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trunk Name</td>
<td>String Up to 20 chars.</td>
<td>Instant</td>
<td>Textual, User-defined name assigned to a trunk, enabling the User to identify it intuitively and easily.</td>
</tr>
<tr>
<td>Protocol Type</td>
<td>Enum None, E1EuroIsdn, T1Cas, T1RawCas, T1Transparent, E1Transparent31, E1Transparent30, E1MfcR2, E1CasR2, E1RawCas, T1Ni2Isdn, T14EssIsdn, T15EssIsdn, T15Ess10Isdn, T1Dms100Isdn, J1Transparent, T1NttIsdn, E1AustellIsdn, E1HktIsdn, E1Korlsdn, T1HktIsdn, E1Qsig, E1Tnz22, T1Extra23, V51AN, V51LE, V52AN, V52LE, T1IUA, E1IUA, E1EXTRA30, E1EXTRA31, Extra32, Extra33, T1Eurolsdsn, T1Dms100Meridian Isdn, T1Ni11sdsn, E1DUA</td>
<td>Online</td>
<td>Use this parameter to define the PSTN protocol to be used for this trunk. Users can define any of the supported PSTN protocols for the trunk via this parameter.</td>
</tr>
<tr>
<td>Framing Method Type</td>
<td>Enum extendedSuperFrame, superFrame, E1FramingDdf, E1FramingMffCrc4, E1FramingMffCrc4Ext, E1FramingNil, T1FramingF4, T1FramingF12, T1FramingEsf, T1FramingEsfCrc6, T1FramingF72, T1FramingEsfCrc6Jt, T1FramingNil</td>
<td>Offline</td>
<td>This parameter enables Users to select the T1/E1 framing method to be used for this trunk. Make sure that the <strong>Framing Method Type</strong> parameter matches the <strong>Protocol Type</strong> parameter.</td>
</tr>
<tr>
<td>Parameter Name</td>
<td>Type</td>
<td>Provisioning Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>----------</td>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Line Build-out Loss</td>
<td>Enum db0, db7p5, db15, db22p5</td>
<td>Instant</td>
<td>Use this parameter to select the line build-out loss to be used for this trunk.</td>
</tr>
<tr>
<td>Line Code</td>
<td>Enum b8ZS, aMI, hDB3</td>
<td>Instant</td>
<td>Use this parameter to select the line code type to be used for this trunk.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>B8ZS - use B8ZS line code (for T1 trunks only).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>AMI - use AMI line code.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HDB3 - use HDB3 line code (for E1 trunks only).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>B8ZS or AMI is used for T1 spans; HDB3 or AMI is used for E1 spans.</td>
</tr>
</tbody>
</table>

### 4.11.2 Configuring SDH/SONET

The TP-6310 board provides a PSTN Fiber Group with two SDH/SONET optical links, protected by the APS (Automatic Protection Switching).

➢ **To view status of the PSTN Fiber Group on specific Media Gateway board, take these 5 steps:**

1. Access the MG Status screen.  
2. Double-click on the specific Media Gateway board. TP-6310 Status screen is displayed.  
3. Double-click on the PSTN Fiber Group line item.  
4. Click **PSTN Fiber Group**. The PSTN Fiber Group list appears.  
5. In the **TP-6310 Status** screen, select the PSTN Fiber Group line item and click **Properties**. The PSTN Fiber Group parameters screen appears.  
6. To configure the PSTN Fiber Group parameters, refer to the table below.

#### Table 4-23: Fiber Group Properties

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fiber Group Interface type</td>
<td>Enum unknown, stm1, oc3</td>
<td>Offline</td>
<td>Indicates the Fiber Group Interface type as either STM1 or OC3.</td>
</tr>
<tr>
<td>Active Link</td>
<td>Integer 1-2</td>
<td>Read-Only</td>
<td>Indicates which of the Fiber Links is active, either Link A or B.</td>
</tr>
</tbody>
</table>
### 4. Configuring & Operating the Media Gateway

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revertive Mode</td>
<td>Enum NonRevertive, Revertive</td>
<td>Offline</td>
<td>Defines revertive or non-revertive behavior of 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.</td>
</tr>
</tbody>
</table>

**Note:** Ignore the clock-related parameters in the Fiber Group Provisioning screen. They are not supported in current Media Gateway software version.

#### 4.1.1.3 Configuring NFAS Group Provisioning

When a T1 circuit is used to carry Primary Rate ISDN, one of its timeslots is used to carry the D channel, which is the channel that carries the control and signaling information. NFAS is a configuration where multiple T1 carriers share a single D channel. NFAS configuration reduces cost, but carries a risk -- a failure on the T1 trunk carrying the D channel affects all the other trunks in the NFAS group. You can therefore optionally configure a backup D channel on another trunk. If the primary D channel fails, the backup D channel takes over the signaling.

You can include up to 10 T1 trunks in an NFAS group, and you can define up to nine NFAS groups on each TP-6310 board.

To configure NFAS group provisioning, take these steps:

1. For each trunk you include in an NFAS group, open the Media Gateway board ISDN/DPNSS screen which enables configuring NFAS parameters.
   a. Access the **MG Status** screen.
   b. Double-click the desired Media Gateway board. The **Media Gateway Board Status** screen appears.
   c. For TP-6310 board double-click on the "PSTN Fiber Group" row.
   d. Click **DS1 Trunks**. The **DS1 Carriers List** screen is displayed.
   e. Double-click on the Trunk you wish to include in the NFAS group. The **Trunk Parameters Provisioning** screen appears.
   f. Change **Protocol Type** to **ISDN**.
   g. Click the **ISDN/DPNSS tab**.
2. Lock the trunk.
3. In the ISDN/DPNSS screen, configure the trunk’s NFAS parameters as described in the table, NFAS Parameters of the Trunk on page 162. Keep the following guidelines in mind:
   a. Start with NFAS group 1.
   b. For each NFAS group, define one trunk as a primary D channel, and optionally define another trunk as the backup D channel.
c. Each NFAS group can contain up to 10 trunks.

d. You can define up to 9 NFAS groups.

4. When you finish configuring all the trunks in the NFAS group, unlock them in the following order:

a. The trunk serving as the backup D channel, if you defined a backup D-channel.

b. The trunk serving as the primary D channel.

c. The NFAS bearer trunks.

**Note:** If provisioning changes are required to members of an NFAS group, lock them, prior to provisioning, in the following order:

1. The NFAS bearer trunks.

2. The trunk serving as the backup D channel, if you defined a backup D-channel.

3. The trunk serving as the primary D channel.

### Table 4-24: NFAS Parameters of the Trunk

<table>
<thead>
<tr>
<th>Table Parameter Name</th>
<th>Range</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| D-Channel Configuration | Primary, Backup, NFAS | Online | Defines the NFAS configuration of the trunk:  
  - Primary – specifies the trunk as the primary D channel for this NFAS group.  
  - Backup – specifies the trunk as the backup D channel for this NFAS group.  
  - NFAS – specifies that the trunk belongs to this NFAS group and is a bearer (non-signaling member) of NFAS group. |
| Termination side | User TerminationSide, Network TerminationSide | Online | Defines the termination side. This setting depends on the remote side setting. |
| NFAS Interface Id | Integer 0-255 | Online | Assigns a unique NFAS group member ID to the trunk. Trunks that belong to the same NFAS group must be assigned different Interface Ids. |
| NFAS Group Number | Integer 1-9 | Online | Defines the NFAS group. The first NFAS group you define must be group 1. |
4. Configuring & Operating the Media Gateway

4.12 Configuring the Voice Settings

Voice Settings define different aspects of the voice packetization performed by the Media Gateway boards when transferring the calls over the IP network.

To configure the Voice Settings, take these 3 steps:

1. Access the \( \text{MG Status} \) screen.

2. Select the desired Media Gateway board. Click \( \text{Clock} \). The Media Gateway Board Provisioning Properties screen appears.

3. In the \textbf{Voice} tab, configure parameters as described below.

Table 4-25: Media Gateway Board’s Voice Settings

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSP Load File Version</td>
<td>Integer</td>
<td>Online</td>
<td>Defines the set of the voice coders supported by the Media Gateway board. Only the G.711 and G.729 codecs are certified for this application.</td>
</tr>
<tr>
<td>Default Coder</td>
<td>String</td>
<td>Online</td>
<td>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.</td>
</tr>
<tr>
<td>PCM Law</td>
<td>Enum</td>
<td>Online</td>
<td>Defines the type of PCM encoded on input/output TDM bus.</td>
</tr>
<tr>
<td>RFC 2658 Interleaving</td>
<td>Enum</td>
<td>Online</td>
<td>When enabled, RTP packets include an interleaving byte for VBR coders</td>
</tr>
<tr>
<td>Standard SID Payload Type</td>
<td>Enum</td>
<td>Online</td>
<td>When enabled SID packets are sent with the RTP SID type (RFC 3389).</td>
</tr>
<tr>
<td>Echo Canceller</td>
<td>Enum</td>
<td>Instant</td>
<td>Enables or disables EC (Echo Canceller).</td>
</tr>
<tr>
<td>Parameter Name</td>
<td>Type</td>
<td>Provisioning Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>------------------------------</td>
<td>-------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Echo Canceller Length</td>
<td>Enum 0, 4, 11, 22</td>
<td>Online</td>
<td>Defines the maximum board EC (Echo Canceller) length capability. 0 – EC length determined internally to reach maximum channel capacity. 4 – 32 msec 11 – 64 msec 22 – 128 msec.</td>
</tr>
<tr>
<td>Max Echo Canceller Length</td>
<td>Enum 0, 4, 11, 22</td>
<td>Online</td>
<td>Defines the maximum board EC (Echo Canceller) length capability. 0 – EC length determined internally to reach maximum channel capacity. 4 – 32 milliseconds 11 – 64 milliseconds 22 – 128 milliseconds</td>
</tr>
<tr>
<td>Echo Canceller Aggressive NLP</td>
<td>Enum Disable, Enable</td>
<td>Online</td>
<td>Enables or disables Aggressive NLP in the first 0.5 second of the call.</td>
</tr>
<tr>
<td>Jitter Buffer Min Delay</td>
<td>Integer 0-150</td>
<td>Instant</td>
<td>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.</td>
</tr>
<tr>
<td>DTMF Transport Type</td>
<td>Enum MuteDTMF, Proprietary DTMFRelay, TransparentDTMF, RelayDTMF OverRTP</td>
<td>Online</td>
<td>Defines 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.  Relay DTMF Over RTP - erase digits from the voice stream; relay to remote using RFC 2833 syntax.  Transparent DTMF - digits remain in the voice stream.</td>
</tr>
</tbody>
</table>
### 4. Configuring & Operating the Media Gateway

#### Parameter Name | Type | Provisioning Type | Description
--- | --- | --- | ---
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.

### 4.12.1 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 1:** Pre-configured AMR coder policy is supported for TP-6310 boards only.

**Note 2:** 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.

**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, take these 6 steps:

1. Access the [MG Status] screen.
2. Click [AMR Profile]. The AMR Coder Profiles List screen appears.
3. To add a new AMR Coder Profile, click [ ]. A new row appears.
4. To view the Policy Rules that the AMR Coder Profile contains, double-click on it.
5. To add a new AMR Policy Rule, click [ ].
6. 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

To attach the AMR Coder Profile to the specific Media Gateway board, take these 3 steps:

1. Access the [MG Status] screen.
2. Right-click on the desired Media Gateway board and from the popup menu, select Configuration > Properties.
3. On the Voice tab, from the AMR Coder Profile ID dropdown list, select the appropriate profile name.

4.13 Configuring the SIP Subsystem

SIP (Session Initiation Protocol) 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.

SIP invitations are used to create sessions and carry session descriptions that enable participants to agree on a set of compatible media types. SIP uses elements called Proxy Servers to:

- Help route requests to the user's current location
- Authenticate and authorize users for services
- Implement provider call-routing policies
- Provide features to users
4. Configuring & Operating the Media Gateway

Registration Function

SIP also provides a Registration function that enables users to upload their current locations for use by Proxy Servers.

Independent Media Gateway Board SIP Configuration

Each Media Gateway board operates as a stand-alone SIP Media Gateway. Therefore, the SIP configuration is performed independently for each Media Gateway board.

4.13.1 The SIP Proxy

The SIP Proxy server is used by Media Gateway board to perform the routing of the SIP requests.

Redundancy Mechanisms

The Media Gateway board may operate with up to four SIP Proxy servers. Two different mechanisms for switching between SIP Proxy server 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. Refer to 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. Refer to the parameters **Enable Proxy Hot Swap** and **Proxy Hot Swap Retx**.

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. Refer to the parameters **DNS Query Type** and **DNS Query Type**.

For fallback routing, when communication with SIP Proxy is lost, or for traffic load balancing, you can use internal routing tables (Tel to IP) inside the Media Gateway board. Refer to the parameters **Preferred Routing Table** and **Always Use Proxy**.

➢ To configure SIP Proxy take these 9 steps:

1. Access the **MG Status** screen.
2. Double-click the desired Media Gateway board. The Media Gateway Board Status screen appears.
3. Click [SIP]. The SIP Protocol screen is displayed.

4. Click [Proxy Servers]. The SIP Proxy List screen is displayed.

5. To add a new SIP Proxy Server, click [+] The SIP Proxy Provisioning screen is displayed.

6. Configure name and IP address of the SIP Server. Refer to table, ‘SIP Proxy Server Parameters’ below for details.

7. For the redundant SIP Proxies configuration, add as many SIP Proxy Servers as needed.

8. Click [Proxy Settings]. The SIP Proxy Settings screen is displayed.

9. Configure SIP Proxy Settings, as described in table, ‘SIP Proxy Settings’ below.

### Table 4-26: SIP Proxy Server Parameters

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>String Up to 20 chars.</td>
<td>Online</td>
<td>Textual, user-defined name assigned to the entity (MO), enabling users to identify it intuitively and easily.</td>
</tr>
<tr>
<td>Proxy Ip</td>
<td>String Up to 49 chars.</td>
<td>Instant_apply</td>
<td>IP address (and optionally port number) or domain name (FQDN) of the SIP Proxy Server.</td>
</tr>
</tbody>
</table>

### Table 4-27: SIP Proxy Settings

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| Enable Proxy   | Enum No, Yes | Instant | Enables use of the SIP Proxy Server.  
  - No – Proxy isn’t used, the internal routing table is used instead.  
  - Yes – Proxy is used.  
  **Default: No.** |
<p>| Proxy Name     | String Up to 49 chars. | Instant | Home Proxy Domain Name. If specified, the name is used as Request-URI in REGISTER, INVITE and other SIP messages. If the proxy name isn't specified, the Proxy IP address is used instead. |</p>
<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| Enable Proxy Keep Alive | Enum       | Instant           | Enables Proxy Keep Alive Redundancy mode (via keep-alive messages).  
- No – Disable.  
If Proxy Keep Alive Redundancy is enabled, an 'OPTIONS' SIP message is sent every 'Proxy Keep-Alive Time'.  
Note: When the active Proxy doesn't respond to INVITE messages sent by the gateway, the Proxy is marked as OFFLINE. The behavior is similar to the keep-alive failure.  
**Default: No.** |
| Keep Alive Time         | Integer    | Instant           | Defines the Proxy keep-alive time interval (in seconds) between OPTIONS messages. |
| Enable Proxy Hot Swap   | Enum       | Instant           | Enables Proxy Hot Swap Redundancy mode.  
- No – Disable.  
- Yes – Enable Proxy Keep-Alive Redundancy. An 'OPTIONS' SIP message is sent every 'Proxy Keep-Alive Time'.  
If Proxy Hot Swap Redundancy is enabled, an 'INVITE' SIP message is first sent to the Primary Proxy server. If there is no response from the Primary Proxy server for 'ProxyHotSwapRtx' retransmissions, the 'INVITE' message is resent to the Redundant Proxy server. |
| Proxy Hot Swap Rtx      | Integer    | Instant           | Number of retransmitted INVITE messages before call is routed (hot swap) to another Proxy. |
| Proxy Redundancy Mode   | Enum       | 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'). |
<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Routing Table for host names</td>
<td>Enum No, Yes</td>
<td>Instant</td>
<td>Use the internal Tel to IP routing table to obtain the URL Host name and (optionally) an IP profile (per call), even if Proxy server is used.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Note: This Domain name is used, instead of Proxy name or Proxy IP address, in the INVITE SIP URL.</td>
</tr>
<tr>
<td>Always use proxy</td>
<td>Enum No, Yes</td>
<td>Instant</td>
<td>Defines SIP messages routing rules when SIP Proxy server is used:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>▪ No – use standard SIP routing rules</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>▪ Yes – send all SIP messages and responses to SIP Proxy Server</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Note: Applicable only if Proxy server is used.</td>
</tr>
<tr>
<td>Use Routing Table when Proxy fails</td>
<td>Enum No, Yes</td>
<td>Instant</td>
<td>Defines SIP messages routing rules when SIP Proxy server fails:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>▪ No – Gateway fallback is not used.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>▪ Yes – Internal Tel to IP Routing table is used when Proxy servers are not available.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Default: No.</strong></td>
</tr>
<tr>
<td>Send Invite To Proxy</td>
<td>Enum Disable, Enable</td>
<td>Instant</td>
<td>Defines routing rules for SIP 'INVITE' messages:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>▪ 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).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>▪ Enable – All INVITE messages, including those generated as a result of Transfer or Redirect are sent to Proxy.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Note: Applicable only if Proxy server is used and 'Always Send to Proxy' is disabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Default: Disable.</strong></td>
</tr>
<tr>
<td>Is Trusted Proxy</td>
<td>Enum Disable, Enable</td>
<td>Instant</td>
<td>Defines if SIP Proxy is trusted.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>▪ Disable – SIP Proxy is not Trusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>▪ Enable – SIP Proxy is Trusted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>If the Proxy is not Trusted, the P-asserted header is not used.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Default: Disable.</strong></td>
</tr>
</tbody>
</table>
### Parameter Name
```
Use Gateway Name For Options
```

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Gateway Name For Options</td>
<td>Enum</td>
<td>Instant</td>
<td>Defines Request-URI host part in SIP 'OPTIONS' messages, used for keep-alive with SIP Proxy servers</td>
</tr>
<tr>
<td></td>
<td>Disable, Enable</td>
<td></td>
<td>- Disable – Use the gateway's IP address in keep-alive OPTIONS messages (default).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Enable – Use 'GatewayName' in keep-alive OPTIONS messages.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Default: Disable.</td>
</tr>
</tbody>
</table>

### Proxy DNS Query Type
```
Proxy DNS Query Type
```

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy DNS Query Type</td>
<td>Enum</td>
<td>Instant</td>
<td>Enables the use of DNS Naming Authority Pointer (NAPTR) and Service Record (SRV) queries to discover Proxy servers.</td>
</tr>
<tr>
<td></td>
<td>ARecord, SRV, NAPTR</td>
<td></td>
<td>- If set to A-Record, no NAPTR or SRV queries are performed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- 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.</td>
</tr>
</tbody>
</table>

If the Proxy IP address parameter contains a domain name with port definition (e.g., ProxyIP = 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 DNSQueryType is disabled.
## Proxy Load Balancing Method

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy Load Balancing Method</td>
<td>Enum</td>
<td>Instant</td>
<td>Enables usage of the Proxy Load Balancing mechanism.</td>
</tr>
<tr>
<td></td>
<td>Disable,</td>
<td></td>
<td>- Disable – disable Proxy Load Balancing</td>
</tr>
<tr>
<td></td>
<td>RoundRobin,</td>
<td></td>
<td>- RoundRobin - A list of all possible Proxy IP addresses is compiled. This list includes all</td>
</tr>
<tr>
<td></td>
<td>RandomWeights</td>
<td></td>
<td>entries in the ProxyIP table after necessary DNS resolutions (including NAPTR and SRV, if</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>configured). This list can handle up to 15 entries.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>After this list is compiled, the Proxy Keep-Alive mechanism (according to EnableProxyKeepAlive</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>and ProxyKeepAliveTime) is used to mark each entry as Offline or Online. The balancing is</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>only performed on Proxy servers that are marked as Online. All outgoing messages are equally</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>distributed across the Proxy IP list. REGISTER messages are also distributed unless a RegistrarIP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>is configured. The Proxy IP list is refreshed according to ProxyIPListRefreshTime. If a change</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>in the order of the entries in the list occurs, all load statistics are erased and balancing</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>starts over again.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Random Weights – the outgoing requests are not spread out equally between the Proxies. The</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>weights are received from the DNS server by using SRV records. The gateway sends the requests</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>in such fashion that each Proxy receives a percentage of the requests according to its assigned</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>weight. Load Balancing is not used in the following situations:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- More than one SIP Proxy Server is defined</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- The ProxyIP parameter of the only defined SIP Proxy is an IP address and not an FQDN.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- SRV usage is not enabled ('Proxy DNS Query Type').</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- SRV response includes several records with a different Priority value.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Proxy IP List Refresh Time</th>
<th>Integer</th>
<th>Instant</th>
<th>Defines the time interval (in seconds) between refreshes of the Proxy IP list. This parameter is only used when ProxyLoadBalancingMethod=RoundRobin.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>5-2000000</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
4.13.2 The SIP Registrar

The Media Gateway 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 x 70% = 2520 sec.

To configure SIP Registrar take these 5 steps:

1. Access the **MG Status** screen.
2. Double-click the desired Media Gateway board. The **Media Gateway Board Status** screen appears.
3. Click **SIP**. The **SIP Protocol** screen is displayed.
4. Click **Proxy Settings**. The **SIP Proxy Settings** screen is displayed.
5. In the **Registration Options** tab, configure SIP Registration Parameters, as described in the table below.

### Table 4-28: SIP Registration Parameter

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Registration</td>
<td>Enum</td>
<td>Instant</td>
<td>Enables registration with SIP Proxy/Registrar.</td>
</tr>
<tr>
<td></td>
<td>No, Yes</td>
<td></td>
<td>• No – gateway doesn't register to Proxy/Registrar</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Yes – gateway register to Proxy/Registrar at power up</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Default</strong>: No.</td>
</tr>
<tr>
<td>Registrar IP Address</td>
<td>String</td>
<td>Instant</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Up to 15 chars.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Registration Time</td>
<td>Integer</td>
<td>Instant</td>
<td>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 (%)'.</td>
</tr>
<tr>
<td></td>
<td>10-2000000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Registration Retry Time</td>
<td>Integer</td>
<td>Instant</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>10-2000000</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Parameter Name | Type | Provisioning Type | Description
---|---|---|---
Registrar Name | String Up to 49 chars. | Instant | Registrar Domain Name. If specified, the name is used as Request-URI in REGISTER messages. If isn't 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 x 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 | Use this parameter to assign a name to the device (for example: 'gateway1.com'). Ensure that the name you choose is the one that the Proxy is configured with to identify your Media Gateway. 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 (default).

### 4.13.3 Number Manipulation Tables

The Avaya G860 provides four Number Manipulation tables for incoming and outgoing calls. These tables are used to modify the destination and source telephone numbers so that the calls can be routed correctly.

To access Number Manipulation Tables, take these 4 steps:

1. Access the [MG Status](#) screen.
2. Double-Click on the desired Media Gateway Board. The Board Status screen appears.
3. At the top of the screen, click [SIP](#). The SIP Coders List screen appears.
4. Click [Manipulation](#). The [Dst IP to Tel](#) screen is also open. The four Number Manipulation Tables that can be accessed are:
4. Configuring & Operating the Media Gateway

Table 4-29: Number Manipulation Table

<table>
<thead>
<tr>
<th>SIP Manipulation Table</th>
<th>EMS button</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination Phone Number Manipulation Table for IP to Tel calls</td>
<td>[Dst IP to Tel]</td>
</tr>
<tr>
<td>Destination Phone Number Manipulation Table for Tel to IP call</td>
<td>[Dst Tel to IP]</td>
</tr>
<tr>
<td>Source Phone Number Manipulation Table for IP to Tel calls</td>
<td>[Src IP to Tel]</td>
</tr>
<tr>
<td>Source Phone Number Manipulation Table for Tel to IP calls</td>
<td>[Src Tel to IP]</td>
</tr>
</tbody>
</table>

4.13.3.1  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 Avaya G860 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.

4.13.3.2  Configuring the Number Manipulation Tables

To configure Number Manipulation Tables, take these 7 steps:

1. Access the MG Status screen.
2. Double-Click on the desired Media Gateway Board. The Board Status screen appears.
3. At the top of the screen, click SIP. The SIP Coders List screen appears.
4. Click Manipulation. The SIP screen is also open. The other three Number Manipulation Tables that can be accessed appear at the top of the screen as well.
5. Click the Number Manipulation Table you wish to configure. Its Manipulation List screen is displayed.
6. To add a new Number Manipulation Table entry, Click [+] . The Number Manipulation Provisioning screen is displayed.
7. Configure the Number Manipulation Table entry parameters according to the table below.
## Table 4-30: Number Manipulation Table Parameters

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination Prefix</td>
<td>String</td>
<td>Instant_apply</td>
<td>Each entry in the Destination Prefix fields represents a destination telephone number prefix. An asterisk (*) represents any number.</td>
</tr>
<tr>
<td></td>
<td>Up to 19 chars.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Source Prefix</td>
<td>String</td>
<td>Instant_apply</td>
<td>Each entry in the Source Prefix fields represents a source telephone number prefix. An asterisk (*) represents any number.</td>
</tr>
<tr>
<td></td>
<td>Up to 19 chars.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Source IP</td>
<td>String</td>
<td>Instant_apply</td>
<td>Each entry in the Source IP fields represents the source IP address of the call (obtained from the Contact header in the INVITE message).</td>
</tr>
<tr>
<td></td>
<td>Up to 16 chars.</td>
<td></td>
<td>This column only applies to the 'Destination Phone Number Manipulation Table for IP to Tel'.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Note: The source IP address can include the 'x' wildcard to represent single digits. For example: 10.8.8.xx represents all the addresses between 10.8.8.10 to 10.8.8.99.</td>
</tr>
<tr>
<td>Number of Stripped Digits left</td>
<td>Integer</td>
<td>Instant_apply</td>
<td>Enter the number of digits that you want to remove from the left of the telephone number prefix. For example, if you enter 3 and the phone number is 5551234, the new phone number is 1234. Note that a combination of the two options (this parameter with parameter 'Number of Stripped digits right') is allowed (e.g., 2(3)).</td>
</tr>
<tr>
<td></td>
<td>0-70</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Number of Stripped digits right</td>
<td>Integer</td>
<td>Instant_apply</td>
<td>Enter the number of digits (in brackets) that you want to remove from the right of the telephone number prefix. Note that a combination of the two options (this parameter with parameter 'Number of Stripped digits left') is allowed (e.g., 2(3)).</td>
</tr>
<tr>
<td></td>
<td>0-70</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prefix To Add</td>
<td>String</td>
<td>Instant_apply</td>
<td>Prefix - Enter the number / string you want to add to the front of the phone number. For example, if you enter 9 and the phone number is 1234, the new number is 91234. Note: You can enter a prefix and a suffix in the same field (e.g., 9(00)).</td>
</tr>
<tr>
<td></td>
<td>Up to 49 chars.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Suffix to add</td>
<td>String</td>
<td>Instant_apply</td>
<td>Suffix - Enter the number / string (in brackets) you want to add to the end of the phone number. For example, if you enter (00) and the phone number is 1234, the new number is 123400. Note: You can enter a prefix and a suffix in the same field (e.g., 9(00)).</td>
</tr>
<tr>
<td></td>
<td>Up to 49 chars.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Num Of Digits To Leave</td>
<td>Integer</td>
<td>Instant_apply</td>
<td>Enter the number of digits that you want to leave from the right.</td>
</tr>
<tr>
<td></td>
<td>-1-70</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
4. Configuring & Operating the Media Gateway

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number Plan</td>
<td>Enum NotIncluded, Unknown, E164Public, Private, NotConfigured</td>
<td>Instant_apply</td>
<td>Select the Number Plan assigned to this entry. You can select Unknown [0], Private [9] or E.164 Public [1].</td>
</tr>
<tr>
<td>Number Type</td>
<td>Enum NotIncluded, Unknown, InternationalLevel2Regional, NationalLevel1Regional, NetworkSpecificNetworkPISN, SubscriberLevel0Regional, Abbreviated, NotConfigured</td>
<td>Instant_apply</td>
<td>Select the Number Type assigned to this entry. If you selected Unknown as the Number Plan, you can select Unknown [0]. If you selected Private as the Number Plan, you can select Unknown [0], Level 2 Regional [1], Level 1 Regional [2], PSTN Specific [3] or Level 0 Regional (Local) [4]. If you selected E.164 Public as the Number Plan, you can select Unknown [0], International [1], National [2], Network Specific [3], Subscriber [4] or Abbreviated [6].</td>
</tr>
</tbody>
</table>

4.13.3 Manipulation Rules

The manipulation 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 manipulation 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, refer to Dialing Plan Notation on page 178.
4.13.4 Dialing Plan Notation

The dialing plan notation applies to the four Manipulation tables and to the Telephone to IP Routing table on page 180 and IP to Telephone Routing table on page 183.

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
- 54324xxx# represents a 7 digit number that starts with 54324
- 123[100-200]# represents all numbers from 123100 to 123200.

The Avaya G860 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 Avaya G860 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 Avaya G860 applies rule 1 to all numbers that start with 55 including numbers that start with 551.

4.13.4.1 Numbering Plans and Type of Number

Numbers are classified by their Numbering Plan Indication (NPI) and their Type of Number (TON). The Avaya G860 supports all NPI/TON classifications used in the standard. The list of ISDN ETSI NPI/TON values is shown in the table below.
Table 4-31: NPI/TON Values for ISDN ETSI

<table>
<thead>
<tr>
<th>NPI</th>
<th>TON</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown [0]</td>
<td>Unknown [0]</td>
<td>A valid classification, but one that has no information about the numbering plan.</td>
</tr>
<tr>
<td>E.164 Public [1]</td>
<td>Unknown [0]</td>
<td>A public number in E.164 format, but no information on what kind of E.164 number.</td>
</tr>
<tr>
<td>International [1]</td>
<td></td>
<td>A public number in complete international E.164 format. For example: 16135551234</td>
</tr>
<tr>
<td>National [2]</td>
<td></td>
<td>A public number in complete national E.164 format. For example: 6135551234</td>
</tr>
<tr>
<td>Subscriber [4]</td>
<td></td>
<td>A public number in complete E.164 format representing a local subscriber. For example: 5551234</td>
</tr>
<tr>
<td>Private [9]</td>
<td>Unknown [0]</td>
<td>A private number, but with no further information about the numbering plan</td>
</tr>
<tr>
<td>Level 2 Regional [1]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Level 1 Regional [2]</td>
<td></td>
<td>A private number with a location. For example: 3932200</td>
</tr>
<tr>
<td>PISN Specific [3]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Level 0 Regional (local) [4]</td>
<td></td>
<td>A private local extension number. For example: 2200</td>
</tr>
</tbody>
</table>

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

4.13.5 The Routing Tables

The Routing Tables include the following parts:

Table 4-32: SIP Routing Table

<table>
<thead>
<tr>
<th>SIP Routing Table</th>
<th>EMS Button</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing Settings</td>
<td>☐ Routing Settings</td>
</tr>
<tr>
<td>Telephone To IP Routing Table</td>
<td>☐ Tel to IP</td>
</tr>
<tr>
<td>IP To Telephone Routing Table</td>
<td>☐ IP to Tel</td>
</tr>
<tr>
<td>Internal DNS Table</td>
<td>☐ DNS</td>
</tr>
</tbody>
</table>
To access the Routing Tables, take these 5 steps:

1. Access the screen.
2. Double-Click on the desired Media Gateway Board. The Board Status screen appears.
3. At the top of the screen, click . The SIP Coders List screen appears.
4. Click . The screen is open.
5. To access any of the above mentions Routing Tables, click the appropriate button.

4.13.5.1 Telephone to IP Routing Table

The Tel to IP 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 Avaya G860 (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 corresponding IP address. If the number dialed does not match these prefixes, the call is not made.

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 Avaya G860 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.

4.13.5.2 Telephone to IP Routing Provisioning Rules

- The maximum number of prefixes that can be configured on the Tel to IP Routing Table is 50.

- Any telephone number whose destination number matches the prefix defined in the 'Destination Phone Prefix' field and its source number matches the prefix defined in the adjacent 'Source Phone Prefix' field, is sent to the IP address entered in the 'IP Address' field.

The Tel to IP routing can be performed according to a combination of source and destination phone prefixes, or using each independently.
An additional entry of the same prefixes can be assigned to enable alternative routing.

For available notations that represent multiple numbers, refer to Dialing Plan Notation on page 178.

4.13.5.3 Possible Uses for Telephone to IP Routing

Possible uses for Telephone-to-IP routing include the following:

- Can 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. (Refer to 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 Avaya G860 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 is released.

(Refer to the SIP Protocol Definition screen> Call Security tab> Filter Call to IP parameter and to SIP Routing Properties screen> Use Routing Table for the Host Names parameter.)

- 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.

(Refer to Manipulation or Alternate Tel to IP Alternate IP to Tel.)

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, refer to Alternative Routing Provisioning Rules.
- When a release reason that is defined in the ‘Reasons for Alternative Tel to IP Routing’ table is received. For detailed information, refer to Reasons for Alternative Routing on page 186.

Alternative routing (using this table) is commonly implemented when there is no response to an INVITE message (after INVITE retransmissions). The Avaya G860 then issues an internal 408 ‘No Response’ implicit release reason. If this reason is included in the Alternate Tel to IP table, the Avaya G860 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. Refer to the table, SIP Proxy Settings on page 167 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).

**Tip:** Tel to IP routing can be performed either before or after applying the number manipulation rules. Tel to IP routing can be performed either before or after applying the number manipulation rules.

To control when number manipulation is carried out, set the *TEL to IP routing mode* parameter in SIP Proxy settings.

---

### 4.13.5.3.1 Configuring Telephone to IP Routing

To configure Telephone to IP Routing, take these 6 steps:

1. Access the **MG Status** screen.
2. Double-Click on the desired Media Gateway Board. The Board Status screen appears.
3. At the top of the screen, click **SIP**. The SIP Coders List screen appears.
4. Click **Routing**. The **Tel to IP** screen is open. The Telephone to IP Routing List screen is displayed.
5. To add a new Telephone To IP Routing entry, click **+**. The **Tel to IP Routing Provisioning** screen is displayed.
6. Configure Tel to IP Routing entry parameters according to the table below.

#### Table 4-33: Telephone to IP Routing Table Parameters

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>String Up to 20 chars.</td>
<td>Online</td>
<td>Textual, user-defined name assigned to the entity (MO), enabling users to identify it intuitively and easily.</td>
</tr>
</tbody>
</table>
### 4. Configuring & Operating the Media Gateway

#### 4.13.5.4 IP to Telephone Routing Table

The IP to Telephone 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 combination of the following three options (or using each independently):

- Destination phone prefix
- Source phone prefix
- Source IP address

The call is then sent to the Avaya G860 channels assigned to that trunk group. The specific channel, within a trunk group, that is assigned to accept the call is determined according to the trunk group's channel selection mode which is defined in the Trunk Group Settings Table on page 194, or according to the global parameter Channel Select Mode.

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dest Phone Prefix</td>
<td>String Up to 19 chars.</td>
<td>Offline</td>
<td>Each entry in the Destination Phone Prefix fields represents a called telephone number prefix. The prefix can be 1 to 19 digits long. Any telephone number whose destination number matches the prefix defined in the 'Destination Phone Prefix' field and its source number matches the prefix defined in the adjacent 'Source Phone Prefix' field, is sent to the IP address entered in the 'IP Address' field. Tel to IP routing can be performed according to a combination of source and destination phone prefixes, or using each independently.</td>
</tr>
<tr>
<td>Source Phone Prefix</td>
<td>String Up to 19 chars.</td>
<td>Offline</td>
<td>Each entry in the Source Phone Prefix fields represents a calling telephone number prefix. The prefix can be 1 to 19 digits long. Any telephone number whose destination number matches the prefix defined in the 'Destination Phone Prefix' field and its source number matches the prefix defined in the adjacent 'Source Phone Prefix' field, is sent to the IP address entered in the 'IP Address' field. Note that Tel to IP routing can be performed according to a combination of source and destination phone prefixes, or using each independently.</td>
</tr>
<tr>
<td>Dest Address</td>
<td>String Up to 50 chars.</td>
<td>Offline</td>
<td>Can be in dotted format notation or an FQDN. This field can also include a selected port to use (in the format: &lt;IP Address&gt;:&lt;Port&gt;).</td>
</tr>
<tr>
<td>Profile ID</td>
<td>Integer 0-9</td>
<td>Instant_apply</td>
<td>Number of the Tel profile that is assigned to the source address</td>
</tr>
</tbody>
</table>
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, refer to Alternative Routing Provisioning Rules.

