

# Converteon™ Family Management Software

---

**AT-S73 and AT-S99**

## User's Guide

CONVERTEON™ Family Media Converter Products

AT-S73 Version 3.0.0 Management Software for the AT-CM Media Converter Line Card Series

AT-S99 Version 3.0.0 Management Software for the AT-CV5M02 Management Card

Copyright © 2008 Allied Telesis, Inc.

All rights reserved. No part of this publication may be reproduced without prior written permission from Allied Telesis, Inc.

Allied Telesis is a trademark of Allied Telesis, Inc. Microsoft and Internet Explorer are registered trademarks of Microsoft Corporation. All other product names, company names, logos or other designations mentioned herein are trademarks or registered trademarks of their respective owners.

Allied Telesis, Inc. reserves the right to make changes in specifications and other information contained in this document without prior written notice. The information provided herein is subject to change without notice. In no event shall Allied Telesis, Inc. be liable for any incidental, special, indirect, or consequential damages whatsoever, including but not limited to lost profits, arising out of or related to this manual or the information contained herein, even if Allied Telesis, Inc. has been advised of, known, or should have known, the possibility of such damages.

# Contents

---

<b>Preface</b> .....	15
Where to Find Web-based Guides .....	16
Contacting Allied Telesis .....	17
Online Support .....	17
Email and Telephone Support .....	17
Returning Products .....	17
Sales and Corporate Information .....	17
Warranty .....	17
Management Software Updates .....	18
<b>Chapter 1: AT-CV5M02 Management Card</b> .....	19
The Converteon Product Line .....	20
AT-CV5M01 and AT-CV5M02 Management Cards .....	21
AT-S99 Management Software .....	22
Console Port .....	22
10/100Base-TX Port .....	22
IP Address Configuration .....	23
Event Log .....	23
Activity Monitor .....	23
Syslog Client .....	23
Network Time Protocol Client .....	24
Manager and Operator Accounts .....	24
Management Access .....	25
Local Management .....	25
Remote Telnet Management .....	25
Remote Web Browser Management .....	25
SNMP Management .....	25
Redundant Management Cards .....	26
Status Messages .....	27
Access to Your Network .....	28
Configuration Files .....	29
AT-CM Line Cards .....	29
AT-CV Line Cards .....	29
AT-CV5M02 Management Card .....	29
Restoring Configurations to AT-CM Line Cards .....	30
AT-CM Line Cards and Remote Peer Management .....	31
Redundant Management Cards .....	32
Converteon Chassis .....	34
<b>Chapter 2: AT-CM and AT-CV Media Converter Line Cards</b> .....	35
AT-CM Media Converter Line Cards .....	36
AT-CV Media Converter Line Cards .....	40
Operating Modes .....	42
Link Test Mode .....	42
MissingLink Mode .....	43
Smart MissingLink Mode .....	44
OAM Visible Mode .....	45
OAM Bypass Mode .....	45
Setting the Operating Mode .....	45

OAM-based Features.....	46
Remote Peer Management .....	46
Remote Updates of the AT-S73 Management Software .....	50
OAM Loopback Tests .....	51
Dying Gasp Feature .....	52
OAM Variable Requests .....	55
OAM Client Settings .....	56
<b>Chapter 3: Starting a Management Session .....</b>	<b>57</b>
Starting a Local Management Session .....	58
Starting a Telnet Management Session.....	61
Starting a Web Browser Management Session.....	62
Saving Your Configuration Changes.....	64
What to Configure First on the AT-CV5M02 Management Card .....	69
Changing the Manager and Operator Passwords .....	69
Assigning an IP Address Configuration and Changing the Community Strings .....	70
Setting the Date and Time.....	71
Naming the Management Card.....	72
Saving Your Changes.....	72
Configuring the AT-CM Media Converter Line Cards for the OAM-based Features.....	74
<b>Chapter 4: Configuring the AT-CV5M02 Management Card .....</b>	<b>79</b>
Assigning an IP Address Configuration .....	80
Menus .....	80
Web Browser .....	82
Assigning a Name.....	85
Menus .....	85
Web Browser .....	85
Assigning Contact and Location Information .....	86
Menus .....	86
Web Browser .....	86
Configuring the SNMP Community Strings.....	88
Menus .....	88
Web Browser .....	88
Specifying the IP Addresses of SNMP Trap Receivers .....	89
Menus .....	89
Web Browser .....	89
Configuring Management Security.....	90
Menus .....	90
Web Browser .....	92
Manually Setting the Date and Time.....	93
Menus .....	93
Web Browser .....	94
Configuring the Network Time Protocol Client.....	95
Menus .....	95
Web Browser .....	95
Resetting the Management Card .....	96
Menus .....	96
Web Browser .....	97
Viewing the Event Log .....	98
Menus .....	98
Web Browser .....	103
Viewing the Activity Monitor.....	104
Menus .....	104
Web Browser .....	104
Configuring the Syslog Client.....	105
Menus .....	105
Web Browser .....	105
Configuring the 10/100Base-TX Port.....	107
Menus .....	107
Web Browser .....	110

Restoring the Default Setting on the 10/100Base-TX Port .....	112
Menus.....	112
Web Browser.....	112
Restoring the Default Values on the AT-CV5M02 Management Card .....	113
Menus.....	113
Web Browser.....	114
Configuring the Temperature Threshold.....	115
Menus.....	115
Web Browser.....	115
Activating a Standby AT-CV5M02 Management Card .....	117
Menus.....	117
Web Browser.....	118
Setting the Baud Rate of the Console Port.....	119
Menus.....	119
Web Browser.....	120
Displaying the Operational Status of the Chassis.....	121
Menus.....	121
Web Browser.....	123
Pinging Network Devices.....	125
Menus.....	125
Web Browser.....	125
Displaying Management Card Information .....	126
<b>Chapter 5: Configuring AT-CM and AT-CV Media Converter Line Cards .....</b>	<b>127</b>
Displaying the Status of the Line Cards.....	128
Menus.....	128
Web Browser.....	133
Displaying the Parameter Settings on AT-CM Line Cards.....	136
Menus.....	136
Web Browser.....	137
Configuring the Port Parameters on AT-CM Line Cards .....	139
Menus.....	139
Web Browser.....	143
Setting the Operating Mode.....	145
Menus.....	145
Web Browser.....	147
Assigning Names to AT-CM Line Cards .....	149
Menus.....	149
Web Browser.....	149
Configuring the Maximum Frame Size on AT-CM2KOS Line Cards .....	150
Menus.....	150
Web Browser.....	150
Setting the Auto-copy Feature.....	151
Menus.....	151
Web Browser.....	152
Restoring the Default Settings.....	153
Menus.....	153
Web Browser.....	155
Restoring the Last Saved Configuration .....	157
Menus.....	157
Web Browser.....	158
Displaying Port Statistics .....	160
Menus.....	160
Web Browser.....	161
Resetting Media Converter Line Cards.....	162
Menus.....	162
Web Browser.....	163
Displaying the Version Numbers of the Management Software .....	164
Menus.....	164
Web Browser.....	166

Displaying the MAC Addresses and Serial Numbers.....	167
Menus .....	167
Web Browser .....	168
Displaying SFP Module Information.....	170
Menus .....	170
Web Browser .....	172
<b>Chapter 6: Configuring AT-CM Line Cards with Remote Peer Management .....</b>	<b>173</b>
Configuring Remote AT-CM Line Cards from the Menus .....	174
Naming a Remote Line Card .....	179
Displaying the Current Configuration .....	180
Configuring Remote Ports .....	180
Restoring the Default Settings .....	180
Restoring the Last Saved Configuration .....	181
Saving the Parameter Settings .....	181
Configuring Remote AT-CM Line Cards from the Web Browser Windows .....	182
Displaying the Current Configuration .....	184
Configuring Remote Ports .....	184
Restoring the Default Parameter Settings .....	185
Restoring the Last Saved Configuration .....	185
Saving the Parameter Settings .....	186
Displaying the Version Numbers of Remote AT-CM Line Cards .....	187
Menus .....	187
Web Browser .....	188
<b>Chapter 7: Configuring the T1/E1 Ports on the AT-CM70S Media Converter Line Card .....</b>	<b>191</b>
Selecting the Management Method for the T1/E1 Ports .....	192
Configuring the T1/E1 Ports from the AT-CV5M02 Management Card .....	196
Configuring the T1/E1 Ports from the Console Port on the Line Card .....	199
<b>Chapter 8: Configuring the Operations, Administration, and Maintenance Client .....</b>	<b>203</b>
Configuring an OAM Client .....	204
Menus .....	204
Web Browser .....	208
Performing an OAM Loopback Test.....	209
Menus .....	209
Web Browser .....	212
Displaying OAM Information for Local OAM Clients .....	214
Menus .....	214
Web Browser .....	220
Displaying OAM Information for Remote OAM Clients .....	221
Menus .....	221
Web Browser .....	222
Displaying OAM Statistics .....	223
Menus .....	223
Web Browser .....	224
Viewing MIB Variables with OAM Variable Requests .....	225
Menus .....	225
Web Browser .....	226
<b>Chapter 9: Configuring AT-CM Line Cards for Dying Gasp .....</b>	<b>229</b>
Configuring the AT-CM Line Cards.....	230
Testing the Feature.....	235
<b>Chapter 10: Configuring SNMPv3 .....</b>	<b>237</b>
SNMPv3 Overview.....	238
SNMPv3 Authentication Protocols.....	239
SNMPv3 Privacy Protocol.....	239
SNMPv3 MIB Views.....	239
SNMPv3 Storage Types .....	241
SNMPv3 Message Notification .....	241
SNMPv3 Tables.....	242
SNMPv3 Configuration Example .....	246

Configuring SNMPv3 Entities .....	247
Configuring the SNMPv3 User Table.....	248
Configuring the SNMPv3 View Table .....	251
Configuring the SNMPv3 Access Table.....	254
Configuring the SNMPv3 Group Table .....	258
Configuring the SNMPv3 Notify Table .....	261
Configuring the SNMPv3 Target Address Table.....	264
Configuring the SNMPv3 Target Parameters Table .....	267
<b>Chapter 11: Uploading and Downloading Files</b> .....	<b>271</b>
Overview .....	272
Configuring the TFTP Client .....	273
Downloading New Management Software Using TFTP .....	275
Downloading New Management Software Using XMODEM .....	279
Uploading the Master Configuration File from a Management Card .....	281
Menus.....	281
Web Browser .....	282
Downloading the Master Configuration File to a Management Card .....	284
Menus.....	284
Web Browser .....	285
<b>Appendix A: Default Settings for the Management Software Programs</b> .....	<b>287</b>
<b>Appendix B: SNMPv3 Configuration Examples</b> .....	<b>291</b>
SNMPv3 Configuration Examples .....	291
SNMPv3 Manager Configuration.....	291
SNMPv3 Operator Configuration.....	293
SNMPv3 Worksheet .....	294
<b>Appendix C: Packet Rate Limiting on the AT-CM2K0S Line Card</b> .....	<b>297</b>
<b>Index</b> .....	<b>317</b>



# Figures

---

Figure 1. Updating the Master Configuration File on a Standby Card .....	32
Figure 2. Remote Peer Management - Example 1 .....	47
Figure 3. Remote Peer Management - Example 2 .....	48
Figure 4. Remote Module Status and Configuration Menu.....	49
Figure 5. Remote Module Status and Configuration Window.....	49
Figure 6. Downloading New AT-S73 Management Software to Remote AT-CM Line Cards.....	50
Figure 7. Loopback Test.....	51
Figure 8. Dying Gasp Feature .....	52
Figure 9. 1st Failure Signal.....	53
Figure 10. Connecting the Management Cable to the Management Card's Console Port.....	58
Figure 11. Main Menu.....	59
Figure 12. URL Field in a Web Browser .....	62
Figure 13. Chassis View.....	63
Figure 14. Save Commands in the Configuration Menu.....	64
Figure 15. Save Commands in the Files Tab .....	65
Figure 16. Save Command in the Line Card Configuration Menu for a Local AT-CM Line Card .....	65
Figure 17. Save Command in the Line Card Configuration Menu for a Local AT-CM Line Card .....	66
Figure 18. Management Card Redundancy Menu.....	67
Figure 19. Management Card Redundancy Tab .....	67
Figure 20. Module Status and Configuration Menu .....	75
Figure 21. Configuration Menu .....	80
Figure 22. System Configuration Menu .....	80
Figure 23. IP Parameters Menu.....	81
Figure 24. System Tab .....	83
Figure 25. SNMPv1 & SNMPv2c Tab.....	87
Figure 26. Omega Options Menu .....	90
Figure 27. System Clock Menu.....	93
Figure 28. General Tab .....	97
Figure 29. Administration Menu.....	98
Figure 30. Event Log Menu .....	98
Figure 31. Event Log .....	99
Figure 32. Event Log Tab .....	103
Figure 33. Activity Monitor.....	104
Figure 34. Syslog Tab .....	105
Figure 35. Module Configuration Menu (Management Card).....	107
Figure 36. Port Configuration Menu for the 10/100Base-TX Port on the Management Card.....	108
Figure 37. Port Configuration Menu for the 10/100Base-TX Port on the Management Card.....	109
Figure 38. Port A Tab for the Management Card .....	110
Figure 39. 10/100Base-TX Port on the Management Card .....	111
Figure 40. Temperature Threshold Configuration Menu.....	115
Figure 41. Management Card Redundancy Menu.....	117
Figure 42. Confirmation Prompt for Switch Over Management Cards .....	117
Figure 43. Management Card Redundancy Tab .....	118
Figure 44. Terminal Configuration Menu .....	119
Figure 45. Terminal Data Rate Menu .....	120
Figure 46. Diagnostics Menu .....	121
Figure 47. Chassis Diagnostics Menu .....	122
Figure 48. Chassis Diagnostics Tab .....	124
Figure 49. Module Status and Configuration Menu .....	128
Figure 50. Chassis View .....	133

Figure 51. Menu View .....	134
Figure 52. Display Current Configuration Window .....	136
Figure 53. Current Configuration Tab .....	137
Figure 54. Module Configuration Menu (Media Converter Line Card) .....	139
Figure 55. Port Management Menu .....	140
Figure 56. Port Configuration Menu .....	141
Figure 57. Port Configuration Window .....	144
Figure 58. Operating Mode Config Menu .....	145
Figure 59. Setting Window .....	147
Figure 60. Max Frame Size Config Menu .....	150
Figure 61. Auto-copy Line Card Configuration Prompt .....	151
Figure 62. Auto-copy Tab .....	152
Figure 63. Line Card Configuration Menu .....	153
Figure 64. Display Default Configuration Window .....	154
Figure 65. Default Configuration Tab .....	155
Figure 66. Last Saved Configuration Tab .....	158
Figure 67. Show Port Statistics Window .....	160
Figure 68. Port Statistics Window .....	161
Figure 69. General tab .....	163
Figure 70. Line Card Module Software Image Version Window .....	165
Figure 71. Linecard Image Information Tab .....	166
Figure 72. Line Card Module Information Window .....	167
Figure 73. Linecard Information Window .....	169
Figure 74. SFP Information Window (1/2) .....	171
Figure 75. SFP Information Window (2/2) .....	171
Figure 76. SFP Information Tab .....	172
Figure 77. Remote Module Status and Configuration Menu .....	174
Figure 78. Remote Module Configuration Menu .....	179
Figure 79. Remote Module Status & Configuration Tab .....	182
Figure 80. Remote Module Status & Configuration Page .....	183
Figure 81. Remote Line Card Module Software Image Version Window .....	187
Figure 82. Remote Linecard Image Information Tab .....	189
Figure 83. UART Setting on the AT-CM70S Line Card .....	193
Figure 84. TDM Management Menu .....	194
Figure 85. UART Configuration Menu .....	195
Figure 86. LIU Mode and Channel Select Menu .....	196
Figure 87. TDM Channel Configuration Menu 1 .....	197
Figure 88. TDM Channel Configuration Menu 2 .....	197
Figure 89. Local Console Menu on the AT-CM70S Line Card .....	200
Figure 90. OAM Configurations Menu .....	204
Figure 91. OAM Configuration Submenu .....	205
Figure 92. OAM Configuration Tab .....	208
Figure 93. OAM Loopback Test Menu .....	209
Figure 94. Show Loopback Test Statistics Window .....	211
Figure 95. OAM Loopback Test Tab .....	212
Figure 96. OAM Test Statistics .....	213
Figure 97. Show Local OAM Information Window .....	215
Figure 98. OAM Local Information Tab .....	220
Figure 99. Show Remote OAM Information Window .....	221
Figure 100. Remote OAM Information Tab .....	222
Figure 101. Show OAM Statistics Window .....	223
Figure 102. OAM Statistics Tab* .....	224
Figure 103. Enter Branch Number Prompt .....	225
Figure 104. Enter Leaf Number Prompt .....	226
Figure 105. OAM Variable Request Tab .....	226
Figure 106. Line Card Module Software Image Version - Hardware Version Numbers .....	231
Figure 107. Line Card Module Software Image Version - AT-S73 Version Numbers .....	232
Figure 108. Module Status and Configuration Menu .....	232
Figure 109. MIB Tree .....	240
Figure 110. SNMPv3 User Configuration Process .....	242

Figure 111. SNMPv3 Message Notification Process .....	243
Figure 112. Configure SNMPv3 User Table Menu .....	248
Figure 113. SNMPv3 User Table Tab.....	249
Figure 114. Configure SNMPv3 View Table Menu .....	251
Figure 115. SNMPv3 View Table Tab .....	252
Figure 116. Configure SNMPv3 Access Table Menu .....	254
Figure 117. SNMPv3 Access Table Tab.....	255
Figure 118. Configure SNMPv3 Group Table Menu.....	258
Figure 119. SNMPv3 Group Table Tab .....	259
Figure 120. Configure SNMPv3 Notify Table Menu.....	261
Figure 121. SNMPv3 Notify Table Tab.....	262
Figure 122. Configure SNMPv3 Target Address Table Menu .....	264
Figure 123. SNMPv3 Target Address Table Tab.....	265
Figure 124. Configure SNMPv3 Target Parameters Table Menu.....	268
Figure 125. SNMPv3 Target Parameters Table Tab .....	268
Figure 126. TFTP Image Download Configuration .....	273
Figure 127. Image Download Menu.....	276
Figure 128. Image Download via TFTP Menu .....	276
Figure 129. Image Download via TFTP Menu .....	280
Figure 130. Configuration File Upload/Download with TFTP.....	281
Figure 131. Files Tab.....	282
Figure 132. Rate Limit Input vs. Hardware Configured Values.....	297



# Tables

---

Table 1. Converteon Chassis .....	34
Table 2. AT-CM Media Converter Line Cards .....	37
Table 3. AT-CV Media Converter Line Cards .....	40
Table 4. Versions of the AT-CM Line Cards that Support Dying Gasp .....	54
Table 5. Versions of the Management Software that Support Dying Gasp .....	54
Table 6. OAM Parameter Settings for the OAM-based Features .....	56
Table 7. Menu Selection Options .....	60
Table 8. Omega Options Menu .....	91
Table 9. Event Log Format .....	99
Table 10. Event Log Messages .....	100
Table 11. Module Configuration Menu for a Management Card .....	108
Table 12. Port Configuration Menu for the 10/100Base-TX Port on the Management Cards .....	109
Table 13. Chassis Diagnostics Menu .....	122
Table 14. Module Status and Configuration Menu .....	128
Table 15. Module Status and Configuration Window .....	134
Table 16. Module Configuration Menu .....	139
Table 17. Port Configuration Menu for Both Fiber Optic Ports and Twisted Pair Ports .....	141
Table 18. Port Statistics .....	160
Table 19. Line Card Module Software Image Version Window .....	165
Table 20. Line Card Module Information Window .....	168
Table 21. Remote Module Status and Configuration Menu .....	174
Table 22. Remote Module Status & Configuration Tab .....	182
Table 23. Line Card Module Software Image Version Window .....	188
Table 24. Line Card Module Software Image Version Window .....	189
Table 25. T1/E1 Port Settings .....	198
Table 26. OAM Client Parameters .....	205
Table 27. Show Local OAM Information Window .....	215
Table 28. Version Numbers of AT-CM Line Cards that Support the Dying Gasp Feature .....	231
Table 29. SNMPv3 User Table Parameters .....	249
Table 30. SNMPv3 View Table Parameters .....	252
Table 31. SNMPv3 Access Table Parameters .....	255
Table 32. SNMPv3 Group Table Parameters .....	259
Table 33. SNMPv3 Notify Table Parameters .....	262
Table 34. SNMPv3 Target Address Table Parameters .....	265
Table 35. SNMPv3 Target Parameters Table Parameters .....	268
Table 36. Default Settings for the AT-S99 Management Software .....	287
Table 37. Default Settings for the AT-S73 Management Software .....	288
Table 38. Rate Limits Equivalents .....	298



# Preface

---

This is the management guide for the Converteon™ product line of media converter line cards and management card. In this guide you'll learn about the features of the AT-CM and AT-CV Media Converter Line Cards and the AT-CV5M02 Management Card, and how to monitor and configure the devices from the menus and the web browser windows in the AT-S99 Management Software on the management card.

This preface contains the following sections:

- “Where to Find Web-based Guides” on page 16
- “Contacting Allied Telesis” on page 17

## Where to Find Web-based Guides

---

The installation and user guides for all of the Allied Telesis products are available for viewing in portable document format (PDF) from our web site at **[www.alliedtelesis.com](http://www.alliedtelesis.com)**.

## Contacting Allied Telesis

---

This section provides Allied Telesis contact information for technical support and for sales and corporate information.

### Online Support

You can request technical support online from the Allied Telesis Knowledge Base at [www.alliedtelesis.com/support/kb.aspx](http://www.alliedtelesis.com/support/kb.aspx). You can submit questions to our technical support staff from the Knowledge Base and review answers to previously asked questions.

### Email and Telephone Support

For Technical Support via email or telephone, refer to the Allied Telesis web site at [www.alliedtelesis.com](http://www.alliedtelesis.com). Select your country from the list on the web site and then select the appropriate tab.

### Returning Products

Products for return or repair must have Return Materials Authorization (RMA) numbers. A product sent to Allied Telesis without an RMA number will be returned to the sender at the sender's expense.

To obtain an RMA number, contact the Allied Telesis Technical Support group at [www.alliedtelesis.com/support/rma.aspx](http://www.alliedtelesis.com/support/rma.aspx).

### Sales and Corporate Information

You can contact Allied Telesis for sales or corporate information at our web site at [www.alliedtelesis.com](http://www.alliedtelesis.com).

### Warranty

The Converteon products listed here have a Lifetime Warranty (Two Years Fan and PSU):

- AT-CM Media Converter Line Cards
- AT-CV Media Converter Line Cards
- AT-CV1000 One-slot Chassis
- AT-CV1200 Two-slot Chassis
- AT-CV1203 Two-slot Chassis

These Converteon products have a Five Year Warranty:

- AT-CV5M01 Management Card
- AT-CV5M02 Management Card

This Converteon product has a Lifetime Warranty (Five Years Fan and PSU):

- AT-CV5000 Eighteen-slot Chassis

Go to **[www.alliedtelesis.com/warranty](http://www.alliedtelesis.com/warranty)** for the terms and conditions of the warranty and for warranty registration.

## **Management Software Updates**

New releases of the management software for our managed products are available from the following Internet sites:

- Allied Telesis web site: **[www.alliedtelesis.com](http://www.alliedtelesis.com)**
- Allied Telesis FTP server: **<ftp://ftp.alliedtelesis.com>**

If the FTP server prompts you to log on, enter “anonymous” as the user name and your email address as the password.

## Chapter 1

# AT-CV5M02 Management Card

---

The sections in this chapter are:

- “The Converteon Product Line” on page 20
- “AT-CV5M01 and AT-CV5M02 Management Cards” on page 21
- “AT-S99 Management Software” on page 22
- “Console Port” on page 22
- “10/100Base-TX Port” on page 22
- “IP Address Configuration” on page 23
- “Event Log” on page 23
- “Activity Monitor” on page 23
- “Syslog Client” on page 23
- “Network Time Protocol Client” on page 24
- “Manager and Operator Accounts” on page 24
- “Management Access” on page 25
- “Redundant Management Cards” on page 26
- “Access to Your Network” on page 28
- “Configuration Files” on page 29
- “Converteon Chassis” on page 34

## The Converteon Product Line

---

The Converteon product line consists of modular fiber optic media converters that connect Fast Ethernet or Gigabit Ethernet networks across distances of up to forty kilometers. The major components of the product line are:

- ❑ AT-CM Media Converter Line Card Series and the AT-S73 Management Software
- ❑ AT-CV Media Converter Line Card Series
- ❑ AT-CV5M01 Management Card and the AT-S70 Management Software
- ❑ AT-CV5M02 Management Card and the AT-S99 Management Software
- ❑ AT-CV1000, AT-CV1200, AT-CV1203, and AT-CV5000 Chassis

Most of the line cards in the AT-CM Series and the AT-CV Series are two port media converters that transfer Ethernet network traffic between a twisted pair port and a fiber optic port or two fiber optic ports. Most of the line cards have fiber optic ports that have fixed operating distances. However, several of the cards can be customized for specific transmission media or distance requirements because they feature one or two slots for SFP fiber optic transceivers.

The AT-CM and AT-CV Line Cards can be used as unmanaged devices. They are fully operational as soon as they are installed in a Converteon chassis and cabled to your network. They feature low latency to minimize the impact on network performance, and cyclic redundancy check (CRC) detection to prevent the propagation of incomplete or fragmented packets on your network.

For network environments where management oversight is necessary, the Converteon product line includes the AT-CV5M01 and AT-CV5M02 Management Cards. These cards let you view the status of the links of the ports on the media converter line cards, display port statistics, and configure the operating modes of the line cards. These cards also let you configure the additional features on the AT-CM Media Converter Line Cards, such as port filters and OAM-based features.

The AT-CV5M01 and AT-CV5M02 Management Cards have simple-to-use menus and support both local (out-of-band) management through a serial RS-232 Console port and remote (in-band) management from a Telnet client. The AT-CV5M02 Card also supports remote web browser management.

## AT-CV5M01 and AT-CV5M02 Management Cards

---

The AT-CV5M02 Management Card and its predecessor, the AT-CV5M01 Management Card, support many of the same features and management functions. Both cards let you locally or remotely monitor the status of the AT-CM and AT-CV Media Converter Line Cards, configure the operating modes of the line cards, and adjust the port parameters and the OAM-based features on the AT-CM Line Cards. The two management cards share the features listed here:

- ❑ Local (out-of-band) management through an RS-232 Console port.
- ❑ Remote (in-band) management using the card's Telnet server from clients on your network.
- ❑ Easy-to-use menus.
- ❑ Event log for viewing operational messages about the line cards.
- ❑ Activity monitor for viewing the event messages in real-time.
- ❑ Syslog client for storing the event messages on a syslog server on your network.
- ❑ Network Time Protocol (NTP) client for setting the card's date and time from an NTP server on your network or the Internet.
- ❑ Dynamic Host Control Protocol (DHCP) client for assigning the management card's IP address configuration from a BOOTP or DHCP server on your network.

The AT-CV5M02 Management Card has these additional features:

- ❑ Remote (in-band) management using the card's web browser server from web browser clients on your network.
- ❑ Redundant management cards in the AT-CV5000 Chassis.
- ❑ Manual or automatic restoration of previous parameter configurations on local or remote AT-CM Line Cards.

---

**Note**

For instructions on how to use the AT-CV5M01 Management Card and the AT-S70 Management Software, refer to the *AT-S70 Management Software User's Guides*.

---

## AT-S99 Management Software

---

The AT-CV5M02 Management Card uses the AT-S99 Management Software. This program comes pre-installed on the card with default values for all of the operating parameters. New versions of the software can be downloaded onto the card using XMODEM or Trivial File Transfer Protocol (TFTP), as explained in Chapter 11, "Uploading and Downloading Files" on page 271.

## Console Port

---

The management card has an RS-232 Console port for local management of a Converteon chassis with a terminal or a personal computer and a terminal emulator program. The initial management session of a management card has to be a local session. For instructions, refer to "Starting a Local Management Session" on page 58.

## 10/100Base-TX Port

---

To support those management functions that require communications with your network, the management card comes with a standard 10/100Base-TX Ethernet port, which features IEEE 802.3u Auto-Negotiation. Those management functions that rely on this port are listed here:

- Remote Telnet, web browser, or SNMP management
- Sending event messages to a syslog server
- Setting the date and time from a Network Time Protocol server
- Sending SNMP traps to trap receivers
- Uploading or downloading files to a TFTP server
- Pinging remote devices

If the management card will be performing any of these task, be sure to connect the 10/100Base-TX Ethernet port to a network device, such as an Ethernet switch.

## IP Address Configuration

---

To support the functions listed in “10/100Base-TX Port” the management card has to be assigned an IP address configuration consisting of an IP address, a subnet mask, and possibly a default gateway address. The management card can have only one IP address configuration. The configuration can be assigned manually or supplied by a DHCP or BOOTP server on your network. For instructions, refer to “Assigning an IP Address Configuration” on page 80.

## Event Log

---

The management card has a log for recording operational events, like the removal of line cards from a chassis or the loss of links on the ports on the media converter cards. The events are composed of descriptions of the events and the dates and times of when they occurred. If your network encounters a problem, you may be able to more readily identify its cause by reviewing the history of the events in the log. For more information, refer to “Viewing the Event Log” on page 98.

## Activity Monitor

---

The activity monitor displays the same event messages stored in the event log, but in real-time. When you open the activity monitor you can watch for the event messages as they occur. For more information, refer to “Viewing the Activity Monitor” on page 104.

## Syslog Client

---

The management card has a syslog client for sending event messages to a syslog server on your network. For instructions, refer to “Configuring the Syslog Client” on page 105.

## Network Time Protocol Client

---

The management card has a Network Time Protocol (NTP) client for setting its date and time from an NTP server on your network or the Internet. The card adds the date and time to the event messages stored in the event log and to the SNMP traps sent to SNMP trap receivers. Although the date and time can be set manually, the NTP client is the recommended method for setting this information because the card cannot maintain the date and time when it is reset or when the chassis is powered off. For instructions, refer to “Configuring the Network Time Protocol Client” on page 95.

## Manager and Operator Accounts

---

The management software has two accounts. There is a manager account for viewing and configuring the parameter settings and an operator account for just viewing the settings. The manager account has the username “manager” and the default password “friend”. The operator account has the username “operator” and the default password “operator”. The usernames and passwords are case sensitive. For the instructions on changing the passwords, refer to “Configuring Management Security” on page 90.

To change to a different account after you’ve started a management session, you have to log out from your current session and log in again. For example, to configure the parameter settings of the line cards after logging on with the operator account, you have to log out and log in again with the manager account.

---

### **Note**

A management card can support up to one manager session and ten operator sessions at a time.

---

## Management Access

---

There are four ways to manage the Converteon product:

- Local management
- Remote Telnet management
- Remote web browser management
- Remote SNMP management

### **Local Management**

The AT-CV5M02 Management Card has an RS-232 Console port for local (out-of-band) management. This type of management has to be performed at the chassis, hence the term "local." It is accomplished with the management cable that ships with the card and a terminal or a PC with a terminal emulator program. The management card does not need an IP address for local management. Your initial management session of a management card has to be a local session. For instructions, refer to "Starting a Local Management Session" on page 58.

### **Remote Telnet Management**

The management card has a Telnet server for remote management from Telnet clients on your network. Because this type of management is performed over the network, you may find it more convenient than local management, which has to be performed at the wiring closet where the chassis is located. Remote Telnet management, also referred to as in-band management, uses the same menus as local management and supports all of the same management capabilities. The requirements for remote Telnet managed are detailed in "Access to Your Network" on page 28. For further instructions, refer to "Starting a Telnet Management Session" on page 61.

### **Remote Web Browser Management**

The AT-CV5M02 Management Card has web browser windows that you can use as alternatives to the menus for managing the device remotely from a web browser on your workstation on the network. They support nearly all of the same management functions as the menus. The requirements for remote web browser management are detailed in "Access to Your Network" on page 28. To start this type of management session, refer to "Starting a Web Browser Management Session" on page 62.

### **SNMP Management**

The management card can be managed with a Simple Network Management Protocol (SNMP) program, like HP Openview. This type of management requires a familiarity with Management Information Bases (MIBs). To manage the product with SNMP, load and compile the ATCV5000.mib file, found on the Allied Telesis web site, into your SNMP program.

## Redundant Management Cards

---

You can install two AT-CV5M02 Management Cards in the AT-CV5000 Chassis. The second card functions as a backup card should the primary management card fail or have to be removed from the chassis.

When the AT-CV5000 Chassis has two management cards, one of the cards functions as the active card. The other is placed in a standby mode. Your local and remote management sessions have to be performed through the active card. You can discern the states of the cards by examining their RDY LEDs. On the active card this LED will be on; it will be off on the standby card.

The management cards automatically determine their active and standby states when the chassis is powered on. Their states are based on their chassis slot numbers. The management card in the lower numbered slot acts as the active card and the card in the higher numbered slot functions as the standby card. For example, if two management cards are installed in slots 3 and 5 of the chassis, the card in slot 3 becomes the active card and the card in slot 5 is the standby card.

The standby card continuously monitors the state of the active card over the backplane inside the AT-CV5000 Chassis. If the active card fails or is reset or removed from the chassis, the standby card automatically transitions to the active state, usually within twenty seconds.

If a second management card is installed while the chassis is powered on, the new management card is placed in the standby mode even if it occupies a lower numbered slot than the active management card. However, if the chassis is later power cycled or the active card is reset, the management card in the lower numbered slot becomes the active card.

The management software has an option to force the two management cards to change states. You might choose to use this option if the active card is experiencing difficulties and you want to use the standby card to perform your management tasks. The switchover, however, is not permanent. The active and standby states are again determined according to their slot numbers the next time the chassis is power cycled. For instructions, refer to “Activating a Standby AT-CV5M02 Management Card” on page 117.

The requirements and guidelines for redundant AT-CV5M02 Management Cards are:

- This feature is not supported on the AT-CV5M01 Management Card.
- There can be only one redundant management card.
- You can install the active and standby management cards in any of the slots in the AT-CV5000 Chassis.

- ❑ All of your local and remote management sessions have to be conducted through the active management card
- ❑ The RDY LED on the active card will be on. The LED will be off on the standby card.
- ❑ The standby management card automatically transitions to the active state in about 20 seconds if the active card fails or is removed from the chassis or reset.
- ❑ The network operations of the media converter line cards in the chassis are not affected when the management cards change states.
- ❑ The active and standby management cards use the same IP address configuration.
- ❑ To prohibit local or remote management through the standby card, the Console port and the receiver on the 10/100Base-TX port on the card are blocked. However, you can view status messages from the Console port of the standby management card.
- ❑ Even though the 10/100Base-TX port is blocked on the standby card, you should connect it to your network so that those management functions that rely on the card's access to network will be immediately available in the event the card becomes the active card.
- ❑ The two management cards maintain identical master configuration files. For information, refer to "Configuration Files" on page 29.

---

**Note**

When installing a second management card into an existing chassis, you should install it while the chassis is powered on. If the chassis is powered off, you should install it in a higher numbered slot than the existing card. If you install a second management card into a lower numbered slot than the existing card while the chassis is powered off, the master configuration file of the new card, which will become the active card, will overwrite the configuration file on the existing card when you power on the chassis. If the auto-copy settings in the new master configuration file is enabled for the chassis slots, the configuration settings of the line cards may change. For further information, refer to "Configuration Files" on page 29.

---

## Status Messages

You can monitor the communications between the active and standby management cards over the chassis' backplane by connecting a personal computer with a terminal emulator program to the Console port on the standby card. There are Update, Copy, and Heartbeat messages. Update and Copy messages are sent by the active management card when updating the master configuration file on the standby card. Heartbeat messages are generated periodically by the standby card to check the status of the active card.

## Access to Your Network

---

The management card must be able to access your network if it will be performing any of these functions:

- ❑ Supporting remote Telnet, web browser, or SNMP management
- ❑ Sending event messages to a syslog server
- ❑ Setting the date and time from a Network Time Protocol server
- ❑ Sending SNMP traps to trap receivers.
- ❑ Uploading or downloading files to a TFTP server.
- ❑ Pinging remote devices

The requirements for these management functions are listed here:

- ❑ The management card must have an IP address configuration. The configuration can be assigned manually or supplied by a BOOTP or DHCP server on your network. For instructions, refer to “Assigning an IP Address Configuration” on page 80.
- ❑ The card’s 10/100Base-TX port has to be connected to a device on your network, such as an Ethernet switch. The management card communicates with your network through that port.
- ❑ The management card should reside on the same subnet as the remote devices (i.e., Telnet client, syslog server, or SNMP trap receivers) or have access to their subnet through routers or other Layer 3 routing devices.
- ❑ If the management card and the remote devices reside on different subnets, the card’s IP address configuration should include a default gateway address that specifies the IP address of the router interface of the first hop to reaching the remote devices.

## Configuration Files

---

The management card and the media converter line cards store their parameter settings in a series of configuration files. These files enable the cards to retain their settings even when they are removed from the chassis or when the chassis is powered off.

### **AT-CM Line Cards**

The parameter settings of the AT-CM Line Cards are stored in the configuration files in flash memory on the cards. The files contain the operating modes, the port settings, the ingress and egress filters, and the OAM client settings of the line cards.

The cards automatically update their configuration files when you change a parameter setting. There is no command that you have to perform. For example, if you adjust the OAM settings on a line card, the card automatically updates its configuration file so that it retains the new settings even if you immediately afterwards remove the card and install it in another slot or chassis.

### **AT-CV Line Cards**

The configuration files on the AT-CV Line Cards operate the same as the files on the AT-CM Line Cards. The AT-CV Line Cards, however, have only one adjustable parameter, the operating mode. So their configuration files contain just that one parameter. These configuration files are also automatically updated when you change the operating modes of these line cards through a management card.

### **AT-CV5M02 Management Card**

The AT-CV5M02 Management Card has two master configuration files. These files contain the settings of the management card and all of the line cards in the chassis. The management card stores one of the master configuration files in DRAM and automatically updates it by constantly polling the line cards over the backplane in the chassis for their current parameter settings. This file is temporary because it is discarded whenever the chassis is powered off or the management card is reset or removed from the chassis.

The second master configuration file on the AT-CV5M02 Management Card is stored in flash memory and so is retained even when the chassis is powered off. This master configuration file, however, is not updated automatically. Instead, you have to instruct the management card to do it by issuing one of the save commands. When you enter a save command, the management card copies the master configuration file in DRAM to flash memory for permanent storage. For information on the save commands, refer to "Saving Your Configuration Changes" on page 64.

Here are the steps that the management card and the line cards perform when one of their parameter settings is changed.

1. When you enter a new setting on a line card, the management card

sends the change to the designated card over the backplane of the chassis.

2. The line card implements the change and updates its configuration file in flash memory so that it retains the change even if you remove the line card or power off the chassis.
3. The management card automatically updates its master configuration file in DRAM the next time it polls the line card, which it does every few seconds.
4. The next time you issue a save command the management card copies the master configuration file from DRAM to flash memory.

---

**Note**

Unless stated otherwise, all future references to the master configuration file in this guide refer to the permanent file in flash memory on the management card.

---

## Restoring Configurations to AT-CM Line Cards

As just explained, the parameter settings of the AT-CM Line Cards are stored in two locations—the configuration files on the individual line cards and the master configuration file on the management card. The purpose of this redundancy is to make replacing line cards easier. In the event a line card has to be replaced, you can assign the new card the same configuration as its predecessor by restoring the previous configuration from the master configuration file on the management card. This relieves you from having to manually configure new line cards.

A previous configuration of a line card can be restored either automatically or manually. The former is referred to as auto-copy. This is set on a per-slot basis. A line card in a slot where auto-copy is enabled always obtains its parameter settings from the master configuration file on the management card. Thus, a replacement card is automatically assigned the same settings as its predecessor.

You can also restore previous configurations manually. Although a line card in a slot where auto-copy is disabled uses the parameter settings in its individual configuration file, you can manually command the management card to send the previous configuration to the line card.

Here is an overview of the configuration process of an AT-CM Line Card when a card is installed in an active chassis or when a chassis is powered on:

1. The AT-CM Line Card initializes its AT-S73 Management Software, a process that takes approximately one minute to complete. During this process the line card uses the default values for its parameter settings to forward network traffic through its ports.

2. After the line card initializes its software, it queries for a management card over the backplane of the chassis.
3. If the chassis does not have a management card, the line card configures its operating parameters using the settings in its configuration file in flash memory.
4. If the chassis has a management card, the following occurs:
  - a. The management card examines its master configuration file for the auto-copy setting for the line card's slot.
  - b. If auto-copy for the slot is enabled, the management card copies the settings of the line card for that slot from its master configuration file and sends them to the line card over the backplane. When the line card receives the settings, it examines them to determine whether or not they are from the same line card model. If they are, it implements the settings. If they are not, it uses the settings in its own configuration file in flash memory to configure its parameters.
  - c. If auto-copy for the slot is disabled, the line card uses the settings in its own configuration file in flash memory to configure its operating parameters.

The setting for the auto-copy parameter is stored in the master configuration file on the management card. It is not stored in the configuration files on the line cards. Consequently, line cards do not carry this setting with them when they are moved to different slots or chassis.

## **AT-CM Line Cards and Remote Peer Management**

The discussions so far have concerned configuration files on local AT-CM Line Cards that reside in the same chassis as the management card. Most of this information, however, also applies to remote AT-CM Line Cards that are managed through the remote peer management feature. As explained in "Remote Peer Management" on page 46, this feature lets you manage remote line cards through their local AT-CM Line Card counterparts.

When a local line has a remote peer connection to a remote line card, the AT-CV5M02 Management Card stores the remote card's configuration in its master configuration file. You can restore a configuration back to a remote line card just as you can to a local line card. For instance, if you install a new line card in a remote chassis, you can download the last saved configuration to the card from the management card to give the new card the same configuration as the previous card in the remote chassis.

Here are two items of importance to restoring configurations to remote AT-CM Line Cards:

- There is no auto-copy for remote line cards. To restore a previous configuration to a remote line card, you have to do it manually. The

instructions can be found in “Restoring the Last Saved Configuration” on page 181.

- ❑ You have to configure a remote line card for remote peer management before you can remotely restore a previous configuration. For instructions, refer to “Configuring the AT-CM Media Converter Line Cards for the OAM-based Features” on page 74.

## Redundant Management Cards

When the AT-CV5000 Chassis has two management cards, the active card responds to specific events by automatically copying its master configuration file to the standby card. The file is sent over the backplane of the chassis. In this manner, the standby card always has the same master configuration file as the active card. Thus, if the active card is removed from the chassis or fails, the standby card, when it transitions to the active state, will operate with the same parameter settings as its predecessor.

Here are the events that cause an active management card to share its master configuration file with a standby card:

- ❑ When you issue one of the save commands, the active card updates its master configuration file in flash memory and then transmits the changes to the standby card.
- ❑ When the AT-CV5000 Chassis is powered on, the two management cards initialize their AT-S99 Management Software programs and afterwards share their slot numbers to ascertain which is the active card. The card in the lowered numbered slot than transitions to the active state and automatically transmits its master configuration file to the standby card.
- ❑ If you install a second management card in an operating chassis, the active management card waits for the new card to initialize its management software and enter the standby state. Afterwards, it transmits its master configuration file to the new card.

If you install a second management card during a local management session, you’ll be able to watch the process as status messages similar to those in Figure 1 are displayed on your screen.

```
=====
Active Management Card (AT-CV5M02) founded in Slot [ 2 ]
Standby Management Card (AT-CV5M02) founded in Slot [ 5 ]
=====
-> Waiting for Standby to be Ready ... Please wait ..... Not Ready
-> Waiting for Standby to be Ready ... Please wait ..... Not Ready
-> Waiting for Standby to be Ready ... Please wait ..... Not Ready
-> Waiting for Standby to be Ready ... Please wait ..... Ready
<- Copy Configuration to Standby .... Please wait ..078.. Succeeded
```

Figure 1. Updating the Master Configuration File on a Standby Card

(The incrementing number at the bottom of the screen is the ID number of the parameter setting the active card is transmitting to the standby card. All parameter settings have unique ID numbers. The number can be ignored.)

After the management card has sent the entire master configuration file, it displays "Succeeded." To resume managing the chassis, press any key.

The status messages are somewhat different if you install a second management card while viewing the Module Configuration and Status menu or the Remote Module Configuration and Status menu; but their meanings are the same.

## Converteon Chassis

---

Table 1 lists the four chassis in the Converteon product line.

Table 1: Converteon Chassis

<b>Chassis</b>	<b>Number of Slots</b>	<b>Supports Redundant Power Supply</b>	<b>Supports Redundant Management Card</b>
AT-CV1000	1	No	No
AT-CV1200	2	Yes	No
AT-CV1203	2	Yes	No
AT-CV5000	18	Yes	Yes

The AT-CV1200 Chassis and AT-CV1203 Chassis are physically identical. The only difference between them is that the AT-CV1203 Chassis supports the OAM-based dying gasp feature, which is explained in “Dying Gasp Feature” on page 52.

The AT-CM and the AT-CV Media Converter Line Cards can be installed in any of the chassis. The only exception is the double-slot AT-CM70S Line Card, which is not supported in the AT-CV1000 Chassis.

## Chapter 2

# AT-CM and AT-CV Media Converter Line Cards

---

The sections in this chapter are:

- “AT-CM Media Converter Line Cards” on page 36
- “AT-CV Media Converter Line Cards” on page 40
- “Operating Modes” on page 42
- “OAM-based Features” on page 46

## AT-CM Media Converter Line Cards

---

The AT-CM Line Cards are two-port Fast Ethernet and Gigabit Ethernet media converters that transfer network traffic between twisted pair cable and fiber optic cable. Most of the line cards have fiber optic ports with fixed operating distances. However, two of the cards can be customized for specific distances because they have slots for SFP transceivers.

These line cards can be used as unmanaged devices. They have DIP switches for setting the operating modes and LEDs on the front panels for viewing port and card status information. The AT-CM Line Cards support the five operating modes listed here. For background information, refer to “Operating Modes” on page 42.

- Link Test
- MissingLink
- Smart MissingLink
- OAM bypass
- OAM visible

The AT-CM Line Cards have these additional features when used together with the AT-CV5M02 Management Card:

- You can set packet rate limits on the ports of the cards to regulate the amount of forwarded traffic. You might use this feature to prevent traffic bottlenecks on your network.
- You can configure the parameter settings on the twisted pair ports by disabling Auto-Negotiation and setting the speed and duplex mode manually.
- You can enable and disable ports on the line cards to secure them from unauthorized access when the cards are not in use or to isolate portions of a network.
- You can implement the OAM-based features, such as remote peer management and loopback tests. For further information, refer to “OAM-based Features” on page 46.

Table 1 lists the line cards in this series.

Table 1. AT-CM Media Converter Line Cards

Line Card	Type of Port/Slot	Connector	Cable	Speed	Maximum Distance
AT-CM201	Fiber Optic	Dual ST	50/125 or 62.5/125 micron multi-mode	100 Mbps	2 kilometers (1.24 miles)
	Twisted pair	RJ-45	Twisted-pair	10 Mbps or 100 Mbps	100 meters (328 feet)
AT-CM202	Fiber Optic	Dual SC	50/125 or 62.5/125 micron multi-mode	100 Mbps	2 kilometers (1.24 miles)
	Twisted pair	RJ-45	Twisted-pair	10 Mbps or 100 Mbps	100 meters (328 feet)
AT-CM202/1	Fiber Optic	Dual SC	9/125 micron single-mode	100 Mbps	15 kilometers (9.4 miles)
	Twisted pair	RJ-45	Twisted-pair	10 Mbps or 100 Mbps	100 meters (328 feet)
AT-CM202/2	Fiber Optic	Dual SC	9/125 micron single-mode	100 Mbps	40 kilometers (24.8 miles)
	Twisted pair	RJ-45	Twisted-pair	10 Mbps or 100 Mbps	100 meters (328 feet)
AT-CM2KOS	SFP <sup>1</sup>	Varies by SFP transceiver	Varies by SFP transceiver	1.25 Gbps	Varies by SFP transceiver
	Twisted pair	RJ-45	Twisted-pair	10 Mbps, 100 Mbps, or 1000 Mbps	100 meters (328 feet)
AT-CM212A/1 AT-CM212B/1	Fiber Optic	Simplex SC	9/125 micron single-mode	100 Mbps	15 kilometers (9.4 miles)
	Twisted pair	RJ-45	Twisted-pair	100 Mbps	100 meters (328 feet)

Table 1. AT-CM Media Converter Line Cards

Line Card	Type of Port/Slot	Connector	Cable	Speed	Maximum Distance
AT-CM70S	SFP <sup>1</sup>	Varies by SFP transceiver	Varies by SFP transceiver	1.25 Gbps	Varies by SFP transceiver
	Twisted pair	RJ-45	Twisted-pair	10 Mbps or 100 Mbps	100 meters (328 feet)
	T1/E1 <sup>2</sup>	RJ-48	Twisted-pair	n/a	n/a
	RS-232 Console	Mini-DIN	RS-232 Serial	n/a	n/a

1. SFP transceiver sold separately.
2. Four T1/E1 ports.

---

**Note**

The maximum operating distances of the fiber optic ports assume full-duplex operation. The distances are significantly less for half-duplex mode.

---

The fiber optic ports on most of the line cards are standard Ethernet ports that can be connected to other Fast Ethernet or Gigabit Ethernet devices that have compatible fiber optic ports, including other media converters. The operating specifications of the fiber optic ports can be found in the Installation Guides that ship with the line cards.

Two of the line cards, however, have to be used in pairs because their fiber optic ports function as multiplexers, combining two or more data streams onto a single fiber strand to utilize more of the available bandwidth of the fiber optic cable. One of the cards is the AT-CM212 Line Card. It has a simplex SC fiber optic port that combines both the send and receive data streams of the Ethernet traffic onto a single strand of single-mode fiber cable. As shown in Table 1 on page 37, this card has an A version and a B version. The fiber optic port on the version A card has to be connected to the fiber optic port on the version B card.

The AT-CM70S Line Card also has to be used in pairs. It combines the traffic from one 10/100Base-T Ethernet port and four T1/E1 ports onto a single fiber optic port on an SFP transceiver. But unlike the AT-CM212 Line Card, this card does not have two versions.

The AT-CM Line Cards use the AT-S73 Management Software, which comes preinstalled on the line cards with default settings for all of the operating parameters. You do not have direct access to this software. To configure these cards, you have to use the AT-CV5M02 Management Card, which passes your changes to the line cards through the chassis' backplane.

The AT-CM70S Line Card is an exception to this rule because it has an RS-232 port for local management of the T1/E1 ports when the card is installed in a chassis that does not have a management card. For further information, refer to Chapter 7, "Configuring the T1/E1 Ports on the AT-CM70S Media Converter Line Card" on page 191.

## AT-CV Media Converter Line Cards

---

The AT-CV Line Cards are two-port media converters. They have a twisted pair port that connects to a local Ethernet network and a fiber optic port that connects to the remote network over either single-mode or multi-mode fiber optic cable. Most of these cards have fiber optic ports that have fixed operating distances. However, the AT-CV1KSS Line Card has two slots for SFP modules for transferring traffic between a twisted pair port and a fiber optic port, or two fiber optic ports, depending on the modules.

All of the fiber optic ports on these line cards are standard Ethernet ports. They can be connected to other Fast Ethernet or Gigabit Ethernet devices that have compatible fiber optic ports, including other media converters. The operating specifications of the fiber optic ports can be found in the Installation Guides that ship with the line cards.

Although these line cards do not have management software and are primarily intended as unmanaged devices, you can use the AT-CV5M02 Management Card to change their operating modes or to view card and port status. Their port settings are not adjustable. They have DIP switches for setting the cards' operating modes and the MDI/MDI-X setting for the twisted pair ports.

This series supports the following operating modes. For background information, refer to "Operating Modes" on page 42.

- Link Test
- MissingLink
- Smart MissingLink

---

**Note**

These line cards do not support the OAM-based features.

---

Table 2. AT-CV Media Converter Line Cards

Line Card	Type of Port/Slot	Connector	Cable	Speed	Maximum Distance
AT-CV101	Fiber Optic	Dual ST	50/125 or 62.5/125 micron multi-mode	100 Mbps	2 kilometers (1.24 miles)
	Twisted pair	RJ-45	Twisted-pair	100 Mbps	100 meters (328 feet)

Table 2. AT-CV Media Converter Line Cards

Line Card	Type of Port/Slot	Connector	Cable	Speed	Maximum Distance
AT-CV102	Fiber Optic	Dual SC	50/125 or 62.5/125 micron multi-Mode	100 Mbps	2 kilometers (1.24 miles)
	Twisted pair	RJ-45	Twisted-pair	100 Mbps	100 meters (328 feet)
AT-CV102/1	Fiber Optic	Dual SC	9/125 micron single-mode	100 Mbps	40 kilometers (24.8 miles)
	Twisted pair	RJ-45	Twisted-pair	100 Mbps	100 meters (328 feet)
AT-CV102/2	Fiber Optic	Dual SC	9/125 micron single-mode	100 Mbps	15 kilometers (9.4 miles)
	Twisted pair	RJ-45	Twisted-pair	100 Mbps	100 meters (328 feet)
AT-CV1KSS	SFP <sup>1</sup>	Varies by SFP transceiver	Varies by SFP transceiver	1.25 Gbps	Varies by SFP transceiver
	SFP	Varies by SFP transceiver	Varies by SFP transceiver <sup>1</sup>	1.25 Gbps	Varies by SFP transceiver

1. SFP transceiver sold separately.

---

**Note**

The maximum operating distances of the fiber optic ports assume full-duplex operation. The distances are significantly less for fiber optic ports in half-duplex mode.

---

## Operating Modes

---

The AT-CM Line Cards support these operating modes:

- Link Test mode
- MissingLink mode
- Smart MissingLink mode
- OAM visible mode
- OAM bypass mode

The AT-CV Line Cards support these operating modes:

- Link Test mode
- MissingLink mode
- Smart MissingLink mode

The operating modes are used to determine the status of the links on the ports on the line cards, to troubleshoot a link problem, or, in the case of the AT-CM Line Cards, to implement the OAM-based features.

The operating modes are discussed in the following sections:

- “Link Test Mode,” next
- “MissingLink Mode” on page 43
- “Smart MissingLink Mode” on page 44
- “OAM Visible Mode” on page 45
- “OAM Bypass Mode” on page 45

### Link Test Mode

Contrary to its name, the Link Test operating mode is not a diagnostic utility. When a line card is operating in this mode, the states of the links on the ports are reflected on the port LEDs and the management software. A port’s LED will be on and the port’s status in the management software will be Online when the port has established a link to a network device. Conversely, a port’s Link LED will be off and its status in the management software will be Offline when the port has not established a link to a network device.

This operating mode is typically used when the network devices connected to the ports of a line card cannot take advantage of the features of the MissingLink mode, or when you want to use the Link LEDs or the management software to troubleshoot a network problem. This operating mode is also useful after the installation of the line cards to verify whether or not the ports on the cards have established links to their network devices.

## **MissingLink Mode**

The two ports of a media converter line card operating in this mode share their “link” status with each other so that both ports on a line card and, consequently, the network devices connected to the ports, are always aware of a change to the status of the link of one of the ports on the card. When a line card in the MissingLink mode detects the loss of a link on one of its ports, it replicates the loss on the other port by disabling the port's transmitter. This notifies the network device connected to the port of the loss of the link on the other port on the line card. Without the MissingLink mode, a network device connected to a port on a card would be unaware of a loss of a link on the companion port, because its link to the media converter line card would be unaffected. To explain it another way, the MissingLink mode will not allow a port to form a link with its network device unless the companion port on the same line card can also establish a link with its device.

When the link is reestablished on a port, the MissingLink mode automatically reactivates the transmitter on the companion port so that the two network devices can again forward traffic to each other through the two ports of the media converter line card.

The value to this type of fault notification is that some network devices, such as managed Fast Ethernet switches, can respond to the loss of a link on a port by performing a specific action. For example, the network device might send a trap to a network management station, and so alert the network administrator of the problem. Or, if the device is running a spanning tree protocol, it might seek a redundant path to a disconnected node.

Here is an example of how the MissingLink mode works. Assume that the two ports on a media converter line card are connected to two Fast Ethernet switches, one local and the other remote. Switch A, the remote switch, is connected to port A on the line card, while Switch B, the local device, is connected to port B. If the link to Switch A is lost, the line card disables the transmitter on port B to signal Switch B of the loss of the link to Switch A. This notifies Switch B of the problem so it too, along with Switch A, can take remedial action, such as activating a redundant path if it is running a spanning tree protocol, or sending an SNMP trap to a management workstation. Without the MissingLink mode, switch B would be unaware of the problem because it would still have a valid link to the media converter line card.

In the example the initial loss occurred on port A. But the operating mode operates the same when the initial loss of the link is on port B. Here, the transmitter on port A is disabled to notify the node connected to that port of the loss of the link on port B.

The states of the ports on a line card running in this mode operate in tandem. Either both of the ports have a link or neither of the ports. This is reflected on the Link LEDs and in the management software. If both ports can form links with their network devices, their Link LEDs will both be on

and their status in the management software will be Online. If one or both ports cannot establish a link, then the Link LEDs will be off and their status in the management software will be Offline.

This operating mode is useful when the network devices connected to the ports of a line card can react to a loss of a link on a port, such as managed Fast Ethernet switches running SNMP or a spanning tree protocol. Conversely, the MissingLink mode will be of little value if the network devices of a line card cannot react to a lost link. In the latter scenario, the Link Test mode would probably be a better operating mode for a line card during normal network operations.

Furthermore, Allied Telesis does not recommend using the MissingLink mode when troubleshooting a network problem that may have its roots with a link problem. The MissingLink mode will not allow you to use the port's Link LEDs or the management software to diagnose the problem, since neither port will show a link. Rather, the Link Test and the Smart MissingLink modes are more useful when troubleshooting a link problem.

### **Smart MissingLink Mode**

The Smart MissingLink mode is nearly identical to the MissingLink mode. It, too, enables the two ports on a media converter line card to share the link status of their connections. This mode is different in that it does not completely shut off the transmitter of a port on a line card when the companion port loses its link. Rather, this operating mode pulses the port's transmitter and flashes the port's Link LED once a second to signal that the port can still establish a link to its network device and that the loss of the link originated on the companion port on the line card.

The advantage of this operating mode over the MissingLink mode is that you can use the Link LEDs on a line card to troubleshoot a link failure with the ports. As an example, assume that the fiber optic port on a media converter line card operating in the Smart MissingLink operating mode lost its link to its network device. The mode would respond by pulsing the transmitter on the twisted pair port and flashing the port's Link LED about once a second to signal that the failure originated on the fiber optic port. When the connection is reestablished on the fiber optic port, the twisted pair port would automatically resume normal operations to permit the two ports to forward traffic again.

The operating mode functions the same if the failure starts on the twisted pair port. Here, the mode pulses the transmitter on the fiber optic port.

As with the other operating modes, this mode does not interfere with the flow of network traffic through the ports of a line card during normal network operations of a media converter line card. However, Allied Telesis recommends limiting its use to diagnosing link failures, particularly if the network devices connected to the ports are managed devices. The pulsing of the transmitter on a port and the constantly changing status of a link could prove problematic for some managed devices. For example, the device might send a constant stream of SNMP traps or, if the device is

running a spanning tree protocol, the protocol might become confused as the status of the device's link to the media converter constantly changes.

## **OAM Visible Mode**

OAM is a set of tools and utilities for remotely monitoring, testing, and troubleshooting a network. It provides network operators the ability to monitor the condition of the network and determine the location of the failing links or fault conditions. For background information, refer to the IEEE 802.3ah standard.

AT-CM Line Cards set to the OAM visible operating mode support OAM on port A, the fiber optic port. They can initiate and participate in the OAM discovery process by sending and processing OAM control packets, referred to as OAMPDUs, on the fiber optic ports.

Line cards set to this operating support several additional features, some of which are part of the IEEE 802.3ah standard for OAM while others are specific to the Converteon product line. These features are:

- OAM loopback test to test the quality of the fiber optic cable that links two AT-CM Line Cards.
- Dying gasp to notify you when a remote AT-CV1203 Chassis loses power.
- Remote peer management for monitoring and configuring remote AT-CM Line Cards through their local line card counterparts in a managed chassis.
- Downloads of new versions of the AT-S73 Management Software to remote AT-CM Line Cards.
- OAM variable retrievals to examine the values of MIB objects on OAM-compliant devices.

For background information on these features, refer to "OAM-based Features" on page 46.

## **OAM Bypass Mode**

Cards in this OAM operating mode ignore OAMPDUs and so do not support any of the OAM features. Instead, they forward OAMPDUs as normal network traffic.

## **Setting the Operating Mode**

There are two ways to set the operating modes on the AT-CM and AT-CV Media Converter Line Cards. You can use the DIP switches on the line cards or you can use the AT-CV5M02 Management Card. If you use the management card, the DIP switches are deactivated, and reactivating them requires the management card. For instructions on how to set the operating modes of the line cards, refer to "Setting the Operating Mode" on page 145.

## OAM-based Features

---

The AT-CM Line Cards support five OAM-based features on their fiber optic ports. Some of the features are part of the IEEE 802.3ah standard and others are specific to this product. The features are:

- ❑ “Remote Peer Management,” next
- ❑ “Remote Updates of the AT-S73 Management Software” on page 50
- ❑ “OAM Loopback Tests” on page 51
- ❑ “Dying Gasp Feature” on page 52
- ❑ “OAM Variable Requests” on page 55

### **Remote Peer Management**

This feature, also known as peer-to-peer management, makes it easier to manage your remote line cards because you can configure them through their local counterparts in a managed chassis. This saves you from having to travel to the remote sites when you need to configure the cards, or having to install management cards in all of the remote chassis.

To manage a remote card, you start a local or remote management session on the chassis that has the management card. You then redirect the session to the remote card by selecting its local counterpart. The remote management sessions are conducted over the fiber optic cables that link the local and remote line cards. The sessions do not interfere with the network operations of the line cards.

This feature is illustrated in Figure 1 on page 47. Residing at a central location is the AT-CV5000 Chassis with the AT-CV5M02 Management Card. To manage the remote card, you select its local counterpart in slot 11. This establishes a management connection to the remote line card over the fiber optic cable that links the line cards.

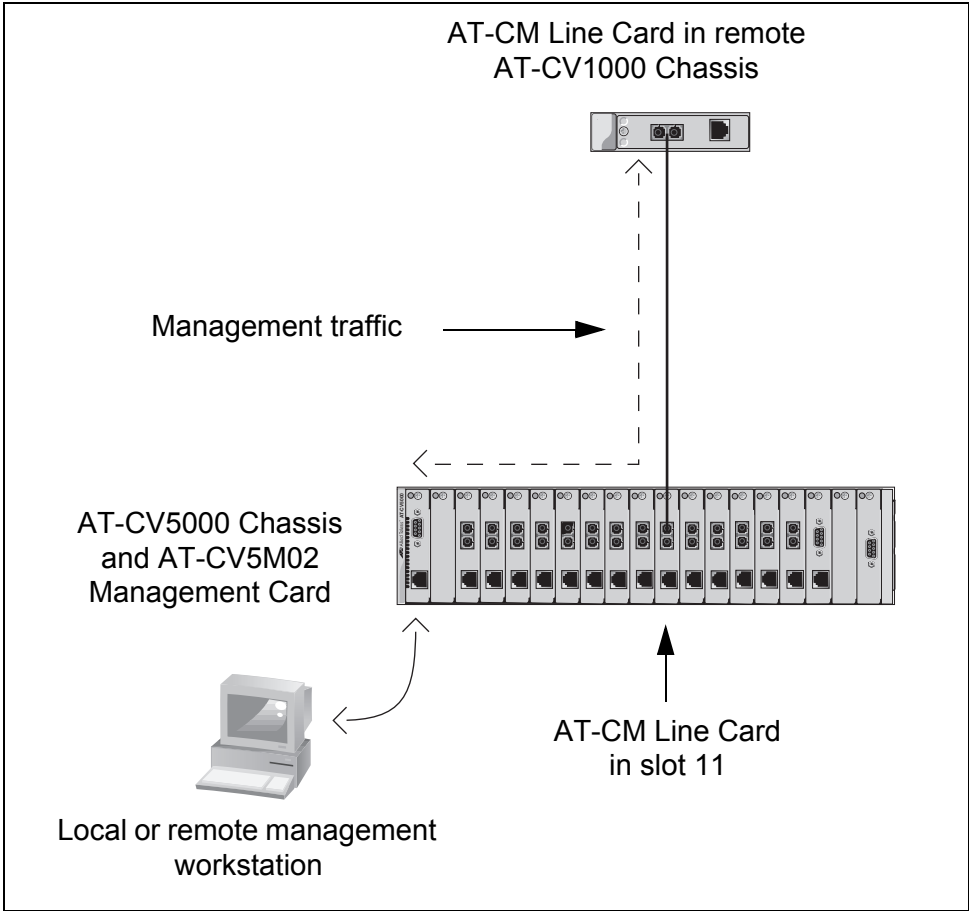


Figure 1. Remote Peer Management - Example 1

This feature is supported on all of the Converteon chassis. In the next example the chassis with the management card is the AT-CV1203 Chassis.

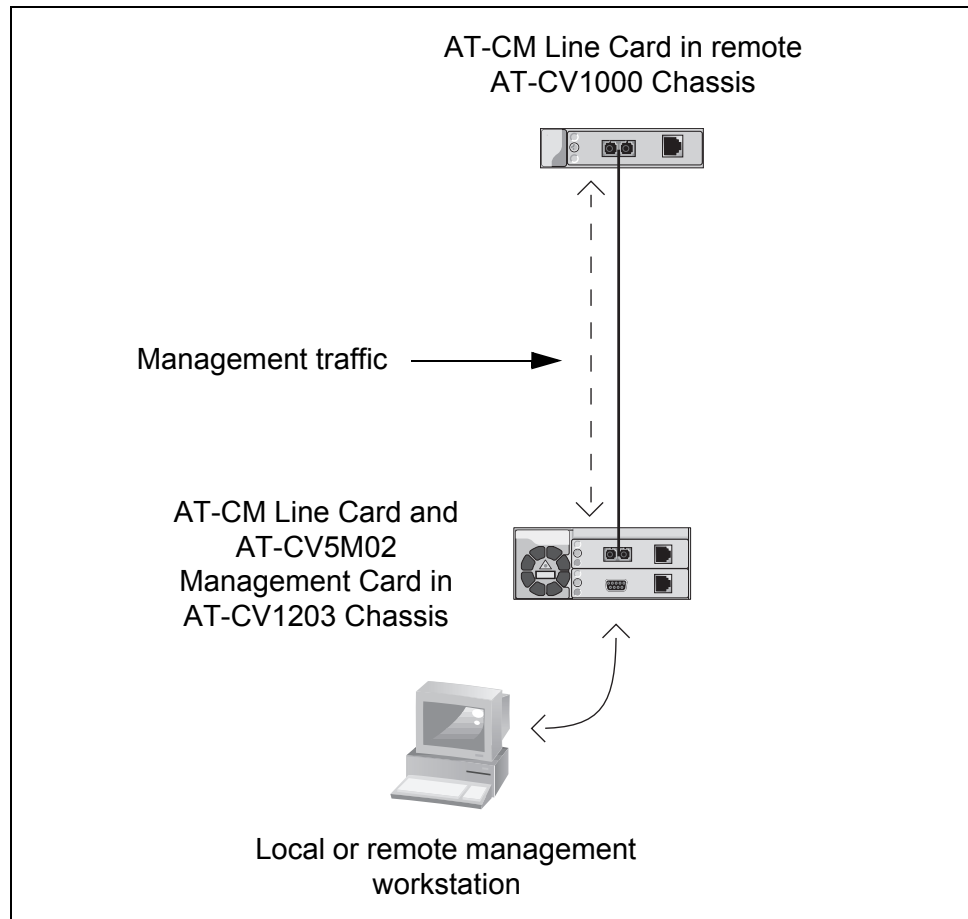


Figure 2. Remote Peer Management - Example 2

You can manage the remote line cards from the menus or the web browser windows. From the menus you use the Remote Module Status and Configuration menu. Selected from the Main Menu, this menu lists all of the media converter line cards in the managed chassis and identifies those remote line cards that have remote peer connections to their local counterparts.

An example of the menu is shown in Figure 3. The columns under LOCAL MODULE lists the line cards in the local chassis. The columns under REMOTE MODULES lists those remote AT-CM Line Cards that have remote peer connections to their local counterparts.

To manage a remote AT-CM Line Card, you select it from the menu. This redirects the session to the remote line card. For more information on this menu, refer to “Configuring Remote AT-CM Line Cards from the Menus” on page 174.

Remote Module Status and Configuration  
Conversion

LOCAL MODULE					REMOTE MODULE					FIBER PORT				COPPER PORT							
Mod_Name	CardTypeVer	ST	OV	IPC VER	Mod_Name	CardTypeVer	VER	OV	SP	FC	IngRL	EgrRL	OAM	ST	SP	FC	IngRL	EgrRL	AN		
1	AT-CV5M02	*	A	502	V300																
2	Reg11	AT-CM202-v2	*	Y	*00	V300	Reg11_r	AT-CM202-v2	V300	Y	100	Y	0	0	***	o	100	Y	0	0	Y
3	Reg20	AT-CM202-v2	*	Y	*00	V300	Reg20_r	AT-CM202-v2	V300	Y	100	Y	0	0	***	o	100	Y	0	0	Y
4	Reg21	AT-CM202-v2	*	Y	*00	V300	Reg21_r	AT-CM202-v2	V300	Y	100	Y	0	0	***	o	100	Y	0	0	Y
5	Area2a	AT-CM202-v2	*	Y	*00	V300	Area2a	AT-CM202-v2	V300	Y	100	Y	0	0	***	o	100	Y	0	0	Y
6	Area2b	AT-CM202-v2	*	Y	*00	V300	area2b	AT-CM202-v2	V300	Y	100	Y	0	0	***	o	100	Y	0	0	Y
7	Reg12	AT-CM202-v2	*	Y	*00	V300	Reg12_r	AT-CM202-v2	V300	Y	100	Y	0	0	***	o	100	Y	0	0	Y
8	AT-CV102	-	-	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---
9	AT-CV102	-	-	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---
10	AT-CV102	-	-	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---
11	AT-CV102	-	-	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---
12	AT-CV102	-	-	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

Figure 3. Remote Module Status and Configuration Menu

The corresponding window in the web browser windows has the same name as its menus peer and is used in much the same way. To manage a remote AT-CM Line Card from the window, you select the card's local counterpart. This redirects the session to the remote line card. For more information on this window, refer to "Configuring Remote AT-CM Line Cards from the Web Browser Windows" on page 182.

Remote Module Status & Configuration

Local Module	Card Type	Version	Link (A)
1 AT-CV5M02	No Support	No Support	No Support
2 AT-CM202	AT-CM202	V3.0.0	Online
3 AT-CM202	AT-CM202	V3.0.0	Online
4 AT-CM202	AT-CM202	V3.0.0	Online
5 AT-CM202	AT-CM202	V3.0.0	Online

Figure 4. Remote Module Status and Configuration Window

For instructions on how to use this feature, refer to Chapter 6, "Configuring AT-CM Line Cards with Remote Peer Management" on page 173.

## Remote Updates of the AT-S73 Management Software

Allied Telesis may periodically release new versions of the AT-S73 Management Software for the AT-CM Media Converter Line Cards. New software can be downloaded to remote media converter line cards through the OAM-based remote peer management feature. This saves you from having to visit the remote sites where the line cards are located when you want to update their management software.

Figure 5 illustrates this feature. The remote AT-CM Line Card receives a new version of the AT-S73 Management Software over the fiber optic link on Port A from its line card counterpart in the managed chassis, in this case the AT-CV5000 Chassis. The file is downloaded through the management card from a local management session using XMODEM or from a remote TFTP server. For instructions, refer to Chapter 11, "Uploading and Downloading Files" on page 271.

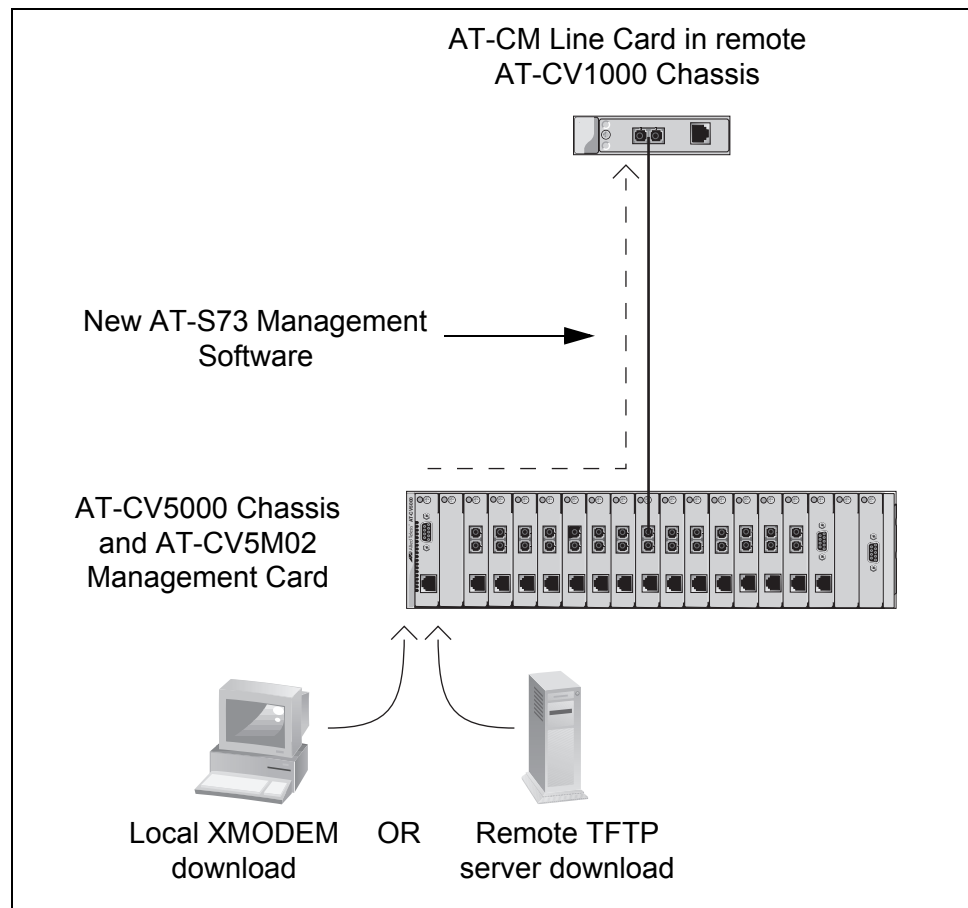


Figure 5. Downloading New AT-S73 Management Software to Remote AT-CM Line Cards

## OAM Loopback Tests

OAM loopback tests are used to test the quality of the fiber optic connection that serves as the link between two AT-CM Line Cards or between an AT-CM Line Card and another OAM-compliant device. Test packets are exchanged by the line cards over the fiber optic link on Port A. The test packets are generated by the local line card in the Converteon chassis that has the AT-CV5M02 Management Card. The remote line card returns the test packets over the same fiber optic connection. As the local line card receives its original test packets, it checks for lost packets and for packets with errors, and displays the results in statistics counters.

Figure 6 illustrates a loopback test between two AT-CM Line Cards. The test packets are generated by the line card in the AT-CV5000 Chassis at the central office and are returned by the line card in the AT-CV1000 Chassis at a remote site.

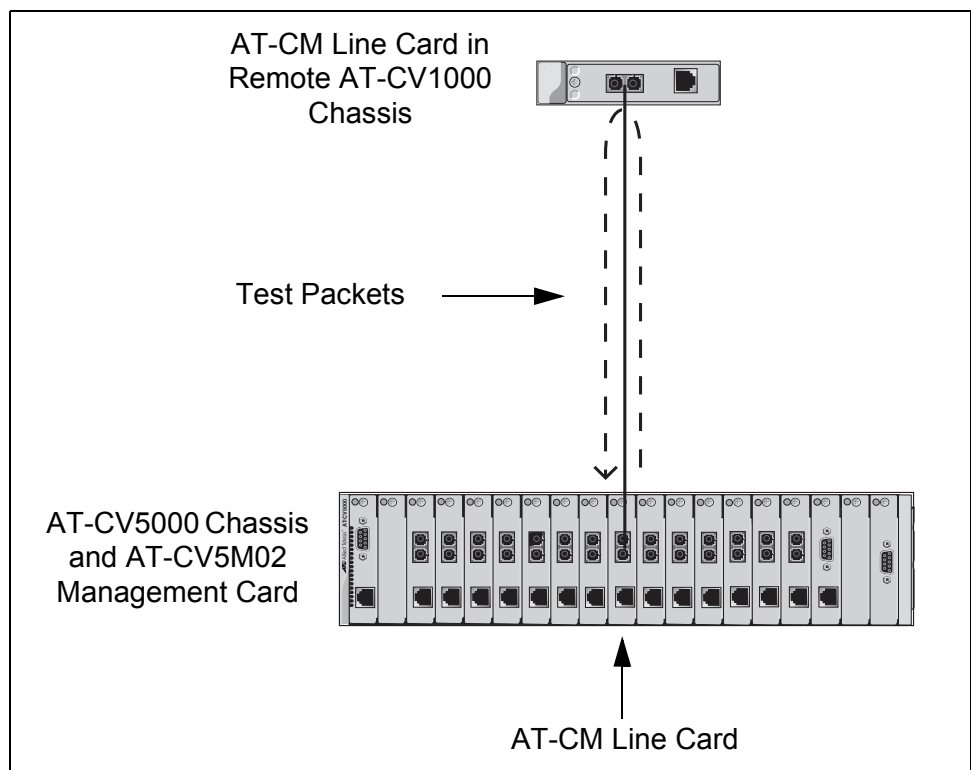


Figure 6. Loopback Test

For instructions, refer to “Performing an OAM Loopback Test” on page 209.



### Caution

The loopback test is disruptive to network operations. Local and remote line cards do not forward network traffic during the test. Some network traffic may be lost.

## Dying Gasp Feature

Dying gasp is a signal that AT-CM Line Cards in the AT-CV1203 Chassis transmit if the chassis has a power failure. This feature can make it easier to identify power supply or power source problems at remote sites.

If a remote AT-CV1203 Chassis loses power, the AT-CM Line Card in the chassis transmits the dying gasp signal from Port A over its fiber optic link to its line card counterpart in the AT-CV5000 Chassis at the central office. The local card sends the signal over the chassis' backplane to the management card which enters the event in its event log and sends an SNMP trap to alert you to the problem. Figure 7 illustrates the sequence of events of this feature.

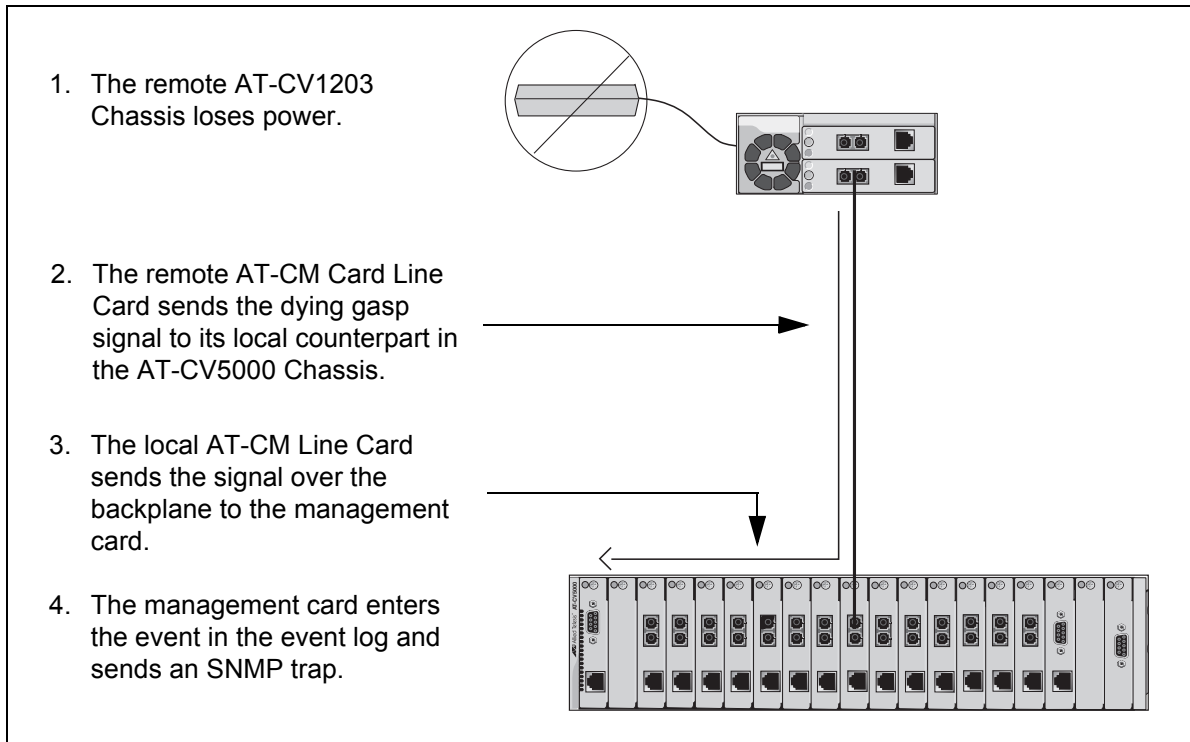


Figure 7. Dying Gasp Feature

If the remote AT-CV1203 Chassis has two AT-CM Line Cards, both cards transmit the signal from their fiber optic ports.

If the AT-CV1203 Chassis has both a primary power supply and a redundant power supply, the dying gasp feature can notify you if one power supply loses power. It accomplishes this by sending the “1st RPS Failure” signal. This signal indicates that the remote chassis has lost power on one power supply, but continues to operate with the remaining power supply.

To support this feature, there has to be an AT-CV5M02 Management Card installed in the remote chassis because only a management card can detect the loss of a single power supply when a chassis has two power supplies. This feature is illustrated in Figure 8.

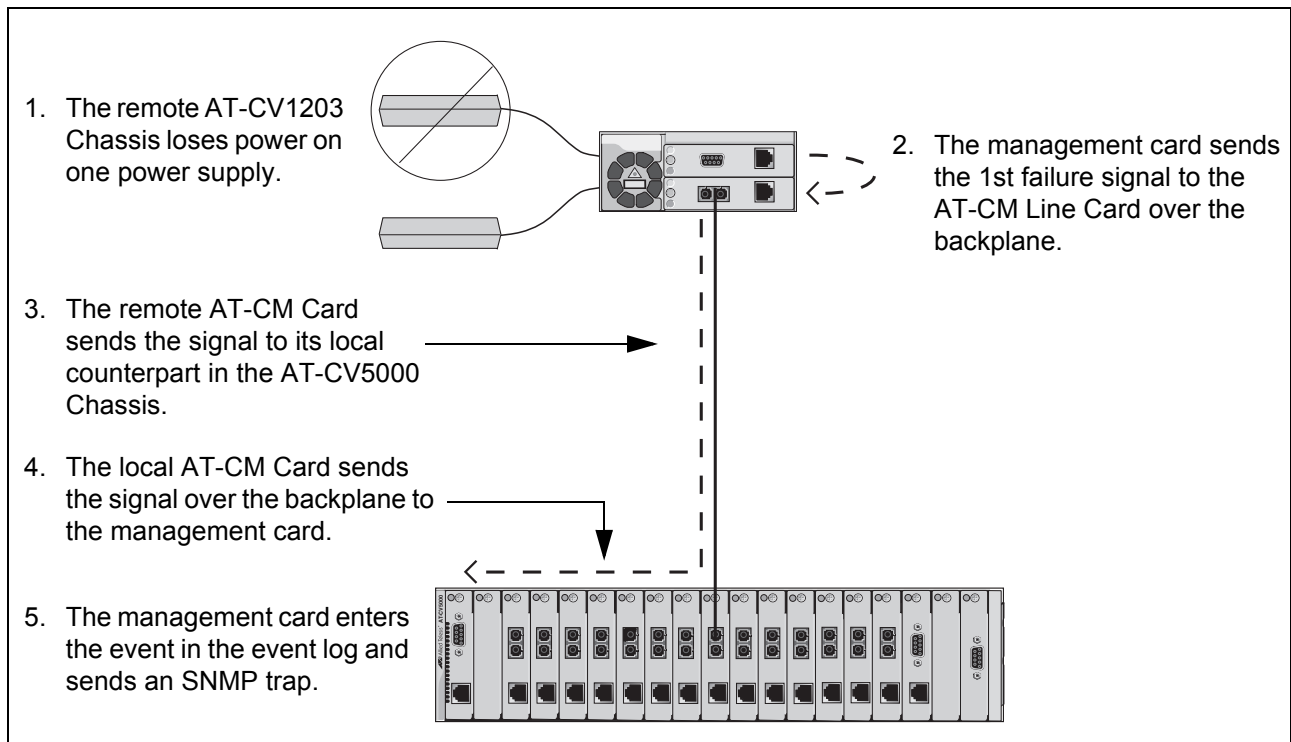


Figure 8. 1st Failure Signal

**Note**

All of the AT-CM Line Cards support the 1st failure signal, except for the double-slot AT-CM70S Line Card. Since that line card occupies both slots in the AT-CV1203 Chassis, there isn't an available slot in the chassis for a management card.

The requirements of the dying gasp feature are:

- ❑ Only AT-CM Line Cards in the AT-CV1203 Chassis can send the signal and only AT-CM Line Cards in the AT-CV5000 Chassis can recognize the signal and pass it to the management card in the chassis. This feature is not supported on the AT-CV Line Cards, the AT-CV1000 Chassis, or the AT-CV1200 Chassis.
- ❑ This feature requires the newest versions of the AT-CM Line Cards listed in Table 3. You have to use a management card to determine the version levels of the line cards because the version levels are not included on the faceplates on the cards. When viewed with the management software, the model names of the new line cards include extensions that contain the version levels, like AT-CM201-v2.