To use trunk groups you must also do the following:

- Assign a trunk group ID to the Avaya G860 E1/T1 B-channels on the Trunk Group Table. For information on how to assign a trunk group ID to a B-channel, refer to Trunk Group Table on page 192.

- Configure the Trunk Group Settings table to determine the method in which new calls are assigned to channels within the trunk groups (a different method for each trunk group can be configured). For information on how to enable this option, refer to Trunk Group Settings Table on page 194.

### 4.13.5.4.1 Configuring IP to Telephone Routing

*To configure IP to Telephone Routing, take these 6 steps:*

1. Access the **MG Status** screen.
2. Double-Click on the desired Media Gateway Board. The Board Status screen appears.
3. At the top of the screen, click **SIP**. The SIP Coders List screen appears.
4. Click **Routing**. The **Tel to IP** screen is open.
5. Click **IP to Tel**. The IP to Telephone Routing List screen is displayed.
6. To add a new IP to Telephone Routing entry, click **+**. The IP to Tel Routing Provisioning screen is displayed.
7. Configure IP to Tel Routing entry parameters according to the table below.

### 4.13.5.4.2 IP to Telephone Routing Provisioning Rules

- 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.

- Any SIP incoming call whose destination number matches the prefix defined in the ‘Destination Phone Prefix’ field and its source number matches the prefix defined in the adjacent ‘Source Phone Prefix’ field and its source IP address matches the address defined in the ‘Source IP Address’ field, is assigned to the trunk group entered in the field to the right of these fields.

- The IP to Tel routing can be performed according to any combination of source / destination phone prefixes and source IP address, or using each independently.
For available notations that represent multiple numbers (used in the prefix columns), refer to Dialing Plan Notation on page 178.

### Table 4-34: IP to Telephone Routing Parameters

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>String Up to 20 chars.</td>
<td>Online</td>
<td>Textual, user-defined name assigned to the entity (MO), enabling users to identify it intuitively and easily.</td>
</tr>
<tr>
<td>Dest Phone Prefix</td>
<td>String Up to 49 chars.</td>
<td>Instant_apply</td>
<td>Each entry in the Destination Phone Prefix fields represents a called telephone number prefix. The prefix can be 1 to 19 digits long. Any telephone number whose destination number matches the prefix defined in the 'Destination Phone Prefix' field and its source number matches the prefix defined in the adjacent 'Source Phone Prefix' field, is sent to the IP address entered in the 'IP Address' field. Tel to IP routing can be performed according to a combination of source and destination phone prefixes, or using each independently.</td>
</tr>
<tr>
<td>Source Phone Prefix</td>
<td>String Up to 49 chars.</td>
<td>Instant_apply</td>
<td>Each entry in the Source Phone Prefix fields represents a calling telephone number prefix. The prefix can be 1 to 19 digits long. Any telephone number whose destination number matches the prefix defined in the 'Destination Phone Prefix' field and its source number matches the prefix defined in the adjacent 'Source Phone Prefix' field, is sent to the IP address entered in the 'IP Address' field.</td>
</tr>
<tr>
<td>Source Address</td>
<td>String Up to 50 chars.</td>
<td>Instant_apply</td>
<td>Source IP address (obtained from the Contact header in the INVITE message).</td>
</tr>
<tr>
<td>Profile ID</td>
<td>Integer 0-9</td>
<td>Instant_apply</td>
<td>Number of the Tel profile that is assigned to the source address</td>
</tr>
<tr>
<td>Trunk Group ID</td>
<td>Integer 1-24</td>
<td>Instant_apply</td>
<td>In each of the Trunk Group ID fields, enter the trunk group ID to which calls that match these prefixes are assigned.</td>
</tr>
</tbody>
</table>

### 4.13.5.5 Internal 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).
4.13.5.5.1 Configuring the Internal DNS Table

To configure the Internal DNS Table, take these 7 steps:

1. Access the [MG Status] screen.
2. Double-Click on the desired Media Gateway Board. The Board Status screen appears.
3. At the top of the screen, click [SIP]. The SIP Coders List screen appears.
4. Click [Routing]. The [Tel to IP] screen is open.
5. Click [DNS]. The Internal DNS Table List screen is displayed.
6. To add new Internal DNS Table entry, click [+]. The Internal DNS Provisioning screen is displayed.
7. Configure the Internal DNS Table entry parameters as described in table below.

Table 4-35: Internal DNS Table Parameters

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>String</td>
<td>Online</td>
<td>Textual, user-defined name assigned to the entity (MO), enabling users to identify it intuitively and easily.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>String</td>
<td>Instant_apply</td>
<td>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.</td>
</tr>
<tr>
<td>First IP Address</td>
<td>IP Address</td>
<td>Instant_apply</td>
<td>First IP address assigned to a hostname.</td>
</tr>
<tr>
<td>Second IP Address</td>
<td>IP Address</td>
<td>Instant_apply</td>
<td>Second IP address assigned to a hostname.</td>
</tr>
</tbody>
</table>

4.13.5.6 Reasons for Alternative Routing

The Reasons for Alternative Routing are defined via two tables - 'Alternate Tel to IP' and 'Alternate IP to Tel'.

Table 4-36: Alternative Routing Table

<table>
<thead>
<tr>
<th>Alternative Routing Table</th>
<th>EMS Button</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reasons for Alternative Telephone To IP Routing Table</td>
<td>[Alternate Tel to IP]</td>
</tr>
<tr>
<td>Reasons for Alternative IP To Telephone Routing Table</td>
<td>[Alternate IP to Tel]</td>
</tr>
</tbody>
</table>
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 Avaya G860 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.

Refer to Telephone to IP Routing Table on page 180 for information on defining an alternative IP address. Refer to IP to Telephone Routing Table on page 183 for information on defining an alternative trunk group.

4.13.5.6.1 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 the SIP > Routing > Routing Settings screen.

4.13.5.6.2 Configuring Alternative Routing

To configure Alternative Routing, take these 7 steps:

1. Access the MG Status screen.
2. Double-Click on the desired Media Gateway Board. The Board Status screen appears.
3. At the top of the screen, click SIP. The SIP Coders List screen appears.
4. Click Routing. The Tel to IP screen is open.
5. Click the alternative Routing table that you wish to configure (either Alternate Tel to IP or Alternate IP to Tel). Its Alternative Routing Table List screen is displayed.
6. To add a new Alternative Routing Table entry, click The Alternative Routing Provisioning screen is displayed.
7. Configure the Alternative Routing Table entry parameters according to the table below.

**Table 4-37: Alternative Routing Parameters**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>String</td>
<td>Online</td>
<td>Textual, user-defined name assigned to the entity (MO), enabling users to identify it intuitively and easily.</td>
</tr>
</tbody>
</table>
### Parameter Table

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Cause</td>
<td>Integer 0-232</td>
<td>Read-Only</td>
<td>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).</td>
</tr>
</tbody>
</table>

### 4.13.5.7 SIP to ISDN Cause and ISDN to SIP Cause Table

The SIP to ISDN Cause and ISDN to SIP Cause tables enable the Avaya G860 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 5000 Programmer’s User Manual - Document # LTRT-914xx*).

**Table 4-38: SIP / ISDN Cause Mapping Tables**

<table>
<thead>
<tr>
<th>SIP / ISDN Cause Mapping Tables</th>
<th>EMS Button</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP to ISDN Cause Mapping</td>
<td>[ISDN to SIP Cause Map]</td>
</tr>
<tr>
<td>ISDN to SIP Cause Mapping</td>
<td>[SIP to ISDN Cause Map]</td>
</tr>
</tbody>
</table>

### 4.13.5.8 Configuring SIP / ISDN Cause Mapping

To configure SIP / ISDN Cause Mapping, take these 6 steps:

1. Access the **MG Status** screen.
2. Double-Click on the desired Media Gateway Board. The Board Status screen appears.
3. At the top of the screen, click **SIP** and **Coders**. The SIP Coders List screen is also open.
4. Click the SIP / ISDN Cause Mapping table that you wish to configure (either [ISDN to SIP Cause Map] or [SIP to ISDN Cause Map]). Its SIP / ISDN Cause Mapping Table List screen is displayed.
5. To add new SIP / ISDN Cause Mapping entry, click [+] . The SIP / ISDN Cause Mapping Provisioning screen is displayed.
6. Configure the SIP / ISDN Cause Mapping entry parameters according to the tables below.
4. Configuring & Operating the Media Gateway

### Table 4-39: SIP to ISDN Cause Mapping Parameters

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>String</td>
<td>Online</td>
<td>Define a name (string) to be assigned to the entity.</td>
</tr>
<tr>
<td>SIP Response</td>
<td>Integer 400-700</td>
<td>Instant_apply</td>
<td>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.</td>
</tr>
<tr>
<td>Q850 Cause</td>
<td>Integer 0-127</td>
<td>Instant_apply</td>
<td>Defines a flexible mapping of SIP Responses and Q.850 Release Causes.</td>
</tr>
</tbody>
</table>

### Table 4-40: ISDN to SIP Cause Mapping Parameters

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>String</td>
<td>Online</td>
<td>Define a name (string) to be assigned to the entity.</td>
</tr>
<tr>
<td>Q850 Cause</td>
<td>Integer 0-127</td>
<td>Instant_apply</td>
<td>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.</td>
</tr>
<tr>
<td>SIP Response</td>
<td>Integer 400-700</td>
<td>Instant_apply</td>
<td>Defines a flexible mapping of Q.850 Release Causes and SIP Responses.</td>
</tr>
</tbody>
</table>

### 4.13.6 Coders Table

Use the Coders table to define the first to fifth preferred coders (and their attributes). 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.
4.13.6.1 Configuring Coders Table

To configure Coders Table, take these 5 steps:

1. Access the MG Status screen.
2. Double-Click on the desired Media Gateway Board. The Board Status screen appears.
3. At the top of the screen, click Coders. The screen is open. The SIP Coders List screen appears.
4. To add new Coder, Click Coders. The Coder Provisioning screen is displayed.
5. Configure the Coder parameters according to the table below.

Table 4-41: Coder Parameters

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>String Up to 20 chars.</td>
<td>Online</td>
<td>Textual, user-defined name assigned to the entity (MO), enabling users to identify it intuitively and easily.</td>
</tr>
</tbody>
</table>
### 4. Configuring & Operating the Media Gateway

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coder Name</td>
<td>Enum G711Alaw64k, G711Ulaw64k, G729, G7231, G726, GsmFr, GsmEfr, MsGsm, NetCoder, Amr, Evrc, Transparent, Qcelp, Ilbc, EvrcB, G722, AmrWb, T38, G711AlawVbd, G711UlawVbd</td>
<td>Instant_apply</td>
<td>Coder name. Each Coder Name may appear in Coder Table only once. Note: The two codecs which Communication Manager supports on a system-wide interoperability basis are G711 and G729.</td>
</tr>
<tr>
<td>Packetization Time</td>
<td>Enum default, t10ms, t20ms, t30ms, t40ms, t50ms, t60ms, t70ms, t80ms, t90ms, t100ms, t110ms, t120ms, t130ms, t140ms, t150ms</td>
<td>Instant_apply</td>
<td>Packetization time (in milliseconds). Determines how many coder payloads are combined into a single RTP packet. If not specified, the ptime gets a default value. The ptime specifies the packetization time the gateway expects to receive. The gateway always uses the ptime requested by the remote side for sending RTP packets. Note: For optimum performance, select either t20ms or t30ms.</td>
</tr>
<tr>
<td>Coder Rate</td>
<td>Enum default, r4dot75, r5dot15, r5dot3, r6dot3, r6dot4, r6dot6, r6dot7, r7dot2, r7dot4, r7dot95, r8, r8dot8, r8dot85, r10dot2, r12dot2, r12dot65, r13, r14dot25, r15, r15dot85, r16, r18dot25, r19dot85, r23dot05, r23dot85, r24, r32, r40, r48, r56, r64, r1over8, r1over4, r1over2, variable, full</td>
<td>Instant_apply</td>
<td>Coder Bit Rate (in Kbps).</td>
</tr>
<tr>
<td>Payload Type</td>
<td>Integer 0-120</td>
<td>Instant_apply</td>
<td>Payload type. Applicable to coders with dynamic payload only. Specifies the format of the RTP payload. If not specified – a default is used.</td>
</tr>
</tbody>
</table>
### 4.13.7 Trunk Group 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 Telephone calls with common rules. Channels that are not defined are disabled.

#### 4.13.7.1 Configuring Trunk Group Table

➢ **To configure Trunk Group Table, take these 6 steps:**

1. Access the `MG Status` screen.
2. Double-Click on the desired Media Gateway board. The Media Gateway Board Status screen appears.
3. At the top of the screen, click `SIP` and `SIP Protocol`. The screen is open. The SIP Coders List screen appears.
4. Click `Trunk Groups`. The Trunk Groups List screen is displayed.
5. To add a new Trunk Group, click `+`. The Trunk Group Provisioning screen is displayed.
6. Configure the Trunk Group parameters according to the table below.

### Table 4-42: Trunk Group Parameters

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>String Up to 20 chars.</td>
<td>Online</td>
<td>Textual, user-defined name assigned to the entity (MO), enabling users to identify it intuitively and easily.</td>
</tr>
</tbody>
</table>
## 4. Configuring & Operating the Media Gateway

### Parameter Name | Type | Provisioning Type | Description
--- | --- | --- | ---
Trunk Group ID | Integer 1-24 | Offline | In each of the Trunk Group ID fields, enter the trunk group ID (1-99) 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 Routing Table (assigns incoming IP calls to the appropriate trunk group). If you do not configure the IP to Tel Routing Table, calls do not complete.

First Trunk ID | Integer 1-84 | Offline | Starting physical trunk number.

Last Trunk ID | Integer 1-84 | Offline | Ending physical trunk number.

Starting Channel | Integer 1-31 | Offline | Starting trunk’s B-channel.

Ending Channel | Integer 1-31 | Offline | 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).

Starting Phone Number | String Up to 19 chars. | Offline | In each of the Phone Number fields, enter the first number in an ordered sequence that is assigned to the range of channels defined in the adjacent 'Channels' field.

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).
4.13.8  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.

(Refer to PSTN Interworking tab.)

4.13.8.1  Configuring Trunk Group Settings Table

➢ To configure Trunk Group Settings Table, take these 6 steps:

1. Access the MG Status screen.
2. Double-Click on the desired Media Gateway Board. The Board Status screen appears.
3. At the top of the screen, click SIP. The screen is open. The SIP Coders List screen appears.
4. Click Trunk Group Settings. The Trunk Group Settings List screen is displayed.
5. To add a new Trunk Group Settings entry, click . The Trunk Group Settings Provisioning screen is displayed.
6. Configure the Trunk Group Settings parameters according to the table below.

Table 4-43: Trunk Group Settings Parameters

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>String Up to 20 chars.</td>
<td>Online</td>
<td>Textual, user-defined name assigned to the entity (MO), enabling users to identify it intuitively and easily.</td>
</tr>
<tr>
<td>Trunk Group ID</td>
<td>Integer 1-24</td>
<td>Instant_appl_y</td>
<td>Trunk Group ID number.</td>
</tr>
</tbody>
</table>
### 4. Configuring & Operating the Media Gateway

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channel Select Mode</td>
<td>Enum</td>
<td>Instant_apply</td>
<td>Determines the method in which new calls are assigned to B-channels within the Trunk group.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- By phone number – Select the gateway port according to the called number, defined in the Trunk Group table.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- 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 gateway reaches the highest channel number in the Trunk Group, it selects the lowest channel number in the Trunk Group and then starts ascending again.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Cyclic Descending – Select the next available channel in descending cycle order. Always select the next lower channel number in the Trunk Group. When the gateway reaches the lowest channel number in the Trunk Group, it selects the highest channel number in the Trunk Group and then starts descending again.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Number + Cyclic Ascending – First select the gateway port according to the called number (refer to 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- AccordingToSourceNumberSelect – Select the gateway port according to the calling number.</td>
</tr>
</tbody>
</table>

#### 4.13.9 Profiles Tables

Utilizing the Profiles feature, the Avaya G860 provides high-level adaptation when connected to a variety of equipment (from both Tel and IP sides) and protocols, each of which requires different system behavior. Using Profiles, users can assign different
Profiles (behavior) on a per-call basis, using the Tel to IP and IP to Tel Group Routing tables, or associate different Profiles to the gateway’s B-channels. The Profiles contain parameters such as: Coders; T.38 Relay; Voice and DTMF Gains; Silence Suppression; Echo Cancellor; RTP DiffServ; and Current Disconnect. The Profiles feature allows users to tune these parameters or to enable/disable them, per source or destination routing and/or the specific gateway or its ports. For example, specific ports can be designated to have a profile which always uses G.711.

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.

<table>
<thead>
<tr>
<th>SIP Profiles Table</th>
<th>EMS Button</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coders Table</td>
<td><img src="#" alt="SIP Protocol" /> <img src="#" alt="Coders" /></td>
</tr>
<tr>
<td>Telephone Profile Table</td>
<td><img src="#" alt="Trunk Groups" /> <img src="#" alt="Tel Profile" /></td>
</tr>
<tr>
<td>IP Profile Table</td>
<td><img src="#" alt="Routing" /> <img src="#" alt="IP Profile" /></td>
</tr>
</tbody>
</table>

### 4.13.9.1 Coders Table

Use the Coders table to define the first to fifth preferred coders (and their attributes). 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.

#### Note 1:
Each coder may be defined only once in the table.

#### Note 2:
The ptime specifies the packetization time the gateway expects to receive. The gateway always uses the ptime requested by the remote side for sending RTP packets.

#### Note 3:
Only the ptime of the first coder in the defined coder list is declared in INVITE / 200 OK SDP, even if multiple coders are defined.

#### Note 4:
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 (IsCiscoSCEMode).

### 4.13.9.2 Configuring Coders Table

To configure Coders Table, take these 5 steps:

1. Access the ![MG Status](#) screen.

196 Installation & Operation Manual
2. Double-Click on the desired Media Gateway Board. The Board Status screen appears.

3. At the top of the screen, click the [Coders] button. The Coders screen is open. The SIP Coders List screen appears.

4. To add new Coder, click the [+] button. The Coder Provisioning screen is displayed.

5. Configure the Coder parameters according to the table below.

### Table 4-45: Coder Parameters

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>String Up to 20 chars.</td>
<td>Online</td>
<td>Textual, user-defined name assigned to the entity (MO), enabling users to identify it intuitively and easily.</td>
</tr>
<tr>
<td>Coder Name</td>
<td>Enum G711Alaw64k, G711Ulaw64k, G729, G7231, G726, GsmFr, GsmEfr, MsGsm, NetCoder, Amr, Evrc, Transparent, Qcelp, Ilbc, EvrcB, G722, AmrWb, T38, G711AlawVbd, G711Ul awVbd</td>
<td>Instant_apply</td>
<td>Coder name. Each Coder Name may appear in Coder Table only once.</td>
</tr>
<tr>
<td>Packetization Time</td>
<td>Enum default, t10ms, t20ms, t30ms, t40ms, t50ms, t60ms, t70ms, t80ms, t90ms, t100ms, t110ms, t120ms, t130ms, t140ms, t150ms</td>
<td>Instant_apply</td>
<td>Packetization time (in milliseconds). Determines how many coder payloads are combined into a single RTP packet. If not specified, the $ptime$ gets a default value. The $ptime$ specifies the packetization time the gateway expects to receive. The gateway always uses the $ptime$ requested by the remote side for sending RTP packets.</td>
</tr>
</tbody>
</table>
Avaya G860 Media Gateway

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coder Rate</td>
<td>Enum</td>
<td>Instant_apply</td>
<td>Coder Bit Rate (in Kbps).</td>
</tr>
<tr>
<td></td>
<td>default, r4dot75,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>r5dot15, r5dot3,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>r5dot9, r6dot3,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>r6dot4, r6dot6,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>r6dot7, r7dot2,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>r7dot4, r7dot95,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>r8, r8dot8, r8dot85,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>r10dot2, r12dot2,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>r12dot65, r13, r14dot25, r15, r15dot85, r16, r18dot25, r19dot85, r23dot05, r23dot85, r24, r32, r40, r48, r56, r64, r1over8, r1over4, r1over2, variable, full</td>
<td>Instant_apply</td>
<td>Payload type. Applicable to coders with dynamic payload only. Specifies the format of the RTP payload. If not specified – a default is used.</td>
</tr>
<tr>
<td>Silence Suppression</td>
<td>Enum</td>
<td>Instant_apply</td>
<td>Enables/disables the silence suppression. For G.729 it is also possible to select the silence suppression without adaptations.</td>
</tr>
<tr>
<td></td>
<td>Disable, Enable, EnableWithoutAdaptations</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4.13.9.3 Tel Profile Table

Use the Tel Profile table to define up to four different Tel Profiles. These Profiles are used in the Trunk Group Table to associate different Profiles to the gateway’s channels, thereby applying different behavior to different channels.

➢ To configure Tel Profile Table, take these 6 steps:

1. Access the MG Status screen.
2. Double-Click on the desired Media Gateway board. The Media Gateway Board Status screen appears.
3. At the top of the screen, click SIP > Trunk Groups. The Trunk Group screen is displayed.
4. Click Tel Profile. The Tel Profiles List screen is displayed.
5. To add a new Tel Profile, click . The Tel Profile Provisioning screen is displayed.
6. Configure the Tel Profile parameters according to the table below.

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>String</td>
<td>Online</td>
<td>Textual, user-defined name assigned to the entity (MO), enabling users to identify it intuitively and easily.</td>
</tr>
<tr>
<td>Preference</td>
<td>Integer</td>
<td>Instant_apply</td>
<td>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.</td>
</tr>
<tr>
<td>Coders Group ID</td>
<td>Integer</td>
<td>Instant_apply</td>
<td>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.</td>
</tr>
<tr>
<td>Parameter Name</td>
<td>Type</td>
<td>Provisioning Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>------</td>
<td>-------------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Is Fax Used    | Enum NoFax, T38, G711, FallBack | Instant_apply | 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 (refer to note 1).  
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).  
**Note 1:** Fax adaptations:  
Echo Canceller = On  
Silence Compression = Off  
Echo Canceler Non-Linear Processor Mode = Off  
Dynamic Jitter Buffer Minimum Delay = 40  
Dynamic Jitter Buffer Optimization Factor = 13  
**Note 2:** 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'.  
**Note 3:** When 'IsFaxUsed' is set to any value besides NoFax the parameter 'FaxTransportMode' is ignored.  
**Note 4:** 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_apply | Dynamic jitter buffer minimum delay in msec. |
Note: Set to 13 for data (fax & modem) calls. |
### 4. Configuring & Operating the Media Gateway

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Diff Serv</td>
<td>Integer</td>
<td>Instant_apply</td>
<td>Sets the Diff Serv value for Premium Media service class content (only if IP Diff Serv is not set in the selected IP Profile).</td>
</tr>
<tr>
<td></td>
<td>0-63</td>
<td></td>
<td>Note: The value for the Premium Control Diff Serv is determined by (according to priority):</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1. IPDiffServ value in the selected IP Profile.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2. Premium Service Class Media Diff Serv.</td>
</tr>
<tr>
<td>Sig IP Diff Serv</td>
<td>Integer</td>
<td>Instant_apply</td>
<td>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).</td>
</tr>
<tr>
<td></td>
<td>0-63</td>
<td></td>
<td>Note: The value for the Premium Control Diff Serv is determined by (according to priority):</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1. ‘Control IP Diff serv’ value in the selected IP Profile.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2. Premium Service Class Control Diff Serv.</td>
</tr>
<tr>
<td>Voice Volume</td>
<td>Integer</td>
<td>Instant_apply</td>
<td>Voice gain control in dB. Sets the level for the transmitted (IP to PSTN) signal.</td>
</tr>
<tr>
<td></td>
<td>0-63</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DTMF Volume</td>
<td>Integer</td>
<td>Instant_apply</td>
<td>DTMF gain control in dBm.</td>
</tr>
<tr>
<td></td>
<td>0-31</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Input Gain</td>
<td>Integer</td>
<td>Instant_apply</td>
<td>PCM input gain control in dB. Sets the level for the received (PSTN-IP) signal.</td>
</tr>
<tr>
<td></td>
<td>0-63</td>
<td></td>
<td>Note: This parameter is intended for advanced users. Changing it affects other gateway functionalities.</td>
</tr>
<tr>
<td>Enable Digit Delivery</td>
<td>Enum</td>
<td>Instant_apply</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Disable,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enable</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Parameter Name | Type | Provisioning Type | Description
--- | --- | --- | ---
ECE | Enum Disable, Enable | Instant_apply | Enable/disable Echo Canceller.
Flash Hook Period | Integer 25-1500 | Instant_apply | Defines the flash-hook period (in msec)
Enable Early Media | Enum Disable, Enable | Instant_apply | 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_apply | 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.

### 4.13.9.4 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, take these 6 steps:

1. Access the MG Status screen.
2. Double-Click on the desired Media Gateway board. The Media Gateway Board Status screen appears.
3. At the top of the screen, click Routing List screen is displayed.
4. Click IP Profile. The IP Profiles List screen is displayed.
5. To add a new Tel Profile, click. The IP Profile Provisioning screen is displayed.
6. Configure the IP Profile parameters according to the table below.

Table 4-47: IP Profiles Parameters

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>String</td>
<td>Online</td>
<td>Textual, user-defined name assigned to the entity (MO), enabling users to identify it intuitively and easily.</td>
</tr>
<tr>
<td>Preference</td>
<td>Integer</td>
<td>Instant_apply</td>
<td>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.</td>
</tr>
<tr>
<td>Coders Group ID</td>
<td>Integer</td>
<td>Instant_apply</td>
<td>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.</td>
</tr>
<tr>
<td>Parameter Name</td>
<td>Type</td>
<td>Provisioning Type</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------</td>
<td>-------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Is Fax Used</td>
<td>Enum</td>
<td>Instant_apply</td>
<td>Determines the SIP signaling method used to establish and convey a fax session after a fax is detected.</td>
</tr>
<tr>
<td></td>
<td>NoFax, T38, G711, FallBack</td>
<td></td>
<td>NoFax = No fax negotiation using SIP signaling (default).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>T38 = Initiates T.38 fax relay.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>G711 = Initiates fax using the coder G.711 A-law/m-law with adaptations (refer to note 1).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>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).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Note 1:</strong> T.38 fax relay is the only method that can reliably guarantee interworking with a wide variety of fax client applications.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Note 2:</strong> Fax adaptations:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Echo Canceller = On</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Silence Compression = Off</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Echo Canceler Non-Linear Processor Mode = Off</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Dynamic Jitter Buffer Minimum Delay = 40</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Dynamic Jitter Buffer Optimization Factor = 13</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Note 3:</strong> If the gateway initiates a fax session using G.711, a 'gpmd' attribute is added to the SDP in the following format:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For A-law: 'a=gpmd:0 vbd=yes;ecan=on'.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For m-law: 'a=gpmd:8 vbd=yes;ecan=on'.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Note 4:</strong> When 'IsFaxUsed' is set to any value besides NoFax the parameter 'FaxTransportMode' is ignored.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Note 5:</strong> 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.</td>
</tr>
<tr>
<td>DJ Buf Min</td>
<td>Delay Integer</td>
<td>Instant_apply</td>
<td>Dynamic jitter buffer minimum delay in msec.</td>
</tr>
<tr>
<td>0-150</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0-13</td>
<td></td>
<td></td>
<td>Note: Set to 13 for data (fax &amp; modem) calls.</td>
</tr>
<tr>
<td>Parameter Name</td>
<td>Type</td>
<td>Provisioning Type</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>------------</td>
<td>-------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IP Diff Serv</td>
<td>Integer</td>
<td>Instant_apply</td>
<td>Sets the Diff Serv value for Premium Media service class content (only if IP Diff Serv is not set in the selected IP Profile).</td>
</tr>
<tr>
<td></td>
<td>0-63</td>
<td></td>
<td>Note: The value for the Premium Control Diff Serv is determined by (according to priority):</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1. IPDiffServ value in the selected IP Profile.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2. Premium Service Class Media Diff Serv.</td>
</tr>
<tr>
<td>Sig IP Diff Serv</td>
<td>Integer</td>
<td>Instant_apply</td>
<td>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).</td>
</tr>
<tr>
<td></td>
<td>0-63</td>
<td></td>
<td>Note: The value for the Premium Control Diff Serv is determined by (according to priority):</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1. 'Control IP Diff serv' value in the selected IP Profile.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2. Premium Service Class Control Diff Serv.</td>
</tr>
<tr>
<td>Silence Suppression Mode</td>
<td>Integer</td>
<td>Instant_apply</td>
<td>Silence Suppression Mode</td>
</tr>
<tr>
<td></td>
<td>0-2</td>
<td></td>
<td>0 - Silence Suppression disabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - Silence Suppression enabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 - Enable without adaptation. A single silence packet is sent during silence period (applicable only to G.729).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>EnableSilenceSuppression = 0 to 'annexb=no'.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>EnableSilenceSuppression = 1 to 'annexb=yes'.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>EnableSilenceSuppression = 2 and IsCiscoSCEMode = 0 to 'annexb=yes'.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>EnableSilenceSuppression = 2 and IsCiscoSCEMode = 1 to 'annexb=no'.</td>
</tr>
<tr>
<td>RTP Redundancy Depth</td>
<td>Integer</td>
<td>Instant_apply</td>
<td>RTP Redundancy Depth.</td>
</tr>
<tr>
<td></td>
<td>0-1</td>
<td></td>
<td>0 - disable generation of redundant packets</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - enable generation of RFC 2198 redundancy packets.</td>
</tr>
<tr>
<td>Parameter Name</td>
<td>Type</td>
<td>Provisioning Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------</td>
<td>-------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Remote Base</td>
<td>Integer</td>
<td>Instant_apply</td>
<td>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.</td>
</tr>
<tr>
<td>UDP Port</td>
<td>Integer</td>
<td>0-64000</td>
<td></td>
</tr>
<tr>
<td>CNG Mode</td>
<td>Enum</td>
<td>Instant_apply</td>
<td>Comfort Noise Generation Mode</td>
</tr>
<tr>
<td></td>
<td>Disable,</td>
<td></td>
<td><strong>Disable</strong> - The originating gateway doesn’t detect CNG, the CNG signal passes transparently to the remote side.</td>
</tr>
<tr>
<td></td>
<td>Relay</td>
<td></td>
<td><strong>Relay</strong> - 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).</td>
</tr>
<tr>
<td></td>
<td>EventsOnly</td>
<td></td>
<td><strong>Events Only</strong> - 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.</td>
</tr>
<tr>
<td>Vxx Transport Type</td>
<td>Enum</td>
<td>Instant_apply</td>
<td>V.21/V.22/V.23/V.32/V.34 Modem Transport Type</td>
</tr>
<tr>
<td></td>
<td>Disable,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Relay</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Bypass</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>EventsOnly</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parameter Name</td>
<td>Type</td>
<td>Provisioning Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>---------------</td>
<td>-------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>NSE Mode</td>
<td>Enum Disable, Enable</td>
<td>Instant_apply</td>
<td>Enables/disables Cisco compatible fax and modem bypass mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Note 1: This feature can be used only if VxxModemTransportType=2 (Bypass)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Note 2: If NSE mode is enabled the SDP contains the following line: 'a=rtpmap:100 X-NSE/8000'</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Note 3: To use this feature:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The Cisco gateway must include the following definition: 'modem passthrough nse payload-type 100 codec g711alaw'.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Set the Modem transport type to Bypass mode (VxxModemTransportType=2) for all modems.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Configure the gateway parameter NSEPayloadType=100</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>In NSE bypass mode the gateway starts using G.711 A-Law (default) or G.711u-Law, according to the parameter FaxModemBypassCoderType.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>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).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The parameters defining payload type for the 'old' Avaya Bypass mode FaxBypassPayloadType and ModemBypassPayloadType are not used with NSE Bypass.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The bypass packet interval is selected according to the parameter FaxModemBypassBasicRtpPacketInterval</td>
</tr>
<tr>
<td>Parameter Name</td>
<td>Type</td>
<td>Provisioning Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>------------</td>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Play RB Tone to IP</td>
<td>Enum</td>
<td>Instant_apply</td>
<td>Enables/disables play of ringback 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 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 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. <strong>Note 1:</strong> To enable the gateway to send a 183/180+SDP responses, set EnableEarlyMedia to 1. <strong>Note 2:</strong> If EnableDigitDelivery = 1, the gateway doesn’t play a Ringback tone to IP and doesn’t send 183 or 180+SDP responses.</td>
</tr>
<tr>
<td>Enable Early Media</td>
<td>Enum</td>
<td>Instant_apply</td>
<td>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.</td>
</tr>
</tbody>
</table>
4. Configuring & Operating the Media Gateway

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| Progress Indicator to IP             | Enum        | Instant_apply     | **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. |

4.14 Configuring Security Settings

The Avaya G860 Media Gateway provides numerous security-related features that enable secure operation in a hostile networking environment and provide interworking with secured 3rd party servers.

The following features are available:

<table>
<thead>
<tr>
<th>Feature/Protocol Name</th>
<th>Purpose</th>
<th>Secure Operation Mode</th>
<th>Provisioning Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH/SCP/SFTP</td>
<td>Security for CLI management interface. For more information, refer to SSH/SCP/SFTP on page 228.</td>
<td>Not Required</td>
<td>Not Required</td>
</tr>
<tr>
<td>SSL/TLS</td>
<td>Security for SIP call control traffic. For more information, refer to SSL/TLS.</td>
<td>Optional</td>
<td>Required</td>
</tr>
<tr>
<td>Media Security</td>
<td>Security for voice traffic. For more information, refer to Media Security on page 229.</td>
<td>Optional</td>
<td>Required</td>
</tr>
<tr>
<td>Firewall functionality</td>
<td>Filtering of unwanted inbound traffic on Media Gateway boards. For more information, refer to Configuring Firewall Functionality on page 231.</td>
<td>Optional</td>
<td>Required</td>
</tr>
<tr>
<td>OS patching</td>
<td>Latest OS security patches for SC boards. For more information, refer to OS Patching on page 233.</td>
<td>Optional</td>
<td>Not Required</td>
</tr>
</tbody>
</table>
### Limited Root Access

Media Gateway software version 5.2 and above does not enable you to directly login as a root user over a remote terminal connection (either over a Telnet or SSH connection) to the SC board. This is a common security measure that reduces system vulnerability to remote hacker attacks.

If you need to perform actions with root permissions, instead you must do one of the following:

- Login from RS-232 console (this requires physical presence on the site where equipment is installed or access via Terminal Server that must be properly secured).
- Login from Telnet or SSH as a regular CLI user (see Users on SC Board’s Terminal on page 92) and run `su – root` command to switch current user to root account.

### Enabling a Direct Remote Root Login

If due to exceptional circumstances, you need to enable remote root login to the SC boards, this can be done by running the tools user script.

**Note:** Enabled remote root login constitutes a severe security flaw, therefore after completing the maintenance task, it is strongly recommended that remote root login should be immediately disabled.
To enable direct remote ROOT login, take these 6 steps:

1. Connect to the 1st SC board via the Telnet, SSH, or RS-232 console. For more information, refer to Connecting to the SC Board’s Terminal on page 89.