Table 3. Versions of the AT-CM Line Cards that Support Dying Gasp

Media Converter Line Card	Hardware Version
AT-CM201	Version 2
AT-CM202	Version 2
AT-CM202/1	Version 2
AT-CM202/2	Version 2
AT-CM212A/1	Version 2
AT-CM212B/1	Version 2
AT-CM70S	Version 2
AT-CM2KOS	Version 3

- ❑ Refer to Table 4 for the required version numbers of the management software.

Table 4. Versions of the Management Software that Support Dying Gasp

Management and Media Converter Line Cards	Management Software Versions
AT-CV5M01 Management Card	Version 2.0.2 or later of the AT-S70 Management Software.
AT-CV5M02 Management Card	Version 3.0.0 or later of the AT-S99 Management Software
AT-CM Line Cards	Version 2.0.2 or later of the AT-S73 Line Card Management Software.

- ❑ If you install a management card in the remote AT-CV1203 Chassis so that the chassis can send the 1st failure signal, you do not have to configure the card, nor do you have to connect its 10/100Base-TX port to the network. The card simply has to be present in the AT-CV1203 Chassis.

## OAM Variable Requests

This feature is part of the IEEE 802.3ah Ethernet OAM standard. It allows you to view the performance and error statistics that are stored in the Management Information Bases (MIBs) on remote OAM devices. To use the feature, you specify the branch and leaf of the object identifier (OID) of the MIB object you want to view. These are the last two parts of an OID. The prefix of the OID is predefined in the OAM clients on the line cards and is not adjustable. This feature has the following restrictions:

- ❑ Variable requests use the following MIB tree prefix:  
iso(1) member-body(2) us(840) ieee802dot3(10006) csmacdmgt(30)
- ❑ Variable requests are transmitted from Port A, the fiber optic port, on the line cards. This feature is not supported on Port B, the twisted pair port.
- ❑ You can use OAM variable requests to view, but not change MIB values.
- ❑ This feature cannot be used to view the MIB objects in the private Allied Telesis MIB.

---

### Note

The AT-CM Line Cards do not support any of the MIB objects in the portion of the MIB tree that variable requests can access. So although the line cards can send variable requests to query other OAM-compatible devices for MIB values, they do not respond to variable requests.

---

For instructions, refer to “Viewing MIB Variables with OAM Variable Requests” on page 225.

### OAM Client Settings

Table 5 lists the parameter settings for the OAM clients on the AT-CM Line Cards for the OAM-based features. The instructions on how to configure the clients can be found in “Configuring the AT-CM Media Converter Line Cards for the OAM-based Features” on page 74 and “Configuring an OAM Client” on page 204.

Table 5. OAM Parameter Settings for the OAM-based Features

OAM Parameter	Local AT-CM Line Card in a Managed Chassis	Remote AT-CM Line Card or Other OAM-Compatible Device
Line Card Operating Mode	OAM Visible	OAM Visible
OAM Admin State	Enabled	Enabled
OAM Mode	Active	Active or Passive
<p>OAM Loopback Support</p> <p>This parameter controls whether or not the OAM client on a line card will participate in OAM loopback tests by returning test packets received on port A from another OAM client. This parameter only applies to OAM clients that return the test packets and has no affect on OAM clients that generate the test packets.</p>	<p>This parameter can be set to Yes or No on the local AT-CM Line Cards because these line cards generate the test packets.</p>	<p>The possible settings for this parameter on remote line cards are:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Yes - The remote line cards can participate in loopback tests by returning test packets.</li> <li><input type="checkbox"/> No - The remote line cards cannot participate in loopback tests</li> </ul>
<p>OAM Variable Requests Support</p> <p>This parameter controls whether or not the OAM client on a line card will respond to variable retrieval requests from other OAM clients. A variable retrieval request is a query of an OAM client by another OAM client for the current value of a MIB object. This parameter applies only to OAM clients that are queried, and not to OAM clients that send the variable requests.</p>	<p>This parameter can be set to Yes or No on the local AT-CM Line Cards because these line cards generate the variable requests.</p>	<p>The possible settings for remote OAM-compatible devices are</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Yes - The OAM client responds to variable retrieval requests. This is the default setting.</li> <li><input type="checkbox"/> No - The OAM client does not respond to variable retrieval requests.</li> </ul>

## Chapter 3

# Starting a Management Session

---

This chapter has the following sections:

- “Starting a Local Management Session” on page 58
- “Starting a Telnet Management Session” on page 61
- “Starting a Web Browser Management Session” on page 62
- “Saving Your Configuration Changes” on page 64
- “What to Configure First on the AT-CV5M02 Management Card” on page 69
- “Configuring the AT-CM Media Converter Line Cards for the OAM-based Features” on page 74

## Starting a Local Management Session

---

This procedure explains how to start a local, out-of-band management session using the RS-232 Console port on the AT-CV5M02 Management Card. The management card does not need an IP address for local management. Your initial management session has to be a local session.

The Console port on the management card requires a DEC VT100 or ANSI terminal, or an equivalent terminal emulator program. The large windows in the management software require a terminal or terminal emulator program that can support up to 125 characters per line.

To start a local management session:

1. Connect one end of the management cable included with the management card to the Console port on the management card, as shown in Figure 9. If the chassis has two AT-CV5M02 Management Cards, start the session on the active management card, identified by its green RDY LED.

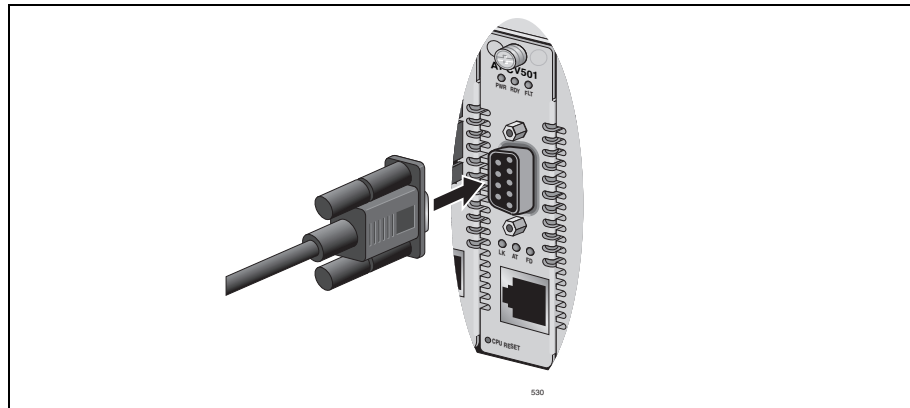


Figure 9. Connecting the Management Cable to the Management Card's Console Port

2. Connect the other end of the cable to an RS-232 port on a terminal or a PC with a terminal emulator program.
3. Configure the terminal or the terminal emulation program as follows:
  - Bits per second: 115200 default (range 2400 to 115200 bps)
  - Data bits: 8
  - Parity: None
  - Stop bits: 1
  - Flow control: None

4. When prompted, enter the username and password of the manager or operator account on the management card. The manager account has the username "manager" and the default password "friend." The operator account has the username "operator" and the default password of "operator." Usernames and passwords are case sensitive. For further information, refer to "Manager and Operator Accounts" on page 24. For instructions on how to change a password, refer to "Configuring Management Security" on page 90.

After you log on, the Main Menu in Figure 10 is displayed on your screen.

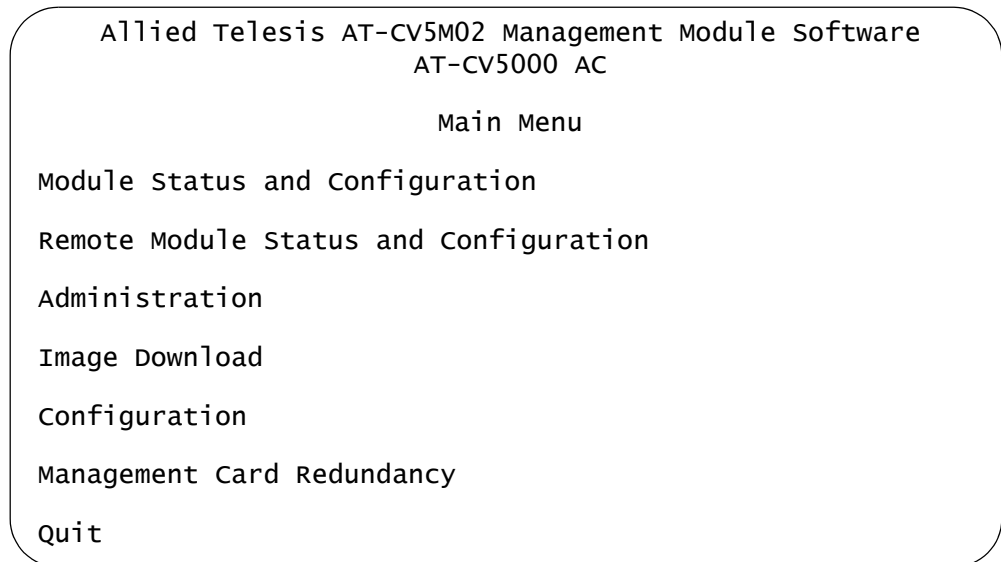


Figure 10. Main Menu

---

**Note**

The Management Card Redundancy option is only supported on the AT-CV5M02 Management Card in the AT-CV5000 Chassis. This feature is not supported on the AT-CV1200 or AT-CV1203 Chassis.

---

---

**Note**

Always remember to select Quit from the Main Menu when you finish managing a chassis. If you close your terminal emulator program without logging out, the management session remains active and all further management is blocked until the console timer times out.

---

The instructions in Table 6 explain how to move through the menus and select menu options.

Table 6. Menu Selection Options

When directed to	You must
Select an option	Highlight the option by pressing the Up ( ↑ ) or Down ( ↓ ) arrow key and then pressing Return.  or  Type the first character of the option at the prompt and press Return. If two or more options have matching initial characters, type the initial characters until the option you want is highlighted and press Return.
Enter information (for example, the IP address of a management card)	Type the information and press Return.
Return to the previous screen	Press Esc or select the “Return to...” option at the bottom of the menu.

Activated options are preceded with the > symbol in a menu. In the following example, the first option is activated:

```
> Enable this port
  Disable this port
```

When you select a field that accepts a value, the -> symbol is displayed. For example:

```
System name:  ->
```

When you see the -> symbol, enter a new value for the parameter. After entering a value, press Return. Unless stated otherwise, all changes are immediately implemented by the AT-CV5M02 Management Card and the AT-CM Line Cards.

## Starting a Telnet Management Session

---

---

### Note

The requirements for remote Telnet management are listed in “Access to Your Network” on page 28.

---

The large windows in the management software require a Telnet client that can support up to 125 characters per line.

To start a remote Telnet management session on a management card:

1. Specify the IP address of the management card in the Telnet client at your workstation. If the chassis has two management cards, enter the IP address of the active card.
2. When prompted, enter the username and password of the manager or operator account of the management card. The manager account has the username “manager” and the default password “friend.” The operator account has the username “operator” and the default password “operator.” Usernames and passwords are case sensitive.

After you log on, the Main Menu in Figure 10 on page 59 is displayed. For instructions on how to use the menus, refer to Table 6 on page 60. You have the same management capabilities from a Telnet management session as you do from a local management session.

3. To end a management session, select **Quit** from the Main Menu. You should always exit from a management session when you finish managing a chassis. This is to prevent blocking future management sessions and to protect the management card and line cards from unauthorized changes,

---

### Note

If you close your Telnet client without logging out, the management session remains active and all further management is blocked until the console timer times out.

---

## Starting a Web Browser Management Session

---

---

### Note

The requirements for remote web browser management are listed in “Access to Your Network” on page 28.

---

To start a remote web browser management session:

1. Enter the IP address of the management card in the URL field of your web browser, as shown in Figure 11. If the chassis has two management cards, enter the IP address of the active card.

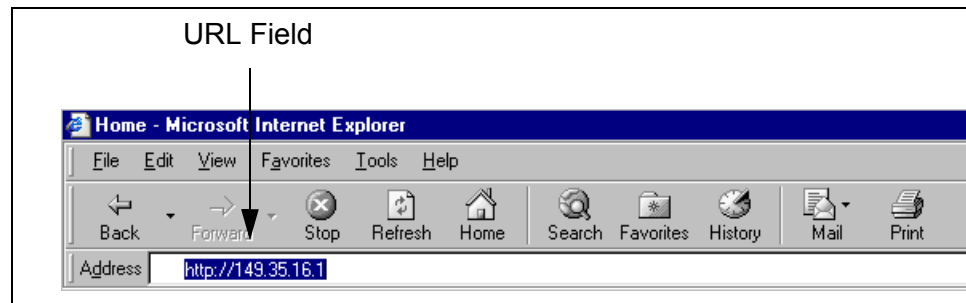


Figure 11. URL Field in a Web Browser

2. When prompted, enter the username and password of the manager or operator account on the management card. For the manager account the username is “manager” and the default password is “friend.” For the operator account the username is “operator” and the default password is “operator.” Usernames and passwords are case sensitive.

After you log on, the Chassis View in Figure 12 is displayed. For a description of the view, refer to “Displaying the Status of the Line Cards” on page 128.

3. To end a management session, click **Log-Out** in the menu bar. You should always exit from a management session when you finish managing a chassis. This is to prevent blocking future management sessions and to protect the management card and line cards from unauthorized changes,

---

### Note

If you close your web browser application without logging out, the management session remains active and all further management is blocked until the console timer times out.

---

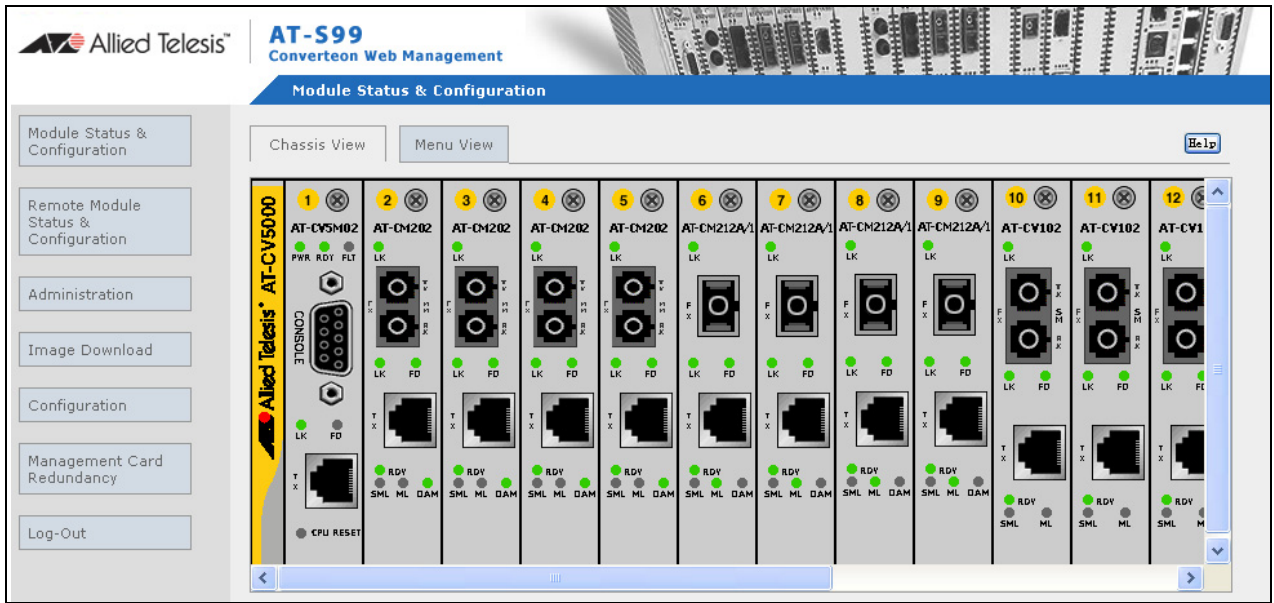


Figure 12. Chassis View

## Saving Your Configuration Changes

---

This section explains the save commands in the AT-S99 Management Software on the AT-CV5M02 Management Card. These commands are used to update the master configuration file in flash memory on the management card with your changes to the parameter settings to the cards. When you issue one of these commands, the management card copies all or part of its master configuration file in DRAM to flash memory for permanent storage. For background information, refer to “Configuration Files” on page 29.

There are many save commands, but they all do the same thing, which is copy the master configuration file from DRAM to flash. Where they differ is in the amount of information that’s copied. This section starts by showing the locations of the commands in the menus and the web browser windows. It then explains the functions of the commands.

Most of the save commands in the menus are located in the Configuration Menu, shown in Figure 13. This menu, displayed by selecting the Configuration option from the Main Menu, has three save commands.

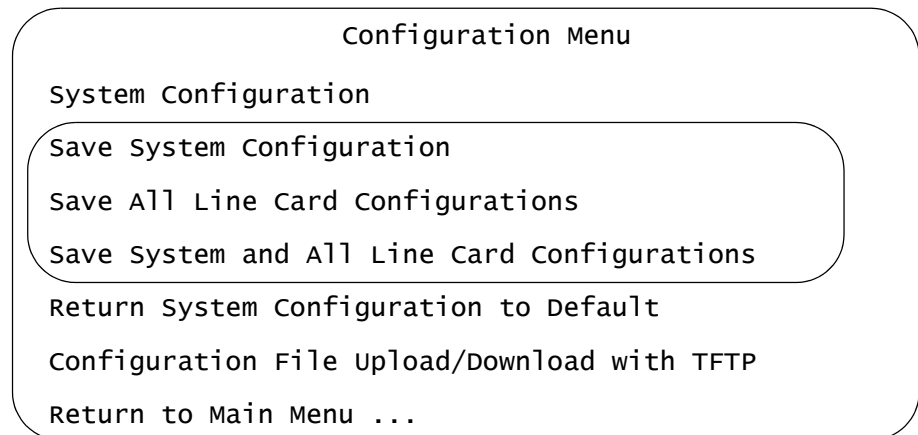


Figure 13. Save Commands in the Configuration Menu

The same commands in the web browser windows are found in the Files tab of the Configuration window, shown Figure 14.

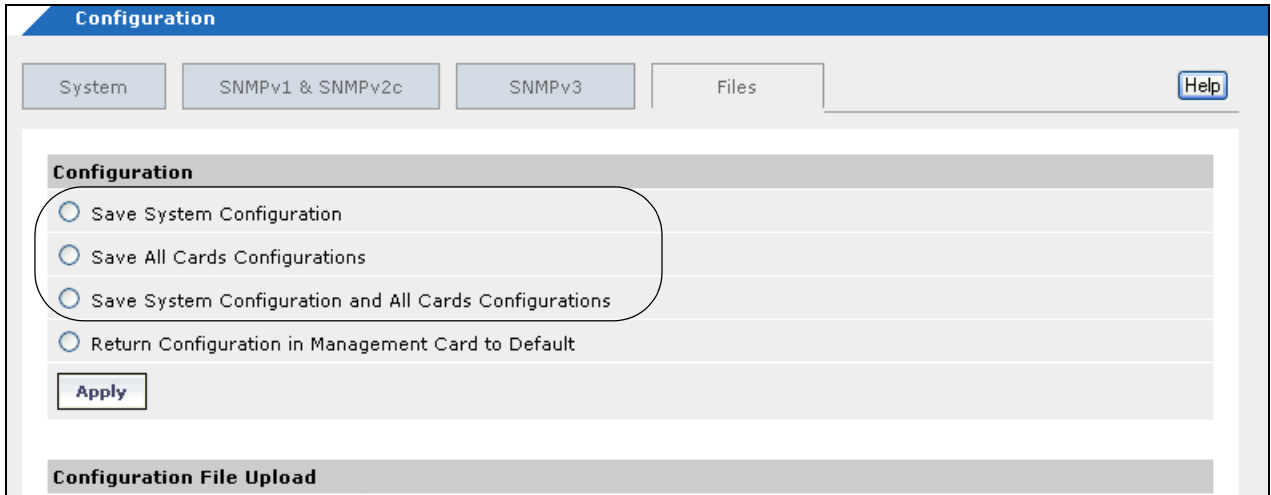


Figure 14. Save Commands in the Files Tab

There are also save commands in the Line Card Configuration menus of the individual local and remote line cards. These menus are part of a series of menus that are used to configure the parameters on the line cards. The example in Figure 16 is from a local line card.

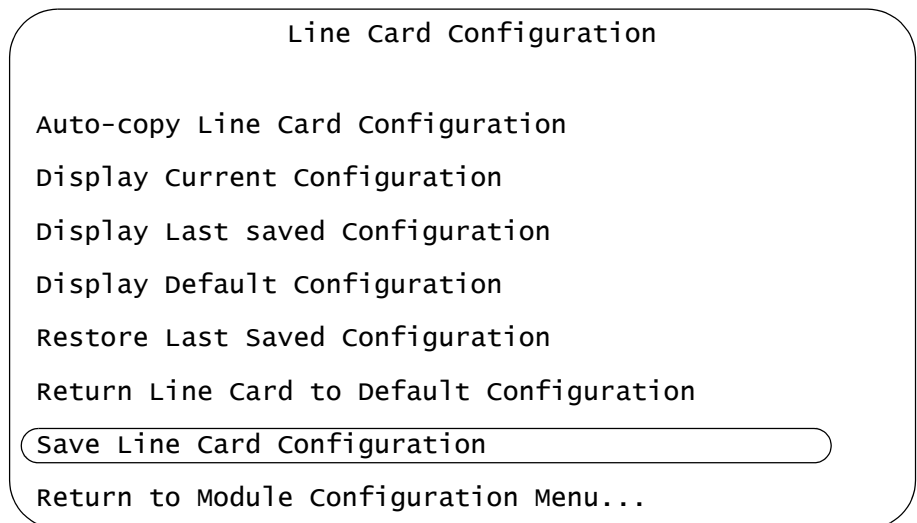


Figure 15. Save Command in the Line Card Configuration Menu for a Local AT-CM Line Card

The web browser windows also have this command for local and remote line cards. Figure 16 shows the location of the command in the web browser windows for a local line card.

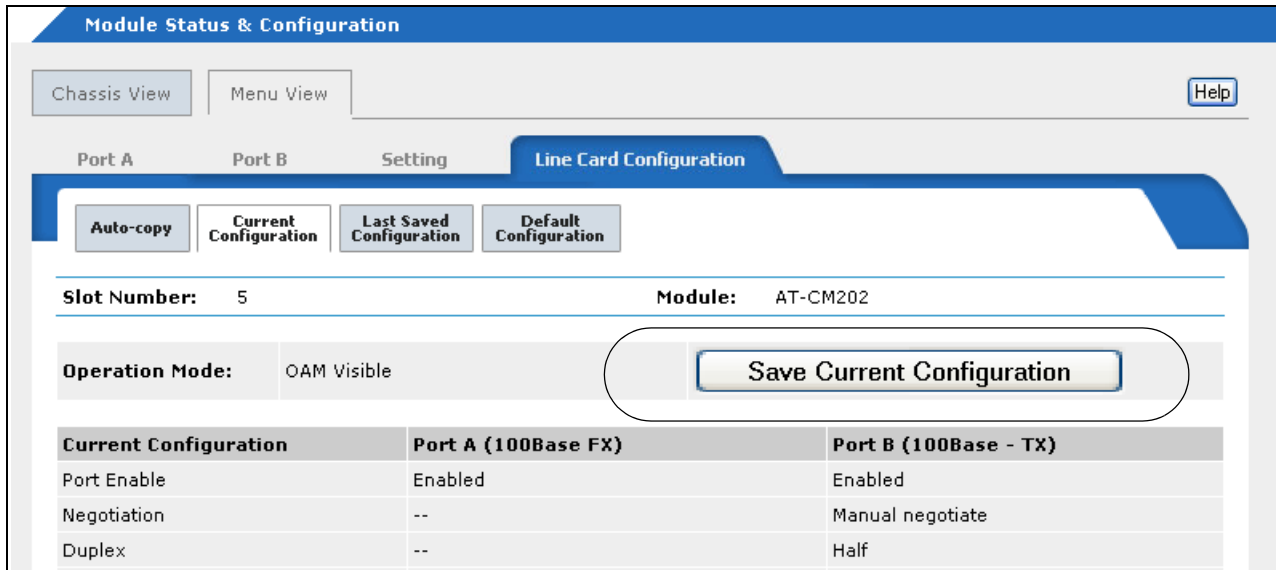


Figure 16. Save Command in the Line Card Configuration Menu for a Local AT-CM Line Card

Here are the functions of the commands:

- ❑ Save System and All Line Card Configuration - Though this is the last of the save commands in the Configuration Menu, it is mentioned here first because it'll probably be the one you use most often. That's because of all the same commands it performs the most comprehensive update of the master configuration file in flash memory. When you select this command, the management card copies its entire master configuration file in DRAM to flash memory for permanent storage. You will find that the last step in many of the procedures in this guide reminds you to save your changes with this command.
- ❑ Save System Configuration - This command updates the master configuration file in flash memory with the current settings of the management card, but ignores any changes to the settings of the AT-CM Line Cards. You might use this command if you changed the parameters on the management card and the line cards, but only want to save your management card changes. Of course, this is unlikely because you'll probably always want to save all of your changes. But the command is here, just in case.
- ❑ Save All Line Card Configurations - This command is similar to the previous command. But instead of saving just your changes to the management card, it ignores those changes and instead saves just your changes to the AT-CM Line Cards.

- ❑ Save Line Card Configuration (menus) and Save Current Configuration (web browser windows) - These commands make it easier for you to save your changes after configuring the individual local or remote AT-CM Line Cards. Rather than having to return to the Main Menu or the Files tab after configuring a line card, you can save your changes with these commands instead.

**Note**

If you're confused by all of these save commands, then just stick with the Save System and All Line Card Configuration command. That command insures that the master configuration file in flash memory on the management card has the current settings from all the cards in the chassis.

There are two more save commands that are related to redundant AT-CV5M02 Management Cards in the AT-CV5000 Chassis. These commands are located in the Management Card Redundancy menu and tab, shown in Figure 17 and Figure 18, respectively.

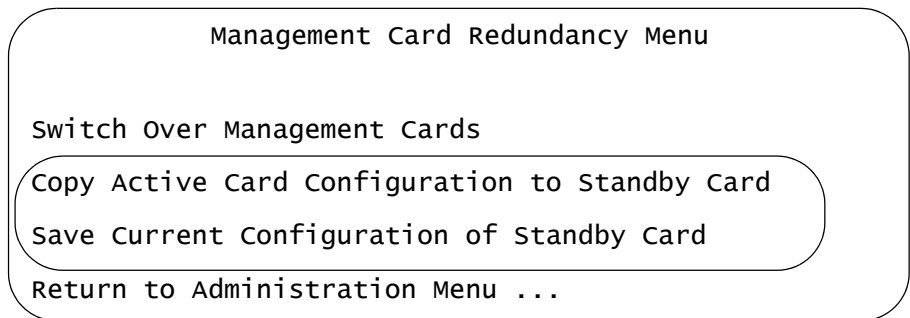


Figure 17. Management Card Redundancy Menu

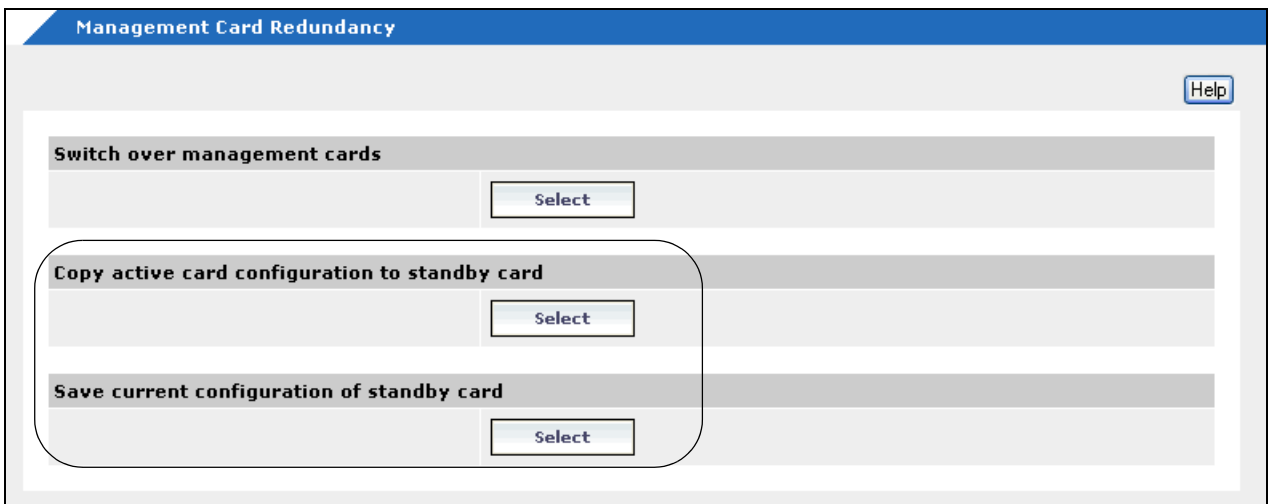


Figure 18. Management Card Redundancy Tab

The functions of these commands are given here:

- ❑ Copy Active Card Configuration to Standby Card - This command copies the temporary master configuration file from DRAM in the active management card to DRAM in the standby card.
- ❑ Save Current Configuration of Standby Card - This command instructs the standby card to copy its master configuration file from DRAM to flash memory for permanent storage.

You use these commands to manually copy the master configuration file from the active management card to the standby card and to store the file in the standby card's flash memory. However, there is little likelihood you'll ever need to use these commands because the active and standby cards do this automatically. The only time you might be inclined to use them is if you suspect that the standby card isn't properly updating its master configuration file. However, a standby management card that is not updating its configuration file might be faulty and should probably be replaced. For more information, refer to "Redundant Management Cards" on page 26.

## What to Configure First on the AT-CV5M02 Management Card

---

This section has a few suggestions on what to configure on the management card during the initial management session. The first management session has to be a local session from the Console port on the card. For instructions on how to start a local management session, refer to “Starting a Local Management Session” on page 58.

### Changing the Manager and Operator Passwords

Since the default passwords for the manager and operator accounts on the management card are included in this guide, you should change them to protect the unit from unauthorized access.

To change the passwords:

1. From the Main Menu, select **Configuration**.
2. From the Configuration Menu, select **System Configuration**.
3. From the System Configuration Menu, select **Omega Options** to display the Omega Options Menu
4. On the Omega Options Menu, select **Manager Password** to change the Manager password or **Operator Password** to change the Operator password.
5. Enter a new password of 0 to 16 alphanumeric characters. A password is case-sensitive and can have the letters A to Z in uppercase and lowercase, and the numbers 1 to 9. Do not use special characters, such as spaces, asterisks (\*), or exclamation points (!). To delete the current password without assigning a new password, enter a space in the password field. The default password for the manager account is “friend” and the default password for the operator account is “operator.”

For information on the other options in the Omega Options Menu, refer to “Configuring Management Security” on page 90.

6. Return to the Main Menu.

## Assigning an IP Address Configuration and Changing the Community Strings

The management card has to be assigned an IP address configuration to perform these management functions:

- Remote Telnet, web browser, or SNMP management
- Sending event messages to a syslog server
- Setting the date and time from a Network Time Protocol server
- Sending SNMP traps to trap receivers.
- Uploading or downloading files to a TFTP server.
- Pinging a remote device.

The IP address configuration has to consist of a unique IP address and a subnet mask. The configuration must also include a default gateway address if the management card and the network devices (e.g., syslog server or TFTP server) are located on different networks. This address is the IP address of the router interface that represents the first hop to reaching the remote networks where the devices reside.

Since a management card with an IP address configuration is vulnerable to unauthorized access from an intruder with an SNMP program, you should change the card's SNMP community strings to protect the card and the chassis. If an intruder were to learn the IP address and the community strings of the management card, he could use an SNMP application program to gain access to the card, without having to know the password to the manager account.

The IP address configuration of the management card can be assigned manually or, since the management card has a DHCP client, from a DHCP server on your network.

To assign the management card an IP address configuration and to change the SNMP community strings:

1. From the Main Menu, select **Configuration**.
2. From the Configuration Menu, select **System Configuration**.
3. From the System Configuration Menu, select **IP Parameters** to display the IP Parameters Menu.
4. To manually assign an IP address configuration to the management card, enter values for the **IP address**, **Subnet mask**, and **Gateway address** parameters. When entering the values, observe the following guidelines:
  - The values have to be entered in this format: xxx.xxx.xxx.xxx.
  - The DHCP client has to be disabled.
  - To delete a value without assigning a new value, enter 0.0.0.0.

- ❑ A default gateway address is needed if the management card will be communicating with a network device, like a TFTP server or a syslog server, on a different subnet. The address has to be a member of the same subnet as the card's IP address and should specify the first hop to reaching the remote subnet.
5. To activate the DHCP client to assign the IP address from a DHCP server on the network, select **Enable DHCP**. If you want to learn the MAC address of the management card to enter on the DHCP or BOOTP server, refer to "Displaying the Operational Status of the Chassis" on page 121. To communicate with your network the management card adopts the MAC address of the backplane of the chassis as its MAC address.

Review the following guidelines before activating the DHCP client:

- ❑ The 10/100Base-TX port on the management card has to be connected to a device on your network, such as a Fast Ethernet switch, because card communicates with your network through that port.
  - ❑ If the card already has a static IP address, the address is overwritten by the address from the DHCP server.
  - ❑ The management card transmits two queries to the DHCP server when the client is activated. If there is no response from the server, the management card operates without an IP address.
6. To change the community strings, enter the new values in the **Get Community String**, **Set Community String**, and **Trap Community String** fields. Community strings are case sensitive and can have up to thirteen characters. Spaces and special characters are permitted.
  7. Return to the Main Menu.

## Setting the Date and Time

The date and time are added by the management card to event messages and SNMP traps. The date and time can be set manually or, since the card has a Network Time Protocol (NTP) client, from an NTP server on your network or the Internet. If you choose to use the NTP client, review the client's requirements in "Access to Your Network" on page 28.

---

### Note

Since the management card does not maintain the date and time when reset or powered off, the NTP client is the recommended method for setting this information.

---

To set the date and time:

1. From the Main Menu, select **Configuration**.
2. From the Configuration Menu, select **System Configuration**.

3. From the System Configuration Menu, select **System Clock Configuration**.
4. To set the date and time manually, do the following:
  - a. Select **System Date (mm/dd/yy)** and enter a new date in the format “mm/dd/yy” format. For example, April 5, 2008 would be 4/5/08.
  - b. Select **System Time (hh:mm:ss)** and enter a new time in 24-hour, “hh:mm:ss” format. The seconds are optional. For example, 8:15 am would be 08:15.
5. To configure the NTP client, do the following:
  - a. Select **NTP Server** and enter the IP address of the NTP server.
  - b. To enable the client, select **Enable NTP**.
6. Return to the Main Menu.

### **Naming the Management Card**

The management card will be easier to identify if you assign it a name. The name is displayed at the top of the menus in the management software. To assign a name to the management card:

1. From the Main Menu, select **Configuration**.
2. From the Configuration menu, select **System Configuration**.
3. Select **System Name** and enter a new name of up to 39 characters for the card. Spaces and special characters are permitted.
4. Return to the Main Menu. The card’s new name does not appear until you return to the Main Menu.

### **Saving Your Changes**

This completes the initial configuration of the management card. To save your changes in the master configuration file on the management card:

1. From the Main Menu, select **Configuration**.
2. From the System Configuration Menu, select **Save System and All Line Card Configurations**. The following message is displayed:

```
saving system and all line card configuration ...
```

After the management card updates its master configuration file, it displays this prompt:

```
saving system and all line card configuration ... OK  
Press any key to continue...
```

3. Return to the Main Menu.

For further instructions on how to configure the management card, refer to Chapter 4, "Configuring the AT-CV5M02 Management Card" on page 79.

## Configuring the AT-CM Media Converter Line Cards for the OAM-based Features

---

Are you planning to implement any of these OAM-based features on the AT-CM Line Cards?

- Remote peer management
- Remote downloads of new management software
- Dying gasp feature
- OAM loopback test
- OAM variable requests

If so, perform this procedure to configure the cards. It explains how to set the operating modes of the cards to the OAM visible mode and how to verify their OAM settings. This procedure has to be performed at a Converteon chassis that has a management card. Thus, those AT-CM Line Cards to be deployed at remote sites have to be initially installed and configured in a chassis with a management card.

---

### Note

If you plan to use the dying gasp feature, perform “Configuring the AT-CM Line Cards” on page 230 instead of this procedure. Although the OAM-based features share many of the same settings, the dying gasp feature has more stringent hardware and software requirements, as explained in that procedure.

---

You can use either the menus or the web browser windows to configure the line cards. This procedure uses the menus.

To configure an AT-CM Line Card for the OAM-based features:

1. Install the AT-CM Line Card in a Converteon chassis that has the AT-CV5M02 Management Card and start a local management session or a remote Telnet management session on the chassis.
2. Wait one minute for the AT-CM Line Card to initialize its AT-S73 Management Software.
3. From the Main Menu select **Module Status and Configuration**.

- In the Module Status and Configuration Menu, examine the operating mode of the line card in the OpMode column. If the line card is not set to the OAM visible mode (OamVisib), you will have to set it to that mode. For information about this menu, refer to "Displaying the Status of the Line Cards" on page 128.)

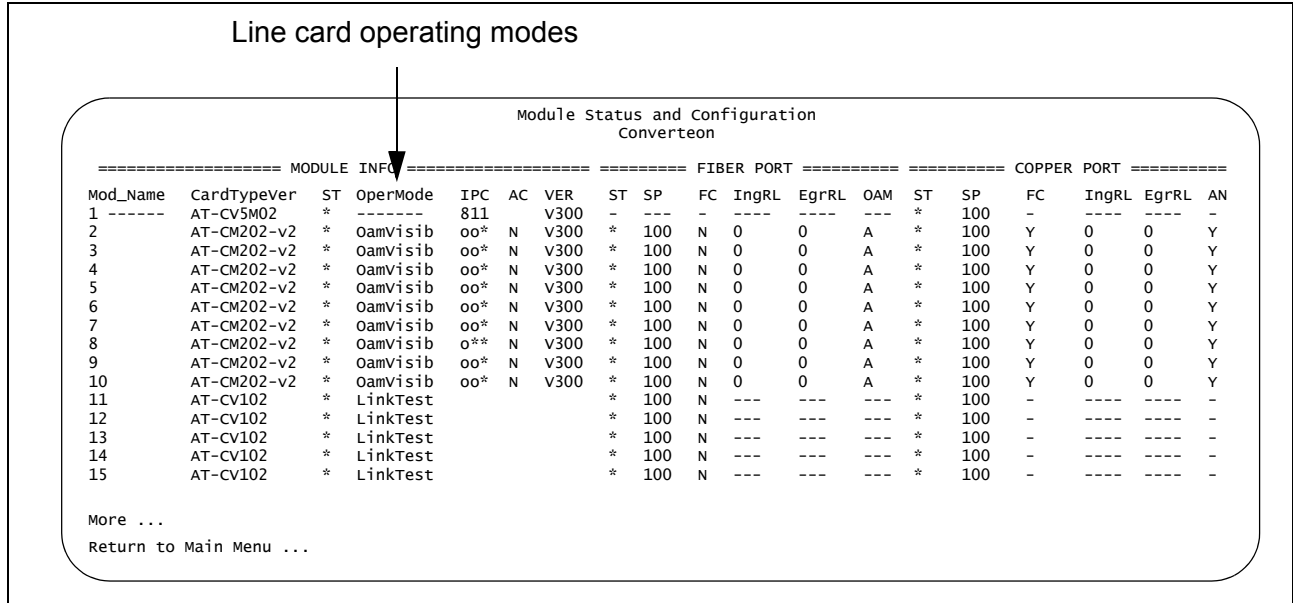


Figure 19. Module Status and Configuration Menu

- Select the AT-CM Line Card you want to configure and press Return to display the Module Configuration Menu for the card.

**Note**

If the line card is already set to the OAM visible mode, go to step 11. Otherwise, continue to the next step.

- Select **Configure Operating Mode** to display the Operating Mode Config Menu for the line card.
- From the Operating Mode Config Menu, select **OAM Visible Mode**. This confirmation prompt is displayed:

warning: Changing the operation Mode will reset the line card.  
Change operation Mode now? (Yes or No):

- Type **Y** to continue or **N** to cancel the procedure. This prompt is displayed:

If auto-copy is enable, operation mode change need to be saved to take affect.  
save line card configuration before rebooting? (Yes or No):

9. Type **Y** for yes to update the master configuration file on the management card with the new setting for the card's operating mode. This step is especially important if the auto-copy feature is activated on the card's slot. If the card's operating mode isn't saved in the master configuration file, the new setting will not take affect because the card, after it resets, will simply revert to its previous operating mode. Since this is the initial configuration, you probably don't know the auto-copy setting for the slot. But respond with Yes anyway. In fact, there is little likelihood you would ever respond with No to this prompt. (This step isn't applicable to the AT-CM70S Line Card because it doesn't support the auto-copy feature.)

The operating mode on the line card is changed to OAM visible and the card resets.

10. Wait one minute for the line card to initialize its management software and then select it again from the Module Status and Configuration Menu:
11. From the line card's Module Configuration Menu, select **Port A**, the fiber optic port, to display the Port Management Menu.
12. Select **OAM Configurations** to display the OAM Configuration menu. (If the menu does not include the OAM configuration selection, the line card isn't set to the OAM visible mode.)
13. Select **OAM Configuration** to display the OAM Configuration submenu.
14. Check the Admin State parameter. It has to be set to Enabled. If it is set to Disabled, select **Admin State** and press Return to toggle the parameter to **Enabled**.
15. Check the Mode parameter. It has to be set to Active. If it is set to Passive, highlight **Mode** and press Return to toggle the parameter to **Active**.
16. If the line card will be installed at a remote site and you want it to support the OAM loopback test, the Loopback Support parameter has to be set to Yes. If it is set to No, highlight **Loopback Support** and press Return to toggle the parameter to **Yes**. This parameter has to be set to Yes only on those remote line cards that will return test packets from remote sites. For those line cards generating the test packets this parameter can be set to Yes or No.

---

**Note**

The Link Event Support and the Variable Request Support parameters can be ignored. For further information, refer to "Configuring an OAM Client" on page 204.

---

17. Return to the Main Menu.
18. The line card is now configured for the OAM-based features. If you do not want to configure any other parameters on the card (such as port speed or the card's name) and if the card will be deployed at a remote site in an unmanaged chassis, you can remove it from the chassis. Entering a save command isn't necessary because your changes are saved automatically by the card in its configuration file.

If, however, the line card will remain in the chassis with the management card, you should update the master configuration file on the management card. This is accomplished by selecting **Configuration** from the Main Menu and **Save System and All Line Card Configurations** from the Configuration menu. Once saved in the master configuration file, the settings can be restored in the event the card is replaced. For further information, refer to "Configuration Files" on page 29.

The line card is now configured for the OAM-based features. Repeat this procedure on the other AT-CM Line Cards.

If you have a large number of AT-CM Line Cards to configure, you can speed up the process with the auto-copy feature. To use the feature, you configure one line card with the necessary settings and then activate the auto-copy feature on the slot. Line cards subsequently installed in the same slot will be assigned the same settings, automatically.

For the auto-copy feature to work, the line cards have to be of the same model. For instance, if you were to install the AT-CM202 Line Card in a slot that had been configured for the AT-CM212A/1 Line Card, the new card would reject the configuration from the management card and would instead use the parameter settings in its own configuration file. For background information, refer to "Configuration Files" on page 29.

To configure multiple AT-CM Line Cards with the same settings, perform the previous procedure up to step 16 and then perform these additional steps:

17. After configuring the parameter settings for the OAM client on the line card, return to the card's Module Configuration Menu.
18. Select **Line Card Configuration**.
19. From the Line Card Configuration menu, select **Auto-copy Line Card Configuration**.
20. From the Display Current Configuration menu, select **Auto-copy Enable**. (Although the setting of the auto-copy feature is set in a card's Module Configuration Menu, it applies to the slot. The setting is not transferred when a line card is installed in a different slot or chassis.)

21. Return to the line card's Module Configuration Menu.
22. To configure other parameters on the line card, refer to Chapter 5, "Configuring AT-CM and AT-CV Media Converter Line Cards" on page 127.
23. Return to the Main Menu and select **Configuration**.
24. From the Configuration menu, select **Save System and All Line Card Configurations**.
25. You can now remove the line card from the slot.
26. To assign the same configuration to another AT-CM Line Card, install the card in the same slot. Wait a full minute for the line card to initialize its management software and to receive its parameter settings from the management card. Afterwards, remove the card. Repeat this step to assign the same settings to other AT-CM Line Cards.

## Chapter 4

# Configuring the AT-CV5M02 Management Card

---

This chapter has the following sections:

- “Assigning an IP Address Configuration” on page 80
- “Assigning a Name” on page 85
- “Assigning Contact and Location Information” on page 86
- “Configuring the SNMP Community Strings” on page 88
- “Specifying the IP Addresses of SNMP Trap Receivers” on page 89
- “Configuring Management Security” on page 90
- “Manually Setting the Date and Time” on page 93
- “Configuring the Network Time Protocol Client” on page 95
- “Resetting the Management Card” on page 96
- “Viewing the Event Log” on page 98
- “Viewing the Activity Monitor” on page 104
- “Configuring the Syslog Client” on page 105
- “Configuring the 10/100Base-TX Port” on page 107
- “Restoring the Default Setting on the 10/100Base-TX Port” on page 112
- “Restoring the Default Values on the AT-CV5M02 Management Card” on page 113
- “Configuring the Temperature Threshold” on page 115
- “Activating a Standby AT-CV5M02 Management Card” on page 117
- “Setting the Baud Rate of the Console Port” on page 119
- “Displaying the Operational Status of the Chassis” on page 121
- “Pinging Network Devices” on page 125
- “Displaying Management Card Information” on page 126

## Assigning an IP Address Configuration

---

This section explains how to assign an IP address, subnet mask and default gateway to the management card. A management card can have only one IP address configuration. The address can be assigned manually or from a DHCP server on your network. For background information, refer to “IP Address Configuration” on page 23.

**Menus** To assign an IP address configuration to the card from the menus:

1. From the Main Menu, select **Configuration** to display the Configuration Menu shown in Figure 20.

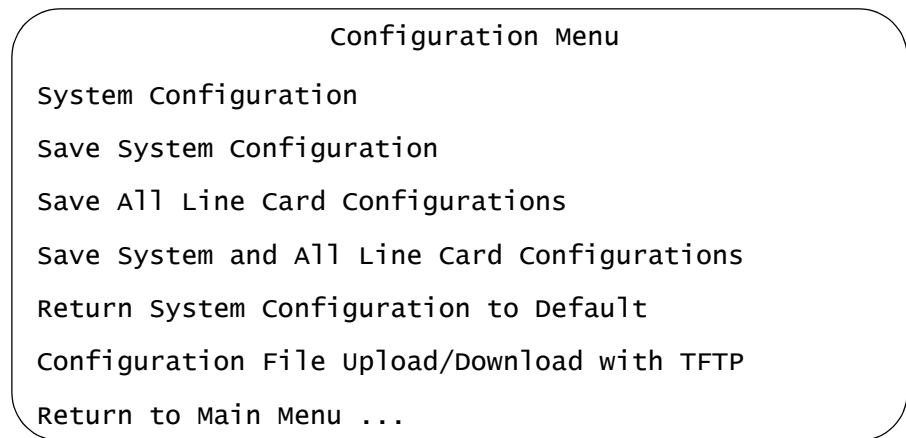


Figure 20. Configuration Menu

2. From the Configuration Menu, select **System Configuration** to display the menu in Figure 21.

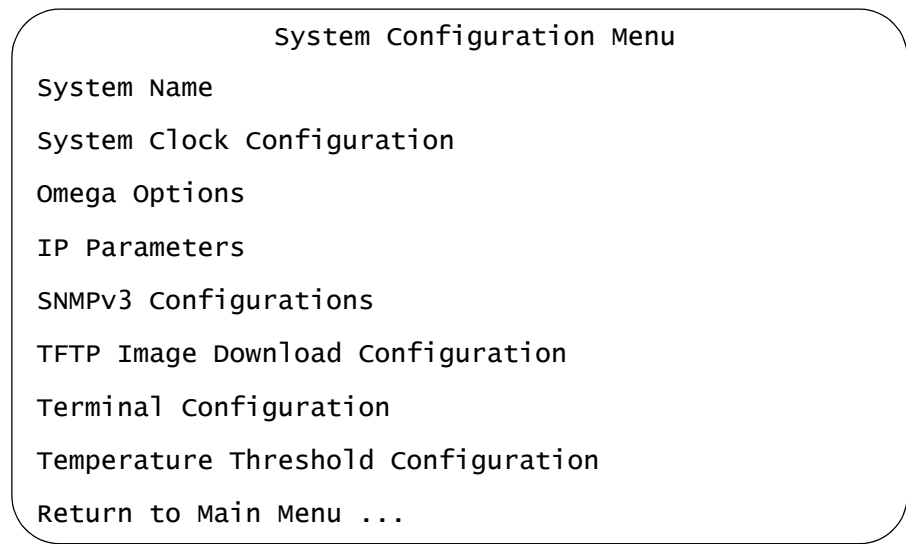


Figure 21. System Configuration Menu

- From the System Configuration Menu, select **IP Parameters** to display the IP Parameters Menu shown in Figure 22.

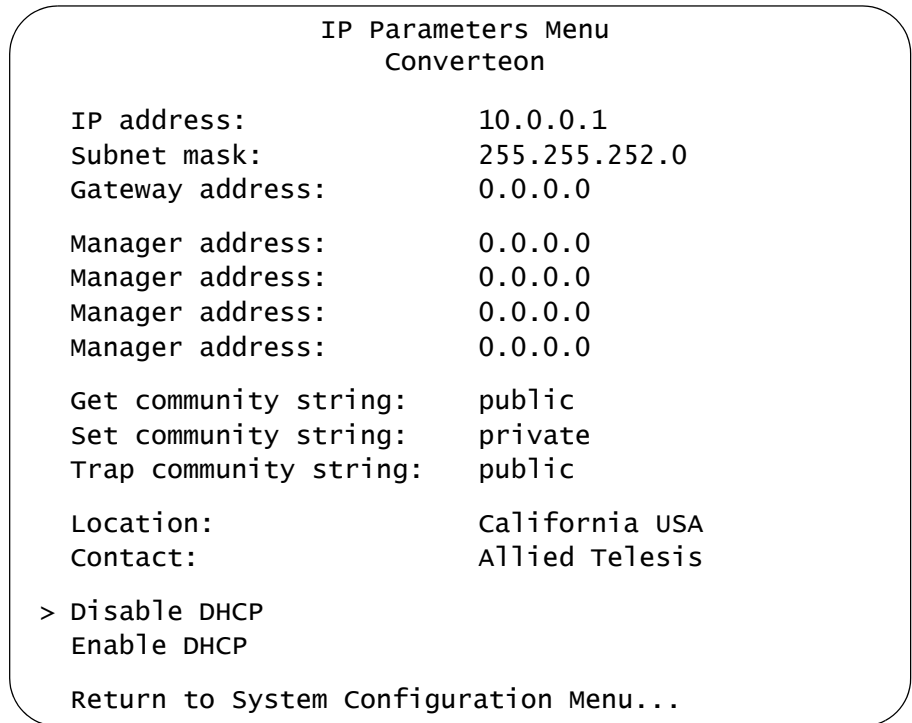


Figure 22. IP Parameters Menu

- To assign a static IP address configuration to the card, enter the values in the **IP address**, **Subnet mask**, and **Gateway address** fields. Here are the guidelines for assigning a static IP address configuration:
  - The values have to be entered in this format: xxx.xxx.xxx.xxx.
  - The DHCP client has to be disabled.
  - To delete a value without assigning a new value, enter 0.0.0.0.
  - The IP address configuration has to include a default gateway address if the management card will be communicating with network devices, like a TFTP server or syslog server, that are located on a different subnet. This address should specify the first hop to reaching the remote subnet and has to be a member of the same subnet as the card's IP address.
  - The default values are 10.0.0.1 for the IP address, 255.255.255.0 for the subnet mask, and 0.0.0.0 for the default gateway address.
- If you want the card to obtain its IP address from a DHCP server on the network, select **Enable DHCP** to activate the DHCP client. Or, to deactivate the client to assign the IP address manually, select **Disable DHCP**. The default setting for the client is disabled.

Here are the guidelines to the DHCP client:

- ❑ The 10/100Base-TX port on the AT-CV5M02 Management Card has to be connected to a network device, such as a Fast Ethernet switch, because the card transmits the DHCP requests from that port.
  - ❑ If the card already has a static IP address, the address is overwritten by the address from the DHCP server.
  - ❑ The management card issues two requests to the DHCP server when the client is activated. If there is no response from the server, the management card operates without an IP address configuration.
  - ❑ If you want to learn the MAC address of the management card to enter on the DHCP server, refer to “Displaying the Operational Status of the Chassis” on page 121. The management card does not actually have a MAC address. Instead, it adopts the MAC address of the backplane of the chassis as its MAC address whenever it communicates with your network.
6. To save your changes in the master configuration file, return to the Configuration Menu and select **Save System and All Line Card Configurations**.

## Web Browser

To change the IP address configuration of the management card from the web browser windows:

---

### Note

Your remote web browser management session of the chassis automatically ends if you change the IP address of the management card from the web browser windows. To resume managing the Converteon chassis, start a new session using the card’s new IP address.

---

1. Select **Configuration** from the menu bar.
2. If the System tab is not selected, select it. The System tab is shown in Figure 23.

Configuration			
System	SNMPv1 & SNMPv2	SNMPv3	Files
<a href="#">Help</a>			
<b>System Information</b>			
System Name:			
System Date:	00/00/00	System Time:	00:04:24
NTP Server:	0.0.0.0	NTP:	Disable
			<a href="#">Edit</a>
<b>Omega Options</b>			
Manager Password:	*****	Local Omega:	Enable
Operator Password:	*****	Remote Omega:	Enable
Timeout:	10		
			<a href="#">Edit</a>
<b>Terminal Setting</b>			
Baudrate	1152000		
			<a href="#">Edit</a>
<b>Temperature Threshold</b>			
Maximum Temperature Threshold	60 C		
			<a href="#">Edit</a>
<b>IP Parameters</b>			
IP Address	10.0.0.1	Subnet Mask	255.255.252.0
Gateway Address	0.0.0.0	DHCP	Disable
			<a href="#">Edit</a>

Figure 23. System Tab

3. Click **Edit** in the IP Parameters section of the window to display the IP Parameters pop-up window.
4. To assign a static IP address configuration to the card, enter the desired values in the **IP Address**, **Subnet Mask**, and **Gateway Address** fields. Here are the guidelines for entering a static IP address configuration:
  - The values have to be entered in this format: xxx.xxx.xxx.xxx.
  - The DHCP client has to be disabled.
  - To delete a value without assigning a new value, enter 0.0.0.0.
  - The IP address configuration has to include a default gateway address if the management card will be communicating with network devices, like a TFTP server or syslog server, that are located on a different subnet. This address should specify the first

hop to reaching the remote subnet and has to be a member of the same subnet as the card's IP address.

- The default values are 10.0.0.1 for the IP address, 255.255.255.0 for the subnet mask, and 0.0.0.0 for the default gateway address.
5. To activate the DHCP client so that the card obtains its IP address from a DHCP server on the network, select **Enable DHCP**. Or, to deactivate the client so that you can assign the IP address manually, select **Disable DHCP**. Here are the guidelines to using the DHCP client:
- The 10/100Base-TX port on the management card has to be connected to a network device, such as a Fast Ethernet switch. The DHCP requests are transmitted from that port.
  - If the card already has a static IP address, the address is overwritten by the address from the DHCP server.
  - When the client is activated, the management card issues two requests for an IP address configuration from the DHCP server. If the DHCP server does not respond, the management card operates without an IP address configuration.
6. Click **Update**.

If you changed the IP address of the management card, your management session ends. To continue managing the unit and to save your changes, start a new management session with the card's new IP address.

7. To save your changes in the master configuration file, select the **Files** tab in the Configuration window and click **Save System Configuration and All Cards Configurations** and **Apply**.

## Assigning a Name

---

By assigning a name to the management card, you make the card and the chassis easier to identify. The name is displayed at the top of the menus of the management software during your local management sessions and remote Telnet sessions. (The web browser windows do not display the system name.)

**Menus** You can assign a name to the management card from the System Configuration Menu or the Omega Options Menu. This procedure uses the System Configuration Menu. To assign a name to the management card from the menus:

1. From the Main Menu, select **Configuration** to display the Configuration Menu shown in Figure 20 on page 80.
2. From the Configuration Menu, select **System Configuration** to display the menu in Figure 21 on page 80.
3. From the System Configuration Menu, select **System Name** and enter a new name for the card of up to 40 characters. Spaces and special characters are permitted. To delete the current name without entering a new name, press the space bar once.
4. To save your changes in the master configuration file, return to the Configuration Menu and select **Save System and All Line Card Configurations**.

**Web Browser** To assign a name to the management card from the web browser windows:

1. Select **Configuration** from the menu bar.
2. If the **System** tab is not selected, select it. An example of the System tab is shown in Figure 23 on page 83.
3. Click **Edit** in the System Information section of the tab.
4. In the pop-up window, select the **System Name** field and enter a new name for the card of up to 40 characters. Spaces and special characters are permitted. To delete the current name without entering a new name, press the space bar once.
5. Click **Update**.
6. To save your changes in the master configuration file, select the **Files** tab in the Configuration window and click **Save System Configuration and All Cards Configurations** and **Apply**.

## Assigning Contact and Location Information

---

- Menus** To enter the chassis' location and the name of the network manager responsible for managing the chassis:
1. From the Main Menu, select **Configuration** to display the Configuration Menu shown in Figure 20 on page 80.
  2. From the Configuration Menu, select **System Configuration** to display the menu in Figure 21 on page 80.
  3. Select **IP Parameters** to display the menu in Figure 22 on page 81.
  4. To enter the location of the chassis, select **Location**. The location can be up to 20 alphanumeric characters. Spaces and special characters are permitted. To delete the current location without entering a new location, press the space bar once.
  5. To enter the name, phone number, or other information that identifies the person responsible for managing the system, select **Contact** and enter a value of up to 20 alphanumeric characters. Spaces and special characters are permitted. To delete the current location without entering a new location, press the space bar once.
  6. To save your changes in the master configuration file, return to the Configuration Menu and select **Save System and All Line Card Configurations**.

- Web Browser** To enter the contact and location information from the web browser windows:
1. Select **Configuration** from the left menu bar.
  2. Select the **SNMPv1 & SNMPv2c** tab. The SNMPv1 & SNMPv2c tab is shown in Figure 24.

Configuration				
System	SNMPv1 & SNMPv2c	SNMPv3	Files	Help
Manager Address	0.0.0.0			
Manager Address	0.0.0.0			
Manager Address	0.0.0.0			
Manager Address	0.0.0.0			
Get Community String	public			
Set Community String	private			
Trap Community String	public			
Location	California USA			
Contact	Allied Telesis			
<input type="button" value="Edit"/>				

Figure 24. SNMPv1 &amp; SNMPv2c Tab

3. To change the contact and location information, click **Edit** to display a pop-up window.
4. To enter the location of the chassis, select **Location** and enter a new location of up to 20 alphanumeric characters. Spaces and special characters are permitted. To delete the current location without entering a new location, press the space bar once.
5. To enter the name, phone number, or other information that identifies the person responsible for managing the system, select **Contact** and enter a value of up to 20 alphanumeric characters. Spaces and special characters are permitted. To delete the current location without entering a new location, press the space bar once.
6. Click **Update** to close the popup window.
7. To save your changes in the master configuration file, select the **Files** tab in the Configuration window and click **Save System Configuration and All Cards Configurations** and **Apply**.

## Configuring the SNMP Community Strings

---

The procedures in this section are used to set the three SNMP community strings Get, Set, and Trap on the management card. The strings are used to manage the media converter with an SNMP application and for trap verification. To protect the card from unauthorized access, you should change the community strings even if you do not plan to employ an SNMP application. Anyone who learns the device's IP address and community strings can alter its settings with an SNMP program, without having to know the manager account password.

**Menus** To change the SNMP community strings from the menus:

1. From the Main Menu, select **Configuration**. This displays the Configuration Menu shown in Figure 20 on page 80.
2. From the Configuration Menu, select **System Configuration** to display the menu in Figure 21 on page 80.
3. Select **IP Parameters** to display the menu in Figure 22 on page 81.
4. Enter the new community strings in the **Get Community String**, **Set Community String**, and **Trap Community String** fields. A community string can have up to thirteen characters. Spaces and special characters are permitted. Community strings are case sensitive.
5. To save your changes in the master configuration file, return to the Configuration Menu and select **Save System and All Line Card Configurations**.

**Web Browser** To change the SNMP community strings from the web browser windows:

1. Select **Configuration** from the menu bar.
2. Select the **SNMPv1 & SNMPv2c** tab. The SNMPv1 & SNMPv2c tab is shown in Figure 24 on page 87.
3. To change the community strings, click **Edit** to display a pop-up window.
4. Enter the new community strings in the **Get Community String**, **Set Community String**, and **Trap Community String** fields. A community string can have up to thirteen characters. Spaces and special characters are permitted. Community strings are case sensitive.
5. Click **Update**.
6. To save your changes in the master configuration file, select the **Files** tab in the Configuration window, click **Save System Configuration and All Cards Configurations** and click **Apply**.

## Specifying the IP Addresses of SNMP Trap Receivers

---

The management card can send SNMP traps to up to four trap receivers on your network. The traps alert you to significant events in the operations of the Converteon chassis, like the removal of line cards, the failure of a cooling fan, or the loss of a link on a port on a media converter line card.

The requirements for this feature are described in “Access to Your Network” on page 28.

**Menus** To specify the IP addresses of SNMP trap receivers from the menus:

1. From the Main Menu, select **Configuration**. This displays the Configuration Menu shown in Figure 20 on page 80.
2. From the Configuration Menu, select **System Configuration** to display the menu in Figure 21 on page 80.
3. Select **IP Parameters** to display the menu in Figure 22 on page 81.
4. In the **Manager Address** fields enter the IP addresses of the trap receivers. To remove an IP address, enter 0.0.0.0.
5. To save your changes in the master configuration file, return to the Configuration Menu and select **Save System and All Line Card Configurations**.

**Web Browser** To specify the IP addresses of SNMP trap receivers from the web browser windows:

1. Select **Configuration** from the left menu bar.
2. Select the **SNMPv1 & SNMPv2c** tab. The SNMPv1 & SNMPv2c tab is shown in Figure 24 on page 87.
3. To change the addresses of the SNMP trap receivers, click **Edit** to display a pop-up window.
4. In the **Manager Address** fields enter the IP addresses of up to four trap receivers.
5. Click **Update**.
6. To save your changes in the master configuration file, select the **Files** tab in the Configuration window, click **Save System Configuration and All Cards Configurations** and click **Apply**.

## Configuring Management Security

---

The AT-S99 Management Software on the AT-CV5M02 Management Card has several security features that protect the card from unauthorized access. There are manager and operator passwords and a console time-out feature that automatically ends inactive management sessions. Additionally, there are controls for enabling or disabling local or remote access to the management card.

**Menus** To configure the security features from the menus:

1. From the Main Menu, select **Configuration**. This displays the Configuration Menu shown in Figure 20 on page 80.
2. From the Configuration Menu, select **System Configuration** to display the menu in Figure 21 on page 80.
3. From the System Configuration Menu, select **Omega Options** to display the Omega Options Menu in Figure 25.

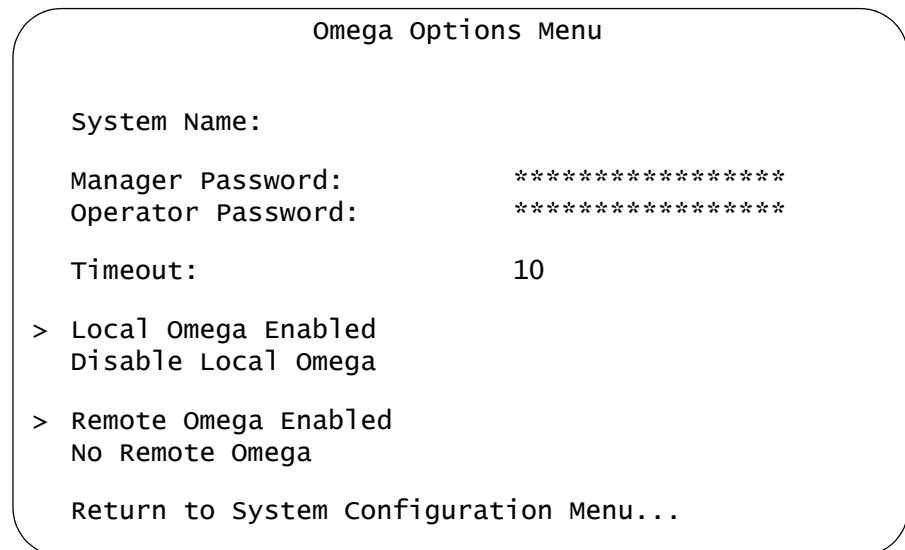


Figure 25. Omega Options Menu

4. Configure the parameters as needed. The options are described in Table 7.

Table 7. Omega Options Menu

Parameter	Description
System Name	<p>This parameter assigns a name to the management card. The name can have up to 40 characters. Spaces and special characters are permitted. To delete an existing name without entering a new name, press the space bar once.</p>
Manager Password Operator Password	<p>These parameters are used to set the manager and operator passwords. Passwords can have 0 to 16 alphanumeric characters of the letters A to Z in uppercase and lowercase, as well as the numbers 1 to 9. Passwords are case-sensitive and should not contain special characters, such as spaces, asterisks (*), or exclamation points (!). The default passwords are "friend" for the manager account and "operator" for the operator account.</p> <p>The password is displayed as a series of asterisks. To delete the current password without assigning a new password, enter a space in the password field.</p>
Timeout	<p>This parameter is used to set the amount of time in minutes the management software waits before it automatically ends an inactive local or remote management session. The management software automatically logs off a management session if there is no management activity for the duration of the timer. This security feature can prevent unauthorized individuals from using your management station to alter the configuration settings of the media converter chassis should you step away from your system during a management session.</p> <p>The console timer has a range of 1 to 60 minutes. The default value is 10 minutes.</p>
Local Omega Enabled Disable Local Omega	<p>These parameters are used to enable or disable the Console port on the management card. When the Console port is disabled, local management of the chassis through the RS-232 Console port is prohibited. The default setting for the Console port is enabled.</p> <p>If you disable local management during a local management session, your current session is not interrupted. However, the card will not allow you to establish any new local management sessions.</p>

Table 7. Omega Options Menu

Parameter	Description
Remote Omega Enabled No Remote Omega	These parameters are used to enable or disable the Telnet server on the management card. The default setting is enabled. When this option is set to disabled, you cannot manage the chassis from a remote Telnet client. <hr/> <p><b>Note</b>                      A management card where both local and remote management are disabled can still be managed with a web browser.</p>

- To save your changes in the master configuration file, return to the Configuration Menu and select **Save System and All Line Card Configurations**.

### Web Browser

To configure the security features of the management software from the web browser windows:

- Select **Configuration** from the left menu bar.
- If the **System** tab is not selected, select it. An example of the System tab is shown in Figure 23 on page 83.
- To configure the security features, click **Edit** in the Omega Options section of the tab to display a popup window.
- Configure the parameters as needed. The options are defined in Table 7, “Omega Options Menu” on page 91.
- Click **Update**.
- To save your changes in the master configuration file, select the **Files** tab in the Configuration window, click **Save System Configuration and All Cards Configurations** and click **Apply**.

## Manually Setting the Date and Time

---

To manually set the date and time on the management card, perform the procedures in this section. The date and time are added to event messages and SNMP traps.

---

### Note

When the date and time are set manually, they are not retained when the chassis or management card is reset or powered off.

---

**Menus** To manually set the management card's date and time from the menus:

1. From the Main Menu, select **Configuration**. This displays the Configuration Menu shown in Figure 20 on page 80.
2. From the Configuration Menu, select **System Configuration** to display the menu in Figure 21 on page 80.
3. From the System Configuration Menu, select **System Clock Configuration** to display the menu in Figure 26.

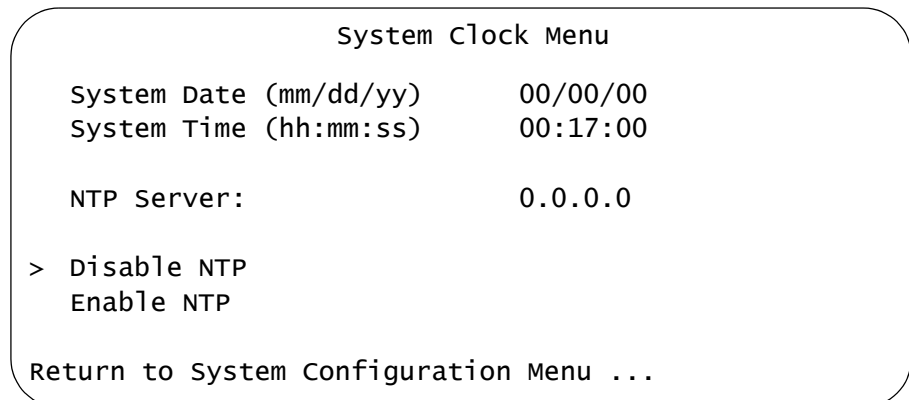


Figure 26. System Clock Menu

4. To set the date, select **System Date (mm/dd/yy)** and enter a new value in the format "mm/dd/yy" format. For example, here is April 5, 2008: 4/5/08.
5. To set the system time, select **System Time (hh:mm:ss)** and enter a new value in 24-hour, "hh:mm:ss" format. The seconds are optional. Each part requires two digits. For example, 8:15 a.m. would be 8:15.

**Web Browser** To manually set the date and time from the web browser windows:

1. Select **Configuration** from the left menu bar.
2. If the **System** tab is not selected, select it. The System tab is shown in Figure 23 on page 83.
3. To manually set the date and time, click **Edit** in the System Information section of the tab.
4. In the popup window, select **System Date** and enter the date in the format “mm/dd/yyyy” format. For example, here is April 5, 2008: 04/05/2008.
5. Select **System Time** and enter the time in 24-hour, “hh:mm:ss” format. For example, 8:15 am would be 8:15:00.
6. Click **Update**.

## Configuring the Network Time Protocol Client

---

The AT-CV5M02 Management Card has an NTP client for setting the date and time from a Network Time Protocol (NTP) server on your network or the Internet. The card adds the date and time to event messages and SNMP traps. Refer to “Access to Your Network” on page 28 for the NTP client requirements.

**Menus** To configure the NTP client from the menus:

1. From the Main Menu, select **Configuration**. The Configuration menu is shown in Figure 20 on page 80.
2. From the Configuration menu, select **System Configuration**.
3. From the System Configuration Menu, select **System Clock Configuration** to display the menu in Figure 26 on page 93.
4. Select the **NTP Server** field and enter the IP address of the NTP server.
5. To enable the client, select **Enable NTP**.
6. To save your changes in the master configuration file, return to the Configuration Menu and select **Save System and All Line Card Configurations**.

**Web Browser** To configure the NTP client from the web browser windows:

1. Select **Configuration** from the menu bar.
2. If the **System** tab is not selected, select it. The System tab is shown in Figure 23 on page 83.
3. in the System Information section, click **Edit**.
4. Select the **NTP Server** field in the popup window and enter the IP address of the NTP server.
5. Select **Enable** from the NTP pull-down menu to activate the client. Or, to disable the client, select **Disable**.
6. Click **Update**.
7. To save your changes in the master configuration file, select the **Files** tab in the Configuration window and click **Save System Configuration and All Cards Configurations and Apply**.

## Resetting the Management Card

---

This procedure is used to reset the management card in the chassis. You might reset the card if it is experiencing a problem. You can also reset the card using the CPU Reset button on the card's front panel.

Review the following information before resetting the management card:

- ❑ In most situations, resetting the management card should not affect the network operations of the media converter line cards in the chassis. However, if you've changed but not saved the parameter settings of a media converter line card in a slot where the auto-copy feature is enabled, the line card will revert to its previous settings after the management card resets. This may affect the operations of the line card.
- ❑ Any changes you've made to the parameter settings of the management card but not saved in the master configuration file are discarded when the card is reset. To save the parameter settings, return to the Main Menu and select **Configuration** and **Save System Confirmation** or **Save System and All Line Card Confirmations**.
- ❑ Resetting the management card ends your management session. To continue managing the chassis, wait approximately one minute for the management card to initialize its management software and afterwards start a new management session.
- ❑ If the chassis has two AT-CV5M02 Management Cards, resetting the active card activates the standby management card. To resume managing the chassis, wait 20 seconds for the standby card to transition to the active state and then start a new management session. For more information, refer to "Redundant Management Cards" on page 26.

### Menus

To reset the management card from the menus interface:

1. From the Main Menu, select **Module Status and Configuration**.
2. Select the management card to display the Module Configuration Menu.
3. Select **Reset Management Card and Restart System Software**.
4. At the confirmation prompt, select **Yes** to reset the card or **No** to cancel the procedure.
5. To resume managing the chassis, wait about one minute for the management card to initialize its management software and then start a new management session.

**Web Browser** To reset the management card from the web browser windows:

1. Select **Module Status and Configuration** from the menu bar.
2. From the Chassis View, click the 10/100Base-TX port on the AT-CV5M02 Management Card. Alternatively, select the Menu View and click the model name of the management card.
3. Click the **General** tab, shown in Figure 27.

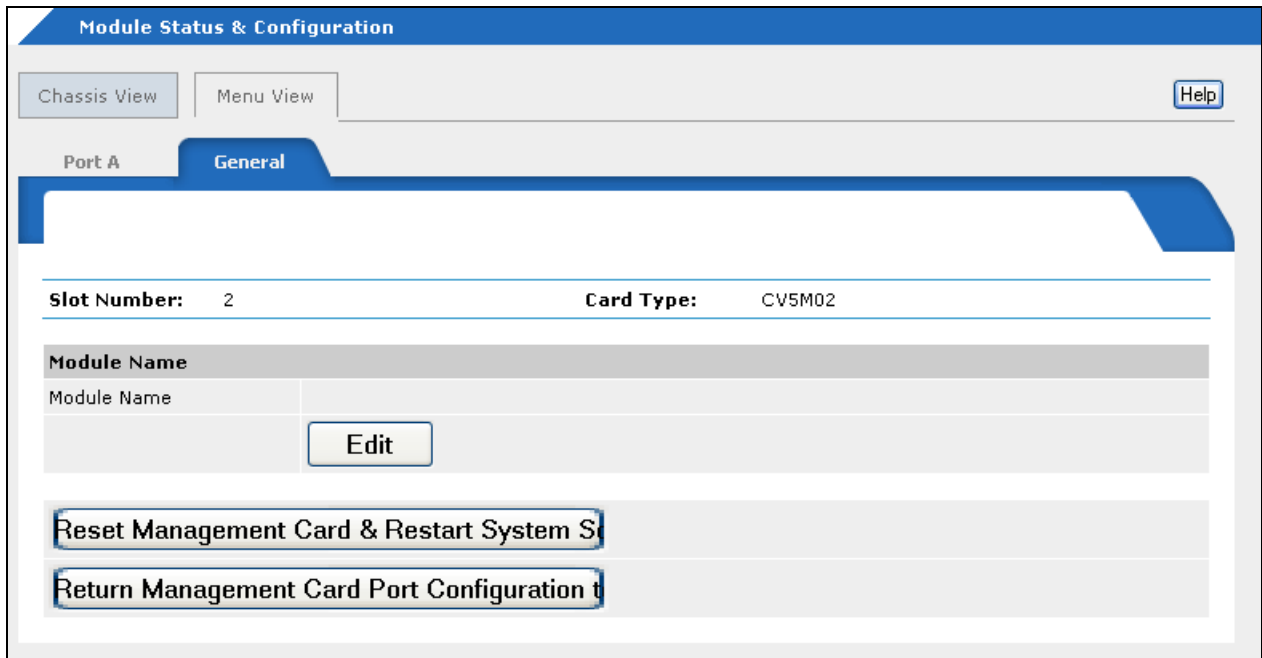


Figure 27. General Tab

4. Click **Reset Management Card and Restart System Software**.
5. At the confirmation prompt, click **OK** to reset the management card or **Cancel** to cancel the procedure.
6. To resume managing the chassis, wait one minute for the management card to initialize its management software and then start a new management session.

## Viewing the Event Log

---

For background information, refer to “Event Log” on page 23.

**Menus** To display the event log from the menus:

1. From the Main Menu, select **Administration**. The Administration Menu is shown in Figure 28.

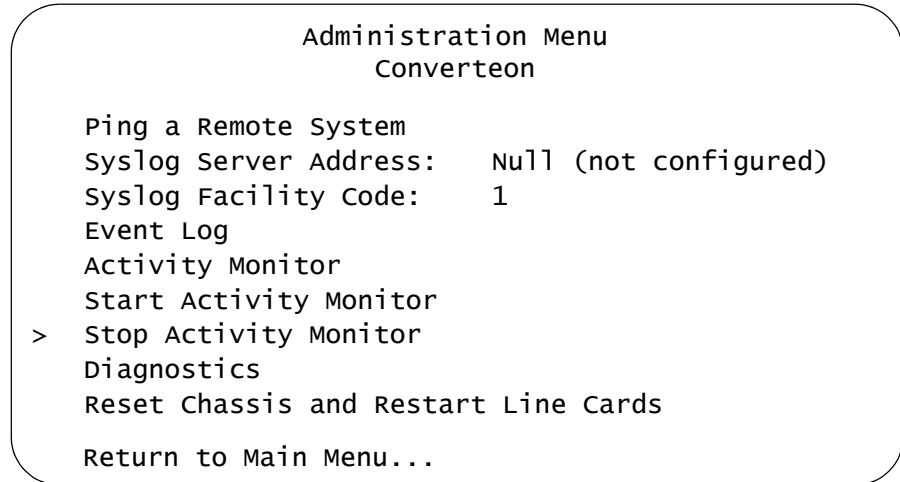


Figure 28. Administration Menu

2. From the Administration Menu, select **Event Log** to display the Event Log Menu window shown in Figure 29.

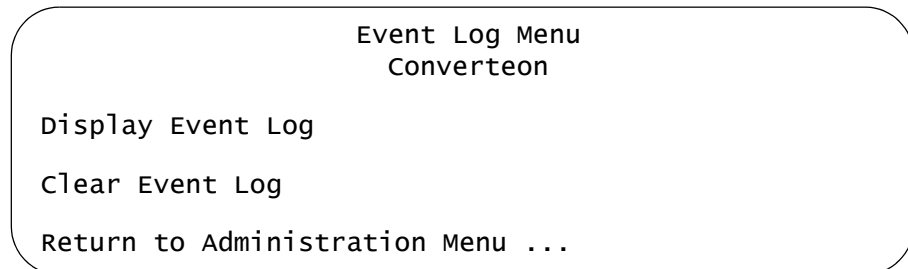


Figure 29. Event Log Menu

3. From the Event Log Menu, select **Display Event Log**. An example of the event log is shown in Figure 30. The messages are displayed from oldest to newest.

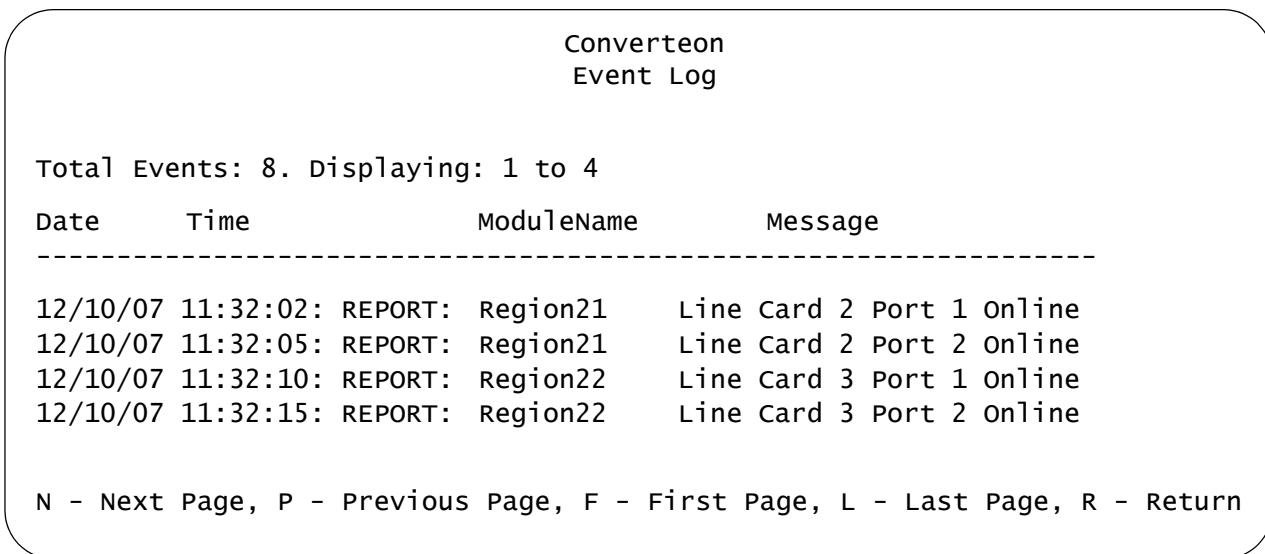


Figure 30. Event Log

The columns in the event log are described in Table 8.

Table 8. Event Log Format

Column	Definition
Date	This column displays the dates of the events.
Time	This column displays the times of the events.
(Classification)	<p>This unlabeled column displays the classifications of the events. An event's classification can be REPORT or CLEAR. A report signals an event's occurrence while a clear signifies the resolution of a prior event. For example, if a chassis' operating temperature were to exceed the temperature threshold, the management module would mark the event's occurrence by entering a "High Temperature Threshold" event in the log with a classification of report. After the temperature returned below the threshold, the management card would log the same event message with a clear classification.</p> <p>All of the messages can be reports, but only a few can also be clear signals.</p>
ModuleName	This column displays the names of the line cards that generated the event messages.
Message	This column displays the event messages. The messages are described in Table 9.

Table 9 lists the event messages.

Table 9. Event Log Messages

Message	Chassis	Classification	Definition
<i>n</i> Voltage Failed	AT-CV5000	Report	The AT-PWR14 or AT-PWR15 Power Supply Module in the AT-CV5000 Chassis had an output voltage failure. The variable <i>n</i> can be 3.3V, 5V, or 12V and signals which voltage failed.
		Clear	The AT-PWR14 or AT-PWR15 Power Supply Module resumed normal operations or was replaced.
Copper port failure on remote linecard <i>n</i> .	AT-CV1200 AT-CV1203 AT-CV5000	Report	The twisted pair port on a remote AT-CM Line Card lost its link to its network device. This message requires remote peer management.
		Clear	The twisted pair port on a remote AT-CM Line Card established a link to its network device. This messages requires remote peer management.
CPM Card Reboot	AT-CV1200 AT-CV1203 AT-CV5000	Report	The AT-CV5M02 Management Card was reset.
CV1203 Local RPS Failure A/B	AT-CV1203	Report	One of the two external power supplies connected to the AT-CV1203 Chassis failed. (A failed power supply has no detectable output voltages.) “A” and “B” designate the power connectors on the back panel of the chassis. This message only appears if the AT-CV1203 Chassis has two power supplies and just one of the power supplies fails.
		Clear	A power supply connected to the AT-CV1203 Chassis resumed normal operations or was replaced.

Table 9. Event Log Messages

Message	Chassis	Classification	Definition
CV1203 RPS Failure on Remote Line Card <i>n</i>	AT-CV1203 AT-CV5000	Report	<p>The media converter line card in slot <i>n</i> of the AT-CV5000 Chassis received a report from its line card counterpart in a remote AT-CV1203 Chassis that one of the two power supplies connected to the remote chassis lost power. This message requires remote peer management. For background information, refer to “Dying Gasp Feature” on page 52. For instructions on how to configure the line cards for this feature, refer to Chapter 9, “Configuring AT-CM Line Cards for Dying Gasp” on page 229.</p> <p>If a remote AT-CV1203 Chassis loses all power and has at least one AT-CM Media Converter Line Card, it sends the dying gasp signal instead of this signal.</p>
		Clear	The media converter line card in slot <i>n</i> of the AT-CV5000 Chassis received a clear signal from its line card counterpart in a remote AT-CV1203 Chassis, indicating that power has been restored. This message requires peer-to-peer management.
Dying Gasp has Occurred on Remote Line Card <i>n</i>	AT-CV1203 AT-CV5000	Report	The media converter line card in slot <i>n</i> in the AT-CV5000 Chassis received the dying gasp signal from its line card counterpart in a remote AT-CV1203 Chassis. The remote line card sent the signal because the AT-CV1203 Chassis lost power. For further information, refer to Chapter 9, “Configuring AT-CM Line Cards for Dying Gasp” on page 229.
Fan Tray A/B: Fan Temperature Exceeds Limit	AT-CV1200 AT-CV1203 AT-CV5000	Report	The temperature of the chassis exceeded the temperature threshold.
		Clear	The temperature of the chassis returned below the temperature threshold.
Fan Tray A/B has been Installed	AT-CV5000	Report	The AT-CVFAN Fan Module was installed in the AT-CV5000 Chassis.