2. Login as the root user. For more information, refer to Users on SC Board’s Terminal on page 92.

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
   remote_root_login -- REMOTE ROOT LOGIN: enable/disable remote root user login
   ```

4. At the Choose submenu prompt, type remote_root_login and press Enter. The REMOTE ROOT LOGIN menu appears.

   ```
   Choose submenu : remote_root_login
   -------------------------
   REMOTE ROOT LOGIN
   -------------------------
   ```

5. At the Enable/Disable Remote root Login prompt, type enable and press Enter. Remote root login is enabled on the 1st SC board.

   ```
   Enable/Disable Remote root Login ([disable]/enable) : enable
   ```
   Remote root login was enabled.

6. Repeat steps 1–5 on the 2nd SC board to enable root access to it as well.
4.14.1.2 Disabling a Direct Remote Root Login

This section describes how to disable the remote root login. You should perform this procedure as a result of the following circumstance:

- If you have manually enabled the remote root login, it should be disabled as soon as possible after you have performed required actions.

Note: Enabled direct remote root login constitutes a severe security flaw. Therefore, Media Gateway should be configured to disable remote root login in all field deployments.

➢ To disable a direct remote ROOT login, take these steps:

- Repeat the steps described in Enabling a Direct Remote Root Login on page 210; however at the Enable/Disable Remote root Login prompt, type disable and press Enter.

4.14.2 Secure Operation Mode

The Avaya G860 Media Gateway must be configured for Secure Operation mode prior to enabling other specific security-related features. For more information, refer to Configuring Security Settings on page 209.

Secure Operation mode must be configured via CLI (SSH or RS232 console). Further configuration may be performed both via SNMP interface (EMS GUI) and CLI.

Note: To configure the Secure Operation mode, the Media Gateway's service must be stopped.

In Secure Operation mode, communication with all SNMP managers (including the EMS server) is protected via IPSEC/IKE protocols. An IKE pre-shared key must be configured for each SNMP manager and EMS server in particular. The same key must be provisioned in the SNMP manager (and EMS server) to enable communication with the Media Gateway.

Note: Secure Operation mode enforces secure IPSEC/IKE communication only on SNMP managers that access Media Gateway board's MIB via GET/SET SNMP primitives – i.e. EMS and NMS servers. The OSS server may be configured to receive unencrypted and unsecured SNMP traps even when the Media Gateway operates in secure operation mode.

All insecure CLI management interfaces (Telnet and FTP) are disabled in Secure Operation mode. Secure management tools (SSH, SCP and SFTP) are used instead.
4.14.2.1 Enabling Secure Operation Mode

To enable Secure Operation Mode, take these 5 steps:

1. Connect to both of the SC boards via the Secure Shell (SSH) or RS232 console. For more information, refer to Connecting to the SC Board's Terminal on page 89.

   Note: Secure operation mode can not be configured via Telnet.

2. Login as root user. For more information, refer to Users on SC Board's Terminal on page 92.

3. On both of the SC board, stop the software using the command, tools sc dn.

4. On the 1st SC board:
   a. Run the installation script /install.pl.
   b. Select option 3 – Change installed configuration.
   c. For Enable Security, select y.
   d. Provide the IKE pre-shared key for the EMS server.
   e. Change the root password to your own selection.
   f. Modify the SNMP read/write community strings.

   Note: The Media Gateway with enabled Security must be defined accordingly in the EMS. The same IKE Pre-Shared Key must be entered in the MG Information screen.

5. On the 2nd SC board
   a. Run the installation script /install.pl.
   b. Select option 4 – Copy configuration from 1st SC.
   c. Provide the name of any CLI user, password and the root password set on the 1st SC (the one you changed earlier). For more information, refer to 'Connecting to the SC Board's Terminal'.
   d. The rest of the configuration, including security settings, is copied from the 1st SC board.

6. Reboot both SC boards.

   Note: Secure Operation Mode can also be enabled during the Initial Installation or during First Time Configuration.
4.14.2.2 Disabling Secure Operation Mode

To disable Secure Operation Mode, take this step:

- Repeat the same steps as described in Enabling Secure Operation Mode on page 213; however at the Enable Security, select n and press Enter.

4.14.3 X.509 Certificates

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 being 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. The keys are related mathematically, but the Private Key cannot be practically derived from the Public Key. A message encrypted with the Public Key can be decrypted only with the corresponding 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 trust relationship 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 a certificate from the other party is received, it’s signing entity (CA) is compared with the Trusted Root Certificates list and if the match is found, the certificate is accepted.

Applications that Use X.509 Certificates

In the Avaya G860 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 SC and 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 MEGACO/MGCP call control messaging; X.509 Certificates may be used as an alternative to pre-shared key authentication mode.

Files for Implementing X.509 Public Key

The Avaya G860 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
Supported X.509 Functionality

The Avaya G860 Media Gateway supports the following X.509 functionality:

- Generation of Private Key and Self-Signed Certificate
- Generation of Certificate Signing Request (CSR)
- Expiration alarm for each provisioned Certificate file

4.14.3.1 Initial Configuration

Media Gateway boards are pre-loaded with a private key and a self-signed certificate that enables internal communication between SC and TP boards and allows access to the board’s WEB interface. However, these files cannot be downloaded from the boards and therefore are inapplicable for any other security application (SIP/TLS or IPSEC).

After installing the Media Gateway software, you must manually create a Private Key and a Certificate file (either self-signed or signed by a CA) as described in the sections below, and configure the G860 to use them.

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 Avaya G860 chassis. This reduces the amount of the certification data required to provision a 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.

4.14.3.2 Generating a Private Key

Private Key is the first and most basic file that should be configured on each node that participates in a secure communication that utilizes X.509 certificates. Each node has its own Private Key that is used to encrypt or decrypt messages. The Private Key should be kept in a secure location inside the node and never be exposed.

Note: A Private Key should never be shared with anyone or sent anywhere. Exposure of the Private Key will compromise security of the whole solution.
To generate a new Private Key, take these 7 steps:

1. Connect to the Active SC board via Telnet, SSH, or RS-232 console. Use Global IP address when connecting via Telnet or SSH.

2. Login as the CLI user with administrative privileges (e.g., username cli, password cli_12345).

3. At the prompt, type x509 and press Enter.

4. Choose option 1 - Generate Private Key.

5. At the Enter Private Key File Name prompt, enter a private key file name or press Enter to accept the default name.

6. Wait until a message displays, informing you that the private key was successfully generated and automatically added to the Auxiliary Files repository.

As a next step you should create an X.509 Certificate that matches this Private Key.

- For a self-signed certificate, refer to Generating a Self-Signed Certificate on page 217.

- For a certificate signed by CA, refer to Generating a Certificate Signing Request (CSR) on page 218.
Generating a Self-Signed Certificate

The Self-Signed Certificate is the simplest form of the X.509 Certificate that is issued by the participant on its own without use of any Certificate Authority (CA). A Self-Signed Certificate consists of the Public Key of the party that is signed by the Private Key of the party itself. A Self-Signed Certificate is typically considered to be a very weak form of the X.509 Certificate since it doesn’t utilize CA trust relationships and its authenticity cannot be verified.

**Note:** Use of the Self-Signed Certificates is not recommended for field deployments. You should establish PKI infrastructure and use certificates signed by the real CAs instead. Refer to the sections below for detailed instructions.

When Self-Signed Certificates are used by both parties that participate in secure communication, the Self-Signed Certificate of each party should be used by the other party as a Trusted Root Certificate.

➢ **To generate a new Self-Signed Certificate, take these 8 steps:**

1. Connect to the Active SC board via Telnet, SSH, or RS-232 console. Use Global IP address when connecting via Telnet or SSH.

2. Login as the CLI user with administrative privileges (e.g., username **cli**, password **cli_12345**).

3. At the prompt, type **x509** and press **Enter**.


```
client244 --~--~/moGW
=> x509
-----------------------
X.509 CERTIFICATES TOOL
-----------------------
1 - Generate Private Key
2 - Generate Self-Signed Certificate
3 - Generate Certificate Signing Request (CSR)
4 - Update Certificates Expiration Date
Choose option : 2
-----------------------
GENERATE SELF-SIGNED CERTIFICATE
-----------------------
```

5. The list of Private Keys that currently exist in the Auxiliary Files repository is displayed. Choose the Private Key file for which you wish to generate the Self-Signed Certificate.
The following Private Keys exist in Auxiliary Files repository:

1 - host.key

Choose Private Key [1] : 1

6. At the Enter Self-Signed Certificate File Name prompt, enter a self-signed certificate file name or press Enter to accept the default name.

Enter Self-Signed Certificate File Name [host.cert] : host.cert

7. Wait until the self-signed certificate is generated and automatically added to the Auxiliary Files repository.

Generating self-signed certificate...
Adding self-signed certificate to Auxiliary Files repository...
Done.

Self-Signed Certificate file host.cert was successfully generated and added to the Auxiliary Files repository.

8. To activate the new self-signed certificate, you must configure it in the Media Gateway Security Settings tab and apply the new configuration to the Media Gateway boards. Refer to the section “Activating the new X.509 Certificates on the Media Gateway” below.

4.14.3.4 Generating a Certificate Signing Request (CSR)

Certificate Signing Request (CSR) is a message sent from an applicant to a Certificate Authority (CA) in order to apply for a digital identity certificate. The CSR contains information identifying the applicant and the Public Key. The corresponding Private Key is not included in the CSR, but is used to digitally sign the entire request. The CSR may be accompanied by other credentials or proofs 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 sends back an identity certificate that has been digitally signed with the Private Key of the Certificate Authority. This certificate file must be added to the Media Gateway Auxiliary Files repository and configured in it’s Security Settings. You must also configure 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, take these 9 steps:

1. Connect to the Active SC board via Telnet, SSH, or RS-232 console. Use Global IP address when connecting via Telnet or SSH.
2. Login as the CLI user with administrative privileges (e.g., username cli, password cli_12345).
3. At the prompt, type x509 and press Enter.

```bash
client244 -- ~ -- /moGW
=> x509
-----------------------
X.509 CERTIFICATES TOOL
-----------------------
1 - Generate Private Key
2 - Generate Self-Signed Certificate
3 - Generate Certificate Signing Request (CSR)
4 - Update Certificates Expiration Date
Choose option : 3
-----------------------
GENERATE CERTIFICATE SIGNING REQUEST (CSR)
-----------------------
```

5. The list of Private Keys that currently exist in the Auxiliary Files repository is displayed. Choose the Private Key file for which you wish to generate the Certificate Signing Request.

```bash
The following Private Keys exist in Auxiliary Files repository:
1 - host.key
Choose Private Key [1] : 1
```

6. At the Enter CSR Subject prompt, enter the signing request subject or press Enter to accept the default.

```bash
Enter CSR subject [signing request] : signing request
```

7. Wait until the CSR file is generated.
8. Download the CSR file `/ftp/csr.txt` from the Active SC board via FTP, SCP or SFTP to your PC.

9. Send the downloaded CSR file to the CA.

### 4.14.3.5 Adding Certificates to the Auxiliary Files Repository

When CSR is successful, you receive from the CA a digitally signed X.509 Certificate file. You should also have a certificate of the Trusted Root (depending on the PKI scheme being deployed). Both of these files must be added to the Auxiliary Files repository prior to configuring them in the Media Gateway. Refer to Auxiliary Files Repository on page 270 for detailed instructions.

### 4.14.3.6 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

▸ To configure X.509 files in the Media Gateway Security Settings tab, take these 4 steps:

1. Click `MG Status` in the EMS Navigation bar.
2. Click `Properties` for the Media Gateway. The Media Gateway Parameters Provisioning screen appears.
3. Select the Security tab; the Security Settings screen is displayed.
4. Configure new X.509 files as described in the table below.
5. Click Apply to complete the configuration.

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private Key File</td>
<td>String</td>
<td>Instant</td>
<td>Private Key file</td>
</tr>
</tbody>
</table>
4. Configuring & Operating the Media Gateway

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate File</td>
<td>String</td>
<td>Instant</td>
<td>X.509 Certificate file. Contains the Public Key and identity information, signed by the CA or by the entity itself.</td>
</tr>
<tr>
<td>Trusted Root Certificate File</td>
<td>String</td>
<td>Instant</td>
<td>X.509 Certificate of the Trusted Root. If the root certificate of the CA that the signed remote party certificate matches the Trusted Root Certificate, the remote party certificate is accepted.</td>
</tr>
</tbody>
</table>

When new X.509 certificates are configured for the Media Gateway, they are not immediately applied to the Media Gateway board. This is done intentionally to minimize the effect on the Media Gateway service.

Two read-only parameters, available in the Security Settings Media Gateway tab, are used to indicate the status of the X.509 configuration on Media Gateway boards.

Table 4-50: X.509 Files Status Parameters of the Media Gateway

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TP Boards With Updated Certificates</td>
<td>String</td>
<td>Instant</td>
<td>A list of the Media Gateway boards that have an X.509 configuration that matches the configuration currently configured for the Media Gateway in the Security Settings tab. Normally all Media Gateway boards are listed in this list.</td>
</tr>
<tr>
<td>TP Boards Without Updated Certificates</td>
<td>String</td>
<td>Instant</td>
<td>A list of the Media Gateway boards that have an 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. A Lock/Unlock action on the TP board is used to apply new certificates to it and move it back from this list to the “TP Boards With Updated Certificates” list.</td>
</tr>
</tbody>
</table>

After you complete configuration of the new X.509 Files in the Media Gateway Security Settings tab, all Media Gateway boards will be moved to the “TP Boards Without Updated Certificates” list. This indicates that new configuration was not applied to any Media Gateway board yet.

Now you should activate new X.509 configuration on Media Gateway boards. In order to do so you must lock and unlock the specific Media Gateway board. When the board restarts, new X.509 configuration is applied to it and the board is moved from the “TP Boards Without Updated Certificates” list to the “TP Boards With Updated Certificates” list. It is recommended to choose one Media Gateway board and activate new X.509 configuration on it first. Then test the new configuration and validate that it is good and doesn’t affect the service. Finally, apply the new configuration to all Media Gateway boards.
To apply new X.509 configuration to Media Gateway boards, take these 3 steps:

1. Click  in the EMS Navigation bar.
2. Right-click the desired Media Gateway board and from the popup menu select Maintenance > Lock.
3. Right-click the desired Media Gateway board and from the popup menu select Maintenance > Unlock.

Note: The Media Gateway board must be restarted in order to apply a new X.509 configuration.

4.14.3.7 Configuring an X.509 Certificate Expiration Date Reminder

Each X.509 Certificate is issued for the specified period of time, the so called validity date. The Avaya G860 Media Gateway is capable of producing a Security Alarm to warn the user about certificate expiration.

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 the 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 these two alarms using the Update Certificates Expiration Date parameter in the Update Certificate Expiration Date screen.

To configure a X.509 certificates expiration alarm take the following steps:

- Update the certificates expiration date
- Configure the expiration date reminder

To update the X.509 Certificates expiration date, take these 6 steps:

1. Connect to the Active SC board via Telnet, SSH, or RS-232 console. Use Global IP address when connecting via Telnet or SSH.
2. Login as the CLI user with administrative privileges (e.g., username cli, password cli_12345).
3. At the prompt, type x509 and press Enter.
4. Choose option 4 – Update Certificate Expiration Date.

client244 -- -- -- /moGW
=> x509

--------------------------------------
X.509 CERTIFICATES TOOL
--------------------------------------
1 - Generate Private Key
4. Configuring & Operating the Media Gateway

2. Generate Self-Signed Certificate
3. Generate Certificate Signing Request (CSR)
4. Update Certificates Expiration Date

Choose option: 4

-----------------------------------
UPDATE CERTIFICATES EXPIRATION DATE
-----------------------------------

5. Wait until expiration date for all configured certificates is calculated and updated.

Updating certificate expiration date...
  certificate file name: host.cert
  expiration date: 2009-10-08 16:36:15
Updating trusted root certificate expiration date...
  certificate file name: trusted-root.cert
  expiration date: 2008-02-20 10:41:07
Done.
Expiration date for all configured certificates was successfully updated.

6. Use the EMS GUI to view the updated certificates expiration date.

➤ To configure an expiration date reminder for X.509 Certificates, take these 4 steps:

1. Click 🏡 MG Status in the EMS Navigation bar.

2. Select 📋 Properties for the Media Gateway. The Media Gateway Parameters Provisioning screen appears.


4. Configure the Certificate Expiration Date Reminder Days (for Certificate File) and the Trusted Root Certificate Expiration Date Reminder Days (for Trusted Root Certificate File) parameters.

Note: It is highly recommended to configure expiration date reminder alarms to alert users prior to X.509 Certificate expiration. Set the 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.
4.14.4 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, 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 4-3: IPSec Encryption](image)

The Avaya G860 Media Gateway includes the following Security specifications:

**IKE Protocol**
- Pre-shared Key or X.509 Certificate authentication modes (use of X.509 Certificates is supported for MGC Security Profiles only)
- Main mode is supported for IKE Phase 1
- IKE SA encryption algorithms: DES and 3DES
- IKE SA hash types: SHA1 and MD5

**IPSEC Protocol**
- Transport mode only
- Encapsulated Security Payload (ESP) only
- Support for Cipher Block Chaining (CBC)
- IPSEC SA encryption algorithms: DES and 3DES
- IPSEC SA hash types: SHA1 and MD5

**Note:** You must enable **Secure Operation** mode in order to activate IPSEC and IKE. For more information, refer to Secure Operation Mode on page 212.
4.14.4.1 Configuring IPSEC/IKE for Management Interfaces

IPSEC/IKE security association with EMS server is configured via CLI as part of the secure operation mode enable procedure.

For each additional SNMP manager (NMS, OSS or APS) a separate IPSEC/IKE security association must be configured.

In secure operation mode insecure SNMP managers may receive SNMP traps. However, they may not access the SNMP MIB of the Media Gateway (neither read nor write access).

IPSEC/IKE configuration consists of two parts:
- Creating and configuring OAM Security Profile
- Associating the OAM Security Profile with a specific SNMP manager

![Warning]
Note: A single security profile can be used for the multiple IP addresses of the Media Gateway Controller.

To add and configure OAM Security Profiles, take these 5 steps:

1. Access the MG Status screen.
2. Click Properties. The Media Gateway Parameters Provisioning screen appears.
5. Configure the OAM Security Profile according to the table below.

### Table 4-51: OAM Security Profile Parameters

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IKE Pre-Shared Key</td>
<td>String Up to 100 chars.</td>
<td>Online</td>
<td>Defines the IKE Pre-Shared Key in ASCII format. Once provisioned, the value is hidden from user via asterisks (******) for security reasons.</td>
</tr>
<tr>
<td>IKE Encryption</td>
<td>Enum des, des3, any</td>
<td>Online</td>
<td>Defines IKE SA Encryption algorithm.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- any – auto-negotiates IKE SA encryption with the remote side; DES or 3DES algorithms are offered</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- des – sets the IKE SA encryption to DES algorithm</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- 3des – sets the IKE SA encryption to 3DES algorithm</td>
</tr>
<tr>
<td>IKE Lifetime (sec)</td>
<td>Integer 0-2147483647</td>
<td>Online</td>
<td>Defines IKE SA Lifetime (in seconds).</td>
</tr>
</tbody>
</table>
### Parameter

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| IPSEC Lifetime (sec) | Integer 0-2147483647 | Online            | Defines IPSEC SA Lifetime (in seconds).          

To associate OAM Security Profiles with specific SNMP manager, take these 4 steps:

1. Access the MG Status screen.
2. Click Properties. The Media Gateway Parameters Provisioning screen appears.
3. Select the Network Services tab. The Network Services screen appears.
4. Select Security Profile from a drop-down list for each defined SNMP manager.

#### 4.14.4.2 Configuring IPSEC/IKE for Media Gateway Controllers

IPSEC/IKE security association can be configured for each Media Gateway Controller to protect the call control message exchange. It is not mandatory to configure IPSEC/IKE for each MGC in Secure Operation mode.

The IPSEC/IKE configuration consists of two parts:

- Creating and configuring MGC Security Profile
- Associating the MGC Security Profile with specific SNMP manager

**Note:** Single security profile can be used for multiple IP addresses of the Media Gateway Controllers.

To add and configure MGC Security Profiles, take these 8 steps:

1. Access the MG Status screen.
2. Click MGCs. The Media Gateway Controllers screen appears.
3. Select an MGC from the list.
4. If the selected MGC is not already locked, Right-click on it and from the popup menu, and lock it.
5. Right-click on the selected MGC and from the popup menu, select Properties. The MGC Parameters Provisioning screen appears.
7. To add a new MGC security profile, click +. A new row appears.
8. Configure MGC Security Profile according to the table below.
### Table 4-52: MGC Security Profile Parameters

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| IKE Authentication Method      | Enum PresharedKey, Certificate | Offline           | Defines the IKE Authentication Method.  
  - Pre-shared key: a secret phrase that is used for validating the authenticity of the other side.  
  - X.509 certificates: both parties have a certificate that is signed by the same CA and use them to verify authenticity of the other side.  
  In order to use X.509 Certificates authentication mode, you must first configure X.509 certificates. For more information, refer to X.509 Certificates on page 214. |
| IKE Pre-Shared Key             | String Up to 100 chars. | Online             | Relevant only when IKE Authentication Method is set to PresharedKey.  
  Defines the IKE Pre-Shared Key in ASCII format. Once provisioned, the value is hidden from user via asterisks (*****) for security reasons.  
  When IKE Pre-Shared Key is changed online, a new security association (SA) will be created with the updated pre-shared key string. |
| IKE Encryption                | Enum des, des3 | Offline           | Defines IKE SA Encryption algorithm.  
  - des – sets the IKE SA encryption to DES algorithm  
  - 3des – sets the IKE SA encryption to 3DES algorithm |
| IKE Lifetime (sec)            | Integer 0-2147483647 | Offline           | Defines IKE SA Lifetime (in seconds). |
| IKE Lifetime (KBytes)         | Integer 0-2147483647 | Offline           | Defines IKE SA Lifetime (in KBytes). |
| IPSEC Lifetime (sec)          | Integer 0-2147483647 | Offline           | Defines IPSEC SA Lifetime (in seconds). |
| IPSEC Lifetime (KBytes)       | Integer 0-2147483647 | Offline           | Defines IPSEC SA Lifetime (in KBytes). |
| IPSEC Local Port             | Enum any, specific | Offline           | The local port (on Media Gateway board's side) to be encrypted by the IPSEC protocol.  
  - any – encrypt all ports  
  - specific – encrypt specific port used by the call control protocol (the specific port number is calculated according to the MGC configuration) |
### Avaya G860 Media Gateway

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPSEC Remote Port</td>
<td>Enum any, specific</td>
<td>Offline</td>
<td>The remote port (on the MGC side) to be encrypted by the IPSEC protocol.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>any – encrypt all ports</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>specific – encrypt specific port used by the call control protocol (the specific port number is calculated according to the MGC configuration)</td>
</tr>
<tr>
<td>IPSEC Protocol</td>
<td>Enum any, specific</td>
<td>Offline</td>
<td>The IP protocol to be encrypted by the IPSEC protocol.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>any – encrypt all protocols</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>specific – encrypt specific protocol (UDP or TCP) used by the call control protocol (the specific protocol is calculated according to the MGC configuration)</td>
</tr>
</tbody>
</table>

To associate MGC Security Profiles with specific Media Gateway Controller’s IP addresses, take these 7 steps:

1. Access the **MG Status** screen.
2. Click **MGCs**. The Media Gateway Controllers screen appears.
3. Select an MGC from the list.
4. If the selected MGC is not already locked, Right-click on it and from the popup menu, and lock it.
5. Right-click on the selected MGC and from the popup menu, select **Properties**. The MGC Parameters Provisioning screen appears.
6. Select the **MGC Addressing** tab. The MGC Addressing screen appears.
7. Select Security Profile from a drop-down list for each defined MGC IP address.

### 4.14.5 SSH/SCP/SFTP

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 Avaya G860 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.

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 Avaya G860 Media Gateway. For better performance and shorter file transfer times, use the SCP protocol instead of SFTP.
4. Configuring & Operating the Media Gateway

4.14.6 SSL/TLS

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 Avaya G860 uses TLS over TCP to encrypt SIP transport and (optionally) to authenticate it.

Specifications of the SSL/TLS implementation in the Avaya G860:

- 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, take these 6 steps:

1. Access the MG Status screen.
2. Double-Click on the desired Media Gateway Board. The Board Status screen appears.
3. At the top of the screen, click SIP. The SIP Coders List screen appears.
5. On the General Setting tab, set the Transport Type parameter in to TLS. In this mode, the Media Gateway board initiates a TLS connection only for the next network hop.
6. 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.
7. If you wish the Media Gateway board to validate the certificate of the remote side, set the parameter TLS Two-Way Authentication to Enable.

4.14.7 Media Security

The Avaya G860 Media Gateway supports two different types of Media Security:

- Packet Cable Security
- Secure RTP

4.14.7.1 Packet Cable Security

The Avaya G860 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) and DSP Load File Version to 3 (in Media Gateway board).

4.14.7.2 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 higher-level protocols (MGCP or MEGACO).

Secure RTP specifications:
- Encryption – AES 128 in Counter Mode
- Authentication – HMAC-SHA1
- Support of Key Derivation
- Key management is provided via MGCP and MEGACO

Note: Refer to the version-specific Release Notes to check the availability of the SRTP application in a specific Media Gateway software release.

4.14.7.2.1 Disabling RTCP

If you are enabling secure RTP, you must first disable RTCP in network regions working with G860 or where G860 is configured. To do so:
- Disable RTCP at the Communication Manager. In the "change ip-network-regions" SAT screen, page 1, set RTCP Reporting Enabled? to n.
- Disable RTCP at the EMS as follows:
  a. Select the desired Media Gateway board. Click Properties. The Media Gateway Board Provisioning Properties screen appears.
  b. In the Voice tab, set RTCP interval to 65536.

4.14.7.2.2 Enabling Secure RTP

To enable Secure RTP, take these steps:

1. Access the MG Status screen.
2. Lock the desired Media Gateway Board.
3. Right click on the Media Gateway Board and from the popup menu, select Properties. The Media Gateway Parameters Provisioning screen appears.
5. On the Voice tab, set the DSP Load File Version parameter to 0.
4. Configuring & Operating the Media Gateway


7. Unlock the Media Gateway board.

**Note:** Secure RTP settings take effect only after you reset the Media Gateway board. Reset the board after configuring all the parameters.

### 4.14.7.2.3 Enabling Unencrypted Secure RTP

To enable unencrypted Secure RTP, take these 3 steps:

1. Access the MG Status screen.
2. Right click on the desired Media Gateway Board and from the popup menu, select Properties. The Media Gateway Parameters Provisioning screen appears.
3. In the Call Control tab, set the Unencrypted SRTCP Offer parameter to enable.

### 4.14.8 Configuring Firewall Functionality

The Avaya G860 provides Firewall functionality that helps to protect Media Gateway boards from unauthorized access. Media Gateway boards may be configured to block incoming traffic from a specific IP addresses or from a specific networks. Firewall definitions are not bound to a specific application and are extremely flexible. Advanced functionality, such as being able to limit traffic based on individual packet size and bandwidth allocation, is provided.

For more information, refer to *Avaya Port Matrix: G860 R2*, 131674.

#### 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, a corresponding 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 Firewall Profile does not contain rules that allow specific Media Gateway board to communicate with Media Gateway Controllers and other Media Gateways. Hence such rules must be manually provisioned by user otherwise control/media traffic will be blocked.

The Firewall configuration consists of two parts:

- Create and configure Firewall Profile
- Associate Firewall Profile with specific Media Gateway board
To add and configure Firewall Profiles, take these 6 steps:

1. Access the MG Status screen.
2. Click Firewall Profile. The Firewall Profile screen appears.
3. To add a new Firewall Profile, click . A new row appears.
4. To view the Firewall Rules that the Firewall Profile contains, double-click on it.
5. To add a new Firewall Rules (that enable communication with Media Gateway Controller and other Media Gateways), click .
6. Configure the Firewall Rules according to the table, Firewall Rule Parameters.

To associate the Firewall Profiles with a specific Media Gateway board, take these 2 steps:

1. Access the MG Status screen.
2. Right-click on the desired Media Gateway board and from the popup menu, select Configuration> Properties.
3. On the General Settings tab, from the Firewall Profile dropdown list, select the appropriate profile name.

Table 4-53: Firewall Rule Parameters

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Name</td>
<td>String</td>
<td>Instant</td>
<td>Textual, user-defined name for the Firewall Rule.</td>
</tr>
<tr>
<td>Source IP</td>
<td>String</td>
<td>Instant</td>
<td>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).</td>
</tr>
</tbody>
</table>

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.
### 4. Configuring & Operating the Media Gateway

#### Parameter Name | Type | Provisioning Type | Description
--- | --- | --- | ---
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.
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 - means any protocol.
Packet Size | Integer 0-65535 | Instant | Defines the maximum packet size of incoming traffic. Default value - 0 - means any size.
Byte Rate | Integer 0-2147483647 | Instant | Defines the maximum byte rate of incoming traffic. Default value - 0 - means any rate.
Byte Burst | Integer 0-2147483647 | Instant | Defines the maximum byte burst of incoming traffic. Default value - 0 - means any burst.
Action | Enum allow, block | Instant | Action to be applied for the packets that match a specified rule - allow/block.

#### 4.14.9 OS Patching

SC boards operate using the SUN Solaris™ Operating System (OS). SUN periodically releases security and stability updates for the Solaris™ Operating System (also known as OS patches) that address known product vulnerabilities and functionality bugs. Avaya periodically reviews all available OS patches and determines whether or not they are applicable to the Avaya G860 (only security-related and specific functionality patches are reviewed).

OS patches that are applicable to the Avaya G860 are packed inside the Media Gateway software installation package. They are automatically installed on the SC boards together with the Media Gateway software and no additional version control is required.
4.14.10 OS Hardening

When Avaya G860 Media Gateway software is installed on SC boards, it automatically configures Solaris OS for secure operation mode. The following OS hardening tasks are performed:

- Unrequired Solaris services and daemons are shut down.
- File system permissions are modified to prevent security attacks.
- TCP/IP stack is tuned to prevent DoS attacks (including SYN and Smurf attacks).
- Unrequired Solaris packages and binaries that contain potential security breaches are removed.
- Insecure communication protocols (Telnet, FTP and SNMP) are limited to the IPSEC tunnels only.

Note: Most of the OS hardening tasks are immediately performed during Media Gateway software installation. However, to fully activate the OS hardening feature, in particular limiting insecure communication protocols to the IPSEC tunnels only, you must enable Secure Operation mode. For more information, refer to Secure Operation Mode on page 212.

4.14.11 OS Auditing

The Solaris™ 9 OS, installed on the SC boards, provides the capability to log the activity on a system at a granular level. This logging or auditing ability is part of the Solaris SunSHIELD™ Basic Security Module (BSM). These auditing capabilities were added to provide the features required by the Trusted Computer System Evaluation Criteria (TCSEC) to a security level referred to as C2.

The TCSEC has been superseded by the newer updated and more internationally recognized Common Criteria security requirements. As part of these requirements, the Solaris OS has been evaluated under the Controlled Access Protection Profile (CAPP) at Evaluation Assurance Level (EAL) 4. The CAPP used for the Solaris OS evaluation includes all functionality covered by C2 evaluations.

Auditing Goal

The primary goal of auditing is to record user actions in order 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.

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.

Solaris™ 9 OS provides 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
4. Configuring & Operating the Media Gateway

auditing data; however for advanced auditing analysis and automatic intrusion detection and prevention, 3rd party Intrusion Detection Systems (IDS) should be used.

**OS Auditing on the Avaya G860 Media Gateway**

When Avaya G860 Media Gateway software is installed on SC boards, it automatically configures the Solaris 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` directory. 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 up to one week.

Security administrators may modify the list of audit events recorded on the SC board by manually editing the `/etc/security/audit_control` and `/etc/security/user_control` files.

**Note:** These modifications should be performed with a great deal of care in order to minimize the effect on the Media Gateway performance and in general are not recommended.

When the auditing subsystem can not 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.

**Analyzing Audit Trail File**

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
```

Refer to the man pages of **praudit** and **auditreduce** commands for more information.

**Using 3rd Party Audit Analysis Tools**

**praudit** and **auditreduce** provide very basic auditing analysis capabilities. Advanced analysis may be performed by using the following tools:


Avaya provides no support for these 3rd party tools. Contact the appropriate tool supplier for additional information.

### 4.14.12 File System Integrity

Media Gateway software implements a File System Integrity Check. This check provides an additional security mechanism that helps to mitigate security risks such as hacker intrusion and malicious software installation on the SC boards.

When Media Gateway software is installed, a snapshot of the file system is created. This snapshot covers both 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, an SNMP alarm is sent to the EMS and the integrity status of SC board’s file system is updated accordingly.

Each SC board performs the File System Integrity Check independently and reports the results via the corresponding SC board managed object.

➤ To view status of the File System Integrity, take these 3 steps:

1. Access the **MG Status** screen.
2. Double-click on the SC board. SC Board Parameter Provisioning screen appears.
3. In **Filesystem Integrity** tab, inspect parameters as described in the table below.

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File System Integrity Status</td>
<td>Enum, ok/failure</td>
<td>Read-only</td>
<td>Indicates File System Integrity Status.</td>
</tr>
<tr>
<td>Integrity Unauthorized Files</td>
<td>String</td>
<td>Read-only</td>
<td>When unauthorized modifications to the file system are detected, lists exact names of the modified files. This attribute has a limited length. For a complete list of modified files, use the command tools fs status.</td>
</tr>
</tbody>
</table>

#### 4.14.12.1 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, take these 3 steps:

1. Access the **MG Status** screen.
2. Click **Clock**. The **Media Gateway Parameters Provisioning** screen appears.
3. In the **MG General Settings** tab, modify the **File System Integrity Check Time** parameter according to the table below.

### Table 4-55: Filesystem Integrity Parameters of the Media Gateway

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrity Check Time</td>
<td>String in HH:MM format</td>
<td>Instant</td>
<td>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).</td>
</tr>
</tbody>
</table>

**4.14.12.2 Viewing File System Integrity Status**

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 status of File System Integrity and a complete list of modified files, take these 3 steps:**

1. Connect to the specific SC board via the Telnet, SSH, or RS-232 console. For more information, refer to Connecting to the SC Board's Terminal on page 89.

2. Login as the **CLI** user with administrative privileges (e.g., username `cli`, password `cli_12345`). For more information, refer to Users on SC Board's Terminal on page 92.

3. At the prompt type `tools fs status` and press Enter. The INTEGRITY CHECK STATUS is displayed.

```
client238::~# tools fs status
-------------------------
INTEGRITY CHECKING STATUS
-------------------------

Last Integrity Scan:
Thu Jan 11 15:09:34 GMT 2007

*** Detected Integrity Violation! ***

Affected Files:
-------------

/Project/bin/SystemParams.ini - CHANGED
/Project/bin/SystemParams_bak.ini - ADDED
```
4.14.12.3 Fixing File System Integrity

The Security Administrator must fix all compromised files. This may be done 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 removed from later 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, take these 6 steps:**

1. Connect to the specific SC board via the Telnet, SSH, or RS-232 console. For more information, refer to Connecting to the SC Board's Terminal on page 89.
2. Login as the **root** user. For more information, refer to Users on SC Board's Terminal on page 92.
3. Fix all compromised files as described above.
4. For each compromised file, at the prompt type `tools fs ack <filename>` and press Enter.

```
client238::~# tools fs ack /Project/bin/SystemParams.ini
client238::~# tools fs ack /Project/bin/SystemParams_bak.ini
```

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 ***
```
4. Configuring & Operating the Media Gateway

4.14.13 Advanced Security Features

This section is intended for the advanced administrator and provides information relevant to the Secure Operation mode and the required preparations in the network environment (e.g., configuration of external Firewalls).

For more information, refer to Avaya Port Matrix: G860 R2, 131674.

4.14.13.1 Network Services on SC Board

The Avaya G860 provides the following services configured and enabled on the SC board during normal system operation:

- **TFTP** – used for transferring binary and configuration files to the VoIP boards during board initialization (unlock). The service is limited to the IP addresses of the Media Gateway boards.

- **SSH** – used for remote access to the Command Line Interface (CLI).

4.14.13.2 OpenBoot PROM Security

OpenBoot PROM is a hardware-level user interface environment 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 SC board fails to boot Solaris OS because of some abnormal scenario, it is impossible to recover the SC board.

➢ To enable Open Boot PROM security, take these 6 steps:

1. Connect to the Active SC board via Telnet, SSH, or RS-232 console. For more information, refer to Connecting to the SC Board's Terminal on page 89.

2. Log on as the root user. For more information, refer to Users on SC Board's Terminal on page 92.

3. At the prompt, type `eeprom 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.