Table 9. Event Log Messages

Message	Chassis	Classification	Definition
Fan Tray A/B has been Removed	AT-CV5000	Report	The AT-CVFAN Fan Module was removed from the chassis.
Fan Tray Module A/B Fan <i>n</i> Failed	AT-CV1200 AT-CV1203 AT-CV5000	Report	A cooling fan stopped.
		Clear	A cooling fan resumed operations.
Line Card <i>n</i> Missing	AT-CV1200 AT-CV1203 AT-CV5000	Report	The line card in slot <i>n</i> was removed from the chassis.
		Clear	The line card removed from slot <i>n</i> was reinstalled in the slot.
Line Card <i>m</i> Port <i>n</i> Offline	AT-CV1200 AT-CV1203 AT-CV5000	Report	Port <i>n</i> on the line card in slot <i>m</i> lost its link to a network device.
Line Card <i>m</i> Port <i>n</i> Online	AT-CV1200 AT-CV1203 AT-CV5000	Report	Port <i>n</i> on the line card in slot <i>m</i> established a valid link with a network device.
Line Card <i>n</i> Reboot	AT-CV1200 AT-CV1203 AT-CV5000	Report	The line card in slot <i>n</i> was rebooted from using the AT-CV5M02 Management Card.
Power Module A/B has been Installed	AT-CV5000	Report	The AT-PWR14 or AT-PWR15 Power Supply Module was installed in the AT-CV5000 Chassis.
Power Module A/B has been Removed	AT-CV5000	Report	The AT-PWR14 or AT-PWR15 Power Supply Module was removed from the AT-CV5000 Chassis.

- To clear all the messages from the log, select **Clear Event Log** from the Event Log Menu.

**Web Browser** To view the event log from the web browser windows:

1. Select **Administrator** from the menu bar.
2. Click the **Event Log** tab to display the Event Log tab, shown in Figure 33. The messages are displayed from oldest to newest. Refer to Table 8 on page 99 for the descriptions of the columns and Table 9 on page 100 for the event messages and their meanings.

**Administration**

General Event Log Syslog Diagnostics Help

**Total Events: 11**  
**Displaying: 1 to 11**

Date	Time	Message
04/17/08	11:15:17	REPORT: Region22: Line Card 14 Port B Offline
04/17/08	11:15:17	REPORT: Region21: Line Card 11 Port A Offline
04/17/08	11:15:17	REPORT: Region21: Line Card 11 Port B Offline
04/17/08	11:15:17	REPORT: Region21: Copper port failure on remote linecard 11
04/17/08	11:15:18	REPORT: Region22: Copper port failure on remote linecard 14
04/17/08	11:15:35	REPORT: Region21: Line Card 11 Port A Online
04/17/08	11:15:35	REPORT: Region22: Line Card 14 Port A Online

Figure 31. Event Log Tab

3. To clear all of the messages in the log, click the **Clear Event Log** button at the bottom of the tab.

## Viewing the Activity Monitor

---

The activity monitor displays the event messages in real-time. For background information, refer to “Activity Monitor” on page 23.

**Menus** To view the activity monitor from the menus:

1. From the Main Menu, select **Administration**. The Administration Menu is shown in Figure 28 on page 98.
2. From the Administration Menu, select **Start Activity Monitor**.
3. From the Administration Menu, select **Activity Monitor** to display the monitor. An example of the Activity Monitor is shown in Figure 32. The monitor displays the messages as they occur on the line cards in the chassis.

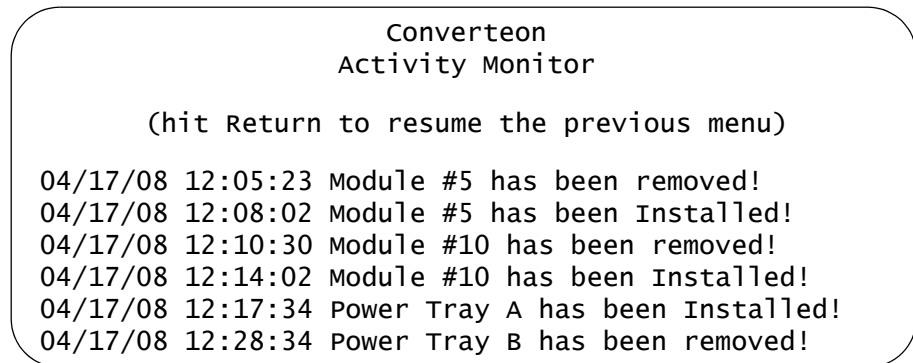


Figure 32. Activity Monitor

For the descriptions of the columns and messages, refer to Table 8 on page 99 and Table 9 on page 100.

4. To return to the Administration menu, press Return.
5. If you return to the Activity Monitor during the same management session, the monitor displays those event messages that occurred in the interim. If you start a new session, the monitor displays those events that occurred since the start of the management session.
6. To stop the activity monitor, select **Stop Activity Monitor**.

**Web Browser** The activity monitor is not supported in the web browser windows.

## Configuring the Syslog Client

---

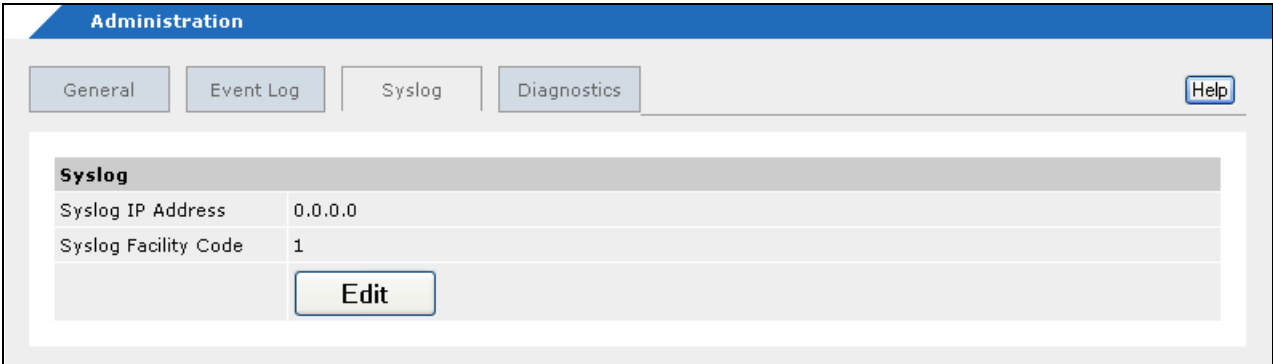
For background information, refer to “Syslog Client” on page 23.

**Menus** To configure the syslog client from the menus:

1. From the Main Menu, select **Administration** to display the Administration Menu shown in Figure 28 on page 98.
2. From the Administration Menu, select the **Syslog Server Address** field and enter the IP address of the syslog server on your network. To stop the management card from sending any further event messages to the server, enter 0.0.0.0 as the server address.
3. Select the **Syslog Facility Code** field and enter a facility code for the events. The management card adds this code to the messages when it sends the messages to the syslog server. The range is 0 to 23. The default is 1. The numerical codes are defined in the RFC 3164 standard.
4. To save your changes in the master configuration file, return to the Main Menu and select **Configuration** and **Save System and All Line Card Configurations**.

**Web Browser** To configure the syslog client from the web browser windows:

1. Select **Administration** from the menu bar.
2. Click the **Syslog** tab to display the tab in Figure 33.



Syslog	
Syslog IP Address	0.0.0.0
Syslog Facility Code	1

Figure 33. Syslog Tab

3. Click **Edit** to display the Syslog pop-up window.

4. Select the **Syslog IP Address** field and enter the IP address of the syslog server on your network. To stop the management card from sending any further event messages to the server, enter 0.0.0.0 as the server address.
5. To specify a facility code, select **Syslog Facility Code** and enter a facility code for the events. The management card adds this code to the messages when it sends the messages to the syslog server. The range is 0 to 23. The default is 1. The numerical codes are defined in the RFC 3164 standard.
6. Click **Update**.
7. To save your changes in the master configuration file, select the **Files** tab in the Configuration window and click **Save System Configuration and All Cards Configurations** and **Apply**.

## Configuring the 10/100Base-TX Port

---

The procedures in this section explain how to set the speed and duplex mode on the 10/100Base-TX port on the AT-CV5M02 Management Card. The management card uses this port to accomplish those management functions that require communications with your network, such as sending event messages to a syslog server or uploading or downloading files to a TFTP server. For background information, refer to “10/100Base-TX Port” on page 22.

---

### Note

The port cannot be disabled. Additionally, the port's wiring configuration is preset to MDI and cannot be changed.

---

**Menus** To configure the settings of the 10/100Base-TX port on the management card from the menus:

1. From the Main Menu, select **Module Status and Configuration**.
2. Select the management card from the menu to display the Module Configuration Menu shown in Figure 34.

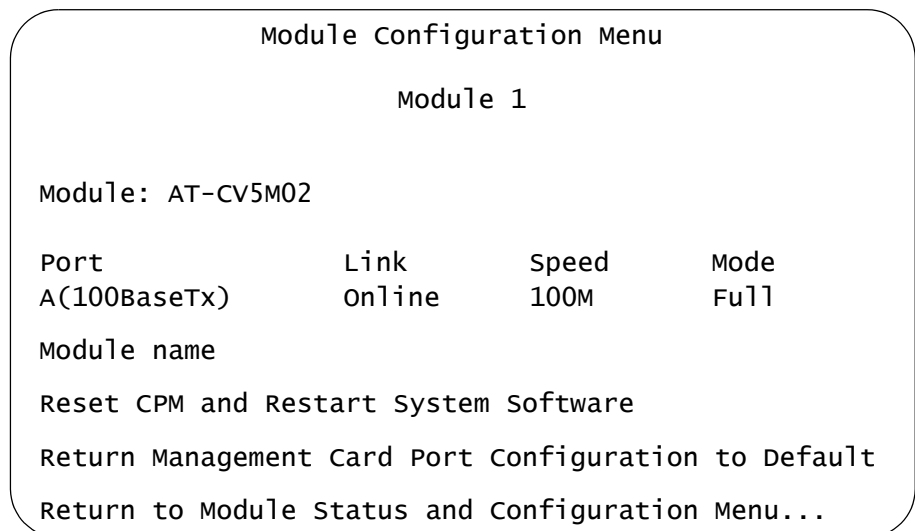


Figure 34. Module Configuration Menu (Management Card)

The columns in the Module Configuration Menu are described in Table 10.

Table 10. Module Configuration Menu for a Management Card

Column	Description
Port	The port type is 10/100Base-TX.
Link	The status of the link on the port. Possible values are: <input type="checkbox"/> Online: The port has established a link to a network device. <input type="checkbox"/> Offline: The port is not connected to a network device or has not established a link to a device.
Speed	The operating speed of the port. Possible values are 10M or 100M.
Mode	The duplex mode of the port. <input type="checkbox"/> Full - The port is operating in full-duplex mode. <input type="checkbox"/> Half - The port is operating in half-duplex mode.

3. Select **Port A (100Base-TX)** to display the Port Configuration Menu shown in Figure 35.

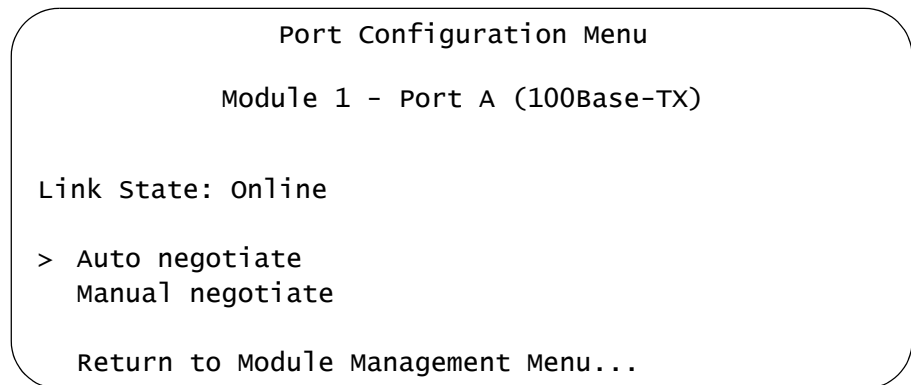


Figure 35. Port Configuration Menu for the 10/100Base-TX Port on the Management Card

4. Configure the settings of the port as needed. To activate Auto-Negotiation, select **Auto negotiate**. To set the speed and duplex mode manually, select **Manual negotiate** to display the additional parameters shown in Figure 36.

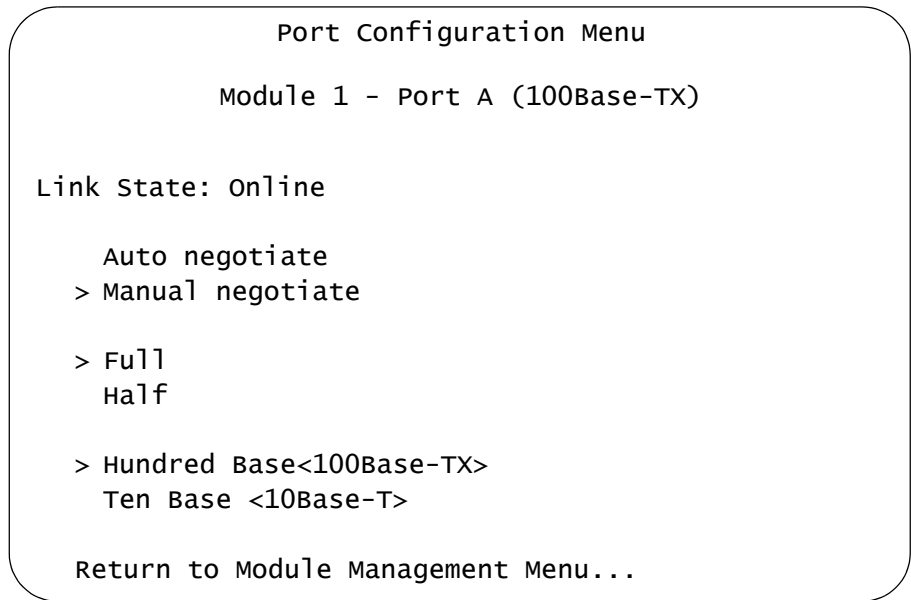


Figure 36. Port Configuration Menu for the 10/100Base-TX Port on the Management Card

The parameters in the menu are described in Table 11.

Table 11. Port Configuration Menu for the 10/100Base-TX Port on the Management Cards

Setting	Description
Auto negotiate Manual negotiate Full Half Hundred Base <100Base-TX> Ten Base <10Base-T>	<p>These selections are used to control the speed and duplex mode settings of the twisted pair port on the management cards. The Auto negotiate setting, the default setting, activates IEEE 802.1u Auto-Negotiation so that the speed and duplex mode of the port are established automatically. Auto-Negotiation is designed to ensure that the ports on the management card and the network device are operating at the same speed and that they are communicating at the highest possible common speed of the devices.</p> <p>The Manual negotiate setting deactivates Auto-Negotiation on a port so that you can set the parameters manually. When you select this option, additional settings are displayed in the menu.</p> <p>The Full and Half settings control the duplex mode of the port, which can be either full-duplex or half-duplex.</p> <p>The Hundred Base and Ten Base selections set a port's speed to 100 or 10 Mbps, respectively.</p>

Table 11. Port Configuration Menu for the 10/100Base-TX Port on the Management Cards

Setting	Description
Auto negotiate Manual negotiate Full Half Hundred Base <100Base-TX> Ten Base <10Base-T> (Continued)	When configuring a port, observe the following guidelines:  <input type="checkbox"/> If the network device connected to a line card port does not use Auto-Negotiation and has a fixed duplex mode of full duplex, disable Auto-Negotiation on the port and set the speed and duplex mode manually to avoid a duplex mode mismatch.

- To save your changes in the master configuration file, go to the Main Menu and select **Configuration** to display the Configuration menu and select **Save System and All Line Card Configurations**.

### Web Browser

To configure the 10/100Base-TX port on the management card from the web browser windows:

- Select **Module Status and Configuration** from the menu bar.
- In the Chassis View, click the 10/100Base-TX port on the management card. Alternatively, select the Menu View tab and click the name of the management card. The Port A tab for the management card is shown in Figure 37.

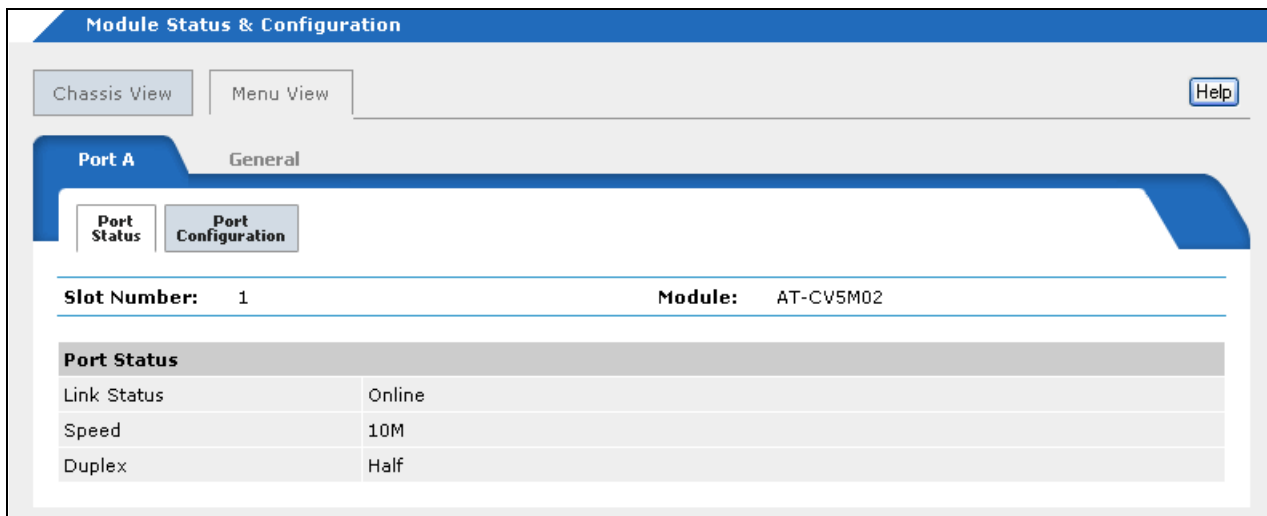


Figure 37. Port A Tab for the Management Card

3. Click the **Port Configuration** tab, shown in Figure 38.

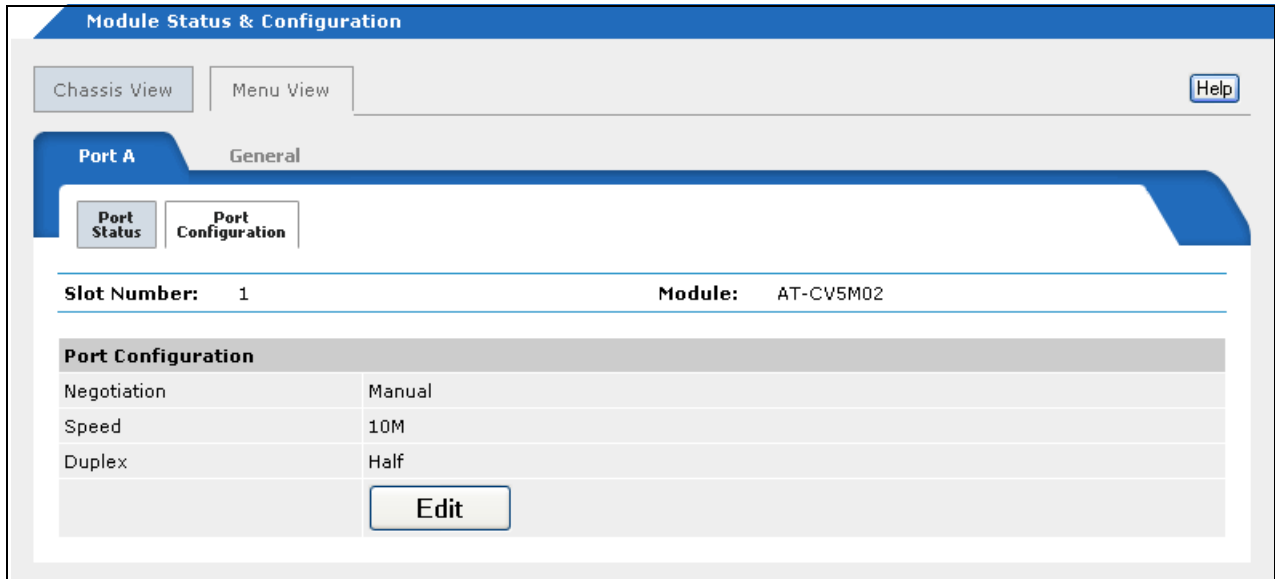


Figure 38. 10/100Base-TX Port on the Management Card

4. To adjust the settings of the port, click **Edit** to display the Port Configuration pop-up window.
5. Adjust the parameters as needed. The parameters are defined in Table 11 on page 109.
6. To save your changes in the master configuration file, select the **Files** tab in the Configuration window and click **Save System Configuration and All Cards Configurations** and **Apply**.

## Restoring the Default Setting on the 10/100Base-TX Port

---

These procedures are used to restore the default setting of Auto-Negotiation on the 10/100Base-TX port on the AT-CV5M02 Management Card. The procedures do not interrupt the network operations of the media converter line cards in the chassis.

---

**Note**

The 10/100Base-TX port has a wiring configuration of MDI. This is not adjustable.

---

- Menus** To restore the default setting of Auto-Negotiation on the 10/100Base-TX port from the menus:
1. From the Main Menu, select **Module Status and Configuration**.
  2. Select the AT-CV5M02 Management Card in the menu to display the Module Configuration Menu shown in Figure 34 on page 107.
  3. Select the **Return Management Card Port Configuration to Default** option.
  4. To save your changes in the master configuration file, go to the Main Menu and select **Configuration** to display the Configuration menu and select **Save System and All Line Card Configurations**.

- Web Browser** To restore the default setting of Auto-Negotiation on the 10/100Base-TX port from the web browser windows:
1. Select **Module Status and Configuration** from the menu bar.
  2. In the Chassis View, click the 10/100Base-TX port on the AT-CV5M02 Management Card. Alternatively, select the Menu View tab and click the name of the management card. The Port A tab for the management card is shown in Figure 37 on page 110.
  3. Select the **General** tab, shown in Figure 27 on page 97.
  4. Click **Return Management Card Port Configuration to Default Setting**.
  5. To save your changes in the master configuration file, select the **Files** tab in the Configuration window and click **Save System Configuration and All Cards Configurations** and **Apply**.

## Restoring the Default Values on the AT-CV5M02 Management Card

---

In this section are the procedures for restoring the default values to all of the following operating parameters on the AT-CV5M02 Management Card:

- IP address configuration
- Name, location, and contact
- IP addresses of SNMP trap receivers
- SNMPv1 and SNMPv2c community strings
- SNMPv3 configurations
- Management security (i.e., passwords, console timer, etc.)
- Network Time Protocol client
- Syslog client
- 10/100Base-TX port
- Temperature threshold
- Console port's baud rate

---

### Note

Before performing these procedures, save the current configurations of the AT-CM Line Cards in the master configuration file. For instructions, refer to "Saving Your Configuration Changes" on page 64.

---



---

### Note

A management card resets when its parameter settings are returned to the default values. It will not respond to management commands for one minute while it initializes its management software. To resume managing the device, start a local management session on the unit.

---

Restoring the default settings on the management card does not interrupt the network operations of the line cards in the chassis.

**Menus** To restore the default settings on the management card from the menus:

1. If the chassis has two management cards, remove the standby card.
2. From the Main Menu, select **Configuration**. The Configuration menu is shown in Figure 20 on page 80.
3. Select **Return System Configuration to Default**. A confirmation prompt is displayed.

4. Enter **Y** for Yes to restore the parameters on the management card to their default values or **N** for No to cancel the procedure.

If you respond with yes, the management card resets and your management session ends.

5. To resume managing the unit, wait one minute for the card to initialize its management software and then start a local management session on the card.
6. If the chassis has two management cards, reinstall the standby card.

## **Web Browser**

To restore the default settings on the management card from the web browser windows:

1. If the chassis has two AT-CV5M02 Management Cards, remove the standby card.
2. Click **Configuration** from the menu bar.
3. Click the **Files** tab, shown in Figure 14 on page 65.
4. Click the radio button for **Return Configuration in Management Card to Default** and click **Apply**.

The management card resets and your remote web browser management session ends.

5. To resume managing the unit, wait one minute for the card to initialize its management software and then start a local management session on the card.
6. If the chassis has two management cards, reinstall the standby card.

## Configuring the Temperature Threshold

---

The management card has a temperature threshold parameter to alert you in the event the temperature of the wiring closet exceeds operating norms. If the threshold is exceeded, the management card enters an event in the event log and sends an SNMP trap. The temperature is measured on the power supply near the cooling vents of the chassis and tends to reflect the ambient air temperature.

**Menus** To set the temperature threshold from the menus:

1. From the Main Menu, select **Configuration** to display the Configuration Menu shown in Figure 20 on page 80.
2. From the Configuration Menu, select **System Configuration** to display the menu in Figure 21 on page 80.
3. Select **Temperature Threshold Configuration** to display the Temperature Threshold Configuration Menu in Figure 39. The temperature threshold is given in Celsius ( $^{\circ}$  C).

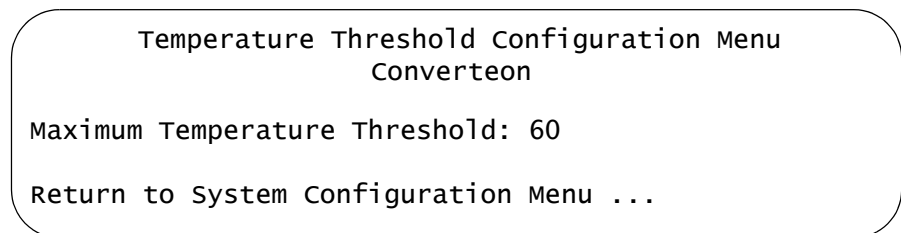


Figure 39. Temperature Threshold Configuration Menu

4. Select **Maximum Temperature Threshold** and enter a new value. The range is 0 to 75 $^{\circ}$  C. The default is 60 $^{\circ}$  C.
5. To save your changes in the master configuration file, return to the Configuration menu and select **Save System and All Line Card Configurations**.

**Web Browser** To set the temperature threshold from the web browser windows:

1. Select **Configuration** from the menu bar.
2. If the System tab is not selected, select it. The System tab is shown in Figure 23 on page 83.
3. Click **Edit** in the Temperature Threshold section.

4. In the Temperature Threshold pop-up window, click the **Maximum Temperature Threshold** field and enter a new value. The range is 0 to 75° C. The default is 60° C.
5. Click **Update**.
6. To save your changes in the master configuration file, select the **Files** tab in the Configuration window, click **Save System Configuration and All Cards Configurations** and click **Apply**.

## Activating a Standby AT-CV5M02 Management Card

---

The procedures in this section activate the standby AT-CV5M02 Management Card in a chassis that has two management cards. You might perform these procedures if the currently active management card is experiencing problems and you want to use the standby card to manage the chassis. For background information, refer to “Redundant Management Cards” on page 26.

These procedures do not interrupt the operations of the media converter line cards in the chassis. However, they do end your management session.

**Menus** To activate the standby management card from the menus:

1. From the Main Menu, select **Management Card Redundancy** to display the Management Card Redundancy Menu, shown in Figure 41.

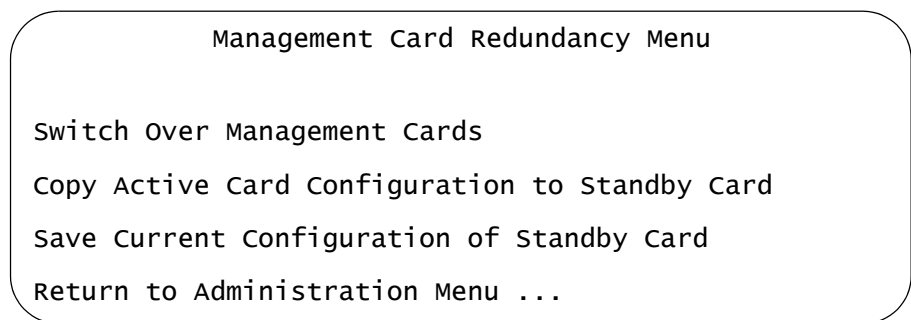


Figure 40. Management Card Redundancy Menu

2. Select **Switch Over Management Cards**. The following confirmation prompt is displayed.

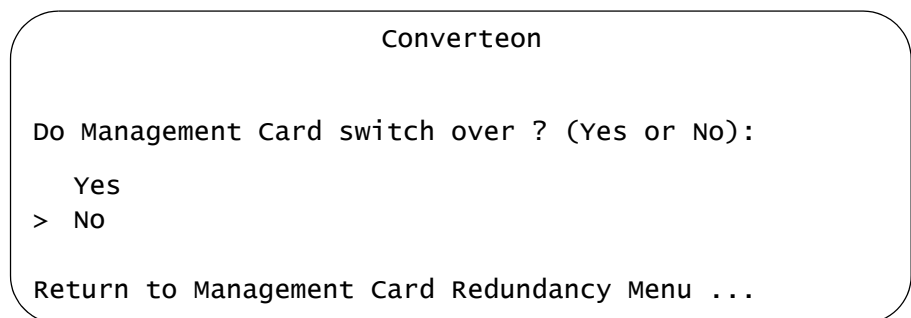


Figure 41. Confirmation Prompt for Switch Over Management Cards

3. Choose **Yes** to activate the switchover or **No** to cancel the procedure. If you select Yes, your management session ends as the active and standby management cards change states.

4. To resume managing the chassis, wait twenty to thirty seconds for the standby card to transition to the active state and, afterwards, start a new management session.

---

**Note**

For explanations of the two other selections in the Management Card Redundancy menu, refer to “Saving Your Configuration Changes” on page 64.

---

**Web Browser**

To activate the standby management card from the web browser windows:

1. Select **Management Card Redundancy** from the menu bar to display the tab in Figure 42.

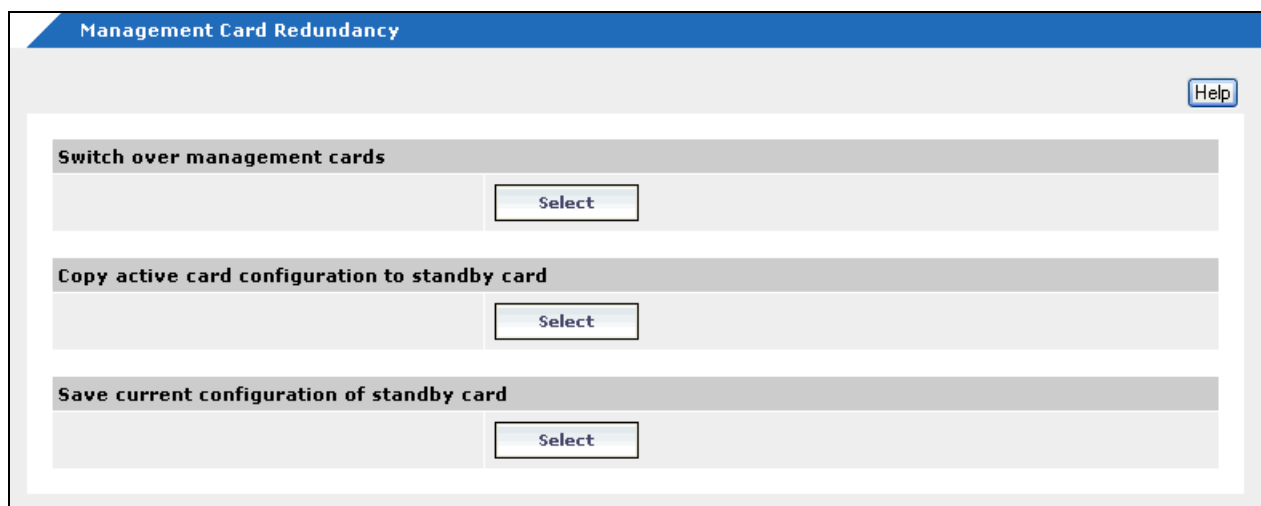


Figure 42. Management Card Redundancy Tab

2. In the section Switch Over Management Cards, click **Select**. A confirmation prompt is displayed.
3. In the confirmation prompt, click **Yes** and **Apply** to activate the standby card or **No** and **Apply** to cancel the procedure. If you select Yes, your management session ends as the active and standby management cards change states.
4. To resume managing the chassis, wait twenty to thirty seconds for the standby card to transition to the active state. Afterwards, start a new management session.

---

**Note**

For explanations of the two other selections in the Management Card Redundancy tab, refer to “Saving Your Configuration Changes” on page 64.

---

## Setting the Baud Rate of the Console Port

---

The RS-232 Console port on the front faceplate of the management card is used to locally manage the card. This type of management session is accomplished with a terminal or a computer with a terminal emulator program.

The following procedures are used to set the baud rate of the Console port. The baud rate is the only adjustable parameter on the port. Refer to "Starting a Local Management Session" on page 58 for all of the Console port settings.

---

**Note**

Changing the baud rate of the Console port during a local management session ends your management session. To resume managing the chassis, change the baud rate of your terminal or terminal emulator program.

---

**Menus** To set the baud rate of the Console port from the menus:

1. From the Main Menu, select **Configuration**. The Configuration Menu is shown in Figure 20 on page 80.
2. From the Configuration Menu, select **System Configuration** to display the menu in Figure 21 on page 80.
3. From the System Configuration Menu, select **Terminal Configuration**. The Terminal Configuration Menu is shown in Figure 43.

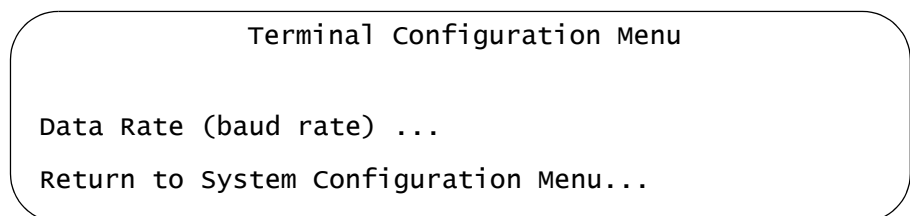


Figure 43. Terminal Configuration Menu

4. Select **Data rate (baud rate)** to display the Terminal Data Rate Menu shown in Figure 44.

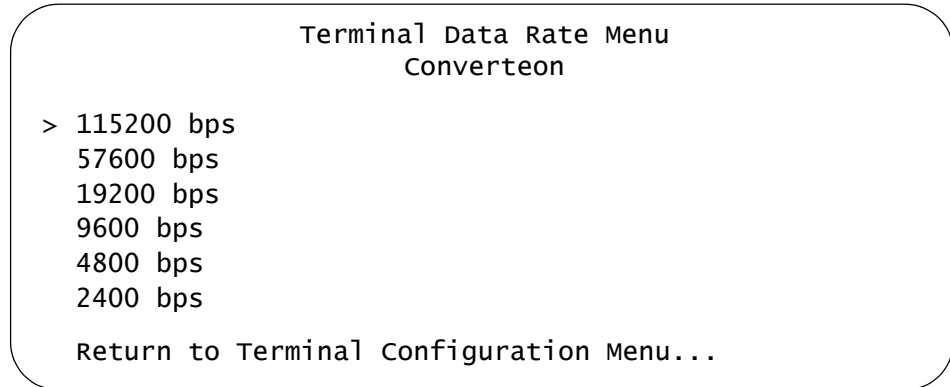


Figure 44. Terminal Data Rate Menu

5. From the Terminal Data Rate Menu, select the desired baud rate. The default is 115200 bps.

---

**Note**

If you are managing the chassis from a local management session, your session ends. To resume managing the chassis, change the baud rate of your terminal or terminal emulator program.

---

6. To save your changes in the master configuration file, return to the Configuration menu and select **Save System and All Line Card Configurations**.

## Web Browser

To set the baud rate of the Console port from the web browser windows:

1. Select **Configuration** from the menu bar.
2. If the System tab is not selected, select it. The System tab is shown in Figure 23 on page 83.
3. Click **Edit** in the Terminal Setting section.
4. In the Terminal Setting pop-up window, select a new baud rate from the pull down menu.
5. Click **Update**.
6. To save your changes in the master configuration file, select the **Files** tab in the Configuration window and click **Save System Configuration and All Cards Configurations** and **Apply**.

## Displaying the Operational Status of the Chassis

---

In this section are procedures for displaying operational information about the power supplies and fans in the chassis. The information also includes information about the management card, including its MAC address and the states of the flash memory and the Console port.

---

**Note**

These procedures do not perform any diagnostic utilities and are not disruptive to the operations of the management card or the line cards in the chassis.

---

**Menus** To view general information about the chassis from the menus:

1. From the Main Menu, select **Administration**. The Administration Menu is shown in Figure 28 on page 98.
2. From the Administration Menu, select **Diagnostics**. The Diagnostics Menu is shown in Figure 45.

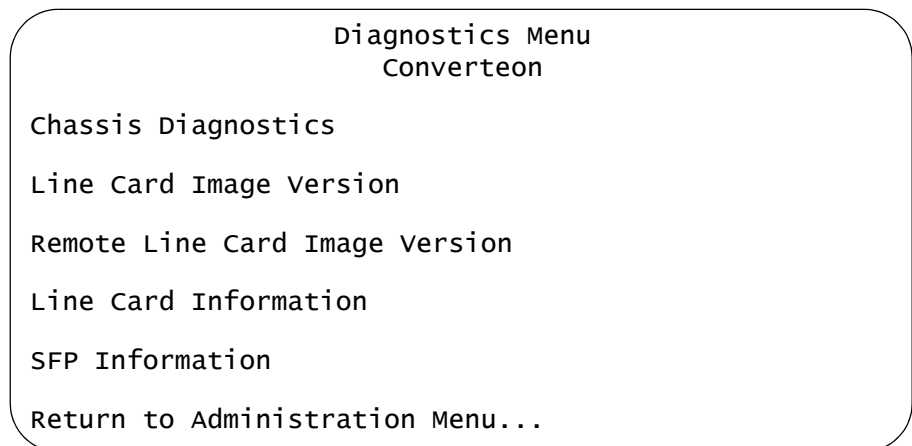


Figure 45. Diagnostics Menu

3. From the Diagnostics Menu, select **Chassis Diagnostics** to display the Chassis Diagnostics Menu. The example in Figure 46 is from the AT-CV5000 Chassis. The windows for the AT-CV1200 Chassis and the AT-CV1203 Chassis do not include power supply information. The information in this window is for viewing purposes only.

```

                                Chassis Diagnostics Menu

Serial Number:A02736
MAC Address 00:0C:46:98:22:5F
CONVERTEON Chassis: AT-CV5000 AC Revision 3.0.0

Running 0 days, 1 hours, 10 minutes, 9 seconds
Current Time: 12/08/07 01:10:47

Diagnostic Results:

Flash PROM           Good
Serial Interface     Good

RPSA                 Good      Temperature: 25 C
3.3V Power:         3.2 V      5V Power:       4.9 V      12V Power:     0.0 V
Fan Status:         Good      Fan1 Speed:    3924 RPM   Fan2 Speed:    3994 RPM

RPSB                 Not Present Temperature: 25 C
3.3V Power:         0 V      5V Power:       0 V      12V Power:     0.0 V
Fan Status:         Not Present Fan1 Speed:    Off       Fan2 Speed:    Off

Hit any key to continue ...

```

Figure 46. Chassis Diagnostics Menu

The information in the Chassis Diagnostics Menu is defined in Table 12.

Table 12. Chassis Diagnostics Menu

Row	Description
Serial Number	This field displays the serial number and hardware revision level of the chassis.
MAC Address	This field displays the MAC address of the backplane in the chassis. The management card uses this address as its MAC address when it communicates with your network through the 10/100Base-TX port.
Converteon Chassis	This field displays the chassis model name and revision level, such as "AT-CV5000 Revision 1.7."
Running	This field displays the number of hours, minutes, and seconds since the management card was last powered on or reset.
Current Time	This field displays the current date and time.

Table 12. Chassis Diagnostics Menu

Row	Description
Flash PROM	This field displays the status of the Flash PROM on the management card.
Serial Interface	This field displays the status of the Console port on the management card.
RPSA and RPSB	This field displays the status of the power supplies and fans, and the temperature and power voltage in the AT-CV5000 Chassis. A status of "Not present" indicates an empty power supply slot in the AT-CV5000 Chassis. Neither the AT-CV1200 Chassis nor the AT-CV1203 Chassis display this information.

**Web Browser** To view the operational information from the web browser windows:

1. Select **Administrator** from the menu bar.
2. Select the **Diagnostics** tab.
3. If the Chassis Diagnostics tab shown in Figure 47 is not selected, select it. This window is for viewing purposes only. The information in the window is described in Table 12 on page 122.

**Administration**

General | Event Log | Syslog | Diagnostics | Help

Chassis Diagnostics | Linecard Image Information | Remote Linecard Image Information | Linecard Information | SFP Information

**Chassis Information**

Serial Number	A02736
Mac Address	00:A0:D2:00:00:11
Converteon Chassis	CV-5000 XX
Running	0 days, 0 hours, 4 minutes, 40 hours
Current Time	00/00/00 00:04:38

**Chassis Dianostics**

Flash PROM	Good
Serial Interface	Good

RPSA	Good	Temperature	41 C		
3.3V Power	3.2 V	5V Power	4.9 V	12V Power	0.0 V
Fan Status	Not Present	Fan 1 Speed	Off	Fan2 Speed	Off

RPSB	Not Present	Temperature	0 C		
3.3V Power	0 V	5V Power	0 V	12V Power	0 V
Fan Status	Not Present	Fan 1 Speed	Off	Fan2 Speed	Off

Figure 47. Chassis Diagnostics Tab

## Pinging Network Devices

---

The procedure in this section is used to test for live connections between the 10/100Base-TX port on the AT-CV5M02 Management Card and other network devices. The management card transmits Internet Control Message Protocol (ICMP) echo requests from the 10/100Base-TX port and reports the results of the ping on the screen. You might perform this procedure if the management card is experiencing a problem communicating with another network device, such as a syslog server or a TFTP server.

The system requirements for this test are described in “Access to Your Network” on page 28

**Menus** To ping a network device from the menus:

1. From the Main Menu, select **Administration** to display the menu in Figure 28 on page 98.
2. Select **Ping a Remote System**. The following message is displayed:  

```
Please enter Station IP Address to ping:
```
3. Enter the IP address of the network device you want the management card to ping. The management card sends three ping echo requests and displays the results on the screen.
4. To return to the Administration Menu, press any key.

**Web Browser** This management function is not supported from the web browser windows.

## **Displaying Management Card Information**

---

To view general information about the AT-CV5M02 Management Card, refer to “Displaying the Version Numbers of the Management Software” on page 164 and “Displaying the MAC Addresses and Serial Numbers” on page 167.