```bash
client238:~# eeprom security-mode=command
Changing PROM password:
New password: *******
Retype new password: *******
```
6. Repeat the steps on the Standby SC board.

➢ To set a new EEPROM password, at the prompt, takes these 5 steps:

1. Connect to the Active SC board via Telnet, SSH, or RS-232 console. For more information, refer to Connecting to the SC Board's Terminal on page 89.

2. Log on as the root user. For more information, refer to Users on SC Board's Terminal on page 92.

3. At the prompt, type `eeprom security-password=` (do not forget the trailing equal sign) and press Enter.

4. At the New Password prompt, type the new password and retype it at the Re-enter password prompt.

```
client238:~# eeprom security-password=
Changing PROM password:
New password: password
Retype new password: password
```

Open Boot PROM security is enabled.

5. Repeat the steps on the Standby SC board.

➢ To disable Open Boot PROM security, take these 4 steps:

1. Connect to the Active SC board via Telnet, SSH, or RS-232 console. For more information, refer to Connecting to the SC Board's Terminal on page 89.

2. Log on as the root user. For more information, refer to Users on SC Board's Terminal on page 92.

3. At the prompt, type `eeprom security-mode=none` and press Enter.

```
client238:~# eeprom security-mode=none
```

Open Boot PROM security is disabled.

4. Repeat the steps on the Standby SC board.

4.14.13.3 Login Banner

When a user logs into the Avaya G860 in secure operation mode, the default login banner appears. This banner can be modified to match specific customer requirements.

➢ To modify the login banner, take the 6 steps:

1. Connect to the Active SC board via Telnet, SSH, or RS-232 console. For more information, refer to Connecting to the SC Board's Terminal on page 89.

2. Log on as the root user. For more information, refer to Users on SC Board's Terminal on page 92.

3. At the prompt, type `edit /etc/banner` and press Enter. The file opens in the default text editor.
4. Configuring & Operating the Media Gateway

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.

6. Repeat the steps 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.

4.14.13.4 SUID Files

The following files on SC boards have an SUID bit set:

- `/Project/scripts/tools`
- `/Project/bin/exe/tg_watchdog`
- `/Project/bin/exe/tg_driver`
- `/Project/cli/log.pl`

4.14.14 Administering Users on SC Boards

The following users are defined on the SC board during normal system operation:

- **root** – administrative super-user. Used for the initial system installation and network configuration. Also used by the EMS server for maintenance tasks (e.g., performing Online Software Upgrade). For more information, refer to ROOT User Administration on page 242.

- **CLI users** – usernames should be configured by the administrator (via the root user). Different privilege levels (administrator or monitor) may be assigned. For stronger security, it is highly recommended to create a separate CLI user for each operator instead of using a shared CLI account. Default software installation creates a cli account that has administrator privileges. This account may be deleted or locked to prevent it’s use. For more information, refer to CLI User Administration on page 243.

- **audcftp** – internal user; used for auxiliary files replication between the SC boards. Use is limited to FTP access only and is therefore inapplicable in the secure configuration (where FTP access from remote is not available). For more information, refer to AUDCFTP User Password Administration on page 247.

- **ems** – username used by EMS server to perform maintenance tasks on the SC boards (starting/stopping Media Gateway software). This user has administrative CLI user privileges and should never be deleted. For more information, refer to EMS User Password Administration on page 249.

User Database (that includes user profiles and authentication information) is normally stored in Solaris OS configuration files on each SC board. Therefore when the user
database is modified (e.g., new users are added or passwords of existing users are modified), the information must be properly updated on both SC boards.

The following sections describe how to properly perform typical user maintenance tasks.

Media Gateway software also supports centralized user authentication via RADIUS protocol. For more information, refer to Centralized User Authentication on page 250.

### 4.14.14.1 ROOT User Administration

This section describes actions used to manage root user account details.

#### 4.14.14.1.1 Lost User Password Recovery

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 1:** Physical access to the RS-232 console of the specific SC board is required to perform this maintenance task.

**Note 2:** The SC board seizes its 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 remains active.

➢ **To reset ROOT password on SC board, take the 7 steps:**

1. Connect to RS-232 console of the specific SC board. For more information, refer to Connecting to the SC Board's Terminal on page 89.

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 is reset. When the SC board reboots, the root password will be reset to the default value `root`.

7. Change root password to a new value as described in ROOT User Password Administration.
4.14.14.2 CLI User Administration

This section describes how to manage CLI users.

4.14.14.2.1 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, take these 14 steps:

1. Connect to the Active SC board via Telnet, SSH, or RS-232 console. For more information, refer to Connecting to the SC Board's Terminal on page 89.

2. Login as the root user. For more information, refer to Users on SC Board's Terminal on page 92.

3. At the prompt, type tools user and press Enter. The CLI USERS MANAGEMENT menu appears.

4. At the Choose submenu prompt, type add and press Enter. The ADD CLI USER menu appears.

5. At the User Name prompt, type the desired username and press Enter. ("george" is an example below.)
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. The administrative super-user (root) may modify the password of any user regardless of any time limitations.

New Password:******

9. At the Re-enter new Password prompt, type the new password again.

Re-enter new Password:******

10. Repeat the above steps 1-10 for all CLI users that you wish to add.

11. Log into the Standby SC board as the root user.

12. At the prompt, type tools user and press Enter. The CLI USERS MANAGEMENT menu appears.

13. Select copy. The configuration is copied from the Active SC board.
4. Configuring & Operating the Media Gateway

4.14.14.2 Deleting a CLI User

CLI user accounts that are not in use should be deleted.

To delete CLI user, take these 9 steps:

1. Connect to the Active SC board via Telnet, SSH, or RS-232 console. For more information, refer to Connecting to the SC Board’s Terminal on page 89.

2. Login as the root user. For more information, refer to Users on SC Board’s Terminal on page 92.

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. The DELETE CLI USER menu appears.

   Choose submenu : del

   ---------------
   DELETE CLI USER
   ---------------

4. 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**

5. Repeat the above steps for all CLI users that you wish to delete.

6. Log into the Standby SC board as the **root** user.

7. At the prompt, type `tools user` and press Enter. The CLI USERS MANAGEMENT menu appears.

8. Select copy. The configuration is copied from the Active SC board.
4.14.14.2.3 Changing Password of 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.

➢ To change the password of a CLI user, take these 13 steps:

1. Connect to the Active SC board via Telnet, SSH, or RS-232 console. For more information, refer to Connecting to the SC Board’s Terminal on page 89.

2. Login as the root user. For more information, refer to Users on SC Board's Terminal on page 92.

3. At the prompt, type tools user and press Enter. The CLI USERS MANAGEMENT menu appears.

4. At the Choose submenu prompt, type pwd and press Enter. The CHANGE USER PASSWORD menu appears.

5. At the User Name prompt, type the desired username and press Enter. ("george" is an example below.)

6. At the When password should expire prompt, type the password expiration date (number of days). To configure password without an expiration date, type 0.

Note: For improved security, it is strongly recommended to use an expiration date for all passwords.
4. Configuring & Operating the Media Gateway

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:*******

    

    Note: For improved security, it is strongly recommended to use an expiration date for all passwords.

10. Repeat the above steps for all CLI users that you wish to change.

11. Log into the Standby SC board as the root user.

12. At the prompt, type tools user and press Enter. The CLI USERS MANAGEMENT menu appears.

13. Select copy. The configuration is copied from the Active SC board.

4.14.14.3 AUDCFTP User Password Administration

AUDCFTP is an internal user that is utilized for auxiliary files replication between SC boards. It is limited to FTP access only and can not be accessed from a remote location when the Secure Gateway Configuration is set because of the access limitations on FTP service.

The AUDCFTP user’s password can be modified by the root Administrator, although there is no clear security advantage to this.

➢ To modify the AUDCFTP user’s password, take these 11 steps:

1. Connect to the Active SC board via Telnet, SSH, or RS-232 console. For more information, refer to Connecting to the SC Board’s Terminal on page 89.

2. Log on as the root user. For more information, refer to Users on SC Board’s Terminal on page 92.

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. The CHANGE USER PASSWORD menu appears.

Choose submenu : pwd

---------------------
CHANGE USER PASSWORD
---------------------

5. At the User Name prompt, type audcftp and press Enter.

User Name : audcftp

6. At the New Password prompt, type the new password and retype it at the Re-enter password prompt.

Enter existing login password:*******
New Password:*******
Re-enter password:*******

7. At the prompt, type cli audcftp password <new password> and press Enter. (in place of <new password> type the text to be the new password. The password must not contain any spaces.)

client238:~# cli audcftp password <new password>

8. Connect and log in to the Standby SC board as the root user.
9. At the prompt, type `tools user` and press Enter. The CLI USERS MANAGEMENT menu appears.

10. Select `copy`. The configuration is copied from the Active SC board.

### 4.14.14.4 EMS User Password Administration

For security reasons, the password of the `ems` user should be modified periodically.

➢ **To modify the EMS user password, take these 10 steps:**

1. Connect to the Active SC board via Telnet, SSH, or RS-232 console. For more information, refer to Connecting to the SC Board's Terminal on page 89.
2. Login as the `root` user. For more information, refer to Users on SC Board's Terminal on page 92.
3. At the prompt, type `tools user` and press Enter. The CLI USERS MANAGEMENT menu appears.

```plaintext
Choose submenu : pwd
---------------------
CHANGE USER PASSWORD
---------------------
```

4. At the Choose submenu prompt, type `pwd` and press Enter. The CHANGE USER PASSWORD menu appears.

```plaintext
User Name : ems
```

5. At the User Name prompt, type `ems` and press Enter.
6. At the **New Password** prompt, type the new password and retype it at the Re-enter password prompt.

New Password: ********
Re-enter password: ********

7. Connect and login to the Standby SC board as the **root** user.

8. At the prompt, type **tools user** and press Enter. The CLI USERS MANAGEMENT menu appears.

9. Select **copy**. The configuration is copied from the Active SC board.

10. For EMS users, also update the root password in the EMS Media Gateway/Server properties.

   a. In the EMS, right-click on the specific Media Gateway in the Media Gateway tree and from the pop-up menu, select **Details**. Change the EMS Password parameter to match the ems password on the SC boards.

**Note:** The password time limitations are not available for ems user because of the hardware limitations (the SC boards do not contain a clock battery and therefore may not maintain correct time after a hardware reset if an NTP server is unreachable.)

### 4.14.15 Centralized User Authentication

The Avaya G860 Media Gateway supports centralized authentication of CLI users via RADIUS protocol. In this mode user profiles (e.g., user name, privilege levels) are still stored locally on SC boards. However, user authentication (password validation) is performed on a centralized authentication server. This provides additional security features (e.g., the time-of-day based login or password complexity validation) and implement alternative authentication methods (e.g., a combination of password and hardware token).

The Avaya G860 implements RADIUS client as defined in IETF RFC 2865. Up to 3 RADIUS servers are supported for redundancy purposes. The following RADIUS packet types are supported:

- **Access-Request** – sent by Avaya G860 to the authentication server upon user login attempt.
- **Access-Accept** – response from the authentication server that allows the user to login; if response contains Reply-Message attribute, it's displayed to the user.
- **Access-Reject** – response from the authentication server that forbids user to login; if response contains Reply-Message attribute, it's displayed to the user.
- **Access-Challenge** – response from the authentication server that asks user to provide additional information; must contain Reply-Message attribute that is displayed to user as a prompt; typically used for multi-level user authentication (e.g., password and hardware token).
When centralized user authentication is in effect, CLI user passwords must be managed via management interfaces provided by RADIUS server and not via tools user script or passwd command.

**Note:** Centralized user authentication is applied to CLI users only. Passwords of root, ems and audcftp users are always stored locally on SC boards to enable correct operation in the event of authentication server failure.

➢ **To configure centralized user authentication, take these 3 steps:**

1. Access the MG Status screen.

2. Click Properties. The Media Gateway Parameters Provisioning screen appears.

3. In the User Management tab, update the parameters according to the table below.

**Table 4-56: Centralized User Authentication Parameters**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>External Authentication Server</td>
<td>Enum</td>
<td>Instant</td>
<td>Defines whether or not centralized authentication server is used for CLI user's authentication.</td>
</tr>
<tr>
<td></td>
<td>None, Radius</td>
<td></td>
<td>• none – users are stored locally on each SC board</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• radius – centralized RADIUS server is used for CLI users authentication</td>
</tr>
<tr>
<td>1st RADIUS Auth Server IP</td>
<td>IP address</td>
<td>Instant</td>
<td>IP address of the 1st RADIUS authentication server</td>
</tr>
<tr>
<td>1st RADIUS Auth Server Port</td>
<td>Integer 0-65535</td>
<td>Instant</td>
<td>Port of the 1st RADIUS authentication server</td>
</tr>
<tr>
<td>1st RADIUS Auth Server Secret</td>
<td>String Up to 80 chars</td>
<td>Instant</td>
<td>Shared secret of the 1st RADIUS authentication server.</td>
</tr>
<tr>
<td>2nd RADIUS Auth Server IP</td>
<td>IP address</td>
<td>Instant</td>
<td>IP address of the 2nd RADIUS authentication server</td>
</tr>
<tr>
<td>2nd RADIUS Auth Server Port</td>
<td>Integer 0-65535</td>
<td>Instant</td>
<td>Port of the 2nd RADIUS authentication server</td>
</tr>
<tr>
<td>2nd RADIUS Auth Server Secret</td>
<td>String Up to 80 chars</td>
<td>Instant</td>
<td>Shared secret of the 2nd RADIUS authentication server.</td>
</tr>
<tr>
<td>3rd RADIUS Auth Server IP</td>
<td>IP address</td>
<td>Instant</td>
<td>IP address of the 3rd RADIUS authentication server</td>
</tr>
</tbody>
</table>
### Parameter Name | Type | Provisioning Type | Description
--- | --- | --- | ---
3rd RADIUS Auth Server Port | Integer 0-65535 | Instant | Port of the 3rd RADIUS authentication server
3rd RADIUS Auth Server Secret | String Up to 80 chars | Instant | Shared secret of the 3rd RADIUS authentication server
RADIUS Auth Retransmit Timeout (sec) | Integer 1-100 | Instant | Timeout (in seconds) between RADIUS request retransmissions Default: 2 sec
RADIUS Auth Number Of Retries Default: 2 attempts | Integer 1-100 | Instant | Number of retransmission attempts against each RADIUS server

### 4.15 Configuring Clock Synchronization

In a traditional TDM service network, such as PSTN, both ends of the TDM connection must be synchronized. If they are not, 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 Avaya G860 Media Gateway supports different Clock Synchronization modes. The following clock synchronization modes are available:

For TP-6310 configurations:
- **Standalone Board Sync Clock Mode**—each Media Gateway board synchronizes itself by the clock received on one of the PSTN interfaces (OC-3/STM-1 optical links or T3 trunks) connected to it; there is no global clock synchronization between different Media Gateway boards. For more information, refer to Standalone Board Sync Clock Mode for TP-6310 configurations on page 252.
- **Timing Module BITS Sync Clock 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 for TP-6310 configurations on page 254.

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.

#### 4.15.1 Standalone Board Sync Clock Mode for TP-6310 Configurations

In Standalone Board Sync clock mode, each TP-6310 board synchronizes its own clock. The clock may be derived from the following sources:
- **PSTN interface (OC-3/STM-1 optical links or 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 Timing Module BITS Sync Clock Mode for TP-6310 configurations on page 254).

Figure 4-4: Standalone Board Sync Clock Mode for TP-6310 Configurations

In Standalone Board Sync clock mode, clock source is derived from the high-level communication layer protocol of the PSTN interface (OC-3, STM-1, T1 on T3) or from the internal board's clock reference.

Connecting Media Gateway to the External Equipment

In Standalone Board Sync clock mode, clock source is derived from the PSTN interface (OC-3, STM-1 or T3) connected to the Media Gateway board or from the internal board's clock reference. If you wish to derive clock from the PSTN interface, you must simply connect 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 Media Gateway to any external equipment.

Configuring Media Gateway Software

This section describes how to configure Standalone Board Sync Clock Mode for TP-6310 configurations.

➢ To configure Standalone Board Sync Clock Mode for TP-6310 configurations, take these 4 steps:

1. Access the screen.
2. Click . The Clock Parameters Provisioning screen appears.
3. In the Sync Mode Settings tab, configure Synchronization Mode parameter as StandaloneBoardSync.
4. In the Standalone Board Mode Setting tab, configure TP6310 Clock Reference parameter 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
The clock is taken from the high-level communication layer protocol of the PSTN interface; for T3 trunks the clock is taken from one of the available DS1 trunks; selection of the DS1 trunk is performed automatically from all trunks that are currently in service.

The above-described settings are applied to all TP-6310 boards; however, it is possible to override Clock Reference settings for the specific TP-6310 board as follows:

- Access the Media Gateway Board Provisioning screen
- In the General Settings tab, configure the None Mode Clock Source parameter as described in step 4.

### Configuring the DS3 Interface

For T3 configurations, the above-described procedures configure the clock settings of individual DS1 trunks as part of the DS3 interface. Timing of the DS3 interface itself (high-level communication protocol on the PSTN interface) is configured as follows:

To configure timing of the DS3 interface, take these 4 steps:

1. Access the MG Status screen.
2. Double-click on the specific Media Gateway board
3. In the DS3 tab, double-click on the specific DS3 interface. The DS3 Parameters Provisioning screen appears.
4. Configure 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

### 4.15.2 Timing Module BITS Sync Clock Mode for TP-6310 Configurations

In Timing Module BITS Sync clock mode, all Media Gateway boards are synchronized with 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.

Note: In order to activate the Timing Module BITS Sync clock mode, you must order SA/RTMs with a resident Timing Module. Consult with an Avaya representative on how to order this module.

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 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 Revert Clock Reference Mode parameter.

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, refer to the figure above.

Configuring Media Gateway Software

To configure Timing Module BITS Sync Clock Mode for TP-6310 configurations, take these 4 steps:

1. Access the MG Status screen.
2. Click Clock. The Clock Parameters Provisioning screen appears.
3. In the Sync Mode Setting tab, configure Synchronization Mode parameter as TimingModuleBITSSync.
4. In the Timing Module Settings tab, configure parameters as described in the below table.
Table 4-57: Timing Module BITS Sync Clock Mode Parameters

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selector Mode</td>
<td>Enum</td>
<td>Instant</td>
<td>Defines the operational mode of the clock reference selection algorithm.</td>
</tr>
<tr>
<td></td>
<td>Manual,</td>
<td></td>
<td>Automatic – selection between clock sources (BITS 1 and 2) is performed automatically; when one source fails, another source is automatically used.</td>
</tr>
<tr>
<td></td>
<td>Automatic</td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Revert Clock Reference Mode</td>
<td>Enum</td>
<td>Instant</td>
<td>Defines system behavior when clock source with higher priority returns to service after the failure.</td>
</tr>
<tr>
<td></td>
<td>Disable,</td>
<td></td>
<td>Enabled: Media Gateway will switch to this source.</td>
</tr>
<tr>
<td></td>
<td>Enable</td>
<td></td>
<td>Disabled; continue using the current source until the latter fails.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Note that when Revert Clock Reference Mode is Enabled 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.</td>
</tr>
<tr>
<td>External Reference Type</td>
<td>Enum</td>
<td>Instant</td>
<td>Defines the external line reference (BITS) transmission format.</td>
</tr>
<tr>
<td></td>
<td>E1, DS1,</td>
<td></td>
<td>T12</td>
</tr>
<tr>
<td>Line Coding</td>
<td>Enum</td>
<td>Online</td>
<td>Defines line coding for the clock synchronization interfaces:</td>
</tr>
<tr>
<td></td>
<td>HDB3, B8ZS, AMI</td>
<td></td>
<td>▪ B8ZS – B8ZS line code (for T1 trunks only)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>▪ AMI – AMI line code</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>▪ HDB3 – High-Density Bipolar 3 line code (for E1 trunks only)</td>
</tr>
<tr>
<td>Framing</td>
<td>Enum</td>
<td>Online</td>
<td>Defines the framing method for the clock synchronization interfaces:</td>
</tr>
<tr>
<td></td>
<td>CRC4, ESF, SF</td>
<td></td>
<td>▪ CRC4 = Multiframe with CRC4 (default, automatic mode, if CRC is identified in the Rx, CRC is sent in Tx, otherwise no CRC).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>▪ ESF = Extended Super Frame</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>▪ SF = Super Frame</td>
</tr>
</tbody>
</table>
### Configuring the DS3 Interface

For T3 configurations, Timing Module on SA-1/RTM rear card controls clock settings of individual DS1 trunks only. Timing of the DS3 interface itself (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, take these 4 steps:

1. Access the **MG Status** screen.
2. Double-click on the specific Media Gateway board
3. In the **DS3** tab, double-click on the specific DS3 interface. The DS3 Parameters Provisioning screen appears.
4. Configure 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

### Performance Monitoring

Performance Monitoring Measurements may be used to analyze functionality and determine abnormal behavior of the <Product Name> 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).

The following chapters provide basic information on performance monitoring operation. For additional information, refer to the Performance Monitoring section in *Element Management System User’s Manual*, Document #: LTRT-910xx.

The Avaya G860 Media Gateway supports two types of Performance Monitoring measurements (PMs):

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tx Pulse Shape</td>
<td>Enum db0, db7p5, db15, db22p5</td>
<td>Instant</td>
<td>Defines the quality of the transmission signal on the clock synchronization interfaces.</td>
</tr>
<tr>
<td>Transmit Control</td>
<td>Enum SystemClock, DerivedLine, AIS, Disable</td>
<td>Instant</td>
<td>Defines the transmission pattern on the clock synchronization interfaces.</td>
</tr>
<tr>
<td>External Ref 1 Clock Priority</td>
<td>Integer 0-2</td>
<td>Instant</td>
<td>Defines the priority of the 1st external reference clock (connected to the BITS 1). Priority 0 means that the specific reference clock is not used.</td>
</tr>
<tr>
<td>External Ref 2 Clock Priority</td>
<td>Integer 0-2</td>
<td>Instant</td>
<td>Defines priority of the 2nd external reference clock (connected to the BITS 2). Priority 0 means that the specific reference clock is not used.</td>
</tr>
</tbody>
</table>
Real-Time PMs

Use real-time PMs to acquire information of the current system state and view the current values of its most critical parameters (such as CPU utilization or Trunk usage).

Historic PMs

Use historic PMs to monitor system state over an extended period of time and perform long-term system analysis.

4.16.1 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, take these 7 steps:

1. Access the screen.
2. Select the entity for which you wish PMs to be displayed. For example, select an SC board to view SC board's PMs.
   The selected entity is displayed.
3. Click on the Performance Monitoring Icon in the Info Pane.
4. In the drop-down menu, select Display Real-Time PMs.

Figure 4-6: Display Real-Time PMS

The "Select Screen" window is displayed.

Figure 4-7: Select Screen
5. Select the screen where you wish to display new data. If you choose new screen, enter the custom screen name.

The Real-Time Performance Measurement Display window is displayed.

Figure 4-8: Real-Time Performance Measurement Display

6. Choose the type of view (Graph or Table).

7. Click the Parameters button. The MG Monitoring window is displayed.

Figure 4-9: MG Monitoring

Two types of the performance measurement parameters are supported – Gauges and Counters. Gauges are indicated by and Counters are indicated by.

8. Select the parameters group for which you wish to display performance measurements (e.g., MG CPU Performance).

All parameters for the selected Parameter Group are displayed.

9. Check the desired parameters from the Parameter Group. You may select up to 5 parameters for the same entity or compare parameters over different entities (e.g. over different trunks or boards).
10. Click **OK** button to return to the Real-Time Performance Measurement Display window.

11. In the Real-Time Performance Measurement Display window, choose polling interval and click the **start** button to start polling.

   A real-time graph or table is displayed.

   You can pause polling by clicking the **pause** button and restart it by clicking the **start** button.

**Figure 4-10: Real Time Performance Measurements Display**

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.

12. When you have completed performance monitoring, click the **stop** button to stop parameter's polling and close the Real-Time Performance Measurement Display window.

### 4.16.2 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.

➢ **To start collection of History Performance Measurements, take these 10 steps:**

1. Access the screen.
2. Click on the **Performance Monitoring** Icon in the Info Pane and from the drop-down menu select **Configure MG PM Profile**.

**Figure 4-11: Configure MG PM Profile**

The **MG Background Monitoring** window is displayed.

**Figure 4-12: MG Background Monitoring**

3. 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.

4. 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.

5. In the Parameters List, right-click on the Parameter group and check all parameters for the group or individually check the desired parameters from the selected Parameter Group.

6. In the Profiles pane, click the Save button. In the New Profile dialog, enter a name for your new PM profile and click OK.

7. Click the Attach button to attach the specific PM Profile to the Media Gateway. The "Question" dialog is displayed.

![Figure 4-13: Question](image)

8. Select Yes to start parameter's polling. The information dialog is displayed.

![Figure 4-14: Start_Polling](image)

9. 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.

10. When you have completed performance monitoring, click the stop button to stop parameter's polling and close the "Real-Time Performance Measurement Display" window.

![Note 1](image)

**Note 1:** You may optionally detach the profile.

**Note 2:** To restart polling for an attached profile, click the start button.
To view collected History Performance Measurements, take these 6 steps:

1. Access the MG Status screen.
2. Select the entity for which you wish PMs to be displayed. For example, select SC board to view SC board's PMs.
3. Click on the Performance Monitoring Icon in the Info Pane and from the drop-down menu select "Display Historical PMs".

Figure 4-15: Display Historical PMs

4. Select the screen where you wish to display history performance measurements data.

Figure 4-16: Select Screen
The History Performance Measurements Display window is displayed.

**Figure 4-17: History Performance Measurements Display**

5. Select 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**.
4. Configuring & Operating the Media Gateway

Historical performance measurements display is comprised of two tables. The upper table displays detailed data and the table below displays the summarized data.

Figure 4-18: Historical Performance Measurements Display

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).

4.17 Media Gateway Inventory

Media Gateway Inventory contains a summary of all hardware components, their serial numbers, hardware and EEPROM versions, IP addresses etc.

➢ To view Media Gateway Inventory, take these 2 steps:

1. Access the MG Status screen.
2. Click Inventory. The Media Gateway Inventory screen appears.

Figure 4-19: MG Inventory

4.18 Checking the Fan Speeds

You may need to check the speeds of the fans in the fan tray modules of the Avaya G860.

➢ To check the speeds of the fan tray modules, take these 2 steps:

1. Access the MG Status screen.
2. On the MG Status screen, double-click on a fan tray module area of the graphic representation of the Avaya G860. The Fans list appears displaying the list of fans in the selected module and their speeds.

Refer to Fan Tray Module on page 28.

4.19 Media Gateway Boards' Configuration Backdoor

Media Gateway Boards are normally configured via the corresponding management objects (MOs) in the Avaya G860 Media Gateway's configuration database. The SC board is responsible for distributing the user configuration among the Media Gateway Boards.

In an unlikely event that you need to configure a parameter for the Media Gateway board that does not exist in the Avaya G860 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 Avaya Tech Support:

- The parameter's ini file name
- The parameter's ini file value
4. Configuring & Operating the Media Gateway

- 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. Access the MG Status screen.
2. Click Properties. The Media Gateway Parameters Provisioning screen appears.
3. Select the Configuration Backdoor tab.
4. To add a new Configuration Backdoor, click and set the parameters according to the table below.
5. Repeat the steps above for each additional parameter that needs to be configured.
6. If the Media Gateway board is not already unlocked, unlock it. Wait until the board becomes enabled.

Table 4-58: Configuration Backdoor Parameters

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boards IDs</td>
<td>String</td>
<td>Online</td>
<td>Defines the Media Gateway boards to which this backdoor parameter is applied. Syntax:</td>
</tr>
<tr>
<td></td>
<td>Up to 40 chars.</td>
<td></td>
<td>- Number value 1 to 20 – the number of board's slot number, e.g., &quot;5&quot; for slot 5.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Multiple number values (delimited by comma or space), e.g., &quot;5,6,7&quot; for slots 5, 6 and 7.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Value range (delimited by dash), e.g., &quot;5-7&quot; for slots 5, 6 and 7.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Mix of value range and numbers, e.g., &quot;5,6-8,10&quot; for slots 5, 5, 7, 8 and 10.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Value &quot;all&quot; – to define the value for all board</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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  
  • "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 ini file. If the Trunk ID is specified (i.e., it is not all/tmp1/tmp2/none) – a Trunk ID is appended to the parameter name. |
| Parameter value        | String Up to 80 chars. | Instant           | Defines the backdoor parameter value as written in the ini file. If the parameter value must be surrounded by quotation marks in the ini 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, TPReset | Online            | Defines how the backdoor parameter is applied.  
  • Instant – the backdoor is instantly applied to all relevant Media Gateway boards  
  • TPReset – backdoor requires the Media Gateway board to be reset (lock/unlock). The reset in not automatically enforced and should be manually performed by the user at the appropriate time. |
4. Configuring & Operating the Media Gateway

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redundancy Support</td>
<td>Enum</td>
<td>Online</td>
<td>Defines how the backdoor parameter affects the Media Gateway boards’ redundancy mechanism.</td>
</tr>
<tr>
<td></td>
<td>Warm, Hot</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Warm – if the parameter differs among the boards, Warm Switchover is to be performed</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Hot – if the parameter differs among the boards, Hot Switchover is to be performed</td>
</tr>
</tbody>
</table>

**Configuration Backdoor in the EMS**

Media Gateway Board's Configuration Backdoor status is represented by the standard *OperationalState* and *AdministrativeState* 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 boards to which the Configuration Backdoor is applied, but the boards must be reset in order to apply the current backdoor settings

**4.19.1 Supported Actions**

The following actions are available on the Media Gateway Board's Configuration Backdoor:

- **Add** – add a Configuration Backdoor parameter.
- **Remove** – remove Configuration Backdoor parameter (backdoor must be locked prior to using the remove action).
- Configuration Backdoor 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** – locking the Backdoor parameter is allowed only when all of the relevant Media Gateway boards are locked.
- **Unlock** – returns the Backdoor parameter to "service". The backdoor parameter is applied to all or the relevant Media Gateway boards according to the *Update mode* attribute.

**4.19.2 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 corresponding configuration parameter. The Backdoor parameter value is merged into the Media Gateway configuration database.
4.20 **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 Avaya G860 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>
<thead>
<tr>
<th>Auxiliary File Type</th>
<th>Description</th>
<th>Can be modified by the user?</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMP (firmware)</td>
<td>The Media Gateway board's software package</td>
<td>No</td>
</tr>
<tr>
<td>Call Progress Tones (CPT)</td>
<td>Defines different Call Progress Tones and User-Defined Tones to be detected/generated by the Media Gateway board</td>
<td>Yes</td>
</tr>
<tr>
<td>Pre-Recorded Tones (PRT)</td>
<td>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)</td>
<td>Yes</td>
</tr>
<tr>
<td>Voice Prompts</td>
<td>User-recorded voice prompts</td>
<td>Yes</td>
</tr>
<tr>
<td>CAS File</td>
<td>The CAS protocol state machine that allows protocol customization and adaptation</td>
<td>Yes</td>
</tr>
<tr>
<td>VXML for IPmedia</td>
<td>Voice XML file (for the IPmedia application)</td>
<td>Yes</td>
</tr>
<tr>
<td>VXML for SIP</td>
<td>Voice XML file (for the SIP application)</td>
<td>Yes</td>
</tr>
<tr>
<td>External Coders</td>
<td>Defines coders that are supported by the Media Gateway board</td>
<td>Yes</td>
</tr>
<tr>
<td>User Information</td>
<td>Defines user information (for the SIP application)</td>
<td>Yes</td>
</tr>
<tr>
<td>X.509 Private Key</td>
<td>X.509 Private Key</td>
<td>Yes</td>
</tr>
<tr>
<td>X.509 Certificate</td>
<td>X.509 Public Certificate</td>
<td>Yes</td>
</tr>
<tr>
<td>X.509 Trusted Root Certificate</td>
<td>X.509 Public Certificate of Trusted Root entity (CA)</td>
<td>Yes</td>
</tr>
</tbody>
</table>

4.20.1 **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, take these 2 steps:

1. Upload the auxiliary file to the EMS Software Manager:
   a. From the Tools menu, select Software Manager. The Software Manager screen appears.
   b. In the upper left corner, click . The add Files screen appears.
   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 appears 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.

2. Add the Auxiliary file to the Avaya G860.
   a. Access the screen.
   b. Click . The Auxiliary Files screen appears.
   c. To add an Auxiliary file, click .
   d. Select the desired file from the list. A row is added to the Files screen.

4.20.2 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 272) 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 277).

**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, take these 4 steps:

1. Access the **MG Status** screen.
2. Right-click on the desired Media Gateway board and, from the popup menu, select **Configuration>Properties**.
3. Select the **Setup Files** tab.
4. From the **Call Progress Setup File** parameter dropdown list, containing the list of CPT files available in auxiliary files repository, select the desired CPT file.

### 4.20.2.1 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.

#### 4.20.2.1.1 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 X<sup>th</sup> 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 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.

**Note 1:** 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.

**Note 2:** The tone frequency should differ by at least 40 Hz from one tone to other defined tones.

### 4.20.2.1.2 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.
4. Configuring & Operating the Media Gateway

- **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.

### 4.20.2.1.3 Default Configuration

The following table describes the default Call Progress Tones configuration of the Media Gateway boards:

**Table 4-60: Default Call Progress Tones**

<table>
<thead>
<tr>
<th>[NUMBER OF CALL PROGRESS TONES]</th>
<th>Number of Call Progress Tones=9</th>
</tr>
</thead>
<tbody>
<tr>
<td>#Dial tone</td>
<td></td>
</tr>
<tr>
<td>[CALL PROGRESS TONE #0]</td>
<td></td>
</tr>
<tr>
<td>Tone Type=1</td>
<td></td>
</tr>
<tr>
<td>Tone Form = 1 (Continuous)</td>
<td></td>
</tr>
<tr>
<td>Low Freq [Hz]=350</td>
<td></td>
</tr>
<tr>
<td>High Freq [Hz]=440</td>
<td></td>
</tr>
<tr>
<td>Low Freq Level [-dBm]=13 (-13dBm)</td>
<td></td>
</tr>
<tr>
<td>High Freq Level [-dBm]=13</td>
<td></td>
</tr>
<tr>
<td>First Signal On Time [10msec]=300</td>
<td></td>
</tr>
<tr>
<td>#Dial tone</td>
<td></td>
</tr>
<tr>
<td>[CALL PROGRESS TONE #1]</td>
<td></td>
</tr>
<tr>
<td>Tone Type=1</td>
<td></td>
</tr>
<tr>
<td>Tone Form = 1 (Continuous)</td>
<td></td>
</tr>
<tr>
<td>Low Freq [Hz]=440</td>
<td></td>
</tr>
<tr>
<td>High Freq [Hz]=0</td>
<td></td>
</tr>
<tr>
<td>Low Freq Level [-dBm]=10 (-10dBm)</td>
<td></td>
</tr>
<tr>
<td>High Freq Level [-dBm]=0</td>
<td></td>
</tr>
<tr>
<td>First Signal On Time [10msec]=300</td>
<td></td>
</tr>
<tr>
<td>#Ringback</td>
<td></td>
</tr>
<tr>
<td>[CALL PROGRESS TONE #2]</td>
<td></td>
</tr>
<tr>
<td>Tone Type=2</td>
<td></td>
</tr>
<tr>
<td>Tone Form = 2 (Cadence)</td>
<td></td>
</tr>
<tr>
<td>Low Freq [Hz]=440</td>
<td></td>
</tr>
<tr>
<td>High Freq [Hz]=480</td>
<td></td>
</tr>
<tr>
<td>Low Freq Level [-dBm]=19 (-19dBm)</td>
<td></td>
</tr>
<tr>
<td>High Freq Level [-dBm]=19</td>
<td></td>
</tr>
<tr>
<td>First Signal On Time [10msec]=200</td>
<td></td>
</tr>
<tr>
<td>First Signal Off Time [10msec]=400</td>
<td></td>
</tr>
</tbody>
</table>
### [NUMBER OF CALL PROGRESS TONES]

**Number of Call Progress Tones**: 9

<p>| | | | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>#Ringback</td>
<td></td>
<td>Tone Type: 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[CALL PROGRESS TONE #3]</td>
<td></td>
<td>Tone Form = 2 (Cadence)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Low Freq [Hz]=440</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>High Freq [Hz]=0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Low Freq Level [-dBm]=16 (-16dBm)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>High Freq Level [-dBm]=0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>First Signal On Time [10msec]=100</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>First Signal Off Time [10msec]=300</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>#Busy</td>
<td></td>
<td>Tone Type: 3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[CALL PROGRESS TONE #4]</td>
<td></td>
<td>Tone Form = 2 (Cadence)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Low Freq [Hz]=480</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>High Freq [Hz]=620</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Low Freq Level [-dBm]=24 (-24dBm)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>High Freq Level [-dBm]=24</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>First Signal On Time [10msec]=50</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>First Signal Off Time [10msec]=50</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>#Busy</td>
<td></td>
<td>Tone Type: 3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[CALL PROGRESS TONE #5]</td>
<td></td>
<td>Tone Form = 2 (Cadence)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Low Freq [Hz]=440</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>High Freq [Hz]=0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Low Freq Level [-dBm]=20 (-20dBm)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>High Freq Level [-dBm]=0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>First Signal On Time [10msec]=50</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>First Signal Off Time [10msec]=50</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>#Reorder tone</td>
<td></td>
<td>Tone Type: 7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[CALL PROGRESS TONE #6]</td>
<td></td>
<td>Tone Form = 2 (Cadence)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Low Freq [Hz]=480</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>High Freq [Hz]=620</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Low Freq Level [-dBm]=24 (-24dBm)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>High Freq Level [-dBm]=24</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>First Signal On Time [10msec]=25</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>First Signal Off Time [10msec]=25</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### [NUMBER OF CALL PROGRESS TONES]

**Number of Call Progress Tones=9**

<table>
<thead>
<tr>
<th>Tone Type</th>
<th>Tone Form</th>
<th>Low Freq [Hz]</th>
<th>High Freq [Hz]</th>
<th>Low Freq Level [-dBm]</th>
<th>High Freq Level [-dBm]</th>
<th>First Signal On Time [10msec]</th>
<th>First Signal Off Time [10msec]</th>
</tr>
</thead>
</table>
| #Confirmation tone
[CALL PROGRESS TONE #7] | 8 | 2 (Cadence) | 350 | 440 | -20 (-20dBm) | 20 | 10 | 10 |
| #Call Waiting Tone
[CALL PROGRESS TONE #8] | 9 | 2 (Cadence) | 440 | 0 | -20 (-20dBm) | 0 | 30 | 900 |

#### 4.20.2.1.4 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 corresponding 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
4.20.3 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:

- 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 278).

To associate a Pre-Recorded Tones (PRT) file with a Media Gateway board, take these 4 steps:

1. Access the MG Status screen.
2. Right-click on the desired Media Gateway board and, from the popup menu, select Configuration>Properties.
3. Select the Setup Files tab.
4. From the Prerecorded Tones File parameter dropdown list, containing the list of PRT files available in auxiliary files repository, select the desired PRT file.

Note 1: The maximum number of prerecorded tones that can be stored in one dat file is 40.

Note 2: The maximum PRT file size for TP-6310 board is 1 MB.

Note 3: If the same tone type is defined as PRT and CPT Tone, the tone is played using the PRT module.

4.20.3.1 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, take these 10 steps:

1. Execute DConvert.exe and click the Process Prerecorded Tones file(s) button. The Prerecorded Tones file(s) window appears.
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 appears.
   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 4-20: 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 on it. The File Data window appears.

   ![Figure 4-21: 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.

### 4.20.4 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 **DConvert utility** (as described in Creating a Voice Prompts File on page 281).

➤ **To associate Voice Prompts file with Media Gateway board, take these 3 steps:**

1. Access the **MG Status** screen.
2. Right-click on the desired Media Gateway board and, from the popup menu, select **Configuration>Properties**.
3. On the **Setup Files** tab, the **Voice Prompts File** parameter dropdown list contains the list of Voice Prompts files available in **auxiliary files repository**. Select the desired Voice Prompts file.
4.20.4.1 Creating a Voice Prompts File

➢ To create a Voice Prompts file, take these 9 steps:

1. Execute DConvert.exe and click the Process Voice Prompts file(s) button. The Voice Prompts window appears.

   ![Figure 4-22: Voice Prompts Screen](image)

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. (Refer to 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 4-23: Select Files Window
4. Configuring & Operating the Media Gateway

Figure 4-24: 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 4-25: 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.

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.

4.20.5 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 284) and convert it to the binary format using the DConvert utility (as described in Converting External Coders File to Binary Format on page 285).

To associate an External Coders file with a Media Gateway board, take these 3 steps:

1. Access the MG Status screen.
2. Right-click on the desired Media Gateway board and, from the popup menu, select Configuration>Properties.
3. On the Setup Files tab, the Coders File parameter dropdown list contains the list of External Coders files available in auxiliary files repository. Select the desired External Coders file.

4.20.5.1 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.

<table>
<thead>
<tr>
<th>[Internal name]</th>
<th>[Coder name]</th>
<th>[Txpayload]</th>
<th>[RxPayload]</th>
<th>[Ptime]</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCMA</td>
<td>PCMA</td>
<td>8</td>
<td>8</td>
<td>20</td>
</tr>
<tr>
<td>PCMU</td>
<td>PCMU</td>
<td>0</td>
<td>0</td>
<td>20</td>
</tr>
<tr>
<td>G726-16</td>
<td>G726-16</td>
<td>35</td>
<td>35</td>
<td>20</td>
</tr>
<tr>
<td>G726-24</td>
<td>G726-24</td>
<td>36</td>
<td>36</td>
<td>20</td>
</tr>
<tr>
<td>G726-32</td>
<td>G726-32</td>
<td>2</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>G726-40</td>
<td>G726-40</td>
<td>38</td>
<td>38</td>
<td>20</td>
</tr>
<tr>
<td>X-G727-16</td>
<td>X-G727-16</td>
<td>39</td>
<td>39</td>
<td>20</td>
</tr>
<tr>
<td>X-G727-24-16</td>
<td>X-G727-24-16</td>
<td>40</td>
<td>40</td>
<td>20</td>
</tr>
<tr>
<td>X-G727-24</td>
<td>X-G727-24</td>
<td>41</td>
<td>41</td>
<td>20</td>
</tr>
<tr>
<td>X-G727-32-16</td>
<td>X-G727-32-16</td>
<td>42</td>
<td>42</td>
<td>20</td>
</tr>
</tbody>
</table>
4. Configuring & Operating the Media Gateway

<table>
<thead>
<tr>
<th>Internal Coder Name</th>
<th>External Coder Name</th>
<th>Payload 1</th>
<th>Payload 2</th>
<th>Maximal Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>X-G727-32</td>
<td>X-G727-32</td>
<td>44</td>
<td>44</td>
<td>20</td>
</tr>
<tr>
<td>X-G727-40-16</td>
<td>X-G727-40-16</td>
<td>45</td>
<td>45</td>
<td>20</td>
</tr>
<tr>
<td>G723HIGH</td>
<td>G723</td>
<td>4</td>
<td>4</td>
<td>30</td>
</tr>
<tr>
<td>G723LOW</td>
<td>G723</td>
<td>80</td>
<td>80</td>
<td>30</td>
</tr>
<tr>
<td>G729</td>
<td>G729</td>
<td>15</td>
<td>15</td>
<td>20</td>
</tr>
<tr>
<td>G728</td>
<td>G728</td>
<td>6</td>
<td>6</td>
<td>20</td>
</tr>
<tr>
<td>GSM</td>
<td>GSM</td>
<td>3</td>
<td>3</td>
<td>20</td>
</tr>
<tr>
<td>X-CCD</td>
<td>X-CCD</td>
<td>102</td>
<td>102</td>
<td>20</td>
</tr>
<tr>
<td>iLBC13</td>
<td>iLBC</td>
<td>100</td>
<td>100</td>
<td>30</td>
</tr>
<tr>
<td>iLBC15</td>
<td>iLBC</td>
<td>101</td>
<td>101</td>
<td>20</td>
</tr>
<tr>
<td>BV16</td>
<td>BV16</td>
<td>102</td>
<td>102</td>
<td>20</td>
</tr>
<tr>
<td>EVRC_C</td>
<td>EVRC</td>
<td>103</td>
<td>103</td>
<td>20</td>
</tr>
<tr>
<td>telephone-event</td>
<td>telephone-event</td>
<td>96</td>
<td>96</td>
<td>20</td>
</tr>
<tr>
<td>RED</td>
<td>RED</td>
<td>104</td>
<td>104</td>
<td>20</td>
</tr>
<tr>
<td>CN</td>
<td>CN</td>
<td>13</td>
<td>13</td>
<td>20</td>
</tr>
</tbody>
</table>

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.

### 4.20.5.1 New Coders Introduced with the Table

- **EVRC0** – This is actually the corrected name (according to RFC 3558) of an existing coder. (It was formerly called EVRC.)
- **BV16** – Supported for BCT only.
- **iLBC** – Supported for BCT only.

### 4.20.5.2 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.

### 4.20.5.2 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,
take these 6 steps:

1. Execute DConvert.exe and click the **Process Coders Description** button. The Coders Window appears.

   ![Figure 4-26: Coders Window](image)

   **Coder List File**
   ![Select File...]

   **Using File**
   ![Output File]

   **User Data**
   ![Description]

   **Process Output**
   ![Make File]

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 1:** This information is **NOT** retained after the window has been closed.

   **Note 2:** The process verifies the input file for validity. Invalid data causes an error and aborts the process. The log box contains further relevant information.

---

**4.20.6 Associating a X.509 File with a Media Gateway**

4. Configuring & Operating the Media Gateway

For more information, refer to X.509 Certificates on page 214 – for a detailed description of the X.509 Certificates and their use.

➢ To associate a X.509 File with a Media Gateway, take these 4 steps:

1. Access the MG Status screen.
2. Click Clock. The Media Gateway Parameters Provisioning screen appears.
4. Select the desired X.509 file from the corresponding dropdown list.
5 Hardware Replacement Procedures

Note: Before starting any replacement procedure, be sure to prepare all replacement components and tools to be used in advance.

5.1 Board Replacement Preliminaries

5.1.1 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 or replacing boards from the chassis, take these 2 steps:

1. Locate the ESD (electrostatic discharge) connections on the Avaya G860 chassis. Refer to the diagrams in Front and Back Views of the Avaya G860 on page 22.

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.

Note: Do not set components down without first protecting them with an anti-static bag.

5.1.2 Slot Cover Requirements

It is imperative to cover all unoccupied slots in both the front cage and the rear cage of the Avaya G860 chassis with blank panels to maintain the mandatory high, internal airflow.

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.
5.1.2.1 Slot Cover Requirements

Figure 5-1: Baffled Blank Panel for Front Slots

Figure 5-2: Blank Panel for Rear Slots

CAUTION

Board types are assigned to specific slots. 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 slide in the full way with ease, check if it is indeed appropriate for the slot in which you are inserting.

5.2 SC Board Replacement Procedure

The faulty SC board must be removed and replaced. The SC board is hot-swappable. Therefore, it can be replaced while the Avaya G860 is under power and operating. After replacing the SC board, the Media Gateway software must be installed and configured on it.

Typically, SC boards are pre-installed with the correct version of the Solaris™ OS. Therefore, there is no need to re-install the OS on them. In the unlikely event that your replacement SC board does not have the correct Solaris™ OS version installed (or is not installed at all), refer to the Appendix, Installing the Solaris™ 9 OS on page 375.

For details about installing the Media Gateway software, refer to Installing the SC Media Gateway Software on the Replaced SC Board on page 291.

➢ To remove an SC board from the chassis, take these 3 steps:

1. Unfasten the screws on the plate of the board.
5. Hardware Replacement Procedures

2. Simultaneously press the red ejector buttons on the two black ejector/injector latches on both ends and wait 60 sec for the Hot Swap blue LED to light, indicating that the board can be removed.

Figure 5-3: 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 Horizontal 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.

5.2.1 Installing the Media Gateway Software on the Replaced SC Board

The Media Gateway software must be installed on a replacement SC board.
WARNING

Be sure to install exactly the same Media Gateway software version on the replacement SC board as was installed on the original SC board prior to failure.

Media Gateway software installation package provides all of the installation and configuration options required for the replacement SC board. It must be uploaded to the SC board prior to starting the installation process. Refer to "Uploading the Installation Package" below.

Possible SC Board Failure Scenarios

The following table summarizes possible SC board failure scenarios and provides detailed instructions on how to install Media Gateway software.

<table>
<thead>
<tr>
<th>SC boards</th>
<th>Scenario Description and Software Installation Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slot 1</td>
<td></td>
</tr>
<tr>
<td>Slot 2</td>
<td></td>
</tr>
<tr>
<td>In service</td>
<td>The SC board in Slot 2 has failed and was replaced. The SC board in Slot 1 continues to operate as the Active SC board. Media Gateway software must be installed on the SC board in Slot 2. Refer to Installing the Media Gateway Software on the 2nd SC Board on page 301.</td>
</tr>
<tr>
<td>Failed</td>
<td>The SC board in Slot 1 has failed and was replaced. The SC board in Slot 2 continues to operate as the Active SC board. Media Gateway software must be installed on the SC board in Slot 1. Refer to Installing the Media Gateway Software on the 2nd SC Board on page 301. Note: The reference to the 2nd SC board in the above scenarios is correct as it applies to the Standby SC board.</td>
</tr>
<tr>
<td>Failed</td>
<td>When both SC boards have failed, do the following: Install the Media Gateway software on the SC board in Slot 1 as described in Installing the Media Gateway Software on the 1st SC Board on page 295. Install the Media Gateway software on the SC board in Slot 2 as described in Installing the Media Gateway Software on the 2nd SC Board on page 301.</td>
</tr>
</tbody>
</table>

5.2.2 Installation Package

The Media Gateway’s software installation package is provided on the Avaya G860 System Software Installation CD included in the accessory kit accompanying the Avaya G860. The following is the software component on the CD:
Table 5-2: SC Installation Package Files

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sc_software.tar.gz</td>
<td>The compressed tar file containing Media Gateway software installation package</td>
</tr>
</tbody>
</table>

5.2.3 Uploading the Installation Package

Use one of the following file transfer protocols to upload the Installation Package to the SC board:

- FTP
- SFTP
- SCP

You can use any standard-compliant FTP/SSH/SCP client software to perform the Installation Package file upload.

The following example shows an upload of the Installation Package from a Windows PC using a simple console FTP client:

![Figure 5-4: SC Software Package Upload Using FTP](image)

Note 1: If you upload the SC Installation Package via FTP, make sure to choose "binary file transfer mode" (command `bin` in a console FTP client).

Note 2: Login as root user and use the corresponding password (the default password is `root`). The uploaded package should be placed in a `/ (root)` directory on the SC board.

➢ To upload the installation package to the `/ftp` directory, take these 3 steps:

1. Open the FTP/SFTP/SCP client and connect to the private SC IP address.
2. Login as CLI user (e.g., user `cli`, password `cli_12345`). For more information, refer to Users on SC Board's on page 92 Terminal.
3. Upload the installation package into the `/ftp` directory.
You can use any standard-compliant FTP/SFTP/SCP client software to perform the Installation Package file upload.

The following example shows an upload of the Installation Package from a Windows PC using a simple console FTP client:

![Figure 5-5: SC Software Package Upload Using FTP](image)

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

After completing transfer of the installation package to the SC board, you must move it from the /ftp directory to the / (root) directory (if you have not already done so).

➢ To move the Installation Package to the / (root) directory, take these 3 steps:

1. Connect to the SC board via Console, Telnet or SSH. For more information, refer to Connecting to the SC Board's Terminal on page 89.
5. Hardware Replacement Procedures

2. Login as the root user. For more information, refer to Users on SC Board's Terminal on page 92.

3. To move the installation package to the / (root) directory, at the prompt type the following commands:

```plaintext
client238:~# rm -f /sc_software.tar.gz
client238:~# mv /ftp/sc_software.tar.gz /sc_software.tar.gz
```

5.2.4 Installing the Media Gateway Software on the 1st SC Board

The Media Gateway software installation process described here is used in the event that both SC boards have failed and are replaced. The SC board in Slot 1 requires this installation process.

➢ To install the Media Gateway software on the SC board to be the Active SC board, take these 16 steps:

1. Connect to the SC board that is to be Active via Telnet, SSH or RS-232 Console. For more information, refer to Connecting to the SC Board's Terminal on page 89.

2. Login as root user. For more information, refer to Users on SC Board's Terminal on page 92.

3. At the prompt, type `/install.pl` and press Enter. The integrity of the software installation package is verified and its version is displayed.

```plaintext
client241:~# /install.pl
Found compressed Avaya installation package - uncompress it...
  >>> uncompressing /sc_software.tar.gz file (this takes around 20 sec)...   
  >>> done
Verify installation package integrity...
Unpack package version information...
  >>> unpacking version information (this takes around 10 sec)...  
  >>> done
Found the following Avaya installation package:

-----------------------------
Core Network Media Gateway  
  Version : 5.0.14
-----------------------------
```

4. When you are asked if you want to install, type `y` and press Enter. The software installation and basic configuration menu appears.

```plaintext
Do you want to install ([y]/n)  
[y]: y
Unpack version-specific installation script...
  >>> unpacking /install.pl file (this takes around 10 sec)...  
  >>> done
```
Run version-specific installation script

SC Software Installation & Basic Configuration

1 - Update SC network parameters.
2 - Install and configure.
3 - Change installed configuration.
4 - Copy configuration from Active SC.
5 - Uninstall the software.
0 - Quit.

5. To select option 2 - Install and configure, at the Choose prompt, type 2 and press Enter. The installation sequence begins.

Choose (0-5) : 2

>>> Verifying the installation package integrity ...
>>> Verifying the OS version ...

************************************************************
************************************************************
**                                                         **
**      WARNING: Installation will delete current          **
**               configuration !!!!                       **
**                                                         **
** For typical Media Gateway systems in which software    **
**  is preinstalled, select option "3 - Change installed **
**   configuration".                                       **
**                                                         **
************************************************************
************************************************************

6. You are prompted if you want to install. Type y and press Enter. The installation sequence proceeds.

Do you want to install? (y/n) [n]: y

Install SC Software

>>> Clean up /tftpboot directory ...
>>> Clean up CDR directory ...
>>> Extract all files from TAR ...

(This sequence is abbreviated)
7. After installation is successfully completed, the basic configuration of SC software must be performed. You are asked whether you are installing the 1st or the 2nd SC board. To select the 2nd SC board, type 1 and press Enter.

Installation complete.

*********************************************************************************
* YOU MUST CONFIGURE THE SYSTEM !!! *
*********************************************************************************

If you are installing the 1st SC, you should configure it now. If you are installing the 2nd SC, you should copy configuration from 1st SC.

Are you installing the 1st or 2nd SC board? (1=1st SC/2=2nd SC) [1]: 1

System Configuration

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

8. At the Global SC IP address prompt, type the IP address to be assigned to the Active SC board and used to interface the Media Gateway OAM by external entities (e.g., EMS).

Global SC IP Address [0.0.0.0]: 10.7.13.90

9. 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

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

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

11. At the EMS server IP Address prompt, enter the IP address of the EMS server.

EMS Server IP Address [0.0.0.0]: 10.7.6.7
12. 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
```

**Note 1:** Time zone names are specified in a standard UNIX tz/zoneinfo format. 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).

Refer to the http://www.timezoneconverter.com for a complete list of supported time zone names, their DST settings and current time in each time zone.

**Note 2:** For major US and European cities, short time zone name (without continent name) is supported as well – e.g. Paris instead of Europe/Paris.

**Note 3:** Complete list of supported time zone names may also be viewed by issuing the following command on the SC board:

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

13. At the Enable Security prompt, to enable Security, type 1. To disable Security, type 0. For more information refer to Configuring Security Settings on page 209.

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

14. If you have enabled Security, you are prompted to enter the EMS IKE Pre-Shared Key. We recommend you type in an IKE Pre-Shared Key consisting of at least 10 characters (no spaces among them).

```
EMS IKE Pre-Shared Key [leave unchanged]: **********
```

**Note:** The Media Gateway with enabled Security must be defined accordingly in the EMS. The same IKE Pre-Shared Key must be entered in the Media Gateway Details screen. Refer to IPSEC and IKE on page 224.

15. You are prompted to enter the SC Root Password and the SNMP Read and Write Community strings. To leave a password unchanged, press Enter. To change a password, enter the new password. It must be at least 8 characters. Re-enter the new password when prompted.
5. Hardware Replacement Procedures

The default password and SNMP community strings are:

- SC Root Password - root
- SNMP Read Community - public
- SNMP Write Community - private

<table>
<thead>
<tr>
<th>SC Root Password</th>
<th>[leave unchanged]: ******</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP Read Community</td>
<td>[leave unchanged]: ******</td>
</tr>
<tr>
<td>SNMP Write Community</td>
<td>[leave unchanged]: ******</td>
</tr>
</tbody>
</table>

**Note:** For security purposes, it is recommended to change these passwords. Make a note of the new passwords you create and keep this record in a secure location for future reference.

16. At the NTP server IP Address prompt, type the IP address of the NTP server or 0.0.0.0 to use EMS server as the NTP server and press Enter.

NTP Server IP Address (0.0.0.0 - use EMS IP; 1.1.1.1 - none) [0.0.0.0]: 0.0.0.0

17. At the Product Type prompt, type the number that correspond to the system that you are installing and press Enter.

Product Type (0-Mediant 8000, 2-Mediant 5000, 4-Mediant 8000 Broadband Access, 5-Mediant 5000 Broadband Access, 6-IPmedia 5000, 7-IPmedia 8000) [2]: 2

A summary of the settings is displayed.

A summary of the settings is displayed.

---------------------------------------------------------------------
Configuration Summary:
---------------------------------------------------------------------
Global SC IP Address : 10.7.9.245
1st SC IP Address : 10.7.13.104
2nd SC IP Address (or 1.1.1.1 if none) : 10.7.13.91
EMS Server IP Address : 10.7.6.21
Enable Security : 0 (no)
SC Root Password : ******
SNMP Read Community : ******
SNMP Write Community : ******
---------------------------------------------------------------------
NTP Server IP Address (0.0.0.0 - use EMS IP; 1.1.1.1 - none) : 0.0.0.0
Product Type : 2 (Mediant 5000)
18. 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 ...
   >>> Restore file /etc/inet/services from the backup ...
   >>> refresh INET daemon ...
   >>> Update root password ...
   >>> Disable IPSEC configuration ...
   >>> Configure Timer Resolution ...
   >>> Make backup of modified file /etc/system ...

(This sequence is abbreviated)

*******************************************************
* NOTE: To configure the OAM VLAN, run 'tools vlan' script *
* on the Active SC (usually the 1st SC) after reboot. *
*******************************************************

*******************************************************
* IF THE CONFIGURATION IS SUCCESSFUL *
* YOU MUST REBOOT THE SC !!!!!!!!!! *
*******************************************************

19. When installing software on both SC boards, proceed with the Installing the SC Software on the 2nd SC Board on page 301. When you complete installing the 2nd SC board, reboot both SC boards.

   Note: When installing software on both SC boards, DO NOT reboot the 1st SC board until you complete configuration of the 2nd SC board. Reboot both SC boards simultaneously.

To reboot the SC board, at the Reboot now prompt, type y or accept the default. Press Enter and confirm, when prompted.

IMPORTANT: If the system configuration includes a 2nd SC, DO NOT REBOOT the 1st SC until the installation of the 2nd SC is complete.

REBOOT now? (y/n) [y]: y
Are you sure (n/y) [y]: y
5. Hardware Replacement Procedures

The SC board reboots and begins operating automatically using the new software configuration.

5.2.5 Installing the Media Gateway Software on the 2nd SC Board

The Media Gateway software installation process described in this chapter is used in the event of one of the following:

- The originally Active SC board in Slot 1 has failed and switchover has taken place enabling the SC board in Slot 2 to take over the Active functionality. The SC board in Slot 1 has been replaced and now requires this installation process.

- Similar to the above scenario, however, the SC board in Slot 2 has failed and the SC board in Slot 1 has taken over the Active status. The SC board in Slot 2 has been replaced and now requires this installation process.

- If both SC boards are replaced, the SC board in Slot 2 requires this installation process.

➢ To install the Media Gateway software on the SC board to be the Standby board, take these 10 steps:

1. Connect to the SC board that is to be Standby via Telnet, SSH or RS-232 Console. For more information, refer to Connecting to the SC Board’s Terminal on page 89.

2. Login as root user. For more information, refer to Users on SC Board’s Terminal on page 92.

3. At the prompt, type /install.pl and press Enter. The integrity of the software installation package is verified and its version is displayed.

```
client241:~# /install.pl

  Found compressed Audiocodes installation package - uncompress it...
     >>> uncompressing /sc_software.tar.gz file (this takes around 20 sec)...
     >>> done

  Verify installation package integrity...

  Unpack package version information...
     >>> unpacking version information (this takes around 10 sec)...
     >>> done

  Found the following Audiocodes installation package:

  --------------------------
  Core Network Media Gateway
  Version : 5.0.14
  --------------------------
```

4. When you are asked if you want to install, type y and press Enter. The software installation and basic configuration menu appears.

```
Do you want to install ([y]/n) [y]: y
```
Unpack version-specific installation script...
   >>> unpacking /install.pl file (this takes around 10 sec)...
   >>> done

Run version-specific installation script

-------------------------------------
SC Software Installation & Basic Configuration
-------------------------------------

1 - Update SC network parameters.
2 - Install and configure.
3 - Change installed configuration.
4 - Copy configuration from Active SC.
5 - Uninstall the software.
0 - Quit.

5. To select option 2 - Install and configure, at the Choose prompt, type 2 and press Enter. The installation sequence begins.

Choose (0-5) : 2

>>> Verifying the installation package integrity ...
>>> Verifying the OS version ...

******************************************************************************
******************************************************************************
**     WARNING: Installation will delete current configuration !!!!
** For typical Media Gateway systems in which software is preinstalled, select option "3 - Change installed configuration".
******************************************************************************
******************************************************************************

6. You are prompted if you want to install. Type y and press Enter. The installation sequence proceeds.

Do you want to install? (y/n) [n]: y

-------------------------------------
Install SC Software
-------------------------------------

>>> Clean up /tftboot directory ...
5. Hardware Replacement Procedures

>>> Clean up CDR directory ...
>>> Extract all files from TAR ...

(This sequence is abbreviated)

Installation complete.

*********************************************************************
*
YOU MUST CONFIGURE THE SYSTEM !!! *
*********************************************************************

7. After installation is successfully completed, the basic configuration of SC software must be performed. You are asked whether you are installing the 1st or the 2nd SC board. To select the 2nd SC board, type 2 and press Enter.

If you are installing the 1st SC, you should configure it now.
If you are installing the 2nd SC, you should copy configuration from 1st SC.

Are you installing the 1st or 2nd SC board? (1=1st SC/2=2nd SC)
[1]: 2

Note 1: When only one SC board is replaced, always choose the 2nd SC board for installation of the replacement board, even if the replaced board physically resides in the Slot #1. This answer significantly simplifies the configuration procedure, because all configuration data is copied from the Active SC board.

Note 2: If, by mistake, you choose 1st SC board option, you can proceed with the configuration, but be sure to answer the configuration prompts as shown in Installing Media Gateway Software on the 1st SC board on page 295. Make sure to provide exactly the same configuration information as set in the Active SC board.

8. At the CLI user name prompt, enter the name of a CLI user on the 1st SC board. (e.g. cli). For more information, refer to Users on SC Board's Terminal on page 92.

Note: You can use any CLI user defined on the 1st SC board.

-------------------------------------------------------------
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.
Please provide the following credentials:
CLI user name [cli]: cli

9. At the CLI user password prompt, enter the password of the specific CLI user on the 1st SC board (e.g., cli_12345).

CLI user password:

10. At the ROOT password prompt, enter the password of root user on the 1st SC board (e.g., root).

ROOT user password:

11. Configuration is copied from the 1st SC board and a summary of the settings is displayed.

Logging into other SC...cli...root...Success!

Copying Files...Done!

A summary of the settings is displayed.

Configuration Summary:

Global SC IP Address            :  10.7.9.245
1st SC IP Address               :  10.7.13.104
2nd SC IP Address (or 1.1.1.1 if none)  :  10.7.13.91
EMS Server IP Address           :  10.7.6.21
Enable Security                 :  0 (no)
SC Root Password                :  *****
SNMP Read Community             :  *****
SNMP Write Community            :  *****

12. You are prompted to start configuring. Type y and press Enter. The configuration begins.

Start configuring (y/n) [y]: y

>>> 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 ...
    >>> refresh INET daemon ...
    >>> Update root password ...
    >>> Disable IPSEC configuration ...
    >>> Configure Timer Resolution ...
    >>> Make backup of modified file /etc/system ...

(This sequence is abbreviated)
5. Hardware Replacement Procedures

13. To reboot the SC board, at the Reboot now prompt, type y or accept the default. Press Enter and to confirm, repeat.

```
IMPORTANT: If the system configuration includes a 2nd SC, DO NOT REBOOT the 1st SC until the installation of the 2nd SC is complete.

Reboot both SCs at the same time.

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

The SC board reboots and begins operating automatically using the new Media Gateway software installed on it.

5.3 Media Gateway Board Replacement Procedure

In the unlikely event of a Media Gateway board failure, the Avaya G860 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 Avaya G860 is under power.

The procedure for removing and inserting the 6310/RTM/STM1-OC3 or 6310/RTM/T3 includes different cabling requirements.

➢ To remove a Media Gateway board from the chassis, take these 4 steps:

1. In the EMS, lock the Media Gateway board to be replaced. For more information refer to the Element Management System User’s Manual, Document #: LTRT-910xx.

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, take these 8 steps:

1. Hold the board Horizontal.
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, refer to the Diagnostics on page 343.)
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 refer to the Element Management System User's Manual, Document #: LTRT-910xx.

To remove the Media Gateway RTM from the chassis, take these 5 steps:

1. In the EMS, lock the Media Gateway board of the RTM to be replaced. For more information refer to the Element Management System User’s Manual, Document #: LTRT-910xx.
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 RTM into the chassis, take these 6 steps:

1. Hold the board Horizontal.
5. Hardware Replacement Procedures

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. Connect the cables as detailed below.

➢ To cable the 6310/RTM STM1-OC3 interfaces, take these steps:

1. Connect the PSTN Fiber Optic Cable.

2. On the 6310/RTM/ (shown in 6310/RTM Diagram, carefully attach twin fiber optic cable with OC-3 connectors to the PSTN transceivers (Tx and Rx).

3. Connect the other end of the twin fiber optic cable with OC-3 connectors to your PSTN network.

4. In the EMS, unlock the Media Gateway board that has been replaced. For more information refer to the *Element Management System User’s Manual*, Document #: LTRT-910xx.

➢ To cable the 6310/RTM T3 interfaces, take these 4 steps:

1. On the 6310/RTM, connect twin single-mini-SMB T3 cables to each of the T3 connectors. Refer to Connecting the PSTN T3 Interfaces on page 86.

2. Place dust covers on the unused ports.

3. Connect the other end of the twin single-mini-SMB T3 cables to your PSTN network.

4. In the EMS, unlock the Media Gateway board that has been replaced. For more information refer to the *Element Management System User’s Manual*, Document #: LTRT-910xx.

5.4 Adding Media Gateway Boards to an Avaya G860 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 an Avaya G860 system, take these 4 steps:

1. In the desired empty slot in the Avaya G860 chasses, physically add the Media Gateway board and the corresponding RTM, using the procedures described in Hardware Replacement Procedures on page 289, and according to the constraints listed in the section below.

2. To add a board to the Media Gateway software, in the EMS, right-click on the corresponding slot and from the popup menu, select Add Board. Refer to the AddBoard action described in Media Gateway Board Actions on page 117.

3. Provision the Media Gateway board's parameters and relevant applications. Refer to Configuring & Operating the Media Gateway on page 109 for details.
4. When the configuration is complete, unlock the Media Gateway board. Right-click on it and from the popup menu, select **Maintenance>Unlock**.

### 5.4 Constraints for Adding Boards to the Avaya G860 System

For system configurations with TP-6310 boards:

Slots 7 to 10 are used for provisioning up to 4 TP-6310 boards (including the redundant TP-6310 board) according to the customer’s requirements. The corresponding RTMs are located in the rear cage of the Avaya G860 Media Gateway in the corresponding slot.

In less than a full configuration, place boards from slot 10 to 7, adding boards from the highest slot number to the lowest slot number. Unused slots must be covered using the appropriate blank panel. Refer to the Board Assembly Order on page 51.

**Note:** The Avaya G860 does not support a combination of T3 PSTN and STM-1/OC-3 PSTN interface types in the same system. When one of the interface types is selected at the board level in the EMS, the other type is disabled:

- STM-1/OC-3 interface type provides 1+1 PSTN. The rest T3 interfaces are disabled.
- T3 interface type provides 3 T3 interfaces only. The STM-1/OC-3 interfaces are disabled.

### 5.4.2 Troubleshooting the Newly installed Media Gateway Board

In rare cases, a newly installed Media Gateway board may not return to service (become Enabled) after performing the **Unlock** action in the EMS.

➢ **If this happens, to solve the problem, take these 7 steps:**

1. In Media Gateway Provisioning screen, change the **Board Provisioning Mode** parameter to **MAC Address**.
   a. Access the **MG Status** screen.
   b. Click **Properties**. The Media Gateway Provisioning Screen appears.
   c. In the **MG General Settings** tab, change the **Board Provisioning Mode** parameter to **MAC Address**.

2. Lock the Media Gateway board
   a. Select the newly added Media Gateway board and right-click on it.
   b. From the popup menu, select **Maintenance > Lock**.

3. Ascertain Media Gateway board's MAC address(es) as described below.

4. In the Media Gateway board's Provisioning Screen, provision the ascertained MAC addresses.
   a. Click **Properties**. The Media Gateway Provisioning Screen appears.
b. In the **General Settings** tab, enter the ascertained MAC address(es) as appropriate.

5. Unlock the Media Gateway board.
   a. Select the newly added Media Gateway board and right-click on it.
   b. From the popup menu, select **Maintenance > Lock**.

6. Wait up to 5 minutes until Media Gateway board becomes Enabled.

7. When finished, in Media Gateway Provisioning screen, turn the **Board Provisioning Mode** parameter to **Geographical Address**.
   a. Return to the **MG Status**.
   b. Click **Properties**. The Media Gateway Provisioning Screen appears.
   c. In the **MG General Settings** tab, return the **Board Provisioning Mode** parameter to **Geographical Address**.

### 5.4.3 Ascertaining the MAC Addresses for the TP-6310

Each TP-6310 board has one CPU module. The CPU module has its own MAC address that is indicated on a sticker attached to the board. Refer to Hardware Replacement Procedures on page 289 for information about removing and inserting the board.

### 5.5 SA/RTM Replacement Procedure

➢ **To remove an SA/RTM from the chassis, take these 4 steps:**

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, take these 9 steps:**

1. Hold the board Horizontal 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.

5.6 Ethernet Switch Board Replacement Procedure

The latest version of the ES boards are pre-loaded with v3.0 software and, therefore, can be inserted into the chassis followed by the lock/unlock procedure in the EMS.

If an older version of the ES board is in stock, it is not pre-loaded with v3.0. In the EMS, this ES board fails to unlock and remains marked in red in EMS. For these ES boards, the IP address must be configured in the ES board and then, in the EMS, repeat the lock/unlock procedure on the ES board. Refer to Configuring the IP Address of the ES Board Software on page 311.

➢ To remove an Ethernet Switch board from the chassis, take these 5 steps:

1. In the EMS, lock the Ethernet Switch board to be replaced. For more information refer to the Element Management System User’s Manual, Document #: LTRT-910xx.

2. Remove the cables attached to the Ethernet Switch board.

3. Unfasten the screws on the plate of the board.

4. 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.

5. Pull on the two ejector/injector latches and ease out the board from the slot.

➢ To insert an Ethernet Switch board into the chassis, take these 9 steps:

1. Hold the board Horizontal 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. Reconnect the cables.

8. In the EMS, unlock the Ethernet Switch board that has been replaced. For more information refer to the Element Management System User’s Manual, Document #: LTRT-910xx.

9. After 5 min., in the EMS, verify that the Ethernet Switch board is enabled.
5. Hardware Replacement Procedures

To remove an Ethernet Switch RTM from the chassis, take these 4 steps:

1. In the EMS, lock the Ethernet Switch board of the RTM to be replaced. For more information refer to the Element Management System User’s Manual, Document #: LTRT-910xx.
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, take these 9 steps:

1. Hold the board Horizontal 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. (Refer to Ethernet Switch Boards on page 44.).
7. In the EMS, unlock the Ethernet Switch board of which the RTM has been replaced. For more information refer to the Element Management System User’s Manual, Document #: LTRT-910xx.
8. In the EMS, verify that the Ethernet Switch board is enabled.
9. In the EMS Main screen, Status pane, double click on the Ethernet Switch board of the RTM that has been replaced. In the dialog box that appears, verify that the uplink port is enabled.

5.6.1 Configuring the IP Address of the ES Board Software

If the ES board fails to unlock in the EMS and remains Disabled (with a Red indicator) the ES board requires that its IP address is reconfigured. Use the procedure below to configure the correct IP address for the ES board.

Note: IP address configured in this section 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 is made invisible to the other equipment in the IP network.

To configure the IP address on the ES board, take these 6 steps:

1. Connect to the Switch Board's RS232 console.
2. Log in using the username: admin and 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).

\[
\text{# ip config sw0 10.1.1.35}
\]

4. In the EMS, open the ES board's Provisioning Screen and provision the same IP address as configured in the previous step.

5. Repeat the lock/unlock procedure on the ES board.

6. After 5 min. verify that the Ethernet Switch board is Enabled.

### 5.7 Power Supply Module Replacement

- **To remove a faulty power supply, take these 4 steps:**
  1. Unfasten the 4 screws on the plate of the power supply to be removed.
  2. Press the red ejector button on the black ejector/injector latch.
  3. Pull on the ejector/injector latch and ease out the power supply from the slot.

- **Caution**
  Use EITHER the AC or the DC power supplies. Never connect both types of power supplies at the same time, as chassis malfunction or permanent damage can result.

- **To insert a replacement power supply, take these 6 steps:**
  1. Hold the power supply horizontally with the black ejector/injector latch pointed outward.
  2. With the black ejector/injector latch in the open (pulled out) position, insert the power supply in the slot.
  3. Ease the power supply all the way into the slot until the ejector/injector latch touches the chassis.
  4. Press the black ejector/injector latch inward, toward the middle until you hear a click.
  5. Fasten the screws.
  6. In the EMS, verify that the alarm trap (regarding the faulty power supply) now displays status **Clear**. If the Power Supply module has not been properly secured.
or is still faulty, a red icon (see figure below) is displayed in the Avaya G860 EMS status screen and alarm traps with details of the fault are displayed in the EMS Alarm window. If the Power supply module is OK and properly secured to the Chassis, a green (see figure below) is displayed in the Avaya G860 EMS status screen and an alarm trap with status Clear is displayed in the EMS Alarm window.

![Figure 5-6: EMS Avaya G860 Status screen-Power Supply Status](image)

**Note:** Ensure you verify the details of all traps in the EMS Alarm window.

### 5.8 Replacing the PEM AC Fuse

The AC inlet contains two fuses, one for each pole.

➢ *To replace a faulty fuse in the PEM AC version:*

1. On the PEM, open the fuse cavity cap as described in Connecting System Power on page 70.
2. Remove the faulty fuse.

### 5.9 Replacing the PEM

➢ *To remove a faulty PEM, take these 6 steps:*

1. Shut off the current to the power inlet of the PEM to be removed.
2. Remove the power cables from the power inlet. Remove the power cable from the power inlet. For a 6310 configuration-one cable per PEM.
3. Remove the Earth connections.
4. Release the screws on the front panel of the PEM. For a 6310 Configuration- 4 screws.
5. For a 6310 Configuration only: release the latch, press the red button. Wait for the Swap Ready LED to turn blue.
6. Open the Latch and pull on the PEM to remove it.

➢ *To insert a replacement PEM, take these 7steps:*

1. Insert the PEM into its slot, until the front panel is flush with the chassis plate.
2. Close the latch and wait for the Swap Ready LED to turn off.
3. Fasten the screws at both ends of the PEM.
4. Attach the Earth connections. Refer to Earthing on page 68.
5. Attach the power cables. Refer to Connecting System Power on page 70.

6. Verify that the Power LED is green.

7. In the EMS, verify that the alarm trap (regarding the faulty PEM) now displays status **Clear**. If the PEM has not been properly secured or is still faulty, a red icon is displayed (see figure below) in the Avaya G860 EMS status screen and alarm traps with details of the fault are displayed in the EMS Alarm window. If the PEM is OK and properly secured to the Chassis, a green icon is displayed (see figure below) in the Avaya G860 EMS status screen and an alarm trap with status **Clear** is displayed in the EMS Alarm window.

![Figure 5-7: EMS Avaya G860 Status screen-PEM Status](image)

**Note:** Ensure you verify the details of all traps in the EMS Alarm window.

### 5.10 Replacing the Fan Tray Unit

**Note 1:** Be sure to prepare a replacement fan tray unit (either FML-5/Left Fan Tray or FMR/5K) before removing the faulty fan tray unit. It is imperative the chassis does NOT remain without the fan tray unit for more than a short period of time (20 sec).

**Note 2:** In a 6310 configuration, this fan tray is labeled **FML-5**.
5.10.1 Replacing the FML-5 Fan Tray Unit

The fan tray unit (FML-5/Left Fan Tray) is located to the left of the chassis cage.

➢ To remove a faulty FML-5 fan tray unit, take these 4 steps:

1. In the EMS, verify that the FML-5/Left Fan Tray fan tray unit is rotating at maximum speed: large fans at 4900 - 5500 RPM; small fans at 5000 - 5650 RPM). Refer to Checking the Fan Speeds on page 266.

2. Release the 2 screws on the top left-hand corner and the bottom left-hand corner of the front panel of the fan tray unit.
3. Pull on the fan tray unit’s handle outward by 2 cm.
4. Wait for the fans to stop rotating and then remove the fan tray completely.

➢ **To insert a replacement FML-5 fan tray unit, take these 5 steps:**

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 2 screws at both ends of the fan tray unit.
3. Verify that the fans are functioning correctly by putting your left hand over the grill on the left side of the Avaya G860 chassis (when facing the front cage), and your right hand over the grill on the right side. Your left hand should feel a reasonably strong suction of the air drawn in by the fans. Your right hand should feel the air blowing reasonably strongly out of the Avaya G860.
4. Verify in the EMS that the Fan Speed settings are within the accepted range: large fans at 4900 - 5500 RPM; small fans at 5000 - 5650 RPM). Refer to Checking the Fan Speeds on page 266.
5. In the EMS, verify that the alarm trap (regarding the faulty fan tray unit) now displays status **Clear**. If one or more of the fans in the Fan Tray unit is faulty, an orange icon is displayed (see figure below); if the fan tray unit has not been properly secured, a red icon is displayed (see figure below) in the Avaya G860 EMS status screen and alarm traps with details of the fault are displayed in the EMS Alarm window. If the Fan Tray unit is OK and properly secured to the Chassis, a green fan is displayed (see figure below) and an alarm trap with status **Clear** is displayed in the EMS Alarm window.

![Figure 5-9: EMS Avaya G860 Status screen-Fan Status](image)

**Note:** Ensure you verify the details of all traps in the EMS Alarm window.

### 5.10.2 Replacing the FMR/5K Fan Tray Unit - 5000

The fan tray unit (FMR/5K) is located to the right of the chassis cage.

➢ **To remove a faulty FMR/5K fan tray unit, take these 5 steps:**

1. In the EMS, verify that the FMR/5K fan tray unit is rotating at maximum speed: 10500 - 12500 RPM. Refer to Checking the Fan Speeds on page 266.
2. Release the 6 screws on the front panel of the FMR/5K fan tray unit.
3. To release the latch, press the red button. Wait for the Swap Ready LED to turn blue.
4. Open the Latch and pull on the fan tray unit’s handle outward by 2 cm.
5. Wait for the fans to stop rotating and then remove the fan tray completely.

To insert a replacement fan tray unit, take these 7 steps:

1. Insert the fan tray module into its slot, until the front panel is flush with the chassis plate.
2. Wait for the Swap Ready LED to turn off and close the latch.
3. Secure the Fan Tray in its slot by fastening the screws at both ends of the fan tray unit.
4. Verify that the Power LED is green.
5. Verify that the fans are functioning correctly by putting your right hand over the grill on the right side of the Avaya G860 chassis (when facing the front cage). Your right hand should feel the air blowing reasonably strongly out of the Avaya G860.
6. Verify in the EMS that the Fan Speed settings are within the accepted range: 10500 - 12500 RPM. Refer to Checking the Fan Speeds on page 266.
7. In the EMS, verify that the alarm trap (regarding the faulty fan tray unit) now displays status **Clear**. If one or more of the fans in the Fan Tray unit is faulty, an orange icon is displayed (see figure below); if the fan tray unit has not been properly secured, a red icon is displayed (see figure below) in the Avaya G860 EMS status screen and alarm traps with details of the fault are displayed in the EMS Alarm window. If the Fan Tray unit is OK and properly secured to the Chassis, a green fan is displayed (see figure below) and an alarm trap with status **Clear** is displayed in the EMS Alarm window.

![Figure 5-10: EMS Avaya G860 Status screen-Fan Status](image)

**Note:** Ensure you verify the details of all traps in the EMS Alarm window.

5.11 Replacing the Fan Power Units

5.11.1 Replacing the FPM/5K Fan Power Module

To remove an FPM/5K fan power module, take these 3 steps:

1. Release the 4 screws on the front panel of the FPM/5K advanced fan power module.
2. To release the latch, press the red button. Wait for the Swap Ready LED to turn blue.
3. Open the Latch and pull on the FPM/5K advanced fan power module’s handle outward. Remove it completely.
To insert a replacement FPM/5K fan power module, take these 4 steps:

1. Insert the FPM/5K advanced fan power module into its slot, until the front panel is flush with the chassis plate.
2. Close the latch and wait for the Swap Ready LED to turn off.
3. Fasten the screws at both ends of the FPM/5K advanced fan power module.
4. Verify the Power LED is green.

5.12 Replacing Air Filters

The NEBS compliant air filters should be replaced approximately every 90 days. Air Filters - View from Front indicates the locations of the filters and shows the air filter partially removed from the Avaya G860.

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, take these 2 steps:

1. Remove the fan tray unit (refer to Replacing the Fan Tray Unit).
2. With your fingertips, grasp the inside of the steel frame of the air filter and pull it out of its slot. It should slide out relatively easily.

To reinsert the air filter, take these 5 steps:

1. Remove the fan tray unit.
2. Slide the air filter into its slot accordingly, pushing it all the way in.
3. Replace the fan tray unit in its location into the chassis (refer to Replacing the Fan Tray Unit).
4. Verify that the fan tray unit is functioning correctly by putting your left hand over the grill on the left side of the Avaya G860 chassis (when facing the front cage), and your right hand over the grill on the right side. Your left hand should feel a reasonably strong suction of the air drawn in by the fan. Your right hand should feel the air blowing reasonably strongly out of the Avaya G860.

5. In the EMS, verify that the alarm trap (regarding the faulty fan tray unit) now displays status **Clear**. If one or more of the fans in the Fan Tray module is faulty, an orange icon is displayed (see figure below); if the fan tray module has not been properly secured, a red icon is displayed (see figure below) in the Avaya G860 EMS status screen and alarm traps with details of the fault are displayed in the EMS Alarm window. If the Fan Tray module is OK and properly secured to the Chassis, a green fan is displayed (see figure below) and an alarm trap with status **Clear** is displayed in the EMS Alarm window.

**Figure 5-12: EMS Avaya G860 Status screen-Fan Status**

![Fan Status Icons]

**Note:** Ensure you verify the details of all traps in the EMS Alarm window.
6 Software Upgrade

Online Software Upgrade is available for the Avaya G860 system. The procedures must be carried out on both SC boards.

To distinguish between the two SC boards, 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

**Note:** To start at a consistent point, it is recommended to perform Online Software Upgrade when the 1st SC board (in Slot 1) is Active and 2nd SC board (in Slot 2) is Standby. If needed, perform SC switchover to achieve this configuration.

6.1 Online Software Upgrade – Overview

The Online Software Upgrade is performed when the Avaya G860 Media Gateway is up and running. Online Software Upgrade upgrades the software on all Media Gateway components, including:

- System Controller boards
- Media Gateway boards
- Ethernet Switch boards

The Media Gateway configuration is preserved throughout the upgrade 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 user to return the Avaya G860 Media Gateway to the pre-upgrade software version and configuration in case of any problem.

**Effect on the Media Gateway Service**

The Avaya G860 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 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 Avaya G860 Media Gateway service, Media Gateway boards are upgraded one at a time.
**Hitless Upgrade Mode**

Starting from ver.5.2, 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;
- Media Gateway board Redundancy was not properly configured for hot switchover prior to 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, refer to section Graceful Shutdown Mode below.

**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.

### 6.2 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.
6. Software Upgrade

Note: This backup should be only 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.

➢ To perform a full configuration backup, take these 2 steps:

1. At the prompt, type `tools bk` and press Enter.

```
client208::~# tools bk
```

2. Store the backup file (default name - `backup bk`) on a third-party server.

For details on performing a backup, refer to Media Gateway Software Backup/Restore Procedures on page 103.

6.3 Preparing for Online Software Upgrade

6.3.1 Preparing the Media Gateway

The following conditions must be met prior to starting the Online Software Upgrade procedure:

- Both SC boards are in service (i.e., UNLOCKED/ENABLED).
- Both ES boards have up-links properly connected and are in service (i.e., UNLOCKED/ENABLED).
- All Media Gateway boards are either in service (i.e., UNLOCKED/ENABLED) 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.

6.3.2 Preparing the Media Gateway Boards

Media Gateway boards must have a License Key that supports the new software version to which you are upgrading. The `Max SW Version` parameter of the License Key must be greater than or equal to v2.

You must ensure that each Media Gateway board has the correct License Key prior to starting the Online Software Upgrade. Otherwise, the Online Software Upgrade will fail to operate.

➢ To verify the status of the License Key of all of the Media Gateway boards, take these 6 steps:

1. Upload the `fk_update.pl` script from the Media Gateway software installation CD to the `/tmp` directory on Active SC board via FTP or SCP/SFTP protocol.
2. Connect to the Active SC board via Telnet, SSH or RS-232 Console (refer to Connecting to the SC Board’s Terminal on page 89).

3. Login as root user (default password is root).

4. Use the following command to analyze the License Keys of all of the Media Gateway boards.

```plaintext
perl /tmp/fk_update.pl dump
```

```
=======
Media Gateway
=======

Global IP address : 10.7.9.242
Product type      : mediant5000(2)
TG version        : 5.2 (CMP 5.2)

... skipped ...

  Feature Key is OK

All TP boards have correct feature keys.
```

5. If any Media Gateway board has a wrong License Key, it is reported in the command output. Capture the command output and send it to Avaya Technical Support.

6. Wait until you are provided with a file containing the corrected License Keys for all of the Media Gateway boards as per your specification. Apply this file as described in the following section.

**Note:** Do not start Online Software Upgrade until the License Keys of all of the Media Gateway boards are correct.

- To update License Key of all of the Media Gateway boards using the provided License Key file, take these 4 steps:

  1. Upload the License Key file and fk_update.pl script from the Media Gateway software installation CD to the /tmp directory on Active SC board via FTP or SCP/SFTP protocol.
  2. Connect to the Active SC board via Telnet, SSH or RS-232 Console (refer to Connecting to the SC Board’s terminal).
  3. Login as root user (default password is root).
  4. Use the following command to update the License Key of all of the Media Gateway boards using the provided License Key file. (In this example, replace <LicenseKeyFile> with the actual file name.)

```plaintext
perl /tmp/fk_update.pl /tmp/<LicenseKeyFile>
```
6. Software Upgrade

6.1 Media Gateway

Global IP address : 10.7.9.242
Product type      : mediant5000(2)
TG version        : 5.2 (CMP 5.2)

... skipped ...

Update Feature Key...  Success!

All TP boards were updated with correct feature keys.

```
client238:~#
```

Note: The License Keys go into effect **only** after the Media Gateway boards are restarted. Optionally, after License Key update, from the EMS, lock/unlock the Media Gateway boards. However, lock/unlock is not a mandatory step, since boards are reset during the Online Software Upgrade.

6.3.3 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:

\[
T_{\text{upload}} = \frac{25}{B} \text{ min}
\]

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 or 10 Mbps, the transfer takes approximately 2.5 minutes.

6.3.4 Verifying that Online Software Upgrade is Supported

Make sure that an upgrade to ver.5.2 from the specific Media Gateway version is supported. Avaya officially supports upgrade to ver.5.2 only.

For additional information and clarifications contact Tech Support.
6.3.5 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):

\[ T_{\text{upgrade}} = 15 \text{ min} + 2 \times T_{\text{upload}} + T_{\text{MGboard}} \times N_{\text{MGboard}} + 2 \times T_{\text{OSpatch}} + 2 \times T_{\text{ESboard}} \]

where:

- \( T_{\text{upload}} \) 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 325. 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 334.

- \( N_{\text{MGboard}} \) 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.

- \( T_{\text{MGboard}} \) is the time of a Media Gateway board's upgrade. For Hitless Upgrade mode, it approximately equals 5 minutes when no VLAN are used, or 10 minutes when VLANs are used. For Graceful Shutdown mode, it may be calculated using the following formula: \( T_{\text{MGboard}} = 2 + T_{\text{ESboard}} \), where \( T_{\text{Graceful Shutdown}} \) 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.

- \( T_{\text{OSpatch}} \) is the time required for Solaris™ 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 to ver.5.2 from an earlier software version (e.g., ver.3.2) the OS patch installation may take more than 1 hour on each SC board. To reduce this time, pre-install the OS patches as described in Pre-installing OS Patches on page 327.

- \( T_{\text{ESboard}} \) is the time of ES board's upgrade. If you upgrade to ver.5.2 from an earlier software version (e.g., ver.3.2), it takes approximately 6 minutes to upgrade each ES board. However, if you are upgrading between minor ver.5.2
6. Software Upgrade

versions 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 typical ver.3.2 to ver.5.2 upgrade of the Avaya G860 chassis with 3 Media Gateway boards in a decent IP network, as follows:

\[
T_{upload} = 2.5 \text{ min} \\
N_{MGboard} = 3 \\
T_{MGboard} = 4 \text{ min} \\
T_{OSpatch} = 60 \text{ min} \\
T_{ESboard} = 6 \text{ min} \\
T_{upgrade} = 15 + 2 \times 2.5 + 4 \times 3 + 2 \times 60 + 2 \times 6 \text{ min} \equiv 2h 45 \text{ min}
\]

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, refer Online Software Upgrade – Overview on page 321). Therefore, when you plan a maintenance time period, perform estimations of the Graceful Shutdown mechanism scenario as well.

6.3.6 Pre-installing OS Patches

When upgrading to ver.5.2 from an older software version (e.g., ver.3.2), a considerable amount of OS patches must be installed on each SC board. These OS patches provide better security and overall system stability.

Note: Upgrade to ver.5.2 from an older software version (e.g., ver.3.2) 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 to ver.5.2. The pre-installation of OS patches does not interrupt Media Gateway service. Old software (ver.3.2) runs normally on a system with new OS patches installed.

The Online Software Upgrade to ver.5.2 is significantly faster if OS patches are pre-installed beforehand. It takes approximately 1 hour depending on the amount of Media Gateway boards and the configured Graceful Shutdown period.

➢ To pre-install OS patches, take these 8 steps:

1. Connect to the 2nd (Standby) SC board via Telnet, SSH or RS-232 Console. For more information, refer to Connecting to the SC Board's Terminal on page 89.

2. Login as root user. If you are pre-installing OS patches on ver.3.2, you may directly login as root user over the remote IP connection (Telnet or SSH). Otherwise, refer to Users on SC Board's Terminal on page 92.
3. To stop currently running software, at the prompt, type `tools sc dn`.

```bash
client238::~# tools sc dn
STOP SC SOFTWARE
--------------
Stop SC software? ([y]/n) : y

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

Note: Media Gateway functionality is not interrupted because 1st (Active) SC board continues to operate. However, there is no SC board High Availability during the OS patches installation.

4. Upload the ver.5.2 software package (`sc_software.tar.tar`) and `install_os_patch.pl` script from the ver.5.2 installation CD to the `/tmp` directory on the 2nd (Standby) SC board (via FTP or SCP/SFTP). If you are re-installing OS patches on ver.3.2 software version, you may use root user for FTP or SCP/SFTP connection. Otherwise use any CLI user (e.g., user `cli`, password `cli_12345`) to perform file transfer.

Note: Upload the above-mentioned files to the `/tmp` directory and not `/` (root).

5. Install the OS patches, as described below. Be patient as the OS patches installation takes approximately 1 hour.

```bash
client238::~# cd /tmp
client238::~# perl install_os_patch.pl sc_software.tar
```

```
INSTALL SOLARIS OS PATCHES

>>> uncompress package file sc_software.tar
>>> extract OS patches...
>>> install OS patches...

(This sequence is abbreviated)

* SOLARIS OS PATCHES WERE INSTALLED *
* THAT REQUIRE SC REBOOT !!!!!!!!!! *

Reboot this SC by issuing the following command:
  reboot -- -r
```

```bash
client238::~#
```
6. When the **install_os_patch.pl** script finishes its sequence, you are informed about whether the SC board needs to be rebooted and are provided with the specific reboot command to be executed.

Reboot the SC board by typing the specific reboot command. Wait until the reboot is complete and verify in EMS GUI that SC board's operative state changes to Enabled.

7. Perform SC switchover to switch activity to the 2nd SC board (where the OS patches were already installed).

8. Install the OS patches on the 1st (initially Active, but currently Standby) SC board repeating the steps 1 to 7 above.

### 6.4 Performing the Online Software Upgrade

Before performing the Online Software Upgrade, verify in the EMS that:

- Both SC boards are green (AdministrativeState=UNLOCKED, OperationalState=ENABLED)
- Both Ethernet Switch boards are green (AdministrativeState=UNLOCKED, OperationalState=ENABLED)
- All unlocked Media Gateway boards are green (AdministrativeState=UNLOCKED, OperationalState=ENABLED); if you have a malfunctioning Media Gateway board – LOCK it

#### 6.4.1 Configuring the EMS and ROOT Passwords of the Avaya G860 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. Refer to EMS User Password Administration on page 249 and ROOT User Password Administration for detailed instructions on how to change **ems** and **root** passwords.

**Note 1:** When performing an Online Software Upgrade from ver.3.2 software, there is no need to enter the ems password, since the ems user account is not a valid account in this software version. Therefore, enter the root password only.

**Note 2:** Both SC boards must have the same **ems** and **root** passwords configured.

➢ **To configure the EMS and ROOT Passwords, take these 4 steps:**

1. In the MG Tree to the left, select the Media Gateway on which maintenance action is required.
2. Right click on the selected Media Gateway and in the popup menu, select the Details option. The MG Information dialog box appears.

![MG Information]

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 Root Password field, change the password to match the current password for the root user configured on both SC boards.

5. Click OK.

### 6.4.2 Starting the Online Software Upgrade Wizard

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, take these 4 steps:

1. In the MG Tree to the left, select the Media Gateway on which maintenance action is required.

2. Click the Maintenance Actions icon located at the top right of the Status screen. The popup menu appears (refer to the figure below).
3. Select the **Sw Upgrade** option. The Files Manager screen appears.
4. In the Files Manager screen, select the Media Gateway software version file to be upgraded to and click **OK**. You are asked to confirm your command. The Software Upgrade Wizard opens and guides you through the process.

**Note:** The Media Gateway software package must be added to the EMS Files Manager prior to starting the Online software Upgrade. During that process, the Media Gateway software package is transferred from the EMS client to the EMS server. This operation takes a few minutes in a typical IP network environment (assuming 10 Mbps bandwidth). However, it may take much longer if the IP network connection between EMS server and client has limited bandwidth. If so, to minimize the upgrade maintenance time period usage, it is recommended to add the Media Gateway software package to the EMS server prior to starting the Online Software Upgrade.

The Online Software Upgrade Wizard GUI includes a Wizard Stages screen section and a 'Summary Table' screen section. The Summary Table includes a summary of the Request / Response messages exchanged between the EMS server and each of the SC boards during the upgrade process. This screen can be used for debugging and to obtain additional information on the process.

The EMS's Online Software Upgrade Wizard guides users through these 6 steps:

1. Welcome Questionnaire
2. Upgrading the 2nd SC Board
3. Upgrading the Media Gateway Boards
4. Upgrading the ES boards
5. Upgrading the 1st SC Board
6. Finish

These steps are described below.

The upgrade procedure pauses after completing each of the major steps. At the finish of each of these major steps, verify the Media Gateway's functionality. Then, to proceed with the upgrade, click the **Next** button.

### 6.4.2.1 Welcome Questionnaire

The Welcome Questionnaire includes basic questions regarding the software upgrade process. 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, refer to Online Software Upgrade – Overview on page 321.
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** - allows the user to pause after the first Media Gateway board is upgraded and test the system to ensure that the upgrade process to the Media Gateway board functions has been successful before upgrading the remaining Media Gateway boards.

- **Pause after each Media Gateway board** - allows the user to pause 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 amount of calls affected by each Media Gateway board's upgrade.

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.

**Note:** 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.

**Note 2:** 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, refer to Online Software Upgrade – Overview). Therefore, set proper value of Graceful Shutdown Period and estimate required worst-case upgrade maintenance time.

**Note 3:** Rollback sequence always uses Graceful Shutdown mechanism. Therefore always set proper value for Graceful Shutdown Period for Abort parameter.
6.4.2.2 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 (assuming 10 Mbps 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 upgrade maintenance time period within the time period for maintenance (Maintenance Window), 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 6-5: EMS Online Software Upgrade Workaround](image)

3. When the software package transfer is complete, the Next button is newly activated.

**WARNING**

DO NOT click **Next**. Instead, proceed with the steps below.

4. To close the Upgrade Wizard, click the ![Close Window](image) 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.

6. The upgrade process continues from the step at which it left off earlier.

**6.4.2.3 Upgrading the 2nd SC Board**

In the first stage, the 2\(^{nd}\) (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 2\(^{nd}\) 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 (refer to the figure below).

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 6-6: Software Upgrade in Process, Managed by the SC Board**

When you upgrade to ver.5.2 from an older software version (e.g., ver.3.2) a large amount 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. The full OS patches installation typically takes **around 1 hour** to complete on each SC board. No user interaction is required.

For subsequent upgrades (e.g., between minor ver.5.2 versions), the "SC board upgrade" phase is considerably faster because all required OS patches are already installed.

**Note:** Upgrade to ver.5.2 from an older software version (e.g., ver.3.2) may take more than 3 hours because of 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 327

After the 2nd SC board is upgraded you can open the EMS and inspect the new Media Gateway configuration and status of the Media Gateway's components. Refrain from performing any configuration changes until the Online Software Upgrade is finished. The ES boards may be **Disabled** (colored red in the EMS) until they are upgraded to the new version. This does not indicate any malfunction.
6. Software Upgrade

6.4.2.4 Upgrading the Media Gateway Boards

The Media Gateway boards are upgraded one after another. The Media Gateway boards (except the Redundant board) are upgraded starting from the lowest slot number. Following this, the Redundant board is 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, refer to Online Software Upgrade – Overview on page 321 and Starting the Online Software Upgrade Wizard on page 330.

Depending on the options you chose in the Welcome Questionnaire on page 332, you can pause after the first Media Gateway board is upgraded (or after each Media Gateway board is upgraded) and verify that the process is successful.

With the first Media Gateway board, as well as the Active SC board upgraded, you can perform extensive testing of the new software in order to decide either to continue with the Upgrade or to Rollback to the previous software configuration.

Note: Media Gateway boards in a locked state are skipped by the Online Software Upgrade Wizard. They will be automatically upgraded as soon as they are unlocked (even after the Upgrade Wizard is no longer running).

6.4.2.5 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 Online Software Upgrade is started).

After upgrading the first (initially standby) ES board, you are prompted to click the Next button to proceed upgrading the second (initially active) ES board.

At this point, the Active SC board, all of the Media Gateway boards and the Active Ethernet Switch board are upgraded to the new software version, making all of the essential parts of the new software distributed across all types of the boards in the chassis. You can perform extensive testing at this point and decide whether to proceed with the Upgrade or to Rollback to the previous software configuration.

6.4.2.6 Upgrading the 1st SC Board

After the 2nd SC board, all of the Media Gateway boards and Ethernet Switch boards are upgraded, the 1st SC (now the Standby SC board) is upgraded to the new version.

6.4.2.7 Finish

The last Software Upgrade Wizard screen states that the upgrade process has finished.

Note: Perform a full software configuration backup as described in SC Software Backup/Restore Procedures on page 103 to assure backup availability should it be required later.
6.4.3 After Completing the Online Software Upgrade

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 ver.5.2 software that are not automatically activated when you upgrade from ver.3.2. You should manually activate these features as described in the relevant section.

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Detailed Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote access by <code>root</code> user</td>
<td>Remote access by <code>root</code> user is disabled on newly installed ver.5.2 software.</td>
</tr>
<tr>
<td></td>
<td>After completing Online Software upgrade, you must manually disable remote access by <code>root</code> user as it poses a severe security risk. For more information, refer to Disabling a Direct Remote Login on page 212.</td>
</tr>
<tr>
<td></td>
<td>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 SC board's terminal over the IP network.</td>
</tr>
<tr>
<td></td>
<td>For more information, refer to Users on SC Board's Terminal on page 92.</td>
</tr>
</tbody>
</table>

6.4.4 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 *X* button (in the top-right window corner).
6. Software Upgrade

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 Ethernet Switch boards are downgraded to the previous version automatically one by one – without any effect on the service (for more information, refer to Online Software Upgrade – Overview on page 321).

Note: The Hitless Upgrade mechanism is not supported for rollback. Rollback is always performed via the Graceful Shutdown mechanism.

6.4.5 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 servers 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, take these 3 steps:

1. Close and re-open the EMS client.
2. Restart the Upgrade Wizard on the specific Avaya G860 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 does not help perform the recovery, click the Connect button to recover from the network failure.

6.4.6 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.

6.4.6.1 Performing a Manual Rollback to the Previous Software Configuration

➢ To perform a manual rollback to the previous software configuration, take these 13 steps:

1. Close the EMS Upgrade Wizard screen.
2. Connect to both SC boards via Telnet, SSH or Console (refer to Connecting to the SC Board's Terminal on page 89).
3. Login as root user. If you are performing Online Software Upgrade from ver.3.2, you may directly login as root user over the remote IP connection (Telnet or SSH). Otherwise, refer to Users on SC Board's Terminal on page 92.
4. To stop the Media Gateway software on both SC boards, type tools sc dn and press Enter.

client208:~# tools sc dn
6. Software Upgrade

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 can not connect to some SC board via Telnet/SSH after completing the previous step, there most probably is some hardware failure on the board or severe software misconfiguration. Remove the failed SC board from the chassis. For details on replacing a failed SC board, refer to SC Board Replacement Procedure on page 290.

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 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, in order to roll them back to the previous software version.
7 Diagnostics & Troubleshooting

This section describes the recommended method for maintaining Avaya G860 Media Gateways. Avaya provides a wide range of diagnostic tools in order to enable users to easily identify an error condition and to provide a consequent solution or work around.