## Chapter 5

# Configuring AT-CM and AT-CV Media Converter Line Cards

---

This chapter has the following sections:

- ❑ “Displaying the Status of the Line Cards” on page 128
- ❑ “Displaying the Parameter Settings on AT-CM Line Cards” on page 136
- ❑ “Configuring the Port Parameters on AT-CM Line Cards” on page 139
- ❑ “Setting the Operating Mode” on page 145
- ❑ “Assigning Names to AT-CM Line Cards” on page 149
- ❑ “Configuring the Maximum Frame Size on AT-CM2KOS Line Cards” on page 150
- ❑ “Setting the Auto-copy Feature” on page 151
- ❑ “Restoring the Default Settings” on page 153
- ❑ “Restoring the Last Saved Configuration” on page 157
- ❑ “Displaying Port Statistics” on page 160
- ❑ “Resetting Media Converter Line Cards” on page 162
- ❑ “Displaying the Version Numbers of the Management Software” on page 164
- ❑ “Displaying the MAC Addresses and Serial Numbers” on page 167
- ❑ “Displaying SFP Module Information” on page 170

## Displaying the Status of the Line Cards

**Menus** To view the states of the ports on the AT-CM and AT-CV Line Cards in the chassis, select **Module Status and Configuration** from the Main Menu. The Module Status and Configuration Menu is shown in Figure 48.

Module Status and Configuration  
Converteon

```

===== MODULE INFO =====
Mod_Name  CardTypeVer  ST  OperMode  IPC  AC  VER  ST  SP  FC  IngRL  EgrRL  OAM  ST  SP  FC  IngRL  EgrRL  AN
1  -----  AT-CV5M02  *  -----  800  -  V300  -  ---  -  ---  -  ---  *  100  -  ---  -  ---  -
2  Reg11  AT-CM202-v2  *  OamVisib  o**  N  V300  *  100  N  0  0  A  *  100  N  0  0  0  Y
3  Reg20  AT-CM202-v2  *  OamVisib  o*o  N  V300  *  100  N  0  0  *oo  *  100  N  0  0  0  Y
4  Reg21  AT-CM202-v2  *  OamVisib  o*o  N  V300  *  100  N  0  0  *oo  *  100  N  0  0  0  Y
5  Area2a  AT-CM202-v2  *  OamVisib  o*o  N  V300  *  100  N  0  0  *oo  *  100  N  0  0  0  Y
6  Area2b  AT-CM202-v2  *  OamVisib  o*o  N  V300  *  100  N  0  0  *oo  *  100  N  0  0  0  Y
7  a121  AT-CM202-v2  *  OamVisib  o*o  N  V300  *  100  N  0  0  *oo  *  100  N  0  0  0  Y
8  Reg12  AT-CM202-v2  *  OamVisib  o*o  N  V300  *  100  N  0  0  +oo  *  100  N  0  0  0  Y
9  AT-CM202-v2  *  OamVisib  o*o  N  V300  *  100  N  0  0  *oo  *  100  N  0  0  0  Y
10 AT-CM202-v2  *  OamVisib  o*o  N  V300  *  100  N  0  0  *oo  *  100  N  0  0  0  Y
11 AT-CV102  *  LinkTest  *  100  N  ---  ---  ---  *  100  -  ---  ---  ---  -
12 AT-CV102  *  LinkTest  *  100  N  ---  ---  ---  *  100  -  ---  ---  ---  -
13 AT-CV102  *  LinkTest  *  100  N  ---  ---  ---  *  100  -  ---  ---  ---  -
14 AT-CV102  *  LinkTest  *  100  N  ---  ---  ---  *  100  -  ---  ---  ---  -
15 AT-CV102  *  LinkTest  *  100  N  ---  ---  ---  *  100  -  ---  ---  ---  -

More ...
Return to Main Menu ...
    
```

Figure 48. Module Status and Configuration Menu

The columns in the menu are described in Table 13.

Table 13. Module Status and Configuration Menu

Column	Description
MODULE INFO	
Mod_Name	This column lists the chassis slot numbers and the names of the AT-CM Line Cards. For instructions on how to assign names to the line cards, refer to “Assigning Names to AT-CM Line Cards” on page 149. The AT-CV Line Cards do not support names.
CardTypeVer	This column displays the model names of the management cards and the line cards in the chassis. The model names of newer versions of the AT-CM Line Cards have suffixes, like “-v2”.
ST	This column displays the states of the management cards and the line cards. The possible states are: <ul style="list-style-type: none"> <li><input type="checkbox"/> * - The line card is operating normally.</li> <li><input type="checkbox"/> - - The state, which applies only to AT-CM Line Cards, indicates that the line card is initializing its management software.</li> </ul>

Table 13. Module Status and Configuration Menu

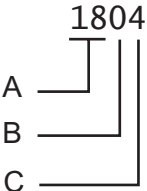
Column	Description
<p>OperMode</p>	<p>This column displays different information depending on the type of card. For the AT-CM and AT-CV Line Cards this column displays the operating modes of the line cards. For background information, refer to “Operating Modes” on page 42. The possible modes are:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> LinkTest - Link Test mode</li> <li><input type="checkbox"/> ML - MissingLink mode</li> <li><input type="checkbox"/> SML - Smart MissingLink mode</li> <li><input type="checkbox"/> OAM Visib - OAM Visible mode</li> <li><input type="checkbox"/> OAM Bypas - OAM Bypass mode</li> <li><input type="checkbox"/> LCMgmt - The operating mode is controlled by the card's DIP switches.</li> <li><input type="checkbox"/> Resetting - The line card is initializing its management software. This state only applies to AT-CM Line Cards.</li> </ul> <p>For the AT-CV5M02 Management Card this column displays the card's state. The possible states are:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Active - The management card is in the active state.</li> <li><input type="checkbox"/> Standby - The management card is in the standby mode. This state only applies to redundant AT-CV5M02 Management Cards. For background information, refer to “Redundant Management Cards” on page 26.</li> </ul>
<p>IPC</p>	<p>This column displays utilization information of the backplane by the management card and the AT-CM Line Cards. This information is intended for manufacturing and test purposes.</p> <p>For the AT-CV5M02 Management Card this column displays the following information:</p> <div style="text-align: center;">  </div> <p>A This is the slot number of the line card the management card is currently polling. For example, the value “12” indicates that the management card is polling the AT-CM Line Card in slot 12. Slots that have AT-CV Line Cards are not polled by the management card.</p> <p>B This is the total number of messages the management card is waiting to transmit over the backplane to the AT-CM Line Cards.</p>

Table 13. Module Status and Configuration Menu

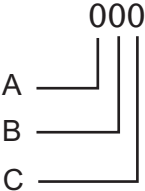
Column	Description
IPC (Continued)	<p>C This is the total number of responses the management card is waiting to receive from the AT-CM Line Cards.</p> <p>For AT-CM Line Cards this column displays the following information:</p> <div style="text-align: center;">  </div> <p>A This toggles to “*” when the management card is sending a message to the line card in the slot.</p> <p>B This toggles to “*” when the management card is waiting to transmit a message to the line card.</p> <p>C This displays the status of a line card’s response to the last transmitted message from the management card. A successful response is indicated by “*” while a bad response or no response is signalled with “o”.</p> <p>This column does not apply to the AT-CV Line Cards.</p>
AC	<p>This column displays the status of the auto-copy feature for those chassis slots that contain AT-CM Line Cards. For background information, refer to “Configuration Files” on page 29. The possible states are:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> N for No - The auto-copy feature is not enabled on the slot. The AT-CM Line Card uses its own configuration file to set its parameter settings.</li> <li><input type="checkbox"/> Y for Yes - The auto-copy feature is activated on the slot. The configuration settings for the AT-CM Line Card in the slot are provided by the management card from the master configuration file.</li> </ul> <p>The AT-CM70S Line Card and the AT-CV Line Cards do not support the auto-copy feature.</p>
VER	<p>This column displays the version numbers of the management software programs on the AT-CV5M02 Management Card and the AT-CM Line Cards. This field will be blank for AT-CM Line Cards that have AT-S73 Management Software earlier than Version 3.0.0. This field will also be blank for AT-CV Line Cards because they do not have management software.</p>

Table 13. Module Status and Configuration Menu

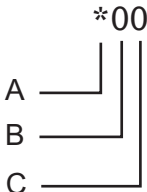
Column	Description
FIBER PORT or COPPER PORT	
ST	<p>This column displays the states of the ports. The possible states are:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> * - The port has establish a link to a network device.</li> <li><input type="checkbox"/> o - The port has not establish a link to a network device.</li> </ul>
SP	<p>This column displays the speeds of the ports. The possible speeds are:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> 10 - 10 Mbps</li> <li><input type="checkbox"/> 100 - 100 Mbps</li> <li><input type="checkbox"/> 1G - 1 Gbps</li> </ul>
FC	<p>This column displays the status of flow control on the ports of the AT-CM Line Cards. The possible states are:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Y - Flow control is enabled on the port.</li> <li><input type="checkbox"/> N - Flow control is disabled on the port.</li> </ul>
IngRL	<p>This column displays the settings of the ingress rate limiting filters on the ports on the AT-CM Line Cards. The value "0" means rate limiting has not been set on the port. This is the default setting. For instructions on setting this parameter, refer to "Configuring the Port Parameters on AT-CM Line Cards" on page 139. This feature is not supported on the AT-CV Line Cards.</p>
EgrRL	<p>This column displays the settings of the egress rate limiting filters on the ports on the AT-CM Line Cards. The value "0" means rate limiting has not been set on the port. This is the default setting. For instructions on setting this parameter, refer to "Configuring the Port Parameters on AT-CM Line Cards" on page 139. This feature is not supported on the AT-CV Line Cards.</p>
OAM	<p>This column applies only to AT-CM Line Cards operating in the OAM visible or the OAM bypass mode. It displays the following OAM client information:</p> <div style="text-align: right; margin-right: 50px;"> <p>*00</p>  </div>

Table 13. Module Status and Configuration Menu

Column	Description
OAM (Continued)	<p>A This displays the operational state of the OAM client on Port A, the fiber optic port, on a line card. The possible states are:</p> <ul style="list-style-type: none"> <li>* - Operational</li> <li>A - Active Send Local</li> <li>D - Disabled</li> <li>L - Active Send Local</li> <li>M - Peer Remote Reject</li> <li>P or W - Passive Wait</li> <li>R - Peer Local Reject</li> <li>1 - Active Send Remote 1</li> <li>2 - Active Send Remote 2</li> </ul> <p>B This alternates between “*” and “o” when the port is transmitting OAMPDUs. Otherwise, it remains “o”.</p> <p>C This alternates between “*” and “o” when the port is receiving OAMPDUs. Otherwise, it remains “o”.</p> <hr/> <p><b>Note</b>                      To support the OAM-based features, the AT-CM Line Cards have to be in the OAM operational state. Achieving this state can take a line card up to two minutes when it is powered on or reset, because it has to initialize its management software and negotiate the OAM state with its remote counterpart.</p> <hr/> <p>This column does not apply to the AT-CV5M02 Management Card or the AT-CV Line Cards.</p>
AN	<p>This column displays the status of Auto-Negotiation on the twisted pair ports on the AT-CM Line Cards. The possible states are:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Y - Auto-Negotiation is enabled on the port. The speed and duplex mode are set automatically. This is the default setting.</li> <li><input type="checkbox"/> N - Auto-Negotiation is disabled on the port. The speed and duplex mode were set manually.</li> </ul>

## Web Browser

To view the states of the ports on the line cards from the web browser windows, click **Module Status & Configuration** in the menu bar. The web browser windows have a Chassis View and a Menu View. The Chassis View is an illustration of the front panel of the chassis. The information is static. To refresh the view, simply click **Module Status & Configuration** again.

To view or configure the parameters of the AT-CM Line Cards or the AT-CV5M02 Management Card, click a port on a card. You can configure only one card at a time.

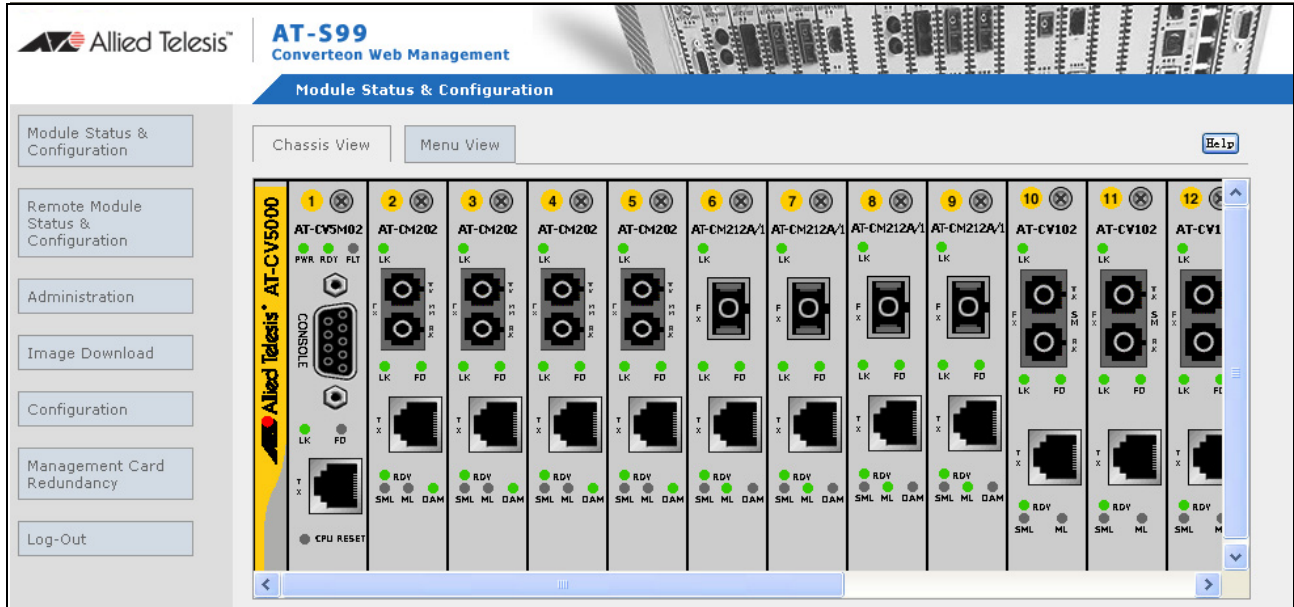


Figure 49. Chassis View

The Menu View, shown in Figure 50 on page 134, lists all of the line cards in the chassis and displays the states of the links of their ports. The information in this view is automatically refreshed every few seconds. The columns in the table are described in Table 14 on page 134. To view or configure the parameters of the line cards or a management card, click the model name of the card. You can configure only one card at a time.

Module Status & Configuration					
Chassis View		Menu View			
Module	Status	Link (A)	Link (B)	Opmode/OAM	
1	AT-CV5M02		Online/10		
2	AT-CM202	On	Online/100	Online/100	OAM Visible/Operational
3	AT-CM202	On	Online/100	Online/100	OAM Visible/Operational
4	AT-CM202	On	Online/100	Online/100	OAM Visible/Operational
5	AT-CM202	On	Online/100	Online/100	OAM Visible/Operational
6	AT-CM212A/1	On	Online/100	Online/100	OAM Visible/Operational
7	AT-CM212A/1	On	Online/100	Online/100	OAM Visible/Operational
8	AT-CM212A/1	On	Online/100	Online/100	OAM Visible/Operational
9	AT-CM212A/1	On	Online/100	Online/100	OAM Visible/Operational
10	AT-CV102	On	Online/100	Online/100	Link Test
11	AT-CV102	On	Online/100	Online/100	Link Test
12	AT-CV102	On	Online/100	Online/100	Link Test
13	AT-CV102	On	Online/100	Online/100	Link Test
14	AT-CV102	On	Online/100	Online/100	Link Test
15	(Not Inserted)				
16	(Not Inserted)				
17	(Not Inserted)				
18	(Not Inserted)				
19	LED	On			
20	(Not Inserted)				
21	RPSA	On			
22	RPSB	Off			

Figure 50. Menu View

Table 14. Module Status and Configuration Window

Column	Description
Module	This column lists the chassis slot numbers and the model names of the management cards and the line cards in the chassis. Model names of newer versions of the AT-CM Line Cards have suffixes, like “-v2”.
Status	This column displays the status of the cards: The possible values are: <ul style="list-style-type: none"> <li><input type="checkbox"/> On - The card is operating normally.</li> <li><input type="checkbox"/> Off - The line card is initializing its management software. This state applies only to AT-CM Line Cards.</li> <li><input type="checkbox"/> Standby - The AT-CV5M02 Management Card is in the standby state. For background information, refer to “Redundant Management Cards” on page 26.</li> </ul>

Table 14. Module Status and Configuration Window

Column	Description
Link (A)	<p>This column displays the states of Port A on the AT-CM and AT-CV Line Cards. This is a fiber optic port on all of the line cards. This column also displays the status of the 10/100Base-TX port on the AT-CV5M02 Management Card. The possible states are:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Online - The port has established a link to a network device. The speed of the port is included.</li> <li><input type="checkbox"/> Offline - The port has not established a link to a network device.</li> </ul>
Link (B)	<p>This column displays the states of Port B on the AT-CM and AT-CV Line Cards. The cable medium of Port B, fiber optic or twisted pair copper, will depend on the line card. The possible states are:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Online - The port has established a link to a network device. This state includes the speed of the port.</li> <li><input type="checkbox"/> Offline - The port has not established a link to a network device.</li> </ul>
OpMode/OAM	<p>This column displays the operating modes of the line cards. The possible modes are:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Link Test</li> <li><input type="checkbox"/> MissingLink</li> <li><input type="checkbox"/> Smart MissingLink</li> <li><input type="checkbox"/> OAM Visible</li> <li><input type="checkbox"/> OAM Bypass</li> </ul> <p>For AT-CM Line Cards that are operating in the OAM visible mode, this column also includes the state of the OAM client on Port A, the fiber optic port. The possible OAM states are:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Operational</li> <li><input type="checkbox"/> Disabled</li> <li><input type="checkbox"/> Passive Wait</li> <li><input type="checkbox"/> Active Send Local</li> <li><input type="checkbox"/> Active Send Remote 1</li> <li><input type="checkbox"/> Active Send Remote 2</li> <li><input type="checkbox"/> Peer Local Reject</li> <li><input type="checkbox"/> Peer Remote Reject</li> </ul> <p>The AT-CM Line Cards have to be in the OAM operational state to support the OAM-based features. Achieving this state can take a line card up to two minutes when it is powered on or reset, because it has to initialize its management software and negotiate the OAM state with its remote counterpart.</p>

## Displaying the Parameter Settings on AT-CM Line Cards

**Menus** To view the current parameter settings of the AT-CM Line Cards from the menus:

1. From the Main Menu, select **Module Status and Configuration** to display the Module Status and Configuration menu shown in Figure 48 on page 128.
2. From the Module Status and Configuration menu, select the AT-CM Line Card you want to view. You can view only one line card at a time. The Module Configuration Menu in Figure 53 on page 139 is displayed.
3. Select **Line Card Configuration** to display the menu in Figure 62 on page 153.
4. Select **Display Current Configuration**. An example of the window is shown in Figure 51.

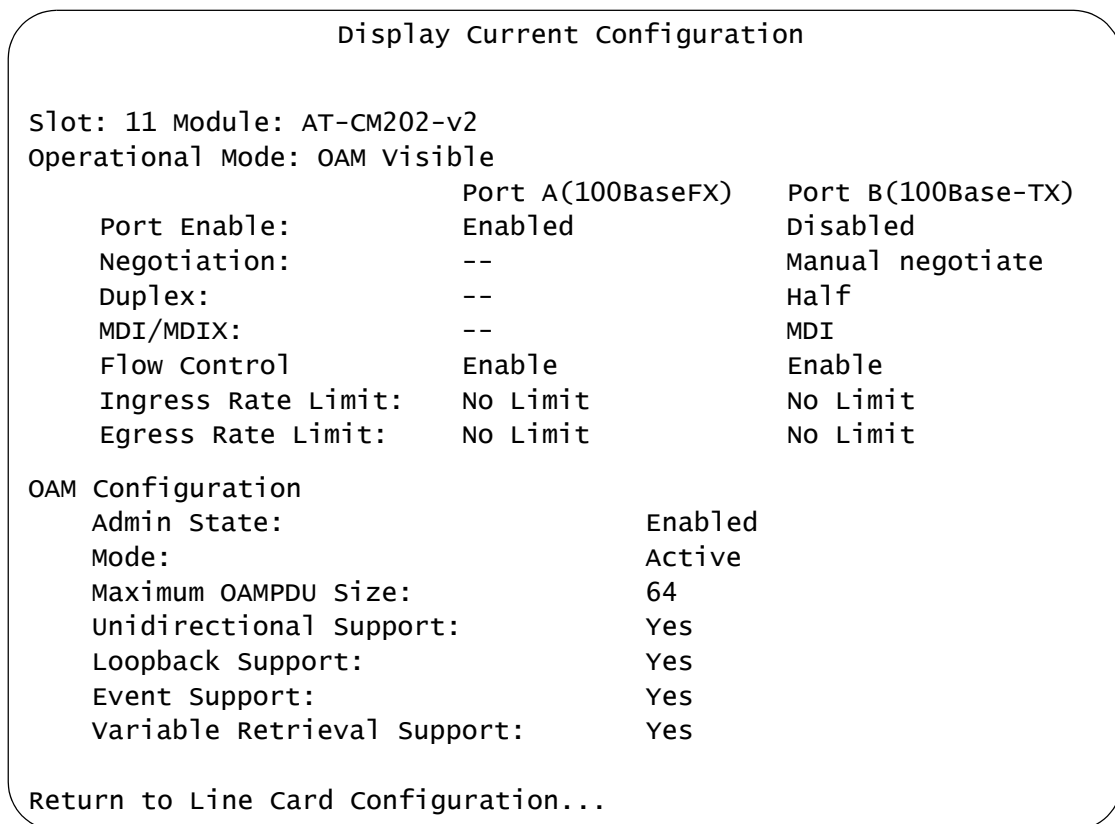


Figure 51. Display Current Configuration Window

This window is for viewing purposes only. The parameters for the fiber optic port and the twisted pair port are described in Table 16 on page 141. The OAM settings, described in Table 25 on page 205, are only displayed for line cards set to the OAM visible mode or the OAM bypass mode.

## Web Browser

To view the current parameter settings of the AT-CM Line Cards from the web browser windows:

1. Select **Module Status & Configuration** from the menu bar.
2. In the Chassis View, click either of the ports on the AT-CM Line Card you want to view. Alternatively, select the Menu View tab and click the model name of the line card. You can view only one line card at a time.
3. Select the **Line Card Configuration** tab.
4. Select the Current Configuration tab, shown in Figure 52.

**Module Status & Configuration**

Chassis View | Menu View | Help

Port A | Port B | Setting | **Line Card Configuration**

Auto-copy | **Current Configuration** | Last Saved Configuration | Default Configuration

**Slot Number:** 5      **Module:** AT-CM202

**Operation Mode:** OAM Visible      **Save Current Configuration**

Current Configuration	Port A (100Base FX)	Port B (100Base - TX)
Port Enable	Enabled	Enabled
Negotiation	--	Manual negotiate
Duplex	--	Half
MDI / MDIX	--	Auto MDI/MDIX
Ingress Rate Limit	8 Mbps	8 Mbps
Egress Rate Limit	8 Mbps	8 Mbps

OAM Configuration	
Admin State	Enabled
Mode	Active
Maximum OAMPDU Size	1518
Unidirectional Supprt	Yes
Loopback Support	Yes
Event Support	No
Variable Retrieval Support	Yes

Figure 52. Current Configuration Tab

This window is for viewing purposes only. The parameters for the fiber optic port and the twisted pair port are described in Table 16 on page 141. The OAM settings, described in Table 25 on page 205, are only displayed when the operating mode of a line card is set to the OAM visible or OAM bypass mode. For an explanation of the Save Current Configuration button, refer to “Saving Your Configuration Changes” on page 64.

## Configuring the Port Parameters on AT-CM Line Cards

### Note

The port settings on AT-CV Line Cards are not adjustable.

**Menus** To configure the parameter settings on the ports on AT-CM Line Cards from the menus:

1. From the Main Menu, select **Module Status and Configuration** to display the Module Status and Configuration menu, shown in Figure 48 on page 128.
2. From the Module Status and Configuration menu, select the AT-CM Line Card you want to configure. You can configure only one line card at a time. The current settings for the line card's two ports are displayed in the Module Configuration Menu. An example is shown Figure 53.

Module Configuration Menu			
Converteon			
Module 4			
Module: AT-CM202-v2			
Port	Link	Speed	Mode
A(100BaseFX)	online	100M	Full
B(100BaseTX)	online	100M	Full
Module Name			
Configure Operating Mode			
Display DIP Switch Setting			
Line Card Configuration			
Return to Module Status and Configuration ...			

Figure 53. Module Configuration Menu (Media Converter Line Card)

The columns in the table are defined in Table 15.

Table 15. Module Configuration Menu

Column	Description
Module	This field displays the model name of the line card. Names of newer versions of the cards include suffixes, like "v2."

Table 15. Module Configuration Menu

Column	Description
Port	This column identifies the port types.
Link	This column displays the states of the links between the ports and the network devices connected to the ports. The possible states are: <ul style="list-style-type: none"> <li data-bbox="683 485 1398 548"><input type="checkbox"/> Online: The port has established a link to a network device.</li> <li data-bbox="683 569 1398 632"><input type="checkbox"/> Offline: The port is not connected to a network device or has not established a link to a device.</li> </ul>
Speed	This column displays the current speeds of the ports, in Mbps. For a port to display a speed, it has to be linked to a network device.
Mode	This column displays the duplex modes of the ports. For a port to display a duplex mode, it has to be linked to a network device. The possible duplex modes for the ports are: <ul style="list-style-type: none"> <li data-bbox="683 936 1024 961"><input type="checkbox"/> Full: Full-duplex mode.</li> <li data-bbox="683 982 1024 1008"><input type="checkbox"/> Half: Half-duplex mode.</li> </ul>

3. Select the port you want to configure. You can configure only one port at a time. This displays the Port Management Menu shown in Figure 54.

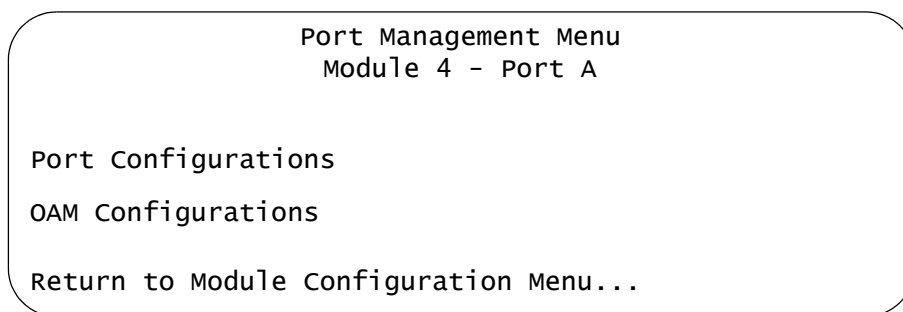


Figure 54. Port Management Menu

**Note**

The OAM Configurations selection only applies to Port A on AT-CM Line Cards set to the OAM visible mode or the OAM bypass mode. Otherwise, the selection is hidden from view. The AT-CV Line Cards do not support OAM.

4. Select **Port Configurations**. The Port Configuration Menu for the selected port is displayed. The options in the menu will vary depending on the type of port and card. The example in Figure 55 is for a twisted pair port.

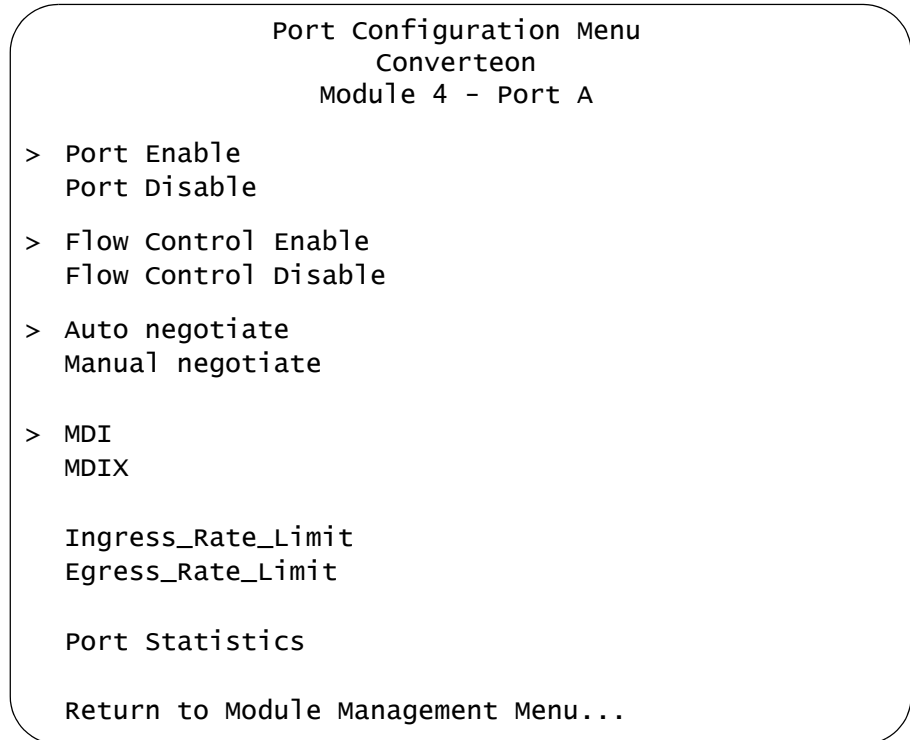


Figure 55. Port Configuration Menu

5. Configure the settings of the port, as needed. Table 16 explains all of the possible parameters for both twisted pair and fiber optic ports.

Table 16. Port Configuration Menu for Both Fiber Optic Ports and Twisted Pair Ports

Setting	Description
Port Enable Port Disable	These two selections enable and disable a port. When a port is enabled, it forwards traffic to and from the network device connected to it. This is the default setting. When a port is disabled, it doesn't forward traffic. You might disable a port if there is a problem with the cable or with the network device connected to it. You might also disable unused ports to secure them from unauthorized connections.
Flow Control Enable Flow Control Disable	Flow control regulates the flow of network traffic on ports set to full-duplex mode. When flow control is enabled on a port on a line card, the port issues pause packets whenever it needs to stop the network device from sending packets. The default setting for flow control is enabled.

Table 16. Port Configuration Menu for Both Fiber Optic Ports and Twisted Pair Ports

Setting	Description
Auto negotiate Manual negotiate Full Half Hundred Base <100Base-TX> Ten Base <10Base-T>	<p>These selections control the speed and duplex mode settings of the twisted pair ports on the AT-CM Line Cards. The Auto negotiate setting, the default setting, activates IEEE 802.1u Auto-Negotiation which configures the speed and duplex mode automatically.</p> <p>The Manual negotiate setting deactivates Auto-Negotiation on a port so that the parameters can be set manually. Selecting this option displays additional settings.</p> <p>The Full and Half settings establish the duplex mode of the port, which can be either full-duplex or half-duplex.</p> <p>The Hundred Base and Ten Base selections set a port's speed to 100 or 10 Mbps, respectively.</p> <p>Here are guidelines for setting the speed or duplex mode on a port:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> If the network device connected to a port on a line card does not support Auto-Negotiation and has a fixed duplex mode of full duplex, disable Auto-Negotiation on the port and set the speed and duplex mode manually to avoid a duplex mode mismatch.</li> <li><input type="checkbox"/> To operate at 1000 Mbps, the twisted pair port on the AT-CM2KOS Line Card has to be set to Auto-Negotiation. You can not manually set the port to 1000 Mbps.</li> </ul>
MDI MDIX	<p>When the twisted pair port is set to Auto-Negotiation, the wiring configuration is set automatically with Auto-MDI/MDIX. When Auto-Negotiation is disabled, the MDI/MDIX setting is manually controlled with these two selections.</p>
Ingress Rate Limit Egress Rate Limit	<p>These selections control the flow of network traffic to and from the ports on the AT-CM Line Cards. The rate limits, which are in kilobits and megabits per second, can be applied separately to the two ports on the line cards. Rate limits are used for storm prevention and to protect against the formation of bottlenecks in a network topology.</p> <p>The Ingress Rate Limit controls the number of bits per second a port accepts from the device connected to it. The port discards any frames exceeding the limit. For example, an ingress rate limit of 128k limits a port to no more than 128 kilobits per second in traffic flow from its network device. Traffic above the threshold is discarded by the port.</p>

Table 16. Port Configuration Menu for Both Fiber Optic Ports and Twisted Pair Ports

Setting	Description
Ingress Rate Limit Egress Rate Limit (Continued)	The Egress Rate Limit controls the number of bits per second a port transmits to the network device connected to it. Again, traffic that exceeds the limit is discarded before it is transmitted by the port.
Port Statistics	For information on this menu option, refer to “Displaying Port Statistics” on page 160.

6. To save your changes in the master configuration file, return to the Module Configuration Menu and select **Line Card Configuration** and **Save Line Card Configuration**.

### Web Browser

To configure the parameter settings of the ports on the AT-CM Line Cards from the web browser windows:

1. Select **Module Status & Configuration** from the left menu bar.
2. In the Chassis View, click the line card port you want to configure. Alternatively, select the Menu View tab and click the name of the line card. You can configure only one line card at a time.
3. Click the **Port A** tab to configure the fiber optic port on the media converter line card or the **Port B** tab to configure the twisted pair port. You can configure only one port at a time.

- Click the **Port Configuration** tab to display the current settings of the port. The example in Figure 56 is from Port B, the twisted pair port, on a line card.

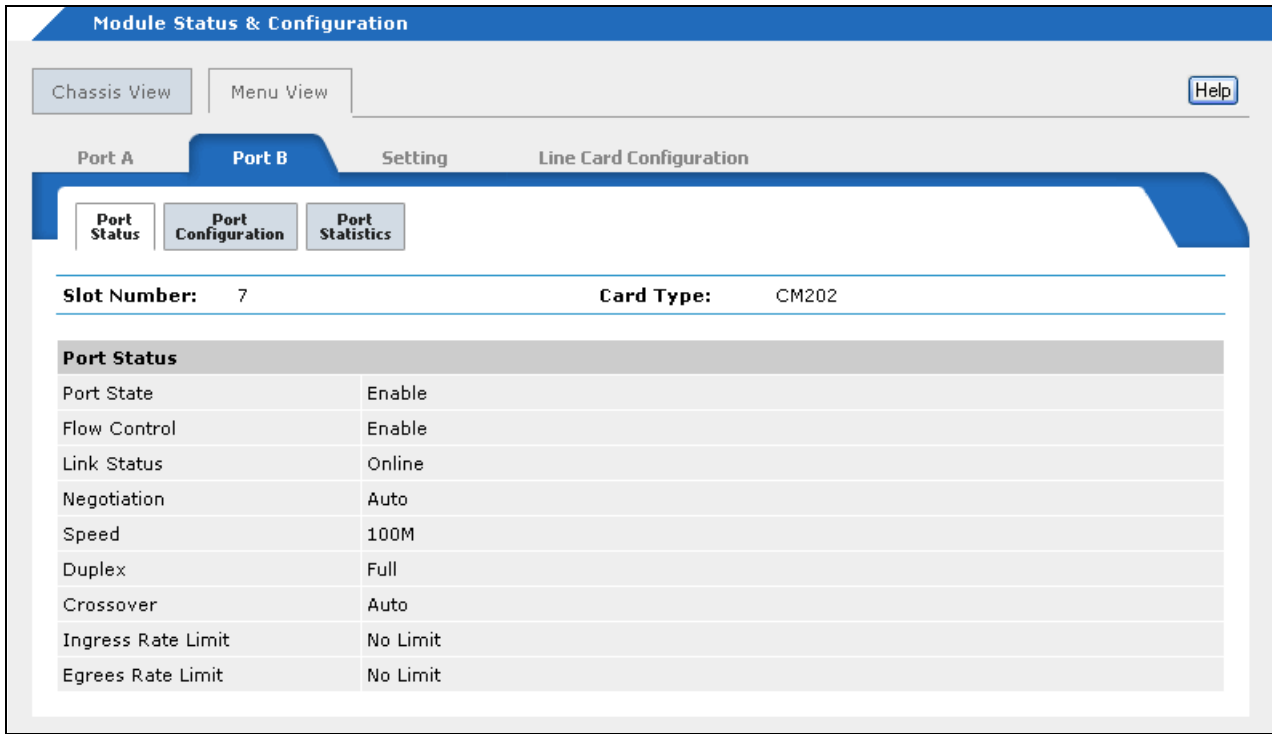


Figure 56. Port Configuration Window

- To adjust the settings, click **Edit** to display the Port Configuration pop-up window.
- Adjust the parameters, as needed. The parameters are defined in Table 16 on page 141.
- Click **Update**. The new parameter settings take effect immediately on the port.
- To save your changes in the master configuration file, click the **Line Card Configuration** tab, the **Current Configuration** tab, and the **Save Current Configuration** button.

## Setting the Operating Mode

---

For background information, refer to “Operating Modes” on page 42.



### Caution

This procedure resets a line card, disrupting its normal operations. Some network traffic may be lost. When an AT-CM Line Card is reset, it immediately resumes forwarding network traffic. However, it uses the default values for its parameter settings while it initializes the management software, which takes approximately one minute. Afterwards, the card configures its operating parameters from the settings in its configuration file or from the management card. The AT-CV Line Cards do not have management software and immediately resume normal network operations.

---

**Menus** To change the operating modes of the AT-CM and AT-CV Line Cards from the menus:

1. From the Main Menu, select **Module Status and Configuration** to display the Module Status and Configuration menu shown in Figure 48 on page 128.
2. From the Module Status and Configuration menu, select the line card you want to configure. You can configure only one line card at a time. The Module Configuration Menu in Figure 53 on page 139 is displayed.
3. From the Module Configuration Menu, select **Configure Operating Mode** to display the Operating Mode Config Menu, shown in Figure 57. The menu lists the available operating modes for the line card. The AT-CV Media Converter Line Cards do not support the OAM bypass and OAM visible modes.

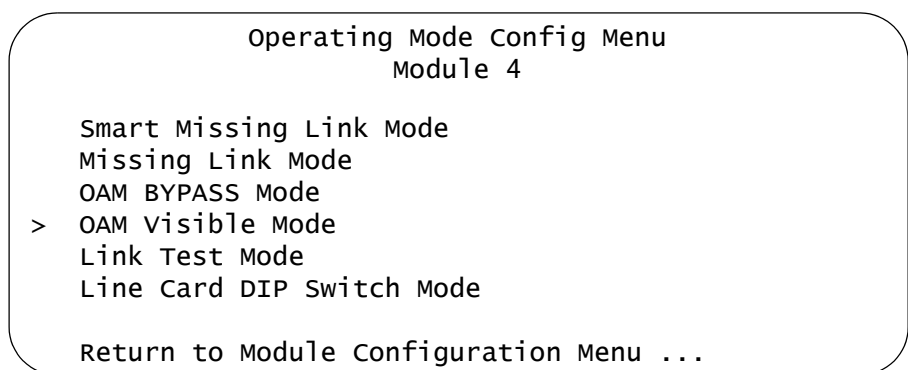


Figure 57. Operating Mode Config Menu

4. Select the new operating mode for the line card from the menu. You can select only one operating mode. The “Line Card DIP Switch Mode” selection activates the DIP switches on the line card so that the operating mode is controlled with the switches instead of the management software.

---

**Note**

If you set the operating mode through the software, the DIP switches on the card remain deactivated even if you move the card to a different slot or a different chassis. To reactivate the switches, install the card in a chassis that has the management card and select “Line Card DIP Switch Mode” from the Operating Mode Config Menu.

---

The following prompt is displayed:

```
warning: Changing the Operation Mode will reset the
line card.
Change Operation Mode now? <Yes or No>:
```

5. Type **Y** to continue or **N** to cancel the procedure. This prompt is displayed:

```
If auto-copy is enable, operation mode change need to be
saved to take affect.
Save line card configuration before rebooting? (Yes or
No):
```

6. Type **Y** for yes to update the master configuration file on the management card with the new setting for the card’s operating mode. This step is especially important if the auto-copy feature is activated on the card’s slot. If the card’s operating mode isn’t saved in the master configuration file, the new setting will not take affect because the card, after resetting, will simply revert to its previous operating mode. If you are not sure whether or not the auto-copy feature is enabled on the slot, select Yes anyway. There is little likelihood you would ever respond with No to this prompt. (This step isn’t applicable to the AT-CM70S Line Card because it doesn’t support the auto-copy feature.)

The line card resets and the management software displays the Module Status and Configuration menu again. AT-CM Line Cards have to initialize their management software and configure their operating parameters, a process that takes approximately one minute, before they can resume normal operations. In contrast, AT-CV Line Cards immediately return to normal operations because they do not have management software.

**Web Browser** To set the operating modes of the AT-CM and AT-CV Line Cards from the web browser windows:

1. Select **Module Status & Configuration** from the menu bar.
2. In the Chassis View, click one of the ports on the line card you want to configure. Alternatively, select the Menu View tab and click the name of the line card. You can configure only one line card at a time.
3. Click the **Setting** tab, shown in Figure 58.

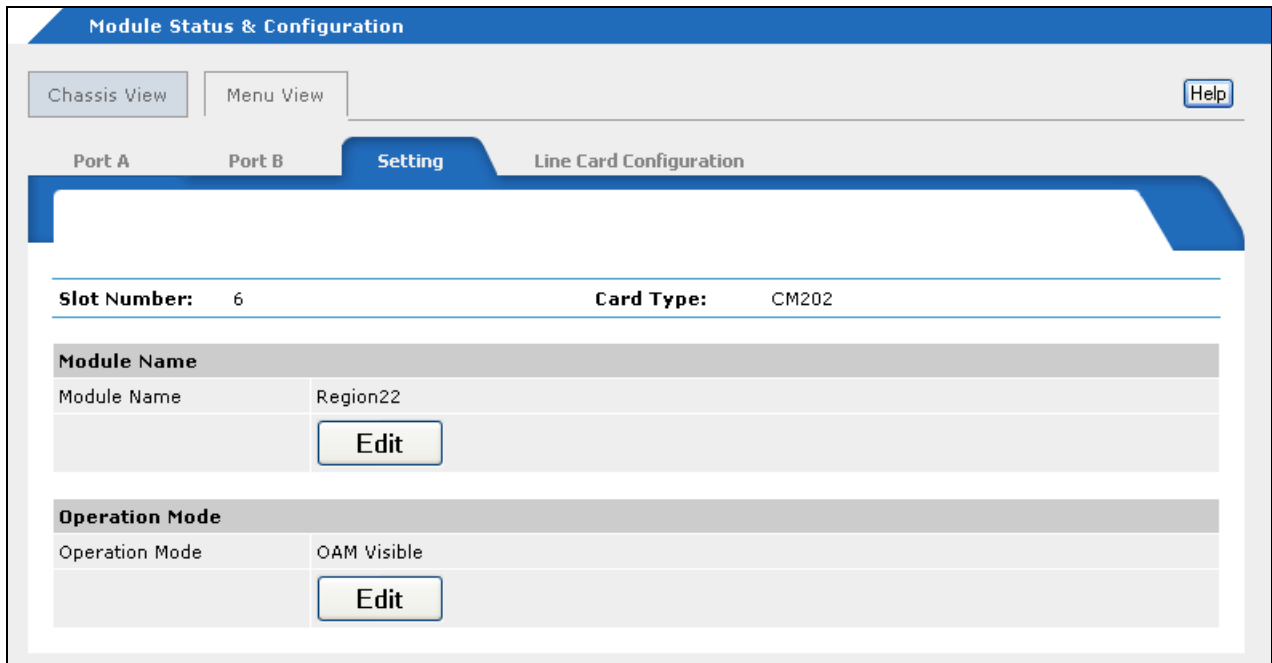


Figure 58. Setting Window

4. Click **Edit** in the Operation Mode section of the window.
5. In the Operation Mode pop-up window, select the new operating mode for the line card from the pull-down menu. You can select only one operating mode. The “Line Card DIP Switch Mode” selection activates the DIP switches on the line card so that the operating mode is controlled with the switches instead of the management software.
6. Click **Update**.

The management card automatically updates its master configuration file with the new setting for the line card's operating mode. Afterwards, the Module Status and Configuration menu is displayed again.

The line card resets. When the operating mode is changed on an AT-CM Line Card, the device has to initialize its management software and configure its operating parameters before resuming normal operations. In contrast, the AT-CV Line Cards immediately return to

normal operations because the cards in that series do not have management software.

## Assigning Names to AT-CM Line Cards

---

- Menus** To assign names to the AT-CM Line Cards from the menus:
1. From the Main Menu, select **Module Status and Configuration** to display the Module Status and Configuration menu shown in Figure 48 on page 128.
  2. From the Module Status and Configuration menu, select the line card you want to name. You can configure only one line card at a time. The Module Configuration Menu in Figure 53 on page 139 is displayed.
  3. From the Module Configuration Menu, select **Module Name** and enter the new name for the card. The name can be up to eight alphanumeric characters. Spaces and special characters are not allowed.
  4. To save your changes in the master configuration file, select **Line Card Configuration** and **Save Line Card Configuration**. *Or*, return to the Main Menu and select **Configuration** and **Save System and All Line Card Configurations**.

- Web Browser** To assign names to the AT-CM Line Cards from the web browser windows:
1. Select **Module Status & Configuration** from the menu bar.
  2. In the Chassis View, click a port on the line card you want to assign a name. Alternatively, select the Menu View tab and click the name of the line card. You can configure only one line card at a time.
  3. Click the **Setting** tab, shown in Figure 58.
  4. Click **Edit** in the Module Name section of the window.
  5. In the Module Name pop-up window, enter the new name for the card. The name can be up to eight alphanumeric characters. Spaces and special characters are not allowed.
  6. Click **Update**.
  7. To save your changes in the master configuration file, select **Configuration** from the menu bar. From the Configuration window, click the **Files** tab, **Save System Configuration and All Cards Configurations**, and **Apply**.

## Configuring the Maximum Frame Size on AT-CM2KOS Line Cards

---

The AT-CM Line Cards can handle packets up to 1522 bytes. This is not adjustable, except on the AT-CM2KOS Line Card, which can handle packets up to 1632 bytes. To adjust the maximum packet size on the AT-CM2KOS Line Card, perform the procedure in this section.

**Menus** To adjust the maximum packet sizes on AT-CM2KOS Line Cards from the menus:

1. From the Main Menu, select **Module Status and Configuration**. The Module Status and Configuration Menu is shown in Figure 48 on page 128.
2. Select the AT-CM2KOS Line Card you want to configure. This displays the Module Configuration Menu for the line card. An example is shown in Figure 53 on page 139.
3. From the Module Configuration Menu, select **Configure Max Frame Size** to display the Max Frame Size Config Menu, shown in Figure 59.

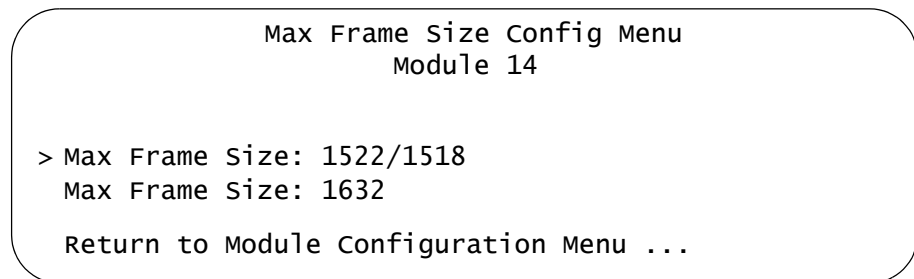


Figure 59. Max Frame Size Config Menu

4. From the **Max Frame Size Config Menu**, select one of the following frame sizes:  
**1522/1518**  
Allows frames up to 1522 bytes. This is the default value.  
**1632**  
Allows frames of up to 1632 bytes.  
The line card immediately implements your change.
5. To save your changes in the master configuration file, return to the Module Configuration Menu and select **Line Card Configuration** and **Save Line Card Configuration**.

**Web Browser** This procedure is not supported in the web browser windows.

## Setting the Auto-copy Feature

---

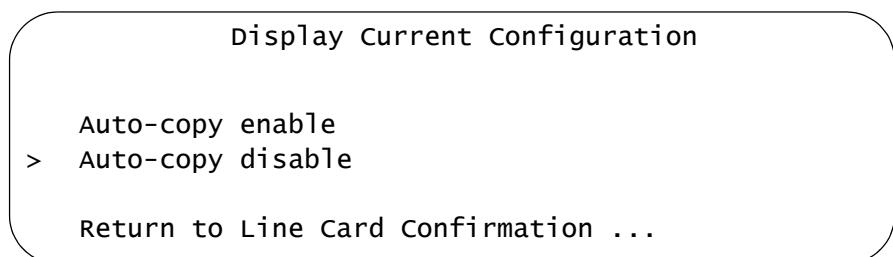
These procedures set the auto-copy feature on the chassis slots that contain AT-CM Line Cards. Auto-copy determines the source of the configuration settings of a line card. A line card in a slot where this feature is disabled use the configuration file in its own flash memory to set its parameters whenever it is reset or powered on. In contrast, a line card in a slot where this feature is enabled receives its configuration settings from the management card on the master configuration file. For further information, refer to “Configuration Files” on page 29.

Review the following before performing these procedures:

- ❑ The auto-copy setting for a slot is stored in the master configuration file on the management card. It is not stored in the configuration file in the flash memory of a line card. Consequently, the AT-CM Line Cards do not carry this setting with them when you install them in different slots or chassis.
- ❑ The auto-copy feature is not supported on the AT-CM70S Line Card or the AT-CV Line Cards.

**Menus** To set the auto-copy feature from the menus:

1. From the Main Menu, select **Module Status and Configuration** to display the Module Status and Configuration menu shown in Figure 48 on page 128.
2. From the Module Status and Configuration menu, select the AT-CM Line Card you want to configure. You can configure only one line card at a time. The Module Configuration Menu in Figure 53 on page 139 is displayed.
3. Select **Line Card Configuration** to display the menu in Figure 62 on page 153.
4. Select **Auto-copy Line Card Configuration**. The following prompt is displayed.



```
Display Current Configuration

Auto-copy enable
> Auto-copy disable

Return to Line Card Confirmation ...
```

Figure 60. Auto-copy Line Card Configuration Prompt

5. Select the desired setting for the auto-copy feature for the line card's slot. The default setting is disabled. If you enable auto-copy and later replace this line card with another card of the same model, the new card will be assigned the same parameter settings as this card.
6. To save your changes in the master configuration file, return to the Line Card Configuration Menu and select **Save Line Card Configuration**.

## Web Browser

To set the auto-copy feature from the web browser windows:

1. Select **Module Status & Configuration** from the menu bar.
2. In the Chassis View, click either of the ports on the AT-CM Line Card you want to configure. Alternatively, select the Menu View tab and click the model name of the line card. You can configure only one line card at a time.
3. Select the **Line Card Configuration** tab.
4. Select the **Auto-copy** tab, shown in Figure 61.

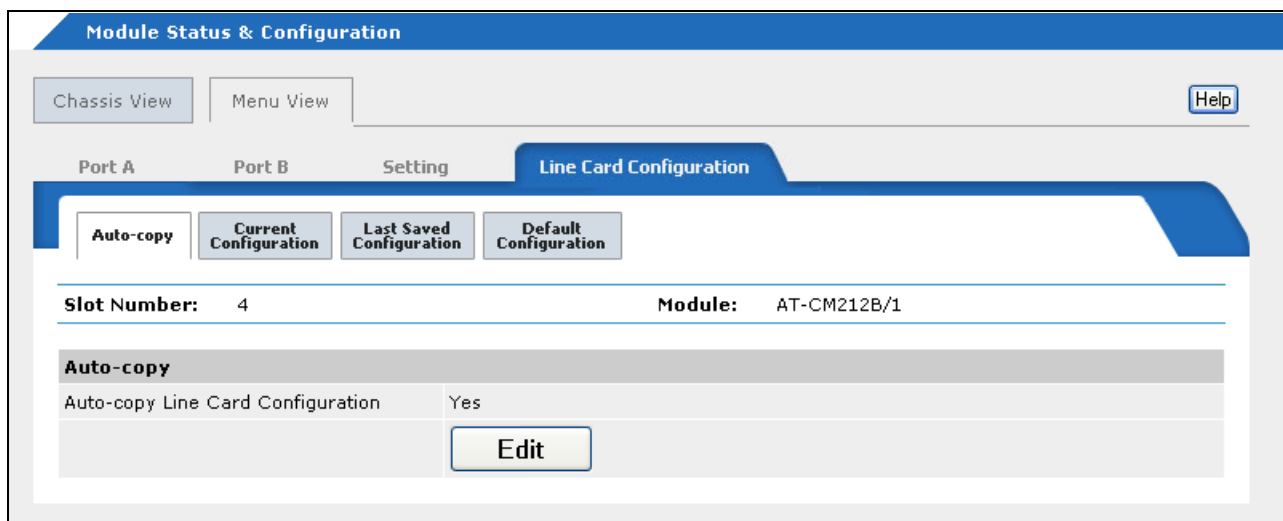


Figure 61. Auto-copy Tab

5. Click **Edit**.
6. In the pop-up window, select the new setting for the auto-copy feature.
7. Click **Update**.
8. To save your changes in the master configuration file, select the **Current Configuration** tab and click **Save Current Configuration**.

## Restoring the Default Settings

---

The procedures in this section are used to restore the default settings on the AT-CM Line Cards.



### Caution

These procedures are disruptive to network operations. Some network traffic may be lost. A line card whose current operating mode is not the OAM visible mode has to initialize its management software after restoring the default values. Although the card immediately resumes forwarding network traffic, it will be unresponsive to management commands for one minute during the initialization process.

---

These procedures are not supported on the AT-CM70S Line Card or the AT-CV Line Cards.

**Menus** To return the parameter settings of the AT-CM Line Cards to the default settings from the menus:

1. From the Main Menu, select **Module Status and Configuration** to display the Module Status and Configuration menu shown in Figure 48 on page 128.
2. From the Module Status and Configuration menu, select the AT-CM Line Card you want to return to the default settings. You can configure only one line card at a time. The Module Configuration Menu in Figure 53 on page 139 is displayed.
3. Select **Line Card Configuration** to display the Line Card Configuration Menu in Figure 62.

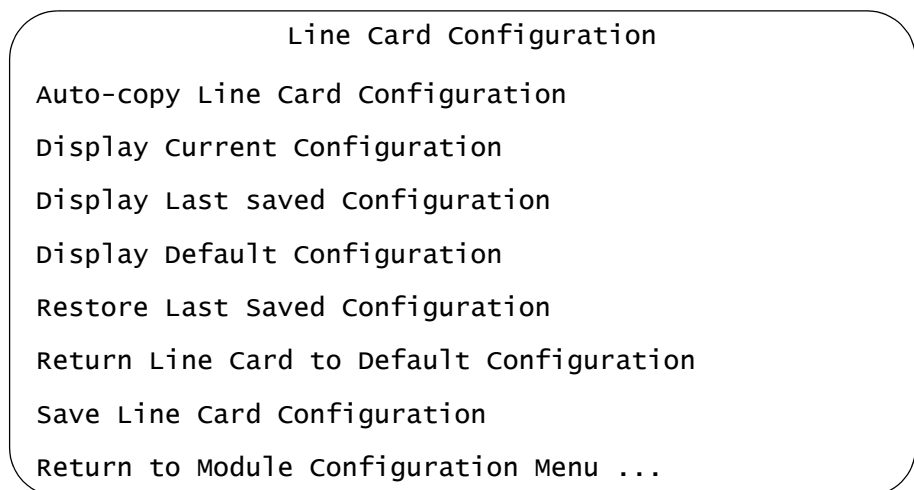


Figure 62. Line Card Configuration Menu

- To view the default settings of the line card prior to activating them, select **Display Default Configuration**. An example of the window is shown in Figure 63.

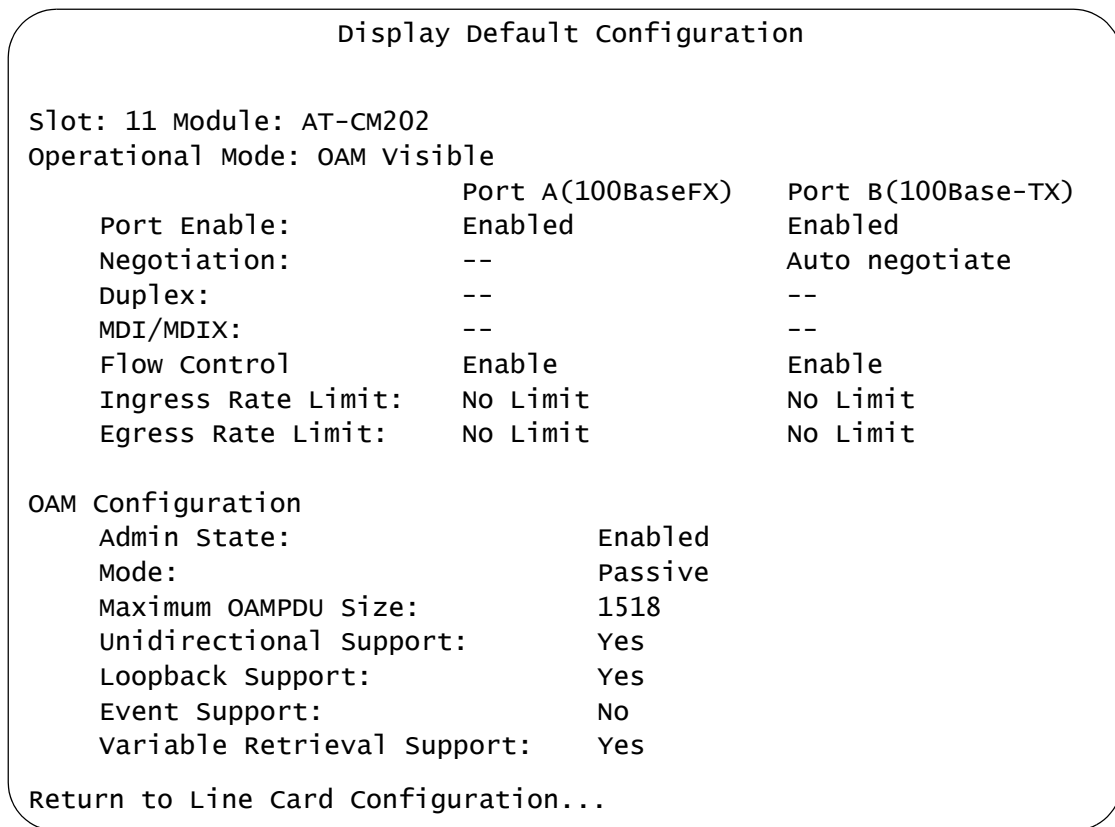


Figure 63. Display Default Configuration Window

- To return the parameter settings on the line card to the default values, select **Return Line Card to Default Configuration** from the Line Card Configuration Menu.
- At the confirmation prompt, select **Yes** to return the parameter settings on the line card to the default values or **No** to cancel the procedure. If you select Yes, the parameter settings on the card return to the default settings. If the card's previous operating mode was OAM visible, the card resumes normal network operations almost immediately. If, however, the card's previous operating mode was another operating mode, the card has to initialize its management software, a process that takes about one minute. During this process, this message is displayed on the screen:

Setting operation mode and resetting line card.

- To save your changes in the master configuration file, wait for the line card to finish initializing its management software and then select **Save Line Card Configuration** from the Line Card Configuration Menu.

## Web Browser

To return the parameter settings of the AT-CM Line Cards to the default settings from the web browser windows:

- Select **Module Status & Configuration** from the menu bar.
- In the Chassis View, click either port on the AT-CM Line Card you want to configure. Alternatively, select the Menu View tab and click the name of the line card. You can configure only one line card at a time.
- Click the **Line Card Configuration** tab.
- Select the **Default Configuration** tab, shown in Figure 64.

**Module Status & Configuration**

Chassis View | Menu View | Help

Port A | Port B | Setting | **Line Card Configuration**

Auto-copy | Current Configuration | Last Saved Configuration | **Default Configuration**

**Slot Number:** 14      **Card Type:** CM202

**Operation Mode**    OAM Visible    [Return to Default Configuration](#)

Default Configuration	Port A (100Base FX)	Port B (100Base - TX)
Port Enable	Enabled	Enabled
Negotiation	--	Auto negotiate
Duplex	--	--
MDI / MDIX	--	--
Flow Control	Enable	Enable
Ingress Rate Limit	No Limit	No Limit
Egress Rate Limit	No Limit	No Limit

OAM Configuration	
Admin State	Enabled
Mode	Passive
Maximum OAMPDU Size	1518
Unidirectional Supprt	Yes
Loopback Support	Yes
Event Support	No
Variable Retrieval Support	Yes

Figure 64. Default Configuration Tab

This tab displays the line card's default settings.

5. To return the parameter settings on the line card to the default values, click **Return to Default Configuration**.

The parameter settings on the line card are returned to their default settings and the Menu View is displayed. A line card whose previous operating mode was OAM visible resumes normal network operations almost immediately. However, if the card's previous operating mode was not OAM visible, it has to initialize its management software, a process that takes approximately one minute.

6. To save your changes in the master configuration file, wait for the line card to finish initializing its management software. Then select **Configuration** from the menu bar. From the Configuration window, select the **Files** tab and click **Save System Configuration and All Cards Configurations** and **Apply**.

## Restoring the Last Saved Configuration

---

These procedures restore AT-CM Line Cards to their last saved configurations. The configurations are obtained from the master configuration file on the management card. You might perform this procedure to discard parameter changes that you made to a line card but did not save, or to configure a new line card with the save settings as its predecessor in the chassis. For more information, refer to “Configuration Files” on page 29.

This procedure is not applicable to the AT-CV Line Cards.



### Caution

Restoring a line card to the last saved configuration may disrupt network operations. Some traffic may be lost. A line card whose current operating mode is different from its last saved configuration has to initialize its management software after it receives the new configuration from the management card. During the initialization process, which takes approximately one minute, the line card forwards network traffic using the default values for its parameter settings.

---

**Menus** To restore the last saved configuration of a line card from the menus:

1. From the Main Menu, select **Module Status and Configuration** to display the Module Status and Configuration menu shown in Figure 48 on page 128.
2. From the Module Status and Configuration menu, select the AT-CM Line Card you want to configure. You can configure only one line card at a time. The Module Configuration Menu in Figure 53 on page 139 is displayed.
3. Select **Line Card Configuration** to display the menu in Figure 62 on page 153.
4. To view the parameter settings of the card's last saved configuration before activating them on the line card, select **Display Last Saved Configuration**.
5. To return the line card to its last saved configuration, return to the Line Card Configuration menu and select **Restore Last Saved Configuration**.
6. At the confirmation prompt, select **Yes** to restore the settings or **No** to cancel the procedure.

**Web Browser** To restore the last saved configuration to an AT-CM Line Card from the web browser windows:

1. Select **Module Status & Configuration** from the menu bar.
2. In the Chassis View, click either of the ports on the line card you want to configure. Alternatively, select the Menu View tab and click the model name of the line card. You can configure only one line card at a time.
3. Select the **Line Card Configuration** tab.
4. To restore the previous configuration to the line card, select the **Last Saved Configuration** tab, shown in Figure 65.

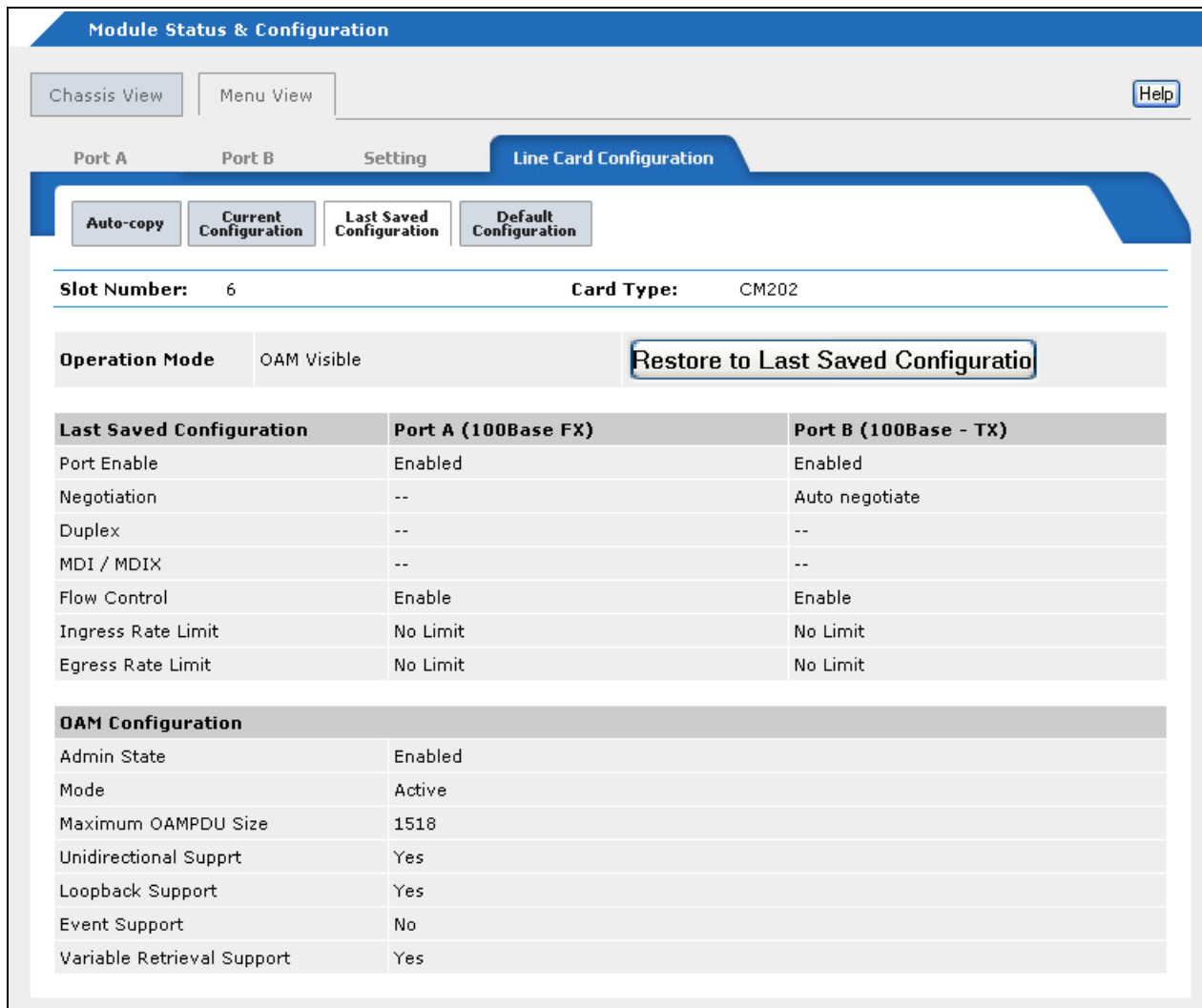


Figure 65. Last Saved Configuration Tab

This tab displays the last saved configuration settings for this card. The settings are obtained from the master configuration file on the management card. If the card is new to the slot, the settings are from the previous card installed in the slot. If the fields are empty, the master configuration file does not have a previous configuration for this slot or the previous and current line cards of the slot are different models.

5. To restore the line card to the last saved configuration, click the **Restore to Last Saved Configuration** button.

## Displaying Port Statistics

**Menus** To display traffic statistics for the ports on the AT-CM Line Cards from the menus:

1. From the Main Menu, select **Module Status and Configuration**. The Module Status and Configuration Menu is shown in Figure 48 on page 128.
2. Select the AT-CM Line Card whose statistics you want to view. An example of the Module Configuration Menu is shown in Figure 53 on page 139.
3. Select a port. You can select only one port. The Port Management Menu is shown in Figure 54 on page 140.
4. Select **Port Configuration**. The Port Configuration Menu for the port is shown in Figure 55 on page 141.
5. From the Port Management Menu, select **Port Statistics**. The example Show Port Statistics window in Figure 66 is from the AT-CM2KOS Line Card. All other AT-CM Line Cards have counters for just CRC errors and collisions.

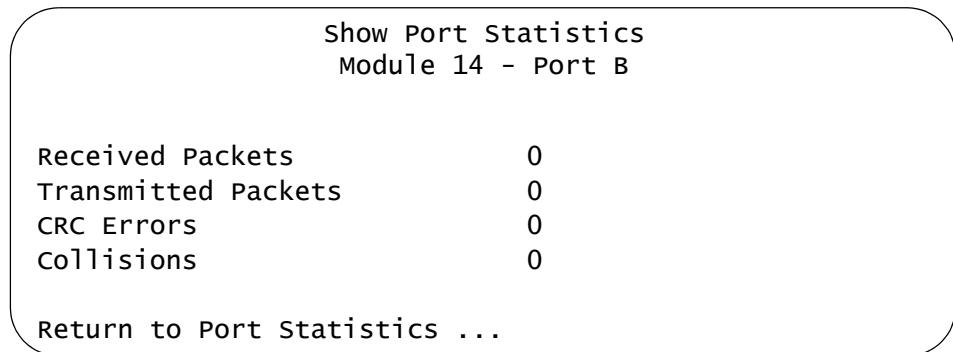


Figure 66. Show Port Statistics Window

The port statistics are described in Table 17.

Table 17. Port Statistics

Row	Description
Received Packets	The number of packets received by the port from the network device connected to it. This statistic is only available on the AT-CM2KOS Line Card.
Transmitted Packets	The number of packets transmitted by the port. This statistic is only available on the AT-CM2KOS Line Card.

Table 17. Port Statistics

Row	Description
CRC Errors	The number of received packets with CRC errors.
Collisions	The number of collisions on the port. This statistic is applicable only when a port is operating in the half-duplex mode.

**Web Browser** To display the traffic statistics for the ports on the AT-CM Line Cards from the web browser windows:

1. Select **Module Status & Configuration** from the menu bar.
2. In the Chassis View, click one of the ports of the line card whose statistics you want to view. Or, select the Menu View tab and click the model name of the line card. You can view the statistics of only one line card at a time.
3. Select the **Port A** tab to view the statistics for the fiber optic port or the **Port B** tab to view the statistics for the twisted pair port.
4. Click the **Port Statistics** tab to display the Port Statistics window for the port you selected. The example in Figure 67 is for Port B, the twisted pair port, on the AT-CM202 Line Card. The window has four statistics counters. However, only the AT-CM2KOS Line Card supports all four counters. The other AT-CM Line Cards support just the CRC errors counter and the collisions counter.

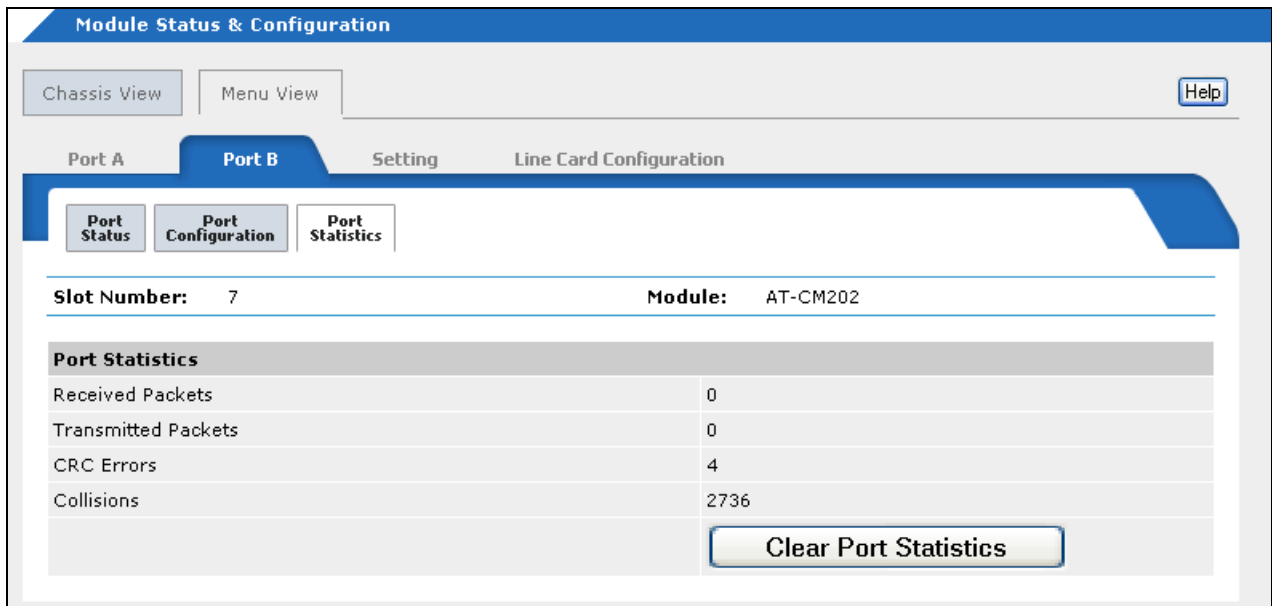


Figure 67. Port Statistics Window

The port statistics are described in Table 17 on page 160.

## Resetting Media Converter Line Cards

---

The procedures in this section are used to reset all of the AT-CM and AT-CV Line Cards in a Converteon chassis. You might reset the cards if they are experiencing a problem.



---

### Caution

These procedures may be disruptive to the operations of your network. Some network traffic may be lost. The AT-CM Line Cards immediately resume forwarding network traffic after they are reset, but they use the default values for their parameter settings while they initialize their management software, a process that takes approximately one minute to complete. Afterwards, they configure their operating parameters according to the settings in their configuration files or the settings received from the management card in the chassis. Because they do not have management software, the AT-CV Line Cards immediately return to normal operations after a reset.

---

You cannot reset individual media converter cards in a chassis.

These procedures do not affect the AT-CV5M02 Management Card. For instructions on how to reset the management card, refer to “Resetting the Management Card” on page 96.

### Menus

To reset all of the media converter line cards in the chassis from the menus:

1. From the Main Menu, select **Administration**. The Administration Menu is shown in Figure 28 on page 98.
2. From the Administration Menu, select **Reset Chassis and Restart Line Cards**.
3. At the confirmation prompt, select **Yes** to reset all of the media converter line cards or **No** to cancel the procedure. If you choose Yes, the following message is displayed:

The chassis will reset when FLASH writes are complete.

Afterwards, the Administration Menu is displayed again.

4. To monitor the status of the AT-CM Line Cards, return to the Main Menu and select **Module Status and Configuration**. When a line card has completed the reset process, its status changes to On.

**Web Browser** To reset all of the media converter line cards in the chassis from the web browser windows:

1. Select **Administration** from the menu bar.
2. If the **General** tab shown in Figure 68 is not selected, select it.

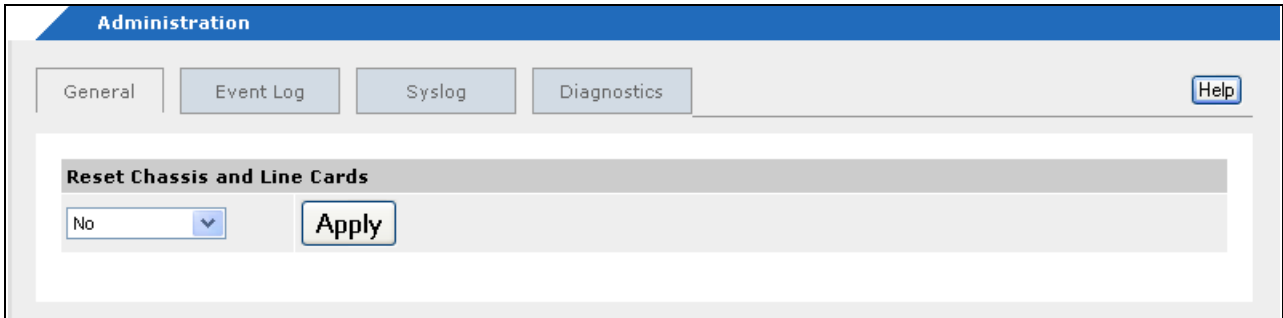


Figure 68. General tab

3. In the Reset Chassis and Line Cards section of the window, select **Yes** from the pull-down menu and click **Apply**.
4. To monitor the status of the AT-CM Line Cards, select the **Menu View** from **Module Status & Configuration**. A line card has completed the reset process when its status changes to On in the Menu View.

## Displaying the Version Numbers of the Management Software

---

The procedures in this section are for displaying the version numbers of the AT-S73 Management Software and the AT-S99 Management Software on the AT-CM Media Converter Line Cards and the AT-CV5M02 Management Card, respectively. This information might be useful if you obtain new versions of the programs and want to ascertain which line cards need the new releases. Also, you might be asked to provide this information if you contact Allied Telesis technical support for assistance.

---

### Note

The AT-CV Media Converter Line Cards do not use management software.

---

**Menus** To view the information from the menus:

1. From the Main Menu, select **Administration**. The Administration Menu is shown in Figure 28 on page 98.
2. From the Administration Menu, select **Diagnostics** to display the Diagnostic Menu shown in Figure 45 on page 121.

- From the Diagnostics Menu, select **Line Card Image Version**. An example of the Line Card Module Software Image Version window is shown in Figure 69. This window is for viewing purposes only.

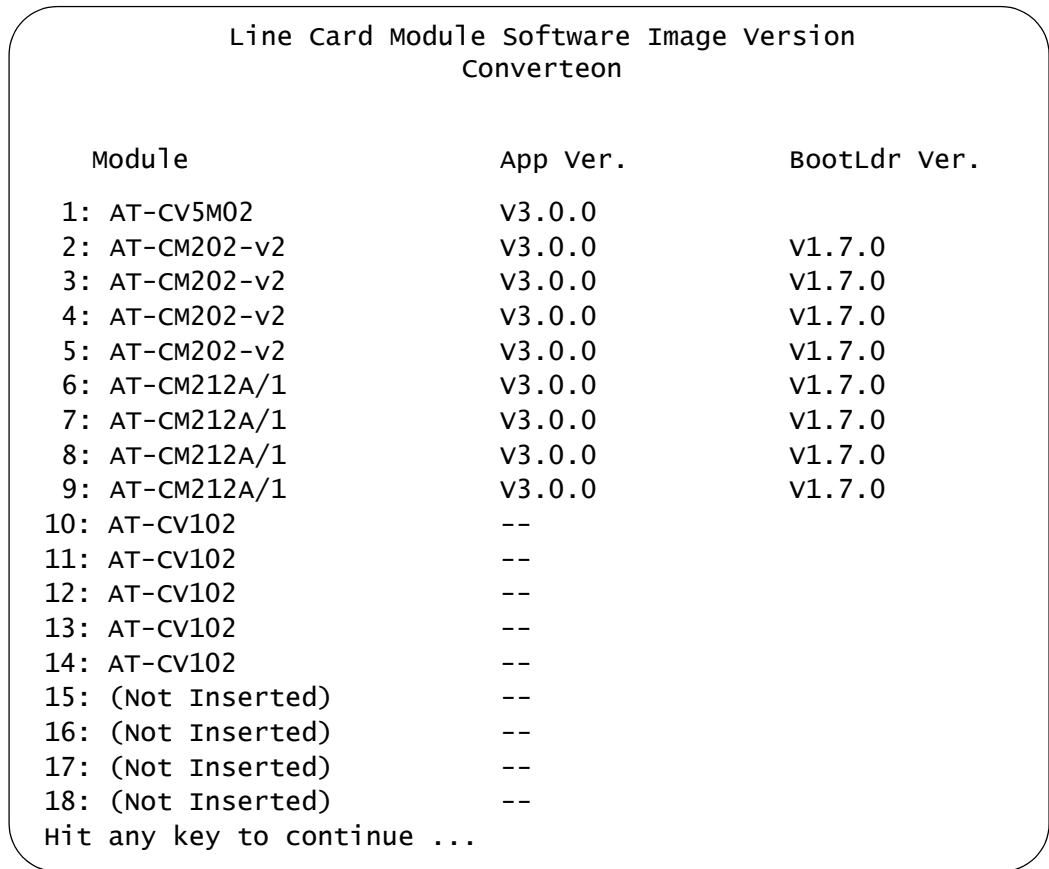


Figure 69. Line Card Module Software Image Version Window

The columns in the window are described in Table 18.

Table 18. Line Card Module Software Image Version Window

Row	Description
Module	This column displays the slot numbers and the model names of the cards.
App Ver.	This column displays the version numbers of the management software on the AT-CV5M02 Management Card and the AT-CM Line Cards. This column does not apply to the AT-CV Line Cards because they do not have management software.

Table 18. Line Card Module Software Image Version Window

Row	Description
BootLdr Ver.	This column displays the version numbers of the bootloader files on the AT-CM Line Cards. This column does not apply to the AT-CV5M02 Management Card and the AT-CV Line Cards because they do not have bootloader files.

### Web Browser

To view the version numbers of the management software and bootloader files on the line cards from the web browser windows:

1. Select **Administration** from the menu bar.
2. Select the **Diagnostics** tab.
3. Select the **Linecard Image Information** tab, shown in Figure 70. The columns in the window are described in Table 18 on page 165.

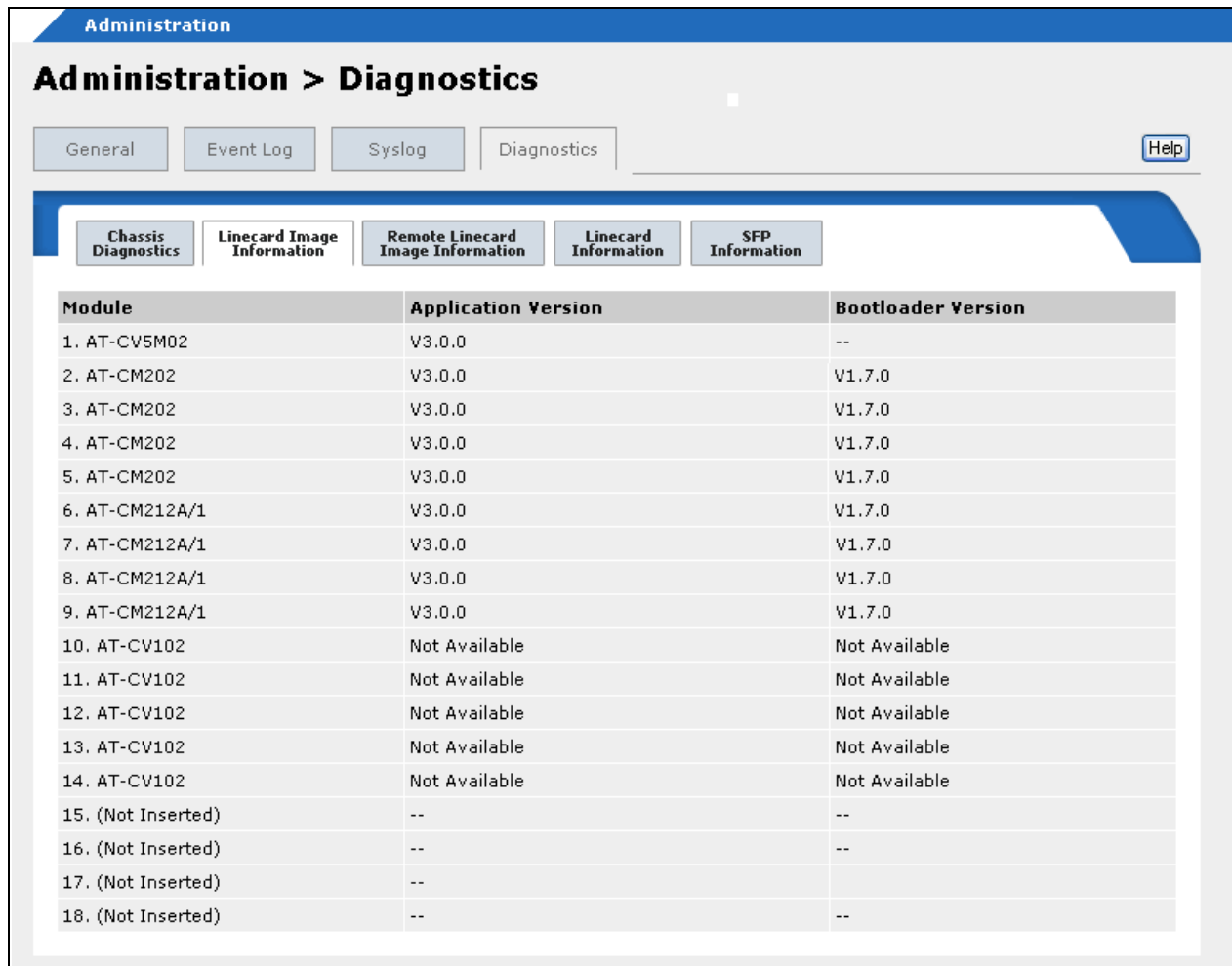


Figure 70. Linecard Image Information Tab

## Displaying the MAC Addresses and Serial Numbers

This section has procedures that explain how to display the MAC addresses and serial numbers of the cards in the chassis. You may be asked to provide this information in the event you contact Allied Telesis for technical assistance.

**Menus** To view the information from the menus:

1. From the Main Menu, select **Administration**. The Administration Menu is shown in Figure 28 on page 98.
2. From the Administration Menu, select **Diagnostics** to display the Diagnostic Menu shown in Figure 45 on page 121.
3. From the Diagnostics Menu, select **Line Card Information**. An example of the Line Card Module Information window is shown in Figure 71.

Line Card Module Information Convertheon		
Module	MAC Address	Serial Number
1: AT-CV5M02	--	A02803L05060001S C
2: AT-CM202	00:0C:46:CE:D9:60	A03572L061100040 B
3: AT-CM202	00:0C:46:CE:D9:72	A03572L061100170 B
4: AT-CM202	00:0C:46:CE:D9:02	A03572L061100014 B
5: AT-CM202	00:0C:46:CE:DA:12	A03572L061100111 B
6: AT-CM212A/1	00:15:77:52:5C:6F	A03578G071400012 A
7: AT-CM212A/1	00:15:77:52:5C:A1	A03578G071400225 A
8: AT-CM212A/1	FF:FF:FF:FF:FF:FF	A03713G070500081 B
9: AT-CM212A/1	FF:FF:FF:FF:FF:FF	A03713G070500120 B
10: AT-CV102	FF:FF:FF:FF:FF:FF	A03713G070500214 B
11: AT-CV102	FF:FF:FF:FF:FF:FF	A03713G070500012 B
12: AT-CV102	FF:FF:FF:FF:FF:FF	A03713G070500087 B
13: AT-CV102	FF:FF:FF:FF:FF:FF	A03713G070500055 B
14: AT-CV102	FF:FF:FF:FF:FF:FF	A02765G070500146 D
15: Mezzanine		
16: (Not Inserted)	--	--
17: (Not Inserted)	--	--
18: (Not Inserted)	--	--

Hit any key to continue ...

Figure 71. Line Card Module Information Window

This window is for viewing purposes only. The columns in the window are described in Table 19.

Table 19. Line Card Module Information Window

Row	Description
Module	This column displays the slot numbers and the model names of the cards.
MAC Address	<p>This column displays the MAC addresses of the AT-CM Line Cards in the chassis.</p> <p>Management cards are not assigned MAC addresses. Rather, they adopt the MAC address of their chassis. To view the MAC address of a chassis, refer to “Displaying the Operational Status of the Chassis” on page 121.</p> <p>The AT-CV Line Cards have the MAC address FF:FF:FF:FF:FF:FF.</p>
Serial Number	This column displays the serial numbers of the cards.

**Web Browser**

To view the MAC addresses and serial numbers of the cards from the web browser windows:

1. Select **Administration** from the menu bar.
2. Select the **Diagnostics** tab.
3. Select the **Linecard Information** tab, shown in Figure 72 on page 169. This window is for viewing purposes only. The columns in the window are described in Table 19 on page 168.

**Administration**

## Administration > Diagnostics

General | Event Log | Syslog | Diagnostics | Help

Chassis Diagnostics | **Linecard Image Information** | Remote Linecard Image Information | Linecard Information | SFP Information

Local Module	Mac Address	Serial Number
1. AT-CV5M02	--	A02803L05060001S C
2. AT-CM202	00:0C:46:CE:D9:72	A03572L061100040 B
3. AT-CM202	00:0C:46:CE:D9:02	A03572L061100070 B
4. AT-CM202	00:0C:46:CE:DA:12	A03572L061100014 B
5. AT-CM202	00:15:77:52:5C:6F	A03572L061100111 B
6. AT-CM212A/1	00:15:77:52:5C:A1	A03578G071400012 A
7. AT-CM212A/1	00:15:77:52:71:62	A03578G071400225 A
8. AT-CM212A/1	00:15:77:52:71:44	A03578G071400081 A
9. AT-CM212A/1	00:15:77:52:71:15	A03578G071400120 A
10. AT-CV102	FF:FF:FF:FF:FF:FF	A03713G070500214 B
11. AT-CV102	FF:FF:FF:FF:FF:FF	A03713G070500122 B
12. AT-CV102	FF:FF:FF:FF:FF:FF	A03713G070500152 B
13. AT-CV102	FF:FF:FF:FF:FF:FF	A03713G070500017 B
14. AT-CV102	FF:FF:FF:FF:FF:FF	A03713G070500222 B
15. (Not Inserted)	--	--
16. (Not Inserted)	--	--
17. (Not Inserted)	--	--
18. (Not Inserted)	--	--

Figure 72. Linecard Information Window

## Displaying SFP Module Information

---

The procedures in this section are for viewing the manufacturer's specifications of the SFP modules in the AT-CM2KOS and AT-CM70S Line Cards.

**Menus** To view SFP information from the menus:

1. From the Main Menu, select **Administration**. The Administration Menu is shown in Figure 28 on page 98.
2. From the Administration Menu, select **Diagnostics** to display the Diagnostic Menu shown in Figure 45 on page 121.
3. From the Diagnostics Menu, select **SFP Information**. The following prompt is displayed:

Enter LineCard Slot Number: ->

4. Enter the slot number of the AT-CM2KOS or AT-CM70S Line Card with the SFP module. The following prompt is displayed:

Enter LineCard Port [A or B]: ->

5. Enter the port of the SFP module.

An example of the SFP Information window is shown in Figure 73 and Figure 74.

```

SFP Information
Slot 4: Port A

Type of Serial Transceiver:      3 (Vendor Specific)
SONET Compliance Codes:         22
Gigabit Ethernet Compliance Codes: 2
Fiber Channel Link Length:      20
Fiber Channel Transmitter Type: 10
Fiber Channel Media Type:       1
Fiber Channel Speed:            15
Encoding:                        5
Normal Baud Rate:                19 (2.5GHz)
9micro, Distance:                14
50micro, Distance:               0
60micro, Distance:               0
CU, Distance:                    0
Transmit Disable:                1
Laser Fault:                     1
Signal Detect (Logical 0)        0
Signal Detect (Logical 1)        1
Upper Baud Rate Margin (in %)    96
Lower Baud Rate Margin (in %)    8

Hit any key to continue ...

```

Figure 73. SFP Information Window (1/2)

```

SFP Information
Slot 4: Port A

Vendor name (OUI)                LUMINENT
Vendor IEEE Company ID:          06b5
Vendor part number:              SFP-2500-SR1
Vendor revision number:          0000
Vendor serial number:            369G120986
Vendor date code:                030609
Vendor specific ID:

Hit any key to continue ...

```

Figure 74. SFP Information Window (2/2)

**Web Browser** To view SFP information from the web browser windows:

1. Select **Administration** from the menu bar.
2. Select the **Diagnostics** tab.
3. Select the **SFP Information** tab, shown in Figure 75.

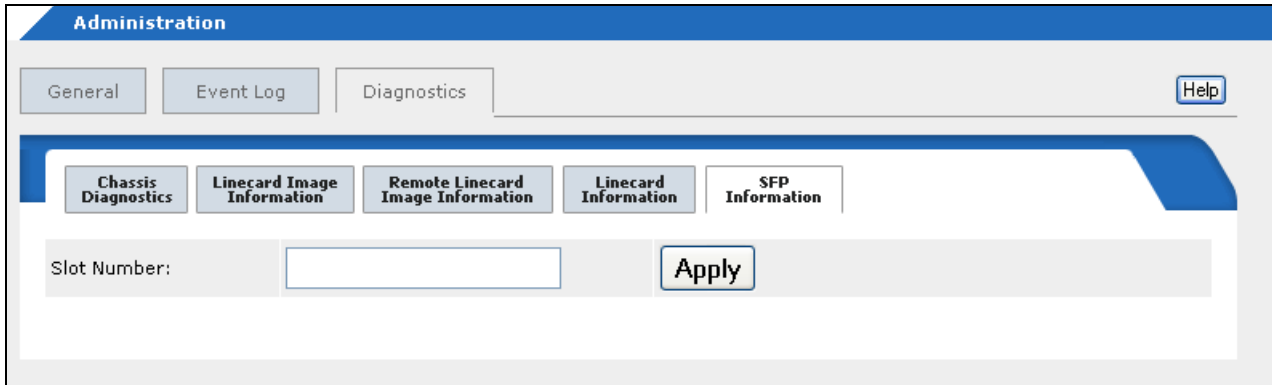


Figure 75. SFP Information Tab

4. Select the **Slot Number** field and enter the slot number of the line card with the SFP module. You can specify only one slot number.
5. Click **Apply**.

## Chapter 6

# Configuring AT-CM Line Cards with Remote Peer Management

---

This chapter has the following sections:

- “Configuring Remote AT-CM Line Cards from the Menus” on page 174
- “Configuring Remote AT-CM Line Cards from the Web Browser Windows” on page 182
- “Displaying the Version Numbers of Remote AT-CM Line Cards” on page 187

For background information, refer to “Remote Peer Management” on page 46. For instructions on how to configure the AT-CM Line Cards for this feature, refer to “Configuring the AT-CM Media Converter Line Cards for the OAM-based Features” on page 74.

## Configuring Remote AT-CM Line Cards from the Menus

To configure remote AT-CM Line Cards from the menus:

1. From the Main Menu, select **Remote Module Status and Configuration** to display the Remote Module Status and Configuration Menu, shown in Figure 76. The menu shows the status of the remote peer connections between the fiber optic ports on the local AT-CM Line Cards in the managed chassis and their remote line card counterparts. It also displays the states of the fiber optic ports and twisted pair ports on the remote line cards. The columns are described in Table 20. (This menu does not display any information for AT-CV Line Cards.)

Remote Module Status and Configuration Converteon																					
LOCAL MODULE					REMOTE MODULE					FIBER PORT				COPPER PORT							
Mod_Name	CardTypeVer	ST	OV	IPC	VER	Mod_Name	CardTypeVer	VER	OV	SP	FC	IngRL	EgrRL	OAM	ST	SP	FC	IngRL	EgrRL	AN	
1	AT-CV5M02	*	A	502	V300																
2	Reg11	AT-CM202-v2	*	Y	00*	V300	Reg11_r	AT-CM202-v2	V300	Y	100	Y	0	0	***	o	100	Y	0	0	Y
3	Reg20	AT-CM202-v2	*	Y	*0*	V300	Reg20_r	AT-CM202-v2	V300	Y	100	Y	0	0	***	o	100	Y	0	0	Y
4	Reg21	AT-CM202-v2	*	Y	*0*	V300	Reg21_r	AT-CM202-v2	V300	Y	100	Y	0	0	***	o	100	Y	0	0	Y
5	Area2a	AT-CM202-v2	*	Y	*0*	V300	Area2a	AT-CM202-v2	V300	Y	100	Y	0	0	***	o	100	Y	0	0	Y
6	Area2b	AT-CM202-v2	*	Y	*0*	V300	area2b	AT-CM202-v2	V300	Y	100	Y	0	0	***	o	100	Y	0	0	Y
7	Reg12	AT-CM202-v2	*	Y	*0*	V300	Reg12_r	AT-CM202-v2	V300	Y	100	Y	0	0	***	o	100	Y	0	0	Y
8	AT-CV102	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
9	AT-CV102	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
10	AT-CV102	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
11	AT-CV102	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
12	AT-CV102	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

Figure 76. Remote Module Status and Configuration Menu

Table 20. Remote Module Status and Configuration Menu

Column	Description
LOCAL MODULE	
Mod_Name	This column lists the chassis slot numbers and the names of the local AT-CM Line Cards in the chassis that contains the management card. For instructions on how to assign names to local line cards, refer to “Assigning Names to AT-CM Line Cards” on page 149.
CardTypeVer	This column displays the model names of the management cards and the line cards in the local chassis. The model names of newer versions of the AT-CM Line Cards have suffixes, like “-v2.”

Table 20. Remote Module Status and Configuration Menu

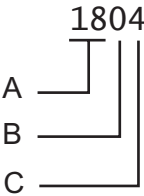
Column	Description
ST	<p>This column displays the states of the remote peer management connections between the local and remote line cards. The possible states are:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> * - The local line card has established a remote peer management connection with a remote line card.</li> <li><input type="checkbox"/> - - The local line card hasn't established a remote peer management connection with a remote line card.</li> </ul>
OV	<p>This column indicates whether or not the local AT-CM Line Cards are set to the OAM visible operating mode, as required by remote peer management. Possible values are:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Y - The local line card is set to the OAM visible mode.</li> <li><input type="checkbox"/> N - The local line card is set to one of the other operating modes.</li> </ul> <p>This column also displays the active or standby state of the management cards in the chassis. (The active or standby state of a management card is unrelated to OAM on the line cards.) The possible values are:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> A - The management card is in the active state.</li> <li><input type="checkbox"/> S - The management card is in the standby state.</li> </ul>
IPC	<p>This column displays utilization information of the backplane by the management card and the AT-CM Line Cards, and is intended for manufacturing and test purposes.</p> <p>For the AT-CV5M02 Management Card this column displays the following information:</p> <div style="text-align: center;">  </div> <ul style="list-style-type: none"> <li>A This is the slot number of the AT-CM Line Card the management card is currently polling. For example, the value "12" indicates that the management card is polling the AT-CM Line Card in slot 12. The management card does not poll slots containing AT-CV Line Cards.</li> <li>B This is the total number of messages the management card is waiting to transmit over the backplane to the AT-CM Line Cards.</li> <li>C This is the total number of responses the management card is waiting to receive from the AT-CM Line Cards.</li> </ul>

Table 20. Remote Module Status and Configuration Menu

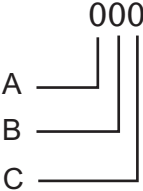
Column	Description
IPC (Continued)	<p>For AT-CM Line Cards this column displays the following information:</p> <div style="text-align: center;">  </div> <p>A This toggles to “*” when the management card is sending a message to the line card in the slot.</p> <p>B This toggles to “*” when the management card has a message to transmit to the line card.</p> <p>C This displays the status of a line card’s response to the last transmitted message from the management card. A successful response is indicated by “*” while a bad response or no response is signalled with “o”.</p>
VER	<p>This column displays the version numbers of the management software programs on the management cards and the AT-CM Line Cards in the local chassis. The AT-CV Line Cards do not have management software.</p>
REMOTE MODULE	
Mod_Name	<p>This column displays the names of those remote AT-CM Line Cards that have remote peer management connections to their local counterparts in the managed chassis.</p>
CardTypeVer	<p>This column displays the model names of the remote line cards.</p>
VER	<p>This column displays the version numbers of the AT-S73 Management Software on the remote line cards.</p>
OV	<p>This column indicates whether or not the remote line cards are operating in the OAM visible mode.</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Y - The remote line card is in the OAM visible mode.</li> <li><input type="checkbox"/> N or - - The fiber optic port on the local line card is not connected to a remote device or the operating mode of the remote device is not set to OAM visible.</li> </ul>

Table 20. Remote Module Status and Configuration Menu

Column	Description
FIBER PORT or COPPER PORT	
ST	<p>This column displays the states of the twisted pair ports on the remote line cards. The possible states are:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> * - The twisted pair port has establish a link to a network device.</li> <li><input type="checkbox"/> o - The twisted pair port has not establish a link to a network device.</li> </ul> <p>This column is omitted for the fiber optic port because remote peer management will not work without a connection between the fiber optic ports of the local and remote line cards.</p>
SP	<p>This column displays the speeds of the remote ports. The possible speeds are:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> 10 - 10 Mbps</li> <li><input type="checkbox"/> 100 - 100 Mbps</li> <li><input type="checkbox"/> 1G - 1 Gbps</li> </ul>
FC	<p>This column displays the status of flow control on the ports of the remote AT-CM Line Cards. The possible states are:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Y - Flow control is enabled on the port.</li> <li><input type="checkbox"/> N - Flow control is disabled on the port.</li> </ul>
IngRL	<p>This column displays the settings of the ingress rate limiting filters on the ports on the remote AT-CM Line Cards. The value "0" means rate limiting has not been set on the port. This is the default setting.</p>
EgrRL	<p>This column displays the settings of the egress rate limiting filters on the ports on the AT-CM Line Cards. The value "0" means rate limiting has not been set on the port. This is the default setting.</p>
OAM	<p>This column displays the status of the OAM clients on the remote AT-CM Line Cards. The following OAM client information is displayed:</p> <div style="text-align: right; margin-right: 50px;"> <p>*00</p> <pre>                 A ---          B ---          C ---                    </pre> </div>

Table 20. Remote Module Status and Configuration Menu

Column	Description
OAM (Continued)	<p>A This displays the operational state of the OAM client on Port A, the fiber optic port, on a remote line card. The possible states are:</p> <ul style="list-style-type: none"> <li>* - Operational</li> <li>A - Active Send Local</li> <li>D - Disabled</li> <li>L - Active Send Local</li> <li>M - Peer Remote Reject</li> <li>P or W - Passive Wait</li> <li>R - Peer Local Reject</li> <li>1 - Active Send Remote 1</li> <li>2 - Active Send Remote 2</li> </ul> <p>B This alternates between “*” and “o” when a remote fiber optic port is transmitting OAMPDUs. Otherwise, it remains “o”.</p> <p>C This alternates between “*” and “o” when a remote fiber optic port is receiving OAMPDUs. Otherwise, it remains “o”.</p>
AN	<p>This column displays the status of Auto-Negotiation on the twisted pair ports on the remote AT-CM Line Cards. The possible states are:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Y - Auto-Negotiation is enabled on the port. The speed and duplex mode are set automatically. This is the default setting.</li> <li><input type="checkbox"/> N - Auto-Negotiation is disabled on the port. The speed and duplex mode were set manually.</li> </ul>

**Note**

Remote peer management requires that the local and remote line cards be in the OAM operational state. Reaching that state may take a line card up to two minutes when it is powered on because it has to initialize its management software and negotiate the OAM state with its counterpart.

- To configure a remote line card, select the card in the menu. This displays the Remote Module Configuration Menu shown in Figure 77.

Remote Module Configuration Menu			
Converteon			
Module 1			
Module: AT-CM202			
Port	Link	Speed	Mode
A(100BaseFX)	Online	100M	Full
B(100BaseTX)	online	100M	Full
Module Name		Module Name	
Line Card Configuration			
Return to Remote Module Status and Configuration ...			

Figure 77. Remote Module Configuration Menu

The menu displays the current settings of the two ports on the remote line card. The columns are described in Table 15 on page 139.

---

**Note**

You cannot disable ports or change the operating modes or the OAM settings on remote line cards.

---

Your changes to the parameter settings on a remote line are automatically saved in the card's configuration file in flash memory. They are retained even if the remote chassis is powered off or the card is removed from the unit. For further information, refer to "Configuration Files" on page 29.

- When you finish configuring the remote line card, return to the Remote Module Configuration Menu and select **Return to Remote Module Status and Configuration** to display the Remote Module Status and Configuration menu again.

## Naming a Remote Line Card

To assign a name to a remote line card:

- From the Remote Module Configuration Menu, select the **Module Name** field.
- Enter a name of up to eight alphanumeric characters.

### Displaying the Current Configuration

To view the current settings of a remote card:

1. Select **Line Card Configuration**.
2. From the Line Card Configuration menu, select **Display Current Configuration**. An example of the window is shown in Figure 51 on page 136. The port parameters are described in Table 16 on page 141 and the OAM parameters in Table 25 on page 205.

### Configuring Remote Ports

To configure the parameter settings of a port on a remote AT-CM Line Card:

1. From the Remote Module Configuration Menu, select the port you want to configure. You can configure only one port at a time.
2. Configure the parameters, as necessary. Refer to Table 16 on page 141 for parameter descriptions.

### Restoring the Default Settings

To restore the default settings on a remote AT-CM Line Card:



#### Caution

This procedure may disrupt network operations. Some network traffic may be lost.

---

#### Note

A remote line card that is returned to its default values continues to support remote peer management because the default operating mode for the AT-CM Line Cards is OAM visible.

---

1. From the Remote Module Configuration Menu, select **Line Card Configuration**.
2. To view the default settings prior to activating them on the line card, select **Display Default Configuration**. An example of the Display Default Configuration window is shown in Figure 63 on page 154.
3. To return the parameter settings on the line card to the default values, return to the Line Card Configuration Menu and select **Return Line Card to Default Configuration**.
4. At the confirmation prompt, select **Yes** to return the parameter settings on the line card to the default values or **No** to cancel the procedure.

## Restoring the Last Saved Configuration

This procedure restores a remote line card to the last saved configuration in the master configuration file on the management card in the local chassis. You might perform this procedure to discard any parameter changes that you made to a line card but did not save, or to configure a new line card with the same settings as its predecessor. For more information, refer to “Configuration Files” on page 29.



### Caution

This procedure may disrupt network operations. Some traffic may be lost.

---

1. From the Remote Module Configuration Menu, select **Line Card Configuration**.
2. To view the parameter settings of the card's last saved configuration before activating them on the line card, select **Display Last Saved Configuration**.
3. To return the line card to its last saved configuration, return to the Line Card Configuration menu and select **Restore Last Saved Configuration**.
4. At the confirmation prompt, select **Yes** to restore the settings or **No** to cancel the procedure.

## Saving the Parameter Settings

Your changes to the parameter settings on remote AT-CM Line Cards are automatically saved in the configuration files in flash memory and are retained even if the remote chassis is powered off or the cards are removed.

If desired, you can add the configuration settings of remote line cards to the master configuration file in the management card in the local chassis so that you can restore them to the remote cards, should that ever be necessary. To save the settings in the master configuration file, select **Line Card Configuration** and **Save Line Card Configuration**. If you ever need to restore the setting to the line card, perform “Restoring the Last Saved Configuration” on page 181.

## Configuring Remote AT-CM Line Cards from the Web Browser Windows

To configure remote AT-CM Line Cards from the web browser windows:

1. Select **Remote Module Status & Configuration** from the menu bar to display the Remote Module Status & Configuration tab shown in Figure 78.

	Local Module	Card Type	Version	Link (A)
1	AT-CV5M02	No Support	No Support	No Support
2	AT-CM202	AT-CM202	V3.0.0	Online
3	AT-CM202	AT-CM202	V3.0.0	Online
4	AT-CM202	AT-CM202	V3.0.0	Online
5	AT-CM202	AT-CM202	V3.0.0	Online
6	AT-CM212A/1	AT-CM212A/1	V3.0.0	Online
7	AT-CM212A/1	AT-CM212A/1	V3.0.0	Online
8	AT-CM212A/1	AT-CM212A/1	V3.0.0	Online
9	AT-CM212A/1	AT-CM212A/1	V3.0.0	Online
10	AT-CV102	No Support	No Support	No Support
11	AT-CV102	No Support	No Support	No Support
12	AT-CV102	No Support	No Support	No Support
13	AT-CV102	No Support	No Support	No Support
14	AT-CV102	No Support	No Support	No Support
15	_UN-EQUIP_	--	--	--
16	_UN-EQUIP_	--	--	--
17	_UN-EQUIP_	--	--	--
18	_UN-EQUIP_	--	--	--

Figure 78. Remote Module Status & Configuration Tab

The columns in the tab are described in Table 21.

Table 21. Remote Module Status & Configuration Tab

Column	Description
Local Module	This column displays the slot numbers, names and model names of the line cards in the local chassis that contains the AT-CV5M02 Management Card.
Card Type	This column displays the model names of the remote AT-CM Line Cards that have established remote peer connections to their local line card counterparts.

Table 21. Remote Module Status & Configuration Tab

Column	Description
Version	This column displays the version numbers of the AT-S73 Management Software on the remote AT-CM Line Cards.
Link (A)	<p>This column displays the status of the remote peer connections between the fiber optic ports on the local and remote AT-CM Line Cards. The possible states are:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> --: The fiber optic port on the local line card in the managed chassis has not established a remote peer management connection with the fiber optic port on the remote line card.</li> <li><input type="checkbox"/> Online: The fiber optic ports on the local and remote line cards have established a remote peer management connection.</li> <li><input type="checkbox"/> No Support: The local line card does not support the feature. Local AT-CM Line Cards display this state if they are not configured for remote peer management or if the remote device is something other than an AT-CM Line Card. This status is also displayed by the AT-CV5M02 Management Card and the AT-CV Line Cards.</li> </ul>

- To configure a remote line card, click the model name of its local line card counterpart to display the Remote Module Status & Configuration page, shown in Figure 79.

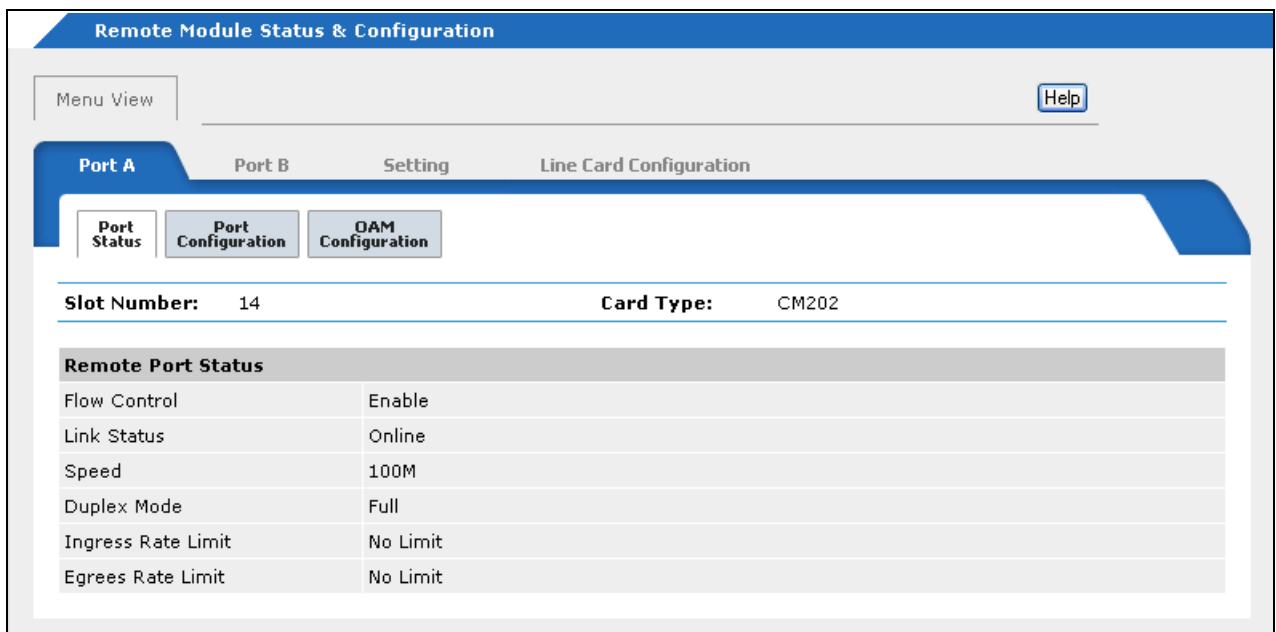


Figure 79. Remote Module Status & Configuration Page

---

**Note**

You cannot disable the ports or change the operating modes or the OAM settings on remote line cards.

---

Your changes to the settings on a remote line card are automatically saved in the card's configuration file in flash memory and are retained even if the remote chassis is powered off or the card is removed from the unit. For further information, refer to "Configuration Files" on page 29.

3. When you finish configuring a remote line card, select **Remote Module Status & Configuration** from the menu bar.
4. You can either select another remote line card to configure or continue managing the local chassis.

### **Displaying the Current Configuration**

To view the current parameter settings of a remote card:

1. Click the **Line Card Configuration** tab.
2. Click the **Current Configuration** tab. An example of the window is shown in Figure 52 on page 137. The port parameters are described in Table 16 on page 141 and the OAM parameters in Table 25 on page 205.

### **Configuring Remote Ports**

To configure the parameter settings of a remote port:

1. From the Remote Module Status & Configuration window, adjust the twisted pair port. You can configure only one port at a time.
2. Click the **Port Configuration** tab.
3. Configure the parameters, as necessary. The parameters are described in Table 16 on page 141.

## Restoring the Default Parameter Settings

To restore a remote line card to its default parameter settings:



### Caution

This procedure may disrupt network operations. Some network traffic may be lost.

---

### Note

A remote line card that is returned to its default values continues to support remote peer management because the default operating mode for the AT-CM Line Cards is OAM visible.

---

1. From the Remote Module Status & Configuration window, select the **Line Card Configuration** tab.
2. Click the **Default Configuration** tab. This tab displays the default settings for the line card. An example of the tab is shown in Figure 64 on page 155.
3. To return the card's parameter settings to the default values, click the **Return to Default Configuration** button. The parameter settings on the card are returned to the default settings.

## Restoring the Last Saved Configuration

This procedure restores a remote line card to the last saved configuration in the master configuration file on the management card in the local chassis. You might perform this procedure to discard any parameter changes that you made to a line card but did not save, or to configure a new line card with the save settings as its predecessor. For more information, refer to "Configuration Files" on page 29.



### Caution

This procedure may disrupt network operations. Some traffic may be lost.

---

1. From the Remote Module Status & Configuration window, select the **Line Card Configuration** tab.
2. Select the **Last Saved Configuration** tab.
3. To return the line card to its last saved configuration, click the **Restore to Last Saved Configuration** button.

## **Saving the Parameter Settings**

Your changes to the parameter settings on remote AT-CM Line Cards are automatically saved in the configuration files in flash memory and are retained even if the remote chassis is powered off or the cards are removed.

If desired, you can add the configuration settings of remote line cards to the master configuration file in the management card in the local chassis so that you can restore them to the remote cards, should that ever be necessary. To update the master configuration file in flash memory on the management card, click the **Line Card Configuration** tab, the **Current Configuration** tab, and the **Save Current Configuration** button. If you ever want to restore the setting to the line card or to a replacement card, perform “Restoring the Last Saved Configuration” on page 185.

## Displaying the Version Numbers of Remote AT-CM Line Cards

These procedures are used to view the version numbers of the AT-S73 Management Software and bootloader files on remote AT-CM Line Cards.

### Note

This procedure requires that the local and remote line cards be configured for remote peer management.

**Menus** To view the information from the menus:

1. From the Main Menu, select **Administration**. The Administration Menu is shown in Figure 28 on page 98.
2. From the Administration Menu, select **Diagnostics** to display the Diagnostic Menu shown in Figure 45 on page 121.
3. From the Diagnostics Menu, select **Remote Line Card Image Version**. An example of the Remote Line Card Module Software Image Version window is shown in Figure 80. The information in this window is for viewing purposes only.

Remote Line Card Module Software Image Version Converteeon			
Module		App Ver.	BootLdr Ver.
1:	AT-CV5M02	V3.0.0	
2: Reg11	AT-CM202-v2	V3.0.0	V1.7.0
3: Reg20	AT-CM202-v2	V3.0.0	V1.7.0
4: Reg21	AT-CM202-v2	V3.0.0	V1.7.0
5: Area2a	AT-CM202-v2	V3.0.0	V1.7.0
6: Area2b	AT-CM212A/1	V3.0.0	V1.7.0
7: Reg12	AT-CM212A/1	V3.0.0	V1.7.0
8: Reg5	AT-CM212A/1	V3.0.0	V1.7.0
9: Reg17	AT-CM212A/1	V3.0.0	V1.7.0
10: -----	AT-CV102	--	
11: -----	AT-CV102	--	
12: -----	AT-CV102	--	
13: -----	AT-CV102	--	
14: -----	AT-CV102	--	
15:	Unequipped	--	
16:	Unequipped	--	
17:	Unequipped	--	
18:	Unequipped	--	
Hit any key to continue ...			

Figure 80. Remote Line Card Module Software Image Version Window

The columns in the window are described in Table 22.

Table 22. Line Card Module Software Image Version Window

Row	Description
Module	This column displays the slot numbers, the names and the model names of the local AT-CM Line Cards in the chassis that has the management card.
App Ver.	This column displays the version numbers of the AT-S73 Management Software on the remote AT-CM Line Cards.
BootLdr Ver.	This column displays the version numbers of the bootloader files on the remote AT-CM Line Cards.

## Web Browser

To view the version numbers of the AT-S73 Management Software and bootloader files on remote AT-CM Line Cards from the web browser windows:

1. Select **Administration** from the menu bar.
2. Select the **Diagnostics** tab.
3. Select the **Remote Linecard Image Information** tab, shown in Figure 81 on page 189.

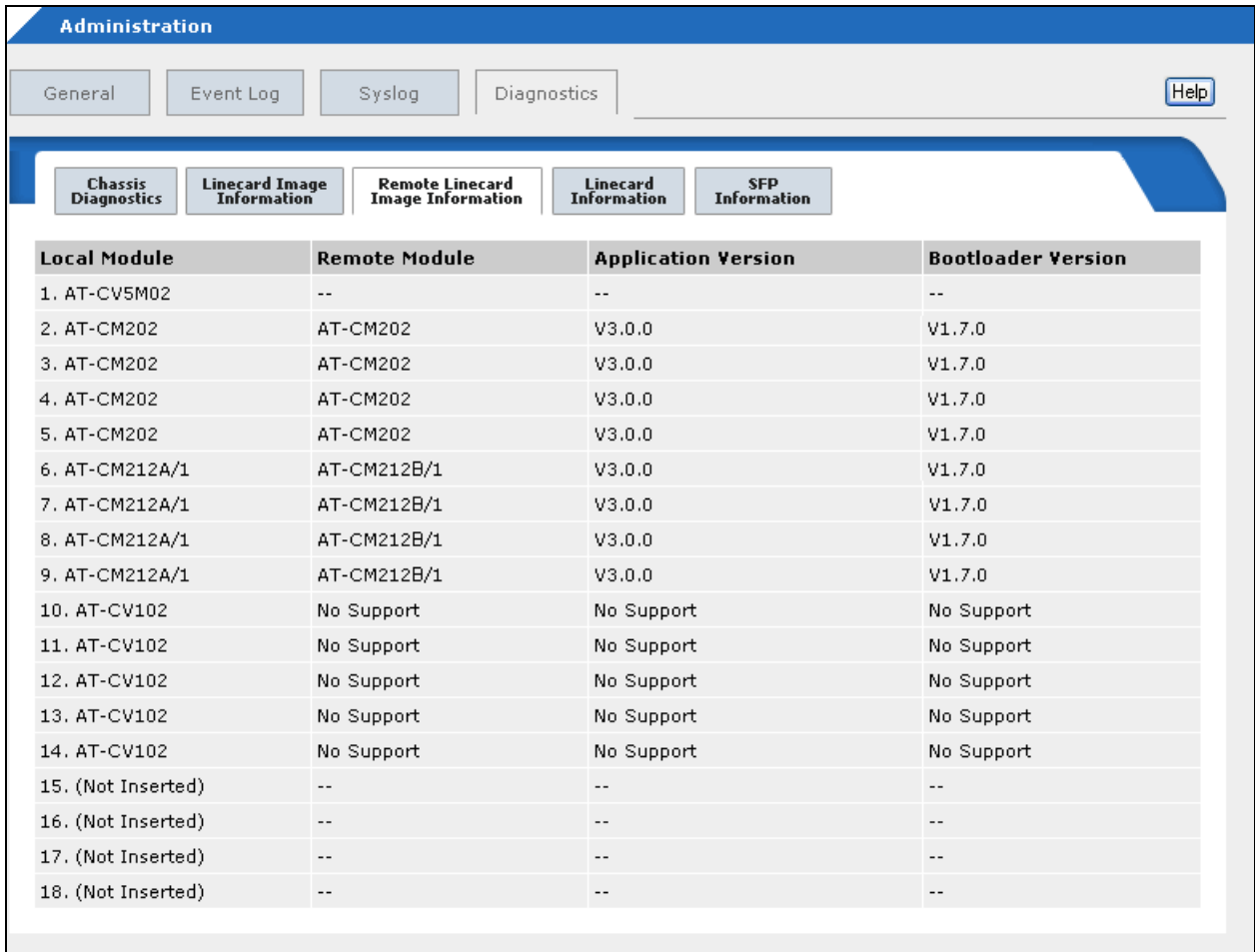


Figure 81. Remote Linecard Image Information Tab

The information in this window is for viewing purposes only. The columns in the window are described in Table 23.

Table 23. Line Card Module Software Image Version Window

Row	Description
Local Module	This column displays the slot numbers and the model names of the local AT-CM Line Cards in the chassis that has the management card.
Remote Module	This column displays the model names of the remote AT-CM Line Cards.
Application Version	This column displays the version numbers of the management software on the remote AT-CM Line Cards.
Bootloader Version	This column displays the version numbers of the bootloader files on the remote AT-CM Line Cards.



## Chapter 7

# Configuring the T1/E1 Ports on the AT-CM70S Media Converter Line Card

---

This chapter contains the following sections:

- “Selecting the Management Method for the T1/E1 Ports” on page 192
- “Configuring the T1/E1 Ports from the AT-CV5M02 Management Card” on page 196
- “Configuring the T1/E1 Ports from the Console Port on the Line Card” on page 199

## Selecting the Management Method for the T1/E1 Ports

---

The parameter settings for the four T1/E1 ports on the AT-CM70S Line Card can be configured through the management software on the AT-CV5M02 Management Card or through the Console port on the card itself. However, since the card is unable to support both methods at the same time, you have to choose which management method you intend to use and specify the method during the initial configuration of the card.

This is referred to as setting the card's UART (universal asynchronous receiver/transmitted) setting. The card has two settings—UART local console mode and UART backplane mode. The UART local console mode lets you configure the T1/E1 ports from the Console port on the card. This setting, which happens to be the default setting for the UART parameter, is the appropriate setting for an AT-CM70S Line Card that is installed in a chassis that doesn't have a management card.

If the card will be installed in a chassis that has a management card, you should change the management method of the ports to the UART backplane mode. This will allow you to configure the T1/E1 ports using the menus in the management software of the management card. You'll be able to configure these ports much as you can any of the other ports on the card. (The term "backplane" refers to the backplane in the AT-CV5000 Chassis.)

There are a couple of other factors that need to be considered when choosing the UART setting for this card. The AT-CM70S Line Card supports the remote peer management feature for the 10/100/1000Base-T Ethernet port and the SFP slot, but not for the T1/E1 ports. So even if you configure this card for remote peer management, you will not be able to configure the T1/E1 ports on a remote card through that feature.

The AT-CM70S Line Card is a multiplexer that combines the data streams from one 10/100/1000Base-T Ethernet port and four T1/E1 lines onto a single SFP fiber optic port. As such, it has to be used in pairs. However, the cards do not need to have the same UART settings. In fact, they'll have different settings because one of the cards will probably reside in the AT-CV5000 Chassis with a management card and the other at a remote site in a chassis that does not have a management card.

Figure 82 illustrates the idea of the UART setting. It shows a deployment of two AT-CM70S Line Cards and their UART settings. The UART setting of the line card in the AT-CV5000 Chassis is set to UART backplane mode so that the T1/E1 ports on the card can be managed through the management card in the chassis. In contrast, the UART setting of the card at the remote site is set to UART console mode so that the T1/E1 ports can be managed through the card's Console port at the site. If the card at the remote site had a UART setting of UART backplane mode, you would have to remove the card from the chassis and install it into another unit

that had a management card whenever you wanted to configure the T1/E1 ports.

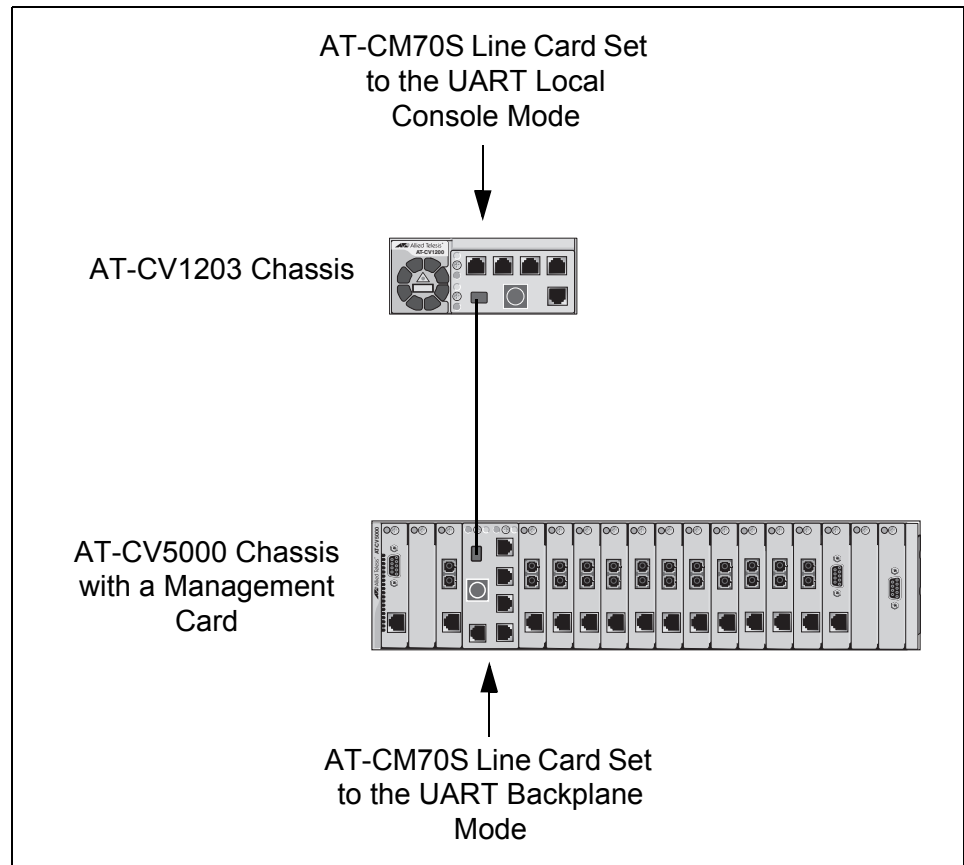


Figure 82. UART Setting on the AT-CM70S Line Card

Here are the general steps to configuring a pair of AT-CM70S Line Cards:

1. For the initial configuration, install both AT-CM70S Line Cards in an AT-CV5000 Chassis that has the AT-CV5M02 Management Card.
2. Using the menus interface in the management card, change the UART setting on both cards to UART backplane mode so that you can configure all of the card's parameter settings, including the T1/E1 ports, using the management card.
3. Using the management card, configure all of the settings of the two AT-CM70S Line Cards, including the settings for the T1/E1 ports, as required by your network.
4. For the AT-CM70S Line Card intended for the remote site, change its UART setting to UART local console mode after configuring its T1/E1 ports. This will make it possible for you to adjust the settings of the T1/E1 ports from the Console port when the line card is installed at the remote site.

How to set the UART setting on the AT-CM70S Line Card is explained in the following procedure. The procedure requires the AT-CV5M02 Management Card. The UART setting cannot be set through the Console port on the card.



**Caution**

This procedure may be disruptive to network operations. The AT-CM70S Line Card resets and initializes its management software when the UART setting is changed. Some network traffic may be lost.

To set the UART setting on the AT-CM70S Line Card from the menus:

1. From the Main Menu, select **Module Status and Configuration**. The Module Status and Configuration Menu is shown in Figure 48 on page 128.
2. Select the AT-CM70S Line Card you want to configure. The Module Configuration Menu is shown in Figure 53 on page 139.
3. From the Module Configuration Menu, select **3: TDM LIU (T1/E1) Configuration** to display the TDM Management Menu shown in Figure 83.

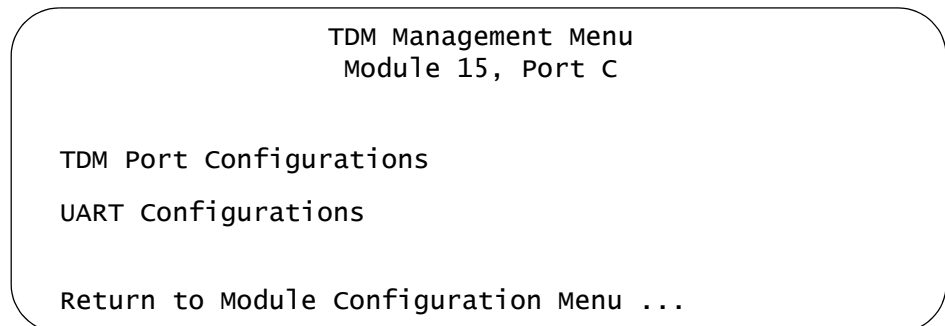


Figure 83. TDM