7.1 Troubleshooting Strategy

The goal of the maintenance procedures described in this section is, in the event 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) 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.
## 7.2 Troubleshooting

The table below presents possible courses of action to remedy faults arising in the Avaya G860 Media Gateway.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Possible Cause(s)</th>
<th>Actions to Take</th>
<th>Refer to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media Gateway is &quot;dead&quot;. All LEDs (on boards and power supply modules) are off or red and there is no sound from the ventilation fans.</td>
<td>Power supply problem&lt;br&gt; If it is a DC power supply, check the DC power connection and voltage. Connect all the power wires and turn on the appropriate switches&lt;br&gt; If it is an AC power supply, check that the AC power is connected and that the AC switch is on. Connect the AC power and turn on the switch.</td>
<td>Extract each power supply to see if it is a DC or AC power supply&lt;br&gt; Connect all the power wires and turn on the appropriate switches&lt;br&gt; Connect the AC power and turn on the switch.</td>
<td>Powering Up on page 69</td>
</tr>
<tr>
<td>Media Gateway operation is silent</td>
<td>Fans problem&lt;br&gt; Check the airflow from the ventilation holes on the chassis sides. Verify that the fan units are inserted properly.</td>
<td>Check the airflow from the ventilation holes on the chassis sides. Verify that the fan units are inserted properly.</td>
<td>Cooling System on page 26</td>
</tr>
<tr>
<td>No Console communication to the SC board.</td>
<td>Console settings&lt;br&gt; Check the communication port settings to verify: 9600, 8, N, 1</td>
<td>Check the communication port settings to verify: 9600, 8, N, 1</td>
<td>Connecting the SC Board's RS-232 Console on page 78</td>
</tr>
<tr>
<td>Cable connection</td>
<td>Cable connection&lt;br&gt; Verify that the Console cable is connected to the appropriate console connection (on SC board's front or on the SA/RTM module)</td>
<td>Verify that the Console cable is connected to the appropriate console connection (on SC board's front or on the SA/RTM module)</td>
<td>Connecting the SC Board's RS-232 Console on page 78</td>
</tr>
<tr>
<td>Wrong cable pinout</td>
<td>Wrong cable pinout&lt;br&gt; Verify that console cable pinout is correct.</td>
<td>Verify that console cable pinout is correct.</td>
<td>Front Panel Mini DIN 8 COM Serial Port on page 37&lt;br&gt; SA Synchronization and Alarm RTM on page 38</td>
</tr>
<tr>
<td>Cable problem</td>
<td>Cable problem&lt;br&gt; Replace the cable</td>
<td>Replace the cable</td>
<td>Replace the cable</td>
</tr>
<tr>
<td>No communication with the Media Gateway (ping to the private SC's IP doesn't work)</td>
<td>Chassis is disconnected from the network</td>
<td>Check that the ES boards' uplinks are properly connected to the external IP network</td>
<td>Cabling the Avaya G860 on page 81</td>
</tr>
<tr>
<td>Problem</td>
<td>Possible Cause(s)</td>
<td>Actions to Take</td>
<td>Refer to:</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>External network problems</td>
<td>Connect to the 1st SC board's RS-232 console and check the ping to the 2nd 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.</td>
<td></td>
<td>Recovering the OAM VLAN Settings on page 350</td>
</tr>
<tr>
<td>VLAN configuration mismatch</td>
<td>Verify that VLAN configuration of the Media Gateway matches VLAN configuration of the external IP network. Re-configure VLAN configuration if needed.</td>
<td></td>
<td>Connecting the SC Board's RS-232 Console on page 78</td>
</tr>
<tr>
<td>Wrong basic IP configuration of SC boards (e.g. subnet mask or default router)</td>
<td>Connect to the RS-232 console of the SC board. Verify it's basic network configuration and re-configure it if needed.</td>
<td></td>
<td>Working with the ES boards on page 121</td>
</tr>
<tr>
<td>ES board malfunction</td>
<td>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 &quot;reset procedure&quot;.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>No communication with the Media Gateway (ping to the private SC's IP works; but Telnet does not)</td>
<td>Media Gateway is in Secure Mode</td>
<td>Use SSH to connect to the Media Gateway's CLI interface on the SC boards in Secure Configuration Mode.</td>
<td>Configuring Security Settings on page 209</td>
</tr>
<tr>
<td>SC board is at the OpenBoot level (ok prompt)</td>
<td>Connect to the RS-232 console of the SC board. If you see the <strong>ok</strong> prompt – type <strong>go</strong> 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.</td>
<td></td>
<td>Connecting the SC Board's RS-232 Console on page 78</td>
</tr>
<tr>
<td>Problem</td>
<td>Possible Cause(s)</td>
<td>Actions to Take</td>
<td>Refer to:</td>
</tr>
<tr>
<td>---------</td>
<td>------------------</td>
<td>----------------</td>
<td>------------</td>
</tr>
<tr>
<td><strong>Duplicate IP address</strong></td>
<td></td>
<td>Verify that no other equipment uses the same IP address as the one assigned to the SC board. Connect to the RS-232 console of the SC board and check for &quot;duplicate IP address&quot; messages (wait a few minutes to see if the messages are recorded). If the &quot;duplicate IP address&quot; 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)</td>
<td>Connecting the SC Board's RS-232 Console on page 78</td>
</tr>
<tr>
<td><strong>Media Gateway software is not running on either SC board</strong></td>
<td></td>
<td>Media Gateway software starts automatically after the SC board is rebooted. If this does not help – one of the following scenarios must have happened: 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.pl script), but the system configuration (options 3 or 4) were not run – run the missing options.</td>
<td>Installing the Media Gateway software on the SC Board on page 291 Configuring the Basic IP Network Parameters of SC Boards on page 78</td>
</tr>
<tr>
<td><strong>Wrong SNMP manager settings</strong></td>
<td></td>
<td>Ensure that the SNMP manager is configured for SNMP v1 or v2 and that it has the correct SNMP community strings configuration.</td>
<td></td>
</tr>
<tr>
<td><strong>Media Gateway software is not running on both SC boards</strong></td>
<td></td>
<td>Start Media Gateway software on both SC boards by typing tools sc up</td>
<td></td>
</tr>
<tr>
<td><strong>External firewall problems</strong></td>
<td></td>
<td>Verify that there is no firewall between the SNMP manager and the Media Gateway chassis that blocks SNMP traffic.</td>
<td></td>
</tr>
<tr>
<td>Problem</td>
<td>Possible Cause(s)</td>
<td>Actions to Take</td>
<td>Refer to:</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>No communication with the Media Gateway</td>
<td>Wrong external IP network configuration</td>
<td>Spanning tree functionality is disabled on the ES boards. Therefore external IP switches/routers can create loops in the network. Packets may sometimes get lost. Make sure that the external switches/routers have the “spanning tree” feature enabled.</td>
<td></td>
</tr>
<tr>
<td>No communication with the Media Gateway (after ES board failure/switchover there is no ping to SC's Global IP)</td>
<td>Each ES board is connected to a separate external router, and the routers are not connected by VRRP protocol</td>
<td>When ES board switchover occurs, all external networks must go through the other external router. This is possible only if the external routers are connected and are using VRRP protocol.</td>
<td></td>
</tr>
<tr>
<td>Problems with ES boards</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ES board is Disabled (colored red in the EMS)</td>
<td>Ethernet Switch board is completing the Unlock action</td>
<td>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.</td>
<td>Working with the ES boards on page 121</td>
</tr>
<tr>
<td>ES board is Disabled (colored red in the EMS) and all it's LEDs are turned off.</td>
<td>The uplink of the Ethernet Switch board is disconnected.</td>
<td>Connect the uplink to the ES board. If the ES board doesn't become Enabled (colored green in the EMS) – reset it by performing Lock/Unlock actions.</td>
<td>Working with the ES boards on page 121</td>
</tr>
<tr>
<td>Problems with Media Gateway boards</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Media Gateway board is Disabled (colored red in the EMS)</td>
<td>Media Gateway board is completing the Unlock action</td>
<td>It may take up to 3 minutes for the Media Gateway board to complete the reboot that accompanies the Unlock action. Wait patiently.</td>
<td>Working with the Media Gateway Boards on page 115</td>
</tr>
<tr>
<td>Problem</td>
<td>Possible Cause(s)</td>
<td>Actions to Take</td>
<td>Refer to:</td>
</tr>
<tr>
<td>---------</td>
<td>------------------</td>
<td>-----------------</td>
<td>-----------</td>
</tr>
</tbody>
</table>
| 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) | | Configuring the IP Addresses of Media Gateway Boards and Network Servers on page 112 |
| 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 BoardProvisioningMode 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 115  
Troubleshooting the Newly Installed Media Gateway Board on page 308 |
| “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. | | |
## 7. Diagnostics & Troubleshooting

<table>
<thead>
<tr>
<th>Problem</th>
<th>Possible Cause(s)</th>
<th>Actions to Take</th>
<th>Refer to:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Other BOOTP/DHCP server exists in the network that replies to the BOOTP requests sent by the Media Gateway board</td>
<td>Check that there is no BOOTP/DHCP server active in the IP subnet where Media Gateway resides. If there is, make sure that this external BOOTP/DHCP server is configured not to reply to BOOTP packets sent by the Media Gateway board. If such configuration is impossible – disconnect the external BOOTP/DHCP server.</td>
<td>Refer to: Working with the Media Gateway Boards on page 115. Redundancy Modes on page 118.</td>
</tr>
<tr>
<td></td>
<td>Active calls are dropped during the switchover from a failed Media Gateway board to the redundant board.</td>
<td>Verify configuration of the Redundancy Group and current &quot;redundancy status&quot; of all Media Gateway boards.</td>
<td>Refer to: Working with the Media Gateway Boards on page 115. Redundancy Modes on page 118.</td>
</tr>
<tr>
<td></td>
<td>Media Gateway board is not reset upon Lock action</td>
<td>Make sure that the Media Gateway board's RTM is inserted properly in the corresponding rear slot and that its latches are firmly closed.</td>
<td>Refer to: Working with the Media Gateway Boards on page 115. Redundancy Modes on page 118.</td>
</tr>
<tr>
<td></td>
<td>A problem with the Media Gateway board’s RTM (Rear Transition Module)</td>
<td>Make sure that the SA/RTM modules of both SC boards are inserted properly in the corresponding rear slots and that their latches are firmly closed. Perform Lock action on another Media Gateway board. If the problem occurs on it too – reset SA/RTM module by extracting it from the chassis and re-inserting it back.</td>
<td>Refer to: Working with the Media Gateway Boards on page 115. Redundancy Modes on page 118.</td>
</tr>
<tr>
<td></td>
<td>Problems with Voice Quality</td>
<td></td>
<td>Refer to: Working with the Media Gateway Boards on page 115. Redundancy Modes on page 118.</td>
</tr>
<tr>
<td>G.711 voice quality is bad (clicks)</td>
<td>Wrong codec definition in the remote Media Gateway</td>
<td>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.</td>
<td>Refer to: Working with the Media Gateway Boards on page 115. Redundancy Modes on page 118.</td>
</tr>
<tr>
<td></td>
<td>Silence Suppression is not compatible with the remote Media Gateway (when remote Media Gateway is not an Avaya Media Gateway)</td>
<td>Disable Silence Suppression and check if quality is improved.</td>
<td>Refer to: Working with the Media Gateway Boards on page 115. Redundancy Modes on page 118.</td>
</tr>
</tbody>
</table>
### Problem

<table>
<thead>
<tr>
<th>Problem</th>
<th>Possible Cause(s)</th>
<th>Actions to Take</th>
<th>Refer to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>No voice</td>
<td>There is no common codec with the remote Media Gateway</td>
<td>Change voice codec definitions.</td>
<td></td>
</tr>
<tr>
<td>Echo on the PSTN terminations</td>
<td>Clock Synchronization</td>
<td>Check and validate the clock synchronization of the PSTN network and update the Media Gateway's configuration.</td>
<td>Clock Synchronization on page 63 For more information, refer to Configuring Clock Settings</td>
</tr>
</tbody>
</table>

---

### 7.3 Recovering the Basic Interface Separation, VLANs & Link Aggregation Default Settings

This section provides details of how to recover the basic Interface Separation, VLANs & Link Aggregation default settings using the `tools vlan` command. This procedure is used to recover from a situation of no IP connectivity with all boards inside the Media Gateway due to faulty VLAN configuration. The latter may be caused by human error during VLANs provisioning or when there is a change in the VLAN settings of the site IP network.

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 allows you to connect to the Media Gateway's management interfaces via EMS or CLI. Use regular VLAN configuration mechanisms to complete the VLAN configuration. Refer to Configuring the IP Network Connectivity on page 157 for details.

➢ **To recover the OAM VLAN settings, take these 6 steps:**

1. Connect to the Active SC board via Console (refer to Connecting to the SC Board's RS-232 Console on page 78)
2. Login as root user (default password is root)
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. (In the example below, the OAM VLAN tag ID is set to 4.)

   ```
   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 is 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 via EMS or CLI.

6. Complete the VLAN configuration as described in Configuring the IP Network Connectivity on page 157.

### 7.4 Collecting Advanced Media Gateway Board Logs

Media Gateway boards are constantly monitored by the Media Gateway software running on the SC boards and corresponding events/alarms are reported via the appropriate management interface (SNMP 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/Server Board Logs may be used for problem troubleshooting. This section describes how to collect and analyze these advanced logs.

#### 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 written somewhat independently, there is little uniformity to 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 boards perform as a Syslog client and are capable of generating messages at 5 error levels:

- Emergency level
- Warning level
- Notice level
- Info level
- Debug level

#### Log Files

The SC board performs as a Syslog server. It intercepts all syslog messages generated by Media Gateway boards and stores them in the log files.

The log files may be viewed via the following CLI command (available both to root and CLI users):

```
log [<options>] board# <slot number> [<tpm id>]
```

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.
For All Media Gateway Boards

With option `-<number>`, the log command displays the last `<number>` of log messages. For example to see the last 100 log messages from Media SG1> board in slot 10, use the log -100 board#10 command.

With option `-f`, the log command displays the complete log file. For example, `log --f board#10`.

Option `-h` allows viewing the history of the log files (10 last log files are stored in the history).

7.4.1 Configuring the Syslog Server

As an alternative to using the Syslog server on the SC board (and viewing the logs via the log command), you can configure 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 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 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`

7.4.2 Collecting Call Data Records (CDRs)

In addition to the Advanced Media Gateway 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 transmitted to the SC board via 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.

*Note:* It is also possible to directly transmit CDR data to any NFS host instead of the SC board. For more information, refer to LTRT-892xx CLI Reference Guide.

➢ To collect CDRs from Media Gateway board, take these 10 steps:

1. Access the MG Status screen.
2. Click Properties. The Media Gateway Parameters Provisioning screen appears.

3. In the Network Services tab, set Enable NFS Server On SC Board parameter to Enable.

4. Connect to the Active SC board via Telnet, SSH or RS232 Console. For more information, refer to Connecting to the SC Board's Terminal on page 89.

5. Login as a CLI user with administrative privileges (e.g., user cli, password cli_12345). For more information, refer to Users on SC Board's Terminal on page 92.

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 that 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/data/cli/cdr.txt
```

9. To view recorded CDR data, at the prompt, type `more filename`.

```
client238:~#
  more /data/cli/cdr.txt
```

10. After you complete CDR recording, open the Media Gateway provisioning screen, select Network Services tab and set Enable NFS Server On SC Board parameter to Disable.

7.5 Accessing Advanced Status of Media Gateway Board via WEB Interface

The Media Gateway board's status is typically examined via the EMS GUI or corresponding CLI commands. The latter contain all required information for detailed operation, configuration and maintenance of the Media Gateway board (for more information, refer to Working with the Media Gateway Boards on page 115).

However in certain scenarios, you may be asked by Avaya 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.
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, take these 3 steps:**

1. Access the **MG Status** screen.
2. Click **Clock**. The Media Gateway Parameters Provisioning screen appears.
3. In the Network Services tab:
   - 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, take these 3 steps:**

1. On the PC, whose IP address you provisioned before, open web browser (e.g., Internet Explorer)
2. Enter the following URL: `https://<IP address>`, where `<IP address>` is the OAM IP address of the Media Gateway board.
3. When asked to enter username and password, enter:
   - username: `monitor_user`
   - password: password, configured as described above.

### 7.6 Collecting Media Gateway Board's Debug Recording Traces

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. Avaya 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.

### 7.6.1 Configuring Debug Recording Rules

Debug Recording Rules must be configured on the Media Gateway board prior to starting the Debug Recording. These rules define specific traffic to be captured and the target (external PC or Standby SC) that the captured packets are forwarded to. Multiple rules may be defined simultaneously.

To define Debug Recording Rule, take these 5 steps:

1. Access the **MG Status** screen.
2. Select the desired Media Gateway board. Click **Properties**. The Media Gateway Board Provisioning screen appears.
3. Select Debug Recording tab. The list of Debug Recording Rules is displayed.
4. To add a new Debug Recording Rule, click **+**. The Debug Recording Provisioning screen appears.
5. Configure Debug Recording Rule properties according to the table below.
6. Unlock Debug Recording Rule after completing its configuration.
### Table 7-2: Debug Recording Rule Properties

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>String</td>
<td>Online</td>
<td>The textual, user-defined name for the Debug Recording Rule, enabling it to be identified intuitively and easily.</td>
</tr>
<tr>
<td>Target IP</td>
<td>IP Address</td>
<td>Online</td>
<td>IP address of the remote machine (PC or Standby SC board) where the Debug Recording Trace is sent.</td>
</tr>
<tr>
<td>Target Port</td>
<td>Integer</td>
<td>Online</td>
<td>Port of the remote machine (PC or Standby SC board) where the Debug Recording Trace is sent. <strong>Port 925 is recommended.</strong></td>
</tr>
</tbody>
</table>
| Type             | Enum none, ipTraffic, ipControl, pstnSignaling, nextCall, trunkBchannel, channelId | Online            | Type of the Debug Recording Rule:  
  - **ipTraffic** – record IP traffic from/to specific destination  
  - **ipControl** – record call control traffic  
  - **pstnSignaling** – record PSTN signaling traffic  
  - **nextCall** – record media traffic for the next N calls  
  - **trunkBchannel** – record media traffic for the specific B-channels  
  - **channelId** – record media traffic for the specific channels |
| Trace Point      | Enum Net2Host, Host2Net | Online            | Relevant for **ipTraffic** and **ipControl** types only.  
  Defines the direction of the IP traffic to be captured:  
  - Net2Host – inbound IP traffic  
  - Host2Net – outbound IP traffic |
| PDU Type         | String              | Online            | Relevant for **ipTraffic** type only.  
  Defines the PDU type of the IP packets to be captured. The following PDU types are currently supported:  
  - **UDP** – UDP traffic  
  - **TCP** – TCP traffic  
  - **ICMP** – ICMP traffic  
  - **IPType** – any other IP type (as defined by IANA)  
  - all traffic types |
<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Type</th>
<th>Provisioning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Type</td>
<td>Enum</td>
<td>Online</td>
<td>Relevant for <strong>ipControl</strong> type only. Defines type of the call control traffic to be captured. The following control types are supported:</td>
</tr>
<tr>
<td></td>
<td>tpncp, sip,</td>
<td></td>
<td>• TPNCP – TPNCP signaling</td>
</tr>
<tr>
<td></td>
<td>megaco, mgc</td>
<td></td>
<td>• SIP – SIP signaling</td>
</tr>
<tr>
<td></td>
<td>p</td>
<td></td>
<td>• MEGACO – MEGACO signaling</td>
</tr>
<tr>
<td></td>
<td>p</td>
<td></td>
<td>• MGCP – MGCP signaling</td>
</tr>
<tr>
<td>Packet Type</td>
<td>Enum</td>
<td>Online</td>
<td>Relevant for <strong>nextCall</strong>, <strong>trunkBchannel</strong> and <strong>channeld</strong> types only.</td>
</tr>
<tr>
<td></td>
<td>all, allWithPcm</td>
<td></td>
<td>• ALL – all media-related packets (internal DSP packets, RTP, RTCP, T.38, events and syslog)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ALL-WITH-PCM – all media-related packets plus PCM traffic</td>
</tr>
<tr>
<td>PSTN Packet</td>
<td>Type</td>
<td>Online</td>
<td>Relevant for <strong>pstmtSignaling</strong> type only.</td>
</tr>
<tr>
<td></td>
<td>Enum</td>
<td></td>
<td>Defines the type of the PSTN packet to be captured. The following packet types are supported:</td>
</tr>
<tr>
<td></td>
<td>cas, isdn, ss7</td>
<td></td>
<td>• CAS – CAS signaling</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ISDN – ISDN signaling. <strong>This is the valid choice for the G860.</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• SS7 – SS7 signaling</td>
</tr>
<tr>
<td>Source Port</td>
<td>Integer</td>
<td>Online</td>
<td>Relevant for <strong>ipTraffic</strong> type only.</td>
</tr>
<tr>
<td></td>
<td>-1 - 65535</td>
<td></td>
<td>Defines the source port of the IP traffic to be captured. When set to -1 captures traffic from all ports.</td>
</tr>
<tr>
<td>Dest Port</td>
<td>Integer</td>
<td>Online</td>
<td>Relevant for <strong>ipTraffic</strong> type only.</td>
</tr>
<tr>
<td></td>
<td>-1 - 65535</td>
<td></td>
<td>Defines the destination port of the IP traffic to be captured. When set to -1 captures traffic from all ports.</td>
</tr>
<tr>
<td>Source IP</td>
<td>IP Address</td>
<td>Online</td>
<td>Relevant for <strong>ipTraffic</strong> type only.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Defines the source IP address of the IP traffic to be captured. When set to 0.0.0.0 captures traffic from all IP addresses.</td>
</tr>
<tr>
<td>Dest IP</td>
<td>IP Address</td>
<td>Online</td>
<td>Relevant for <strong>ip Traffic</strong> type only.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Defines the destination IP address of the IP traffic to be captured. When set to 0.0.0.0 captures traffic from all IP addresses.</td>
</tr>
<tr>
<td>Parameter Name</td>
<td>Type</td>
<td>Provisioning Type</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------------</td>
<td>-------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>From Trunk</td>
<td>Integer</td>
<td>Online</td>
<td>Relevant for <code>trunkBchannel</code> and <code>channelId</code> types only. Defines the start of the trunk range for debug recording. When set to -1 captures traffic from all trunks.</td>
</tr>
<tr>
<td>To Trunk</td>
<td>Integer</td>
<td>Online</td>
<td>Relevant for <code>trunkBchannel</code> and <code>channelId</code> types only. Defines the end of the trunk range for debug recording.</td>
</tr>
<tr>
<td>From BChannel ID</td>
<td>Integer</td>
<td>Online</td>
<td>Relevant for <code>trunkBchannel</code> type only. Defines the start of the B-channel range in the trunk for debug recording. When set to -1 captures traffic from all B-channels.</td>
</tr>
<tr>
<td>To BChannel ID</td>
<td>Integer</td>
<td>Online</td>
<td>Relevant for <code>trunkBchannel</code> type only. Defines the end of the B-channel range in the trunk for debug recording.</td>
</tr>
<tr>
<td>From Channel ID</td>
<td>Integer</td>
<td>Online</td>
<td>Relevant for <code>channelId</code> type only. Defines the start of the channel ID range in the trunk for debug recording. When set to -1 captures traffic from all B-channels.</td>
</tr>
<tr>
<td>To Channel ID</td>
<td>Integer</td>
<td>Online</td>
<td>Relevant for <code>channelId</code> type only. Defines the end of the channel ID range in the trunk for debug recording.</td>
</tr>
<tr>
<td>Number Of Calls</td>
<td>Integer</td>
<td>Online</td>
<td>Relevant for <code>nextCall</code> type only. Defines the number of the calls to be captured.</td>
</tr>
<tr>
<td>Trace Type</td>
<td>Enum</td>
<td>Online</td>
<td>Relevant for <code>nextCall</code> type only. Defines the type of the <code>nextCall</code> trace:</td>
</tr>
<tr>
<td></td>
<td>new, dynamic</td>
<td></td>
<td>- <strong>New</strong> – the next new Number Of Calls will be recorded. When these calls end, new calls will not be recorded.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- <strong>Dynamic</strong> – the next new Number Of Calls will be recorded. When these calls end, new calls will be recorded, overwriting data from the previously recorded calls.</td>
</tr>
</tbody>
</table>

### 7.6.2 Activating and Deactivating Debug Recording

After defining proper Debug Recording Rules, you must activate the debug recording on the Media Gateway board to record the new data.
7. Diagnostics & Troubleshooting

➢ To activate Debug Recording, take these 2 steps:

1. Access the **MG Status** screen.
2. Right-click on the selected Media Gateway board and, from the popup menu, select **Maintenance> Start Debug Recording**.

When the debugging session is finished, deactivate debug recording to return Media Gateway board to normal operation.

➢ To deactivate Debug Recording, take these 2 steps:

1. Access the **MG Status** screen.
2. Right-click on the selected Media Gateway board and, from the popup menu, select **Maintenance> Stop Debug Recording**.

7.6.3 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 Avaya 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, take these 4 steps:

Connect to the Standby board via Console, Telnet or SSH. For more information, refer to Connecting to the SC Board's Terminal on page 89. Use the internal (not Global) SC IP addresses if you connect via Telnet or SSH.

1. Login as the **root** user. For more information, refer to Users on SC Board's Terminal on page 92.

2. To start capturing the Debug Recording Traces, at the prompt, type the command, `snoop –o <file name> 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
```

3. To stop capturing the Debug Recording Traces, press **Ctrl-C** key sequence.

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.
7.7 Internal Software Logs

The Avaya G860 reports all alarms and events 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 Avaya technical support and field engineers and should not be used by customers, unless explicitly directed to by Avaya technical support.

7.7.1 Log Areas

All of the Avaya G860 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
- Avaya Technical Support Log Area - logs intended for Avaya Technical Support and Field Engineers.

7.7.1.1 Customer's Log Area

- `/Project/bin/log/trap` – the directory that logs all the information 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.). Used by CLI users to view data reported via SNMP trap.

- `/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.

7.7.1.2 Avaya 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 Avaya G860 chassis. It includes all internal software logs reported by a specific Media Gateway board via the Syslog interface.

- `/Project/bin/log/boottp` – 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
7. Diagnostics & Troubleshooting

7.7 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/snmp_agt` - the directory that logs information regarding SNMP agent activities

- `/Project/bin/log/snmp_mgr` - the directory that logs information regarding SNMP manager activities (the SNMP manager is used for collecting Performance Monitoring data from the Media Gateway boards)

- `/Project/bin/log/tpncpif` - the directory that logs information regarding TPNCP 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

7.7.2 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 Avaya 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%)

7.7.3 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, tpcnp, sat, trap, upgrade, watchdog, syslog, activity
The log command may also be used for viewing Media Gateway board logs by specifying board <slot number> [<tpm id>] logfile - refer to Media Gateway Boards Log Files on page 351 for details.

Without any options, the log command displays the new logs as they are generated by Media Gateway boards. With option -<number>, it displays the last <number> of lines from the log file (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 log command may also be used for viewing Media Gateway board logs - refer to Media Gateway Boards on page 351Log Files for details.

The example below demonstrates how the current **SNMP trap** logs can be viewed:

**Figure 7-1: Viewing an 'SNMP Trap' Log**

---

**7.7.4 Solaris OS Logs**

Solaris OS logs are stored on each SC board in the **/var/adm/messages** file. The file is rotated on a daily basis. Up to 4 backup versions are preserved.

Use standard UNIX utilities (e.g., **more** or **less**) to view the file content.

**7.7.5 Collecting logs for Avaya Technical Support**

When the customer is asked to collect and send all or part of the log files in the Media Gateway system for analysis, the following command should be executed at the SC prompt:

**tools report**
This command generates a Bug Report file that contains, among the other data, all current log files of the specific SC board.

Example:

```
=> 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.
```

The generated file (report.tar.gz) file should be transferred to the Tech Support for analysis.

Sometimes the customer is asked to collect the log information from both SC boards. For example, it could be required for analysis of problems involving an SC board switch-over. In this situation, the tools report command should be executed on both SC boards.

### 7.8 Information Needed when Contacting Technical Support

When contacting Avaya Technical Support (refer to the title page or last page of this manual for detailed contact information), send the following information:

1. A description of the system configuration - including the number and type of Media Gateway boards, network configuration, signaling protocols being used, exact software version, and the S/N of the failed module.
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. to the system configuration, networking changes, etc.
8 Avaya G860 Selected Technical Specifications

Note: The two codecs which Communication Manager supports on a system-wide interoperability basis are G.711 and G.729.

Table 8-1: Avaya G860 Technical Specifications

<table>
<thead>
<tr>
<th>Function</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Capacity</strong></td>
<td></td>
</tr>
</tbody>
</table>
| Network Ports/DSP Calls (independent digital voice, fax or data ports) | For Avaya G860 Configuration:  
Up to 4 Dual STM-1/OC-3 SDH /SONET Ports; APS protected; Redundant, 3+1 Media Gateway Boards configuration  
Up to 12 T3; Redundant, 3+1 Media Gateway Boards configuration  
Up to 4 Dual OC-3c; APS protected; Redundant, 3+1 Media Gateway Boards configuration  
Wireline/Cable: Up to 6,000 simultaneous VoIP voice calls for 3+1 TP-6310 Media Gateway Boards  
UMTS/GSM/CDMA: Up to 6,000 independent simultaneous VoIP voice calls  
For all Avaya G860 configurations:  
Independent dynamic vocoder, fax or modem selection per channel  
Capacity is transcoding and voice coder type dependent |
| Optional Application Processor | Up to 2 Sun based Single Board Application Computers (Optional) |
| **Media Processing** | |
| IP Transport | VoIP (RTP/ RTCP) per IETF RFC 3550 and RFC 3551 |
| DTMF/MF Transport | DTMF/MF RTP Relay per RFC 2833, Mute, Transparent (transfer in coder as voice) |
| Voice Processing | All voice processing features are supported simultaneously on all ports  
Dynamic Network Jitter Buffer with reordered RTP packets correction  
Call Progress Tones generation and detection  
Integral Announcement support towards PSTN/TDM and IP  
Transcoding of a G.711 RTP stream to any Low Bit-Rate Coder RTP stream using one DSP channel resource |
<table>
<thead>
<tr>
<th>Function</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Mediation between two IP endpoints of the same coder without using any DSP channel resource</td>
</tr>
<tr>
<td></td>
<td>Media duplication (one source to many destinations) using the same coder without using additional DSP channel resources</td>
</tr>
<tr>
<td></td>
<td><strong>Voice Coders</strong></td>
</tr>
<tr>
<td></td>
<td>- Cables: G.711, G.726, G.729E, and iLBC</td>
</tr>
<tr>
<td></td>
<td>- UMTS/GSM: AMR (8 variants/rates), TTY/CTM modem for AMR, AMR2, GSM-FR, GSM-EFR and G.711 (PCM)</td>
</tr>
<tr>
<td></td>
<td>- CDMA: EVRC, EVRC TTY, EVRC-B, TIA IS-96A QCELP-8kbps, TIA IS-733 QCELP-13kbps</td>
</tr>
<tr>
<td></td>
<td>- Additional coders are supported - contact Avaya for further information</td>
</tr>
<tr>
<td></td>
<td><strong>Echo Cancelation</strong></td>
</tr>
<tr>
<td></td>
<td>- G.165 and G.168 2000 compliant 32, 64, 128 msec echo tail</td>
</tr>
<tr>
<td></td>
<td>(128 may reduce channel capacity)</td>
</tr>
<tr>
<td></td>
<td><strong>Gain Control</strong></td>
</tr>
<tr>
<td></td>
<td>- Configurable Input/Output Gain Control: -31 dB to +31 dB in steps of 1 dB</td>
</tr>
<tr>
<td></td>
<td><strong>Silence Suppression</strong></td>
</tr>
<tr>
<td></td>
<td>- G.723.1 Annex A</td>
</tr>
<tr>
<td></td>
<td>- G.729 Annex B</td>
</tr>
<tr>
<td></td>
<td>- PCM and ADPCM - Per RFC 3389 or Proprietary, NetCoder.</td>
</tr>
<tr>
<td></td>
<td><strong>Voice Activity Detection (VAD), Comfort Noise Generation (CNG)</strong></td>
</tr>
<tr>
<td></td>
<td>- 3GPP Voice Activity Detection (VAD) 3GPP 26.094 and Comfort Noise Generation (CNG) 3GPP 26.092</td>
</tr>
<tr>
<td></td>
<td>- GSM 6.10</td>
</tr>
<tr>
<td></td>
<td><strong>Fax and Modem Transport</strong></td>
</tr>
<tr>
<td></td>
<td>- Supported on all ports</td>
</tr>
<tr>
<td></td>
<td>- Group 3 real-time Fax Relay to 14.4 kbps with auto fallback</td>
</tr>
<tr>
<td></td>
<td>- Tolerant of delays of up to 9 seconds</td>
</tr>
<tr>
<td></td>
<td>- T.30 (PSTN) and T. 38 (IP) compliant (real-time fax)</td>
</tr>
<tr>
<td></td>
<td>- CNG tone detection &amp; Relay per T.38</td>
</tr>
<tr>
<td></td>
<td>- Voice-Band Data according to V.152</td>
</tr>
<tr>
<td></td>
<td>- Automatic Fax ByPass (pass-through) to G.711 or ADPCM</td>
</tr>
<tr>
<td></td>
<td><strong>Modem Bypass</strong></td>
</tr>
<tr>
<td></td>
<td>- Automatic switching (pass-through) to PCM or ADPCM for modem signals (V.34 or V.90 modem detection)</td>
</tr>
<tr>
<td></td>
<td><strong>IP Interface</strong></td>
</tr>
<tr>
<td></td>
<td>- 1, 2 or 3 Local Subnets</td>
</tr>
<tr>
<td></td>
<td>- Different Local IP Addresses and Subnet masks for Operation Administration &amp; Maintenance (OAM), Control and Media Protocols</td>
</tr>
<tr>
<td></td>
<td><strong>Static Routes</strong></td>
</tr>
<tr>
<td></td>
<td>- Configurable Static Routes tables</td>
</tr>
</tbody>
</table>
### Function

<table>
<thead>
<tr>
<th>Function</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>VLANs IEEE 802.1q</strong></td>
<td>Up to 4 different IEEE 802.1q VLAN tagging for Operation Administration &amp; Maintenance (OAM), Control and Media (with 2 VLAN tags) Protocols</td>
</tr>
<tr>
<td><strong>Link Aggregation</strong></td>
<td>Up to 3 links can be included in the Aggregation group according to IEEE 802.3ad</td>
</tr>
<tr>
<td><strong>QoS IEEE 802.1p</strong></td>
<td>Configurable IEEE 802.1p routing and marking capabilities for Network, Premium Control, Premium Media, Gold and Bronze QoS classes</td>
</tr>
<tr>
<td><strong>DiffServ RFC2474</strong></td>
<td>Configurable, marking capabilities for Network, Premium Control, Premium Media, Gold and Bronze DiffServ classes</td>
</tr>
</tbody>
</table>

### Control Protocols

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MGCP (RFC 3435)</strong></td>
<td>Call control, Supporting Trunk package, Generic Media package, Basic announcements package, Conferencing, DTMF and RTP Packages, CAS Packages, Fax Package, Media Format Parameter Package and other packages according to Basic MGCP Packages (RFC 3660)</td>
</tr>
<tr>
<td><strong>MEGACO (H.248)</strong></td>
<td>Call control, Supporting Generic Media Package, Base Root, Tone Generator, Tone Detection, DTMF Generator, DTMF Detection, Call Progress Tones Generator, Call Progress Tones Detection, Basic Continuity, Network, RTP, TDM Circuit, Generic Announcement, Expanded Call Progress Tones Generator, Basic Service Tones Generation, Expanded Services Tones Generation, Basic CAS, R2 CAS, MF Generator, MF Detection, Inactivity Timer, Basic Call Progress Tones Generator with Directionality, Call Type Discrimination, IP Fax as well as other more packages, Basic CAS addressing package, Robbed bit signaling package, Operator services and emergency services package, etc.</td>
</tr>
<tr>
<td>Function</td>
<td>Specification</td>
</tr>
<tr>
<td>----------</td>
<td>---------------</td>
</tr>
</tbody>
</table>
| SIP      | **SIP Functions**: User Agent Client (UAC), User Agent Server (UAS)  
**Operation with SIP Horses**: Third party Proxy, Redirect, Registrar servers  
**SIP Methods**: INVITE, ACK, BYE, CANCEL, REGISTER, REFER, NOTIFY, INFO, OPTIONS, PRACK, UPDATE  
**SIP Transport**: UDP, TCP  
**SIP Security**: TLS 0.1 (Transport Layer Security)  
Supported SIP RFCs:  
RFC 3261 - SIP  
RFC 3262 - Reliability of Provisional Responses  
RFC 3263 - Locating SIP Servers  
RFC 3264 - Offer/Answer Model  
RFC 3265 - (SIP)-Specific Event Notification  
RFC 2327 - SDP  
RFC 2782 - A DNS RR for specifying the location of services  
RFC 3323 - Privacy Mechanism  
RFC 3325 - Private Extensions to the SIP for Asserted Identity within Trusted Networks  
RFC 3327 - Extension Header Field for Registering Non-Adjacent Contacts  
RFC 3515 - Refer Method  
RFC 3581 - Symmetric Response Routing  
RFC 3725 - Third Party Call Control  
RFC 3605 - RTCP attribute in SDP  
RFC 2833 - Telephone event  
RFC 2617 - HTTP Authentication: Basic and Digest Access Authentication  
RFC 3891 - “Replaces” Header  
RFC 3311 - UPDATE Method  
*draft-ietf-iptel-trunk-group-02.txt* - Representing trunk groups in tel/sip URIs  
*draft-burger-sipping-netann-10.txt* - Basic Network Media Services with SIP  
*draft-ietf-avt-rtp-clearmode-05.txt* - RTP payload format for a 64 kbit/s transparent call  
*draft-ietf-sip-referredby-04* - The SIP Referred-By Mechanism  
*draft-ietf-sip-session-timer-15* - Session Timers in the Session Initiation Protocol  
*draft-LEVY-sip-diversion-08* - Diversion Indication in SIP  
*draft-vandyke-mscml-04* - Media Server Control Markup Language (MSCML) |
### Function | Specification
--- | ---
**SIP** | *draft-ietf-sipping-qsig2sip-04.txt* - Interworking between SIP and QSIG  
*draft-ietf-sipping-realtimefax-01.txt* - SIP Support for Real-time Fax: Call Flow Examples  
*draft-choudhuri-sip-info-digit-00.txt* - SIP INFO method for DTMF digit transport and collection  
*draft-mahy-sipping-signaled-digits-01.txt* - Signaled Telephony Events in the Session Initiation Protocol

**TGCP (PKT-SP-TGCP)** | PacketCable’s Call control, IT, MO and MT Packages

### Security

**IPSec (ESP) with IKE pre-shared key or X.509 Certificate** | IPSec is supported for the management traffic to EMS/ NMS/ OSS and for control interfaces to MGC (MGCP or H.248 with reduced channel capacity).  
Encryption algorithms - DES and 3DES  
Hash types - SHA1 and MD5

**Media Gateway Boards-Based Firewalls** | Up to 20 Filtering criteria rules according to:  
Source IP-address and subnet  
Destination port range  
Protocol type  
Packet size  
Traffic rate in bytes-per-second

**Access Control Lists** | The control interfaces can be protected by access control lists.

**Media Encryption** | Media encryption is supported per PacketCable specification (with reduced channel capacity).  
AES - 128 (Rijndael) cipher algorithm, in CBC mode  
Optional 2-byte or 4-byte MAC based on MMH algorithm  
Or, SRTP (RFC 3711)* media encryption limited to AES_CM_128_HMAC_SHA1_32 and AES_CM_128_HMAC_SHA1_80 secured suites  
H.248 Keys negotiation as per:  
Or, MGCP proprietary Keys negotiation

**SSH (Secure Shell)** | To secure the Telnet and SFTP Server  
SSH Protocol Version 2  
Supported encryption algorithms: AES-128, BLOWFISH, 3DES  
Supported authentication algorithms: SHA1, MD5  
User/password authentication on each login
<table>
<thead>
<tr>
<th>Function</th>
<th>Specification</th>
</tr>
</thead>
</table>
| SSL/TLS (the Secure Socket Layer)    | To secure SIP control interfaces and Media Gateway Boards web server and telnet  
Supported transports: SSL 2.0, SSL 3.0, TLS 1.0  
Supported ciphers: DES, RC4 compatible  
Authentication: Username & Password, X.509 certificates |
| PSTN Signaling                       |                                                                                                                                                                                                             |
| In-band/Out-of-band Signaling        | DTMF per TIA 464B  
DTMF over RTP per RFC 2833  
MFC-R2, MF-R1, MF-R1 (US) including FG-A/B/D  
Packet side or PSTN side generation/detection of DTMF and User Defined Call Progress Tones (PSTN, IP) & Continuity Test Tones (per ITU-T Q.724) |
| PSTN Protocols                       | CAS - T1 robbed bit: WinkStart, delay dial, immediate start, FGB, FGD, etc.  
MFC/R2 numerous country variants  
Unique script for each county variant, enabling maximum flexibility of the entire state machine of each CAS protocol  
Mercury Exchange Limited CAS (MelCAS) signaling protocol. Supported in MEGACO only  
CCS - ISDN PRI: ETSI EURO ISDN, ANSI NI2, DMS, 5ESS, Japan INS1500, QSIG Basic Call, Australian Telecom, New Zealand Telecom, Hong Kong Variant, Korean MIC |
| CAS Relay                            | ABCD signaling over RTP per RFC 2833                                                                                                                                                                           |
| SS7 Broad-band Links                 | ATM I.363.2, I.366.1, SSCOP & SSCF-NNI (SAAL) over AAL5                                                                                                                                                       |
| SS7 Narrow-band Links                | MTP-2 (ITU / ANSI) link termination                                                                                                                                                                            |
| SIGTRAN                              | IUA (RFC 3057) over SCTP (RFC 2960)  
M2UA, (RFC 3331) over SCTP (RFC 2960)  
M3UA, (RFC 3332) over SCTP (RFC 2960) |
| SS7 Signaling                        | Up to 2 SNs per blade; SS7 Broad-band Signaling Nodes or SS7 Narrow-band Signaling Nodes, providing SP or STP* functionality  
Up to 30 Route Sets per SS7 Node  
Up to 32 SS7 Link Sets per SS7 Node  
Up to 32 SS7 Links per blade & up to 8 Links per Link Set  
Termination of MTP-1, MTP-2, layers and delivery of MTP3 messages over M2UA/SCTP/IP  
Termination of all layers up to MTP3 layer and delivery of SCCP/ISUP messages over M3UA/SCTP/IP |
### Clock Synchronization

Clock Specification (MG equipped with 6310 boards) | ITU G.813 option 1 and 2, ETSI EN 300-462-5-1 and ANSI SMC T1.105.09 and Bellcore GR-1244-core stratum 3.  
Supporting the following Reference input signals:  
- G.703 E1/T1 External Clock Port (SSM isn’t supported);  
- 2048 kHz synchronization signal according to clause 13/G.703 (T12).  
Output synchronization signals on STM-1/OC3 lines.

### 3GPP Services

| 3GPP Core Protocols | IP Core Network: NB IP user plane (RTP as per relevant sections of 3GPP TS 29.415, 25.415) and NB IP transport control plane (IPBCP over Mc as per relevant sections of 3GPP TS 29.414, 29.232)  
ATM RAN (Lu-CS) and Backbone (NB ATM): User Plan (as per relevant sections of 3GPP TS 25.415) and transport control plane (ALCAP/MTP3b/SAAL/AAL5) |

| Circuit Switch Data (CSD) | 64/56 Kbit/s Synchronous & Transparent CS data over Lu-CS and IP Nb (as per relevant sections of 3GPP TS 23.910) |

| Media Gateway Control Protocols | CS Mc - 3GPP TS 29.232, IMS Mn - 3GPP TS 29.332 |

### Cable Services

| PacketCable Vocoder | G.711 (A-law/m-law), G.728 G.729E, and iLBC supporting PacketCable PKT-SP-Codec  
Additional coders such as BV16 may be supported - contact Avaya for further information |

| Media Gateway Control Protocols | TGCP, IT, MO and MT Packages according to PacketCable PKT-SP-TGCP |

| PacketCable Security | Call Control Security, supporting IPSec with pre-shared Key, as per relevant sections of PKT-SP-SEC  
Media (RTP/RTCP) Security - AES - 128, as per relevant sections of PKT-SP-SEC |

| PacketCable CALEA | Electronic Surveillance as per relevant sections of PKT-SP-ESP and PKT-SP-TGCP |

### Maintenance

| Management | Element Management System, SNMP v2  
OAM Single point of access via the System Controller; easy management and provisioning with standard SNMP v2 interface |

| Maintainability | All system modules are hot swappable, including boards, Power Supply modules, fans and Alarm modules |

| Redundancy Scheme | CPUs, Ethernet switches: Active/Standby  
Power supplies, fans: Load Shared  
Media Gateway boards: N+1 |
<table>
<thead>
<tr>
<th>Function</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Diagnostic</td>
<td>Automatic and Manual HW and SW Diagnostic, BIT (Built in Test) fault detection, heart beat, chassis sub-systems monitoring</td>
</tr>
<tr>
<td><strong>Physical Interfaces</strong></td>
<td></td>
</tr>
<tr>
<td><strong>STM-1/OC3 Interfaces</strong></td>
<td>Per TP-6310 Board: Replaceable Dual-LC connectors; 155 Mbps optical SFP modules (complies with the INF-8074i - Small Form-factor Pluggable (SFP) Transceiver MultiSource Agreement (MSA)) Hot Swappable</td>
</tr>
<tr>
<td>T3 Interfaces</td>
<td>Per TP-6310 Board: Three T3 (DS-3) ports using unshielded mini-SMB connectors</td>
</tr>
<tr>
<td>IP Interfaces</td>
<td>Per ES Board: Up to 3 different IP Uplinks, depending on Ethernet Switch type:</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="IP Interfaces Table" /></td>
</tr>
<tr>
<td></td>
<td>100/1000 Base-TX: RJ-45 Connector Interface (CAT5 Twisted pair) 1 Gigabit optical: Multimode, SC-duplex 1000 Base-SX for the Gigabit Ethernet ports</td>
</tr>
<tr>
<td><strong>Hardware Specifications</strong></td>
<td></td>
</tr>
<tr>
<td>Dimensions</td>
<td>222 x 483 x 311 mm (8.7 in. x 19 in. x 12.3 in.)</td>
</tr>
<tr>
<td>Enclosure</td>
<td>10 -slot 5 U cPCI chassis</td>
</tr>
<tr>
<td>Weight</td>
<td>Approx. 27 lbs. (12.3 kg) unloaded. Approx. 45.1 lbs. (20.45 kg), fully loaded</td>
</tr>
<tr>
<td>Mounting</td>
<td>Per EIA Standard RS-310-C in 19-inchrack</td>
</tr>
<tr>
<td>Midplane</td>
<td>PICMG 2.16 cPCI Packet Switching Backplane (cPSB)</td>
</tr>
<tr>
<td></td>
<td>PICMG 2.1 cPCI hot swap specification</td>
</tr>
<tr>
<td></td>
<td>PICMG 2.0 cPCI specification</td>
</tr>
</tbody>
</table>
| Power            | -48 V DC Feed, with 3 DC Power modules OR 100 - 240 V AC with 3 AC Power modules  
                   | Average power consumption for a full complement of boards approximately:  
                   | 600 watts - 5.3 A at 115 VAC  
                   | 600 watts - 2.7 A at 230 VAC  
                   | 640 watts - 13.4 A at 48 VDC                                                                                                                         |
| Cooling          | Easily replaceable fan trays & filter                                                                                                           |
## 8. Avaya G860 Selected Technical Specifications

### Regulatory Compliance

<table>
<thead>
<tr>
<th>Function</th>
<th>Specification</th>
</tr>
</thead>
</table>
| **Telecommunication Standards** | FCC part 68  
TBR4 and TBR13 |
| **Safety and EMC Standards** | UL 60950  
FCC part 15 Class A  
CE Mark (EN 55022 Class A, EN 60950, EN 55024, EN 300386) |
| **Environmental**       | NEBS Level 3: GR - 63-Core, GR -1089-Core Type 1 & 3,  
ETS 300 019 |

* Currently not supported, consult Avaya release notes for up-to-date availability of these features

*Specifications subject to change without notice.*
9. Appendix - Installing the Solaris™ 9 OS

The SUN Solaris™ operating system must be installed on the SC board prior to installing the Media Gateway software. Each version of Avaya G860 software requires a specific version of Solaris™ OS, which is configured specifically for full Avaya G860 hardware compatibility and high performance.

Note: The Avaya G860 version 5.2 software requires Solaris™ 9 9/04.

For a typical SC board that is preinstalled with a correct version of the Solaris™ OS there no need to re-install Solaris™ OS during SC board replacement.

Note: When it becomes necessary to re-install the Solaris™ OS on an SC boards, it is important to use the Solaris OS installation image provided by Avaya.

9.1 Verifying the Current Version of the Solaris™ OS on the SC Board

To access the current version of the Solaris™ OS, take these 4 steps:

1. Connect to the Active SC board via Telnet SSH or Console (refer to Connecting to the SC Board's Terminal on page 89).
2. Login as root user (default password is root).
3. At the prompt, type cat /etc/version and press Enter. The current Solaris™ OS version is displayed.
4. Verify that the Solaris™ OS version matches the version required by the specific Avaya G860 software.

9.2 Installation Requirements

Installation of 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 Avaya G860

Avaya recommends using the EMS server as the Install Server.
9.3 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 boards installation.

To prepare the 'Install Image', take these 5 steps:

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.

9.4 Installing the Solaris™ 9 OS on the SC Board

To install the Solaris™ 9 OS on the SC boards, take these 13 steps:

1. Connect to the Active SC board via RS-232 Console (refer to Connecting to the SC Board's RS-232 Console on page 78)
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.

```plaintext
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
```

**Note:** If after connecting to the SC board's RS-232 console, the OpenBoot level (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 hostname and IP address for the new SC board.

4. Login to the Install Server (EMS) as the root user via Telnet, SSH or X-terminal.
5. 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)

```plaintext
EMS1:/ [root] => cd /jumpstart/Solaris_9_904_v5.2
EMS1:/ [root] => ./add_client.sh client224 10.7.13.94 0:3:ba:78:8e:65
```

6. Return to the RS-232 console terminal connected to the SC board.

**Note 1:** The rest of the steps are performed on the SC board and NOT on the Install Server.

**Note 2:** If, after connecting to the SC board's RS232 console, the OpenBoot level (ok>) prompt appears, skip the following three steps (7, 8 and 9).

7. Copy the new firmware from the Install Server (EMS) to the SC board as described below. (In the example the Install Server (EMS) IP Address, 10.7.8.6, should be replaced with your system's correct one when implementing this procedure.)

```plaintext
client224:~ # mount -F nfs 10.7.8.6:jumpstart /mnt
client224:~ # cd /mnt/Solaris_9_904_v5.2/Firmware
client224:~ # perl copyFW.pl
```

8. To return to the OpenBoot level (ok>) prompt, type sync;halt and press Enter.

```plaintext
client224:~ # sync;halt
ok>
```
9. Install the new firmware on the SC board as described below:

```
ok> setenv auto-boot? false
ok> reset-all
ok> flash-update /pci@1f,0/pci@1/ide@2/disk@0,0:a:,/firmware.bin
ok> setenv auto-boot? true
ok> setenv diag-switch? false
```

Remain at the **OpenBoot** level (i.e., do not reboot the SC board) and proceed to the next step.

10. Configure the firmware to be compatible with Solaris™ 9 OS by executing the following command:

```
ok> setenv legacy-support? false
```

**Note:** The command may fail on certain firmware versions. If this occurs, ignore the failure and proceed with the next step.

11. To install the Solaris™ 9 OS on the SC board, at the prompt, type `boot net-install` and press Enter. Make sure to separate each word with space.

```
ok> boot net - install
```

The Solaris™ 9 OS installation takes from 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 presented.

12. Re-login to the SC board via the RS-232 console as root user (default password is `root`) and, at the prompt, type `lockfs -f /` to stabilize the file system.

```
client224:~# lockfs -f /
```

13. 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_v5.2/Solaris_9/Tools
EMS1:/ [root] => ./rm_install_client client224
```
Appendix - List of Alarms

The Media Gateway supports the following alarms list, where each of the alarms is assigned with its unique MIB Object Identifier (OID):

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 alarm
17. NTP Server Status Changed - NTP server status changed
18. GW Switchover Alarm - GW switchover alarm
19. Configuration Change - configuration change
20. Active Alarm Overflow Trap - overflow of Active Alarms table

For the User’s convenience, all alarms generated by Media Gateway have the same standard structure which includes the following fields:

- **AlarmUniqueId** - the unique ID of alarm according to the MIB.
- **AlarmTitle** - the name of alarm (ID) in more readable form.
- **AlarmSource** - a text field indicating a source of generated alarm. It could be either a logical source (for example MO Managed Object path for such alarm as moOperativeStateChange) or a physical source (for example Fan_Number for FanAlarm).
- **Severity** - indicates alarm severity according to the ITU standard.
- **ProbableCause** - probable cause of the generated alarm according to the ITU standard.
- **ItuAlarmType** - generated alarm type according to the ITU standard.
- **AdditionalParamType1** - free string explaining the specific problem (or problem clearance) caused the alarm generation. It could also contain a numerical value if relevant.
# Regulatory Information

## Declaration of Conformity

| Manufacturer's Name: | AudioCodes Ltd. |
| Manufacturer's Address: | 1 Hayarden Street, Airport City, Lod 70151, Israel |
| Type of Equipment: | Digital VoIP System |
| Model Numbers: | Mediant 5000, Stretto 5000, IPmedia 5000 (with 6310 cPCI card). |

I, the undersigned, hereby declare that the equipment specified above conforms to the above Directives and Standards.

Signature | Date (Day/Month/Year) | Location |
---|---|---|
27th June, 2006 | Airport City, Lod, Israel |

I. Zusmanovich, Compliance Engineering Manager

---

**Czech**

[AudioCodes Ltd] tímto prohlašuje, že tento [Mediant 5000, IPmedia 5000] je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice.“ 73/23/ES 89/336/ES

**Danish**

Undertegnede [AudioCodes Ltd] erklærer herved, at følgende udstyr [Mediant 5000, IPmedia 5000] overholder de væsentlige krav og øvrige relevante krav i direktiv 73/23/EF 89/336/EF

**Dutch**

Hierbij verklaart [AudioCodes Ltd] dat het toestel [Mediant 5000, IPmedia 5000] in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 73/23/EG 89/336/EG

**English**

Hereby, [AudioCodes Ltd], declares that this [Mediant 5000, IPmedia 5000] is in compliance with the essential requirements and other relevant provisions of Directive. 73/23/EC 89/336/EC

**Estonian**


**Finnish**

<table>
<thead>
<tr>
<th>Language</th>
<th>Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>Danish</td>
<td>Undertegnede [AudioCodes Ltd] erklærer herved, at følgende udstyr [Mediant 5000, IPmedia 5000] overholder de væsentlige krav og øvrige relevante krav i direktiv 73/23/EF 89/336/EF</td>
</tr>
<tr>
<td>French</td>
<td>Par la présente [AudioCodes Ltd] déclare que l'appareil [Mediant 5000, IPmedia 5000] est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 73/23/CE 89/336/CE</td>
</tr>
<tr>
<td>Greek</td>
<td>ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ [AudioCodes Ltd] ΔΗΛΩΝΕΙ ΤΙΤΙ [Mediant 5000, IPmedia 5000] ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΑΣΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 73/23/ΕΚ 89/336/ΕΚ</td>
</tr>
<tr>
<td>Hungarian</td>
<td>Alulírott, [AudioCodes Ltd] nyilatkozom, hogy a [Mediant 5000, IPmedia 5000] megfelel a vonatkozó alapvető követelményeknek és az 73/23/EC 89/336/EC irányelv egyéb előírásainak</td>
</tr>
<tr>
<td>Icelandic</td>
<td>að þetta er í samræmi við tilskipun Evrópusambandsins 73/23 89/336</td>
</tr>
<tr>
<td>Italian</td>
<td>Con la presente [AudioCodes Ltd] dichiara che questo [Mediant 5000, IPmedia 5000] è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 73/23/CE 89/336/CE</td>
</tr>
<tr>
<td>Maltese</td>
<td>Hawnhekk, [AudioCodes Ltd], jiddikjara lid an [Mediant 5000, IPmedia 5000] jikkonforma mal-ħtíjjiet esenzjali u ma provvedimenti oħraj relevanti li hemm fid-Direttiva 73/23/EC 89/336/EC</td>
</tr>
<tr>
<td>Norwegian</td>
<td>Dette produktet er I samhørighet med det Europeiske Direktiv 73/23 89/336</td>
</tr>
<tr>
<td>Polish</td>
<td>[AudioCodes Ltd], deklarujemy z pełną odpowiedzialnością, że wyrób [Mediant 5000, IPmedia 5000] spełnia podstawowe wymagania i odpowiada warunkom zawartym w dyrektywie 73/23/EC 89/336/EC</td>
</tr>
<tr>
<td>Portuguese</td>
<td>[AudioCodes Ltd] declara que este [Mediant 5000, IPmedia 5000] está conforme com os requisitos essenciais e outras disposições da Directiva . 73/23/EC 89/336/EC</td>
</tr>
<tr>
<td>Slovak</td>
<td>[AudioCodes Ltd] týmto vyhlasuje, že [Mediant 5000, IPmedia 5000] splňa základné požiadavky a všetky príslušné ustanovenia Smernice. 73/23/ES 89/336/ES</td>
</tr>
<tr>
<td>Spanish</td>
<td>Por medio de la presente [AudioCodes Ltd] declara que el [Mediant 5000, IPmedia 5000] cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 3/23/EB 89/336/EB</td>
</tr>
<tr>
<td>Swedish</td>
<td>Härmad intygar [AudioCodes Ltd] att denna [Mediant 5000, IPmedia 5000] står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv. 73/23/EG 89/336/EG</td>
</tr>
</tbody>
</table>
11. Regulatory Information

Notice
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 the accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions.

Date Published: Jun-30-2006   © 2006 AudioCodes Ltd.   Date Printed: Sep-21-2006

Caution Laser
Note that this device may contain a Class 1 LED/Laser emitting device, as defined by 21CFR 1040 and IEC825. Do NOT stare directly into the beam or fiber optic terminations as this can damage your eyesight.

Safety Notices
Installation and service of this gateway must only be performed by authorized, qualified service personnel.

The protective earth terminal on the back of the 5000 must be permanently connected to protective earth.

The unit is powered from a DC mains and is intended for installation in a Restricted Access Location (RAL) with maximum allowed temperature 45°C (113°F)

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.

Reduced Air Flow - Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.

Mechanical Loading - Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.

25A DP Branch circuit protection for each feeding line.

Telecommunication Safety
The safety status of each port is declared and detailed in the table below:

<table>
<thead>
<tr>
<th>Ports</th>
<th>Safety Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>T3</td>
<td>SELV</td>
</tr>
<tr>
<td>Ethernet (100 Base-TX)</td>
<td>SELV</td>
</tr>
<tr>
<td>DC Input Power Port</td>
<td>SELV</td>
</tr>
</tbody>
</table>

TNV-1: Telecommunication network voltage circuits whose normal operating voltages do not
### Telecommunication Safety

The safety status of each port is declared and detailed in the table below:

exceed the limits for SELV under normal operating conditions and on which over voltages from telecommunication networks are possible.

**SELV**: Safety extra low voltage circuit.

---

### FCC Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

---

*This is a Class A product.* In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.
# 12 Index

## 6

**6310/RTM - Rear Transition Module** ..........................33

## A

Accessing Advanced Status of Media Gateway Board via WEB Interface ..........................353

Activating and Deactivating Debug Recording ..........................................................358

Activating the New X.509 Certificates ..................220

Adding Certificates to the Auxiliary Files Repository.............................................220

Adding Media Gateway Boards to an Avaya G860 System ......................................120, 307

Administering Users on SC Boards ..........241

Advanced Security Features ..............................................239

After Completing the Online Software Upgrade .................................................338

Aggregation Link Distribution Policy-Example .................................................131, 132, 139, 150, 153, 155

Aggregation Switch-Over Logic ..............131, 139, 150, 153, 155

Alarm Indicators ..................................................................29

Alternative Routing Provisioning Rules ..........187

Appendix - Installing the Solaris™ 9 OS .......105, 290, 375

Appendix - List of Alarms ..............................................111, 379

Ascertaining the MAC Addresses for the TP-6310 ..................................................309

Associating a X.509 File with a Media Gateway ..................................................286

AUDCFTP User Password Administration .241, 247

AudioCodes Technical Support Log Areas .360

Automatic Backups .....................................................................106

Auxiliary Files Repository ..................................................270

Avaya G860 Board Configuration ..............21

Avaya G860 Boards ..................................................30, 73

Avaya G860 Boards ..............................55

Avaya G860 Selected Technical Specifications ..................................................365

Avaya G860Accessory Kit ..................22

## B

Board Assembly Order ..........................51, 308

Board Replacement Preliminaries ..........289

Boards' IP Addresses for Avaya G860 Configuration ...........................................57

## C

Cables ..................................................................55

Cabling the Avaya G860 ...........................................81, 344

Call Progress Tones (CPT) Files ..................271

Centralized User Authentication ............242, 250

Changing Password of CLI User ..................246

Changing the Basic Configuration of the SC Boards .............................................81, 88, 109

Changing the Basic SC Configuration of the 1st SC Board .....................................88, 93

Changing the Basic SC Configuration on the 2nd SC Board ..................................88, 98

Checking the Fan Speeds ..........................266, 315, 316, 317

Class of Service (COS) ..................144

CLI User Administration ...........................92, 241, 243

Clock Synchronization ..........................63, 350

Coders Table ..............................................189, 196

Collecting Advanced Media Gateway Board Logs .................................................351, 362

Collecting Call Data Records (CDRs) ..........352

Collecting Debug Recording Traces on the Standby SC board ..........................359

Collecting logs for AudioCodes Technical Support .............................................362, 363

Collecting Media Gateway Board's Debug Recording Traces ..................................354

Configuring & Operating the Media Gateway ..........................................................109, 307

Configuring Alternative Routing ..................187

Configuring an X.509 Certificate Expiration Date Reminder ........................................222

Configuring Clock Synchronization ..............63, 252

Configuring Coders Table ..................................190, 196

Configuring Debug Recording Rules ..............355

Configuring Firewall Functionality ..................209, 231

Configuring IP to Telephone Routing ..................................184

Configuring IPSEC/IKE for Management Interfaces .............................................225

Configuring IPSEC/IKE for Media Gateway Controllers ........................................226

Configuring NFAS group provisioning ............161

Configuring NTP Server ........................................123

Configuring PSTN Connectivity ..................157

Configuring SDH/SONET ..............................................160

Configuring Security Settings ...........209, 212, 298, 345

Configuring SIP / ISDN Cause Mapping ............188

Configuring Telephone to IP Routing ..............182

Configuring the Basic IP Network Parameters of SC Boards ..........................78, 105, 346

Configuring the EMS and ROOT Passwords of the Avaya G860 in the EMS ..........329

Configuring the Internal DNS Table .................186

Configuring the IP Address of the ES Board Software .............................................310, 311

Configuring the IP Addresses of Media Gateway Boards and Network Servers ........112, 348

Configuring the Media Gateway for IP Connectivity .............................................57, 127

Configuring the Number Manipulation Tables ..............................................175

Configuring the SIP Subsystem ..................166

**Issue 2 November 2008** 385
Avaya G860 Media Gateway

Configuring the Syslog Server..................352
Configuring the Trunks..........................157
Configuring the Voice Settings.................163
Configuring Trunk Group Settings Table......194
Configuring Trunk Group Table.................192
Connecting AC Power..........................72, 76
Connecting DC Power..........................70, 74
Connecting Power - 6310 System
  Configuration..............................................74
  Connecting System Power .. 56, 70, 313, 314
  Connecting the ES/6600 IP Network CAT 5
    Copper Cabling ........................................56, 81, 82
  Connecting the Media Gateway to the IP
    Network ................................................61, 124, 350, 351
  Connecting the PSTN Interface - STM-1/OC-3
    Configurations ........................................56, 81, 83
  Connecting the T3 PSTN Interfaces.. 56, 81, 86, 307
  Connecting to the SC Board's RS-232 Console
    ........ 78, 90, 92, 344, 345, 346, 350, 376
  Connecting to the SC Board's Terminal . 79, 89, 93, 98, 103, 105, 211, 213, 237, 238, 239, 240, 242, 243, 245, 246, 247, 249, 294, 295, 301, 324, 327, 340, 353, 359, 375
  Constraints for Adding Boards to the Avaya
    G860 System .............................................308
  Converting External Coders File to Binary
    Format.................................................284, 285
  Converting the Call Progress Tones File to
    Binary Format ........................................272
  Cooling System ........................................26, 344
  COS Queue Configuration.......................145
  Creating a New CLI User .................................243
  Creating a Pre-Recorder Tones File ...........278
  Creating a Voice Prompts File ................280, 281
  Creating the SC Software Backup ...........103, 106
  Customer's Log Area ..................................360

D

Defining IP Parameters ..........................56
Deleting a CLI User ................................245
Diagnostics & Troubleshooting ...............306, 343
Dialing Plan Notation ......................177, 178, 181, 185
DiffServ Priorities .............................58
Disabling a Direct Remote Root Login 212, 338
Disabling Secure Operation Mode ...........214

E

Earthing ..............................................68, 70, 313
Earthing Requirements..........................24, 56
Earthing the Gateway ...........................68
Electrical ..............................................54
Electro Magnetic Compatibility (EMC) Features
  .................................................................25
EMS User Password Administration 241, 249, 329
Enabling a Direct Remote Root Login 210, 212
Enabling Secure Operation Mode ..........213, 214
Environmental Conditions .....................60

Environmental Requirements .................59
Equipment .............................................54
ES 6600 Ethernet Switch Port Allocation ..147
ES 6600-Class of Service (COS) .............144
ES Board Actions ................................123
ES/6600 - Used in Avaya G860 Configurations
  .................................................................44
ES/6600 Panel Indicators ......................47
ES/6600 Physical Slots to Ethernet Port
  Correlation - Avaya G860 Configuration 48
ES/6600/RTM ..........................................44, 50
ESD Requirements ..................................289
Ethernet Switch Board Replacement
  Procedure ...............................................310
Ethernet Switch Boards .........................44, 311
Example 1
  Without Physical Separation .................125
Example 2
  With Physical Separation ....................126
External Alarm Indicator Connections... 81, 86
External Coders Files ..........................284

F

Faults and Alarms Monitoring .................111
File System Integrity ..........................210, 236
Finish .................................................337
FMR/5K - Auxiliary Fan Tray Unit .............27
FPM/5K - Advanced Fan Power Module .........28
Front and Back Views of the Avaya G860....22, 69, 289
Front Panel Mini DIN 8 COM Serial Port 37, 78, 344

G

Gateway Addresses ..............................57
Generating a Certificate Signing Request ..218
Generating a Private Key .......................215
Generating a Self-Signed Certificate .......217
Getting Started with the Avaya G860 .......53

H

Hardware and Application Types ..........116
Hardware Replacement Procedures.......289, 307, 309
History Performance Measurements .......260

I

IEEE 802.1p QoS/CoS Layer 2 Traffic
  Prioritization ........................................58
Information Needed when Contacting
  Technical Support ...............................363
Initial X.509 configuration ..................215
Installation Package .............................292
Installation Process Flow .....................53
Installing the Media Gateway Software on
  the 1st SC Board .........................292, 295, 303
Installing the Media Gateway Software on
  the 2nd SC Board ..............................292, 300, 301
Installing the Media Gateway Software on the Replaced SC Board ........................................ 290, 291, 346
Installing the Solaris™ 9 OS on the SC Board ........................................................................ 376
Interface Separation ........................................... 133
Interfaces Setting Options ................................ 138
Interfaces, Subnets, VLANs and Tags .......... 129, 139, 141, 145, 149, 152, 155
Internal DNS Table ........................................... 185
Internal Software Logs ..................................... 360
Introduction to the Avaya G860 Media Gateway ..................................................................... 184
Introductory Notes ........................................... 17
IP Parameters of the Media Gateway Board Table .................................................. 113, 114
IP Parameters of the Media Gateway Controller Table .................................................. 113
IP Parameters of the Media Gateway Table ......................................................................... 112, 113
IP Profile Table ................................................ 202
IP to Telephone Routing Provisioning Rules ........................................................................ 184
IP to Telephone Routing Table .................. 178, 183, 187
IPSEC and IKE .............................................. 224, 298
IPSEC Configuration ............................................. 59
Limited Root Access ........................................... 93, 210
Link Aggregation in the Avaya G860 .............. 130
Link Aggregation Options ......................... 131, 139, 150, 153, 155
Log Areas ........................................................ 360
Log Files Storage ............................................. 361
Logging in as a CLI User ................................. 93
Logging in as a ROOT User ............................. 92
Login Banner .................................................. 240
Lost User Password Recovery ....................... 242
Managed Objects, Administrative and Operational State .............................................. 110
Manipulation Rules .......................................... 177
Media Gateway Block Diagrams ................. 20
Media Gateway Board Actions ..................... 117, 307
Media Gateway Board Replacement Procedure ............................................................. 305
Media Gateway Boards’ Configuration Backdoor ............................................................... 266
Media Gateway Inventory ............................... 265
Media Gateway Software Backup/Restore Procedures ........................................................ 103, 323, 337
Media Security ................................................... 209, 229
Midplane Keying ............................................. 26
Modifying the .................................................. 272, 284
Modifying the Media Gateway Configuration ................................................................... 111
Mounting the Chassis on a Rack .................... 65
Network Servers’ IP Addresses ...................... 57
Network Services on SC Board ...................... 239
Networks .......................................................... 124
Number Manipulation Tables ....................... 174
Numbering Plans and Type of Number .............. 178
Online Software Upgrade – Overview ............. 321, 327, 332, 337, 339
OpenBoot PROM Security .............................. 239
OS Auditing ....................................................... 210, 234
OS Hardening ................................................. 210, 234
OS Patching ..................................................... 209, 233
Overview ........................................................ 109
Packet Cable Security ....................................... 229
Performance Monitoring .............................. 257
Performing a Manual Rollback to the Previous Software Configuration ........................... 340
Performing the Online Software Upgrade ........ 329
Physical Requirements ................................. 54
Planning the Maintenance Time Period ............ 326
Possible Uses for Telephone to IP Routing ....... 181
Possible Uses for the Number Manipulation Tables .................................................... 175
Post-Power Connection Test Procedures Checklist ............................................................ 76
Power Consumption ........................................ 25
Power Requirements ........................................ 24
Power Supply Module Replacement ............... 312
Powering Up ..................................................... 69, 344
Pre-installing OS Patches ......................... 326, 327, 336
Preparing for Online Software Upgrade ......... 323
Preparing the 'Install Image' on the Install Server (EMS) .................................................. 376
Preparing the IP Network ......................... 325, 326
Preparing the IP Network Connectivity ....... 54, 61
Preparing the Media Gateway ..................... 323
Preparing the Media Gateway Boards .......... 323
Preparing the PSTN Network Connectivity ...... 62
Pre-Recorded Tones (PRT) Files ................... 278
Pre-Upgrade Configuration Backup ............... 322
Profiles Tables ................................................. 195
Real-Time Performance Measurements ......... 258
Reasons for Alternative Routing ................. 181, 186
Recovering the Basic Interface Separation, VLANs & Link Aggregation Default Settings .... 97, 345, 350
Recovery from a Network Failure or EMS Server/Client Crash ....................................... 339
Redundancy Modes ......................................... 118, 349
Regulatory Information ................................. 381
Replacing Air Filters ....................................... 318
Recovering a SC Board..................................................................................35
Replacing the Fan Power Modules .............................................317
Replacing the Fan Tray Modules .........................................................314
Replacing the FPM/5K Fan Tray Module ...........................................315
Replacing the FPM/5K Advanced Fan Power Module - 5000 ....316
Replacing the PEM..................................................................................313
Replacing the PEM AC Fuse.................................................................313
Restoring Media Gateway Software from Backup.................................105, 106, 107
Rollback ...............................................................................................338
ROOT User Administration .................................................................241, 242
S
SA Synchronization and Alarm RTM......................................................38, 344
SA/RTM Card and Panel .....................................................................40
SA/RTM Replacement Procedure .......................................................309
SC (System Controller) Board ............................................................35
SC Board Actions ..................................................................................115
SC Board Replacement Procedure .....................................................88, 290, 341
SDH/SONET Network Connections ......................................................62
Secure Operation Mode ......................................................................90, 212, 224, 234
Secure RTP ..........................................................................................230
Setting Networks .................................................................................142
Setting up the Physical Interfaces, VLANs & Subnet Separation ....134, 148
SIP to ISDN Cause and ISDN to SIP Cause Table..............................188
Site Preparation ...................................................................................54
Slot Cover Requirements ...................................................................289, 290
Software Upgrade ................................................................................321
Software Upgrade/Rollback Troubleshooting .....................................340
Solaris OS Logs ....................................................................................362
SSH/SCP/SFTP ....................................................................................209, 228
SSL/TLS ................................................................................................229
Standalone Board Sync Clock Mode for TP-6310 Configurations ....252
Starting the Online Software Upgrade Wizard .....................................303, 327, 338, 340, 353, 359
Static Route Settings ...........................................................................141
Subnet & VLAN Settings ...................................................................134
Subnet Separation Options ................................................................140
SUID Files ............................................................................................241
Supported Actions ................................................................................269
System Controller Panel Indicators & Controls ....................................37
T
T3 6310 Board Panel T3 LED Indicators ............................................33
T3 Network Connections ....................................................................62
Tel Profile Table ....................................................................................198
Telephone to IP Routing Provisioning Rules .......................................180
Telephone to IP Routing Table.............................................................178, 180, 187
Testing the Configured System ..........................................................100
The Chassis ..........................................................................................23
The Routing Tables .............................................................................179
The SIP Proxy .......................................................................................167, 182
The SIP Registrar ...............................................................................173
The TP-6310 Media Gateway Board ...................................................30
Timing Module BITS Sync Clock Mode for TP-6310 Configurations ...252, 253, 254
Transferring the SC Software Package to the SC Boards.................336, 337
Troubleshooting ................................................................................344
Troubleshooting Strategy ...................................................................343
Troubleshooting the Newly installed Media Gateway Board ............308, 348
Trunk Group Settings Table ...............................................................183, 184, 194
Trunk Group Table .............................................................................184, 192
U
Unpacking/Checking Contents ..............................................................63
Upgrading the 1st SC Board ................................................................337
Upgrading the 2nd SC Board ...............................................................335
Upgrading the ES Boards ..................................................................337
Upgrading the Media Gateway Boards ...............................................337
Uploading the Installation Package .....................................................293
Usage Tips .........................................................................................269
Use Case
Connecting Using One Physical Interface, No VLANs and One Subnet 152
Connecting Using One Physical Interface, Three VLANs and Three Subnets 149
Connecting Using Three Physical interfaces, Three VLANs and Three Subnets 154
Use Cases for IP Network Connectivity
Configuration .......................................................................................61, 134, 148
Users on SC Board’s Terminal ..... 79, 92, 93, 98, 101, 104, 105, 210, 211, 213, 237, 238, 239, 240, 243, 245, 246, 247, 249, 293, 295, 301, 303, 327, 338, 340, 353, 359
Using Auxiliary Files ............................................................................270
V
Verifying that Online Software Upgrade is Supported .........................325
Verifying the Current Version of the Solaris™ OS on the SC Board ....375
Viewing Log Files ................................................................................361
VLAN Tagging .....................................................................................129
VLANs Configuration ..........................................................................58
Voice Prompts Files ............................................................................280
W
Welcome Questionnaire ....................................................................332, 337
Working with System Controller Boards ...........................................114
Working with the Ethernet Switch Boards .........................................121, 345, 347
Working with the Media Gateway Boards .........................................115, 347, 348, 349, 353
Working with VLANs .........................................................................128
Working with VRRP/HSRP Protocols ........128

X

X.509 Certificates .......................214, 227, 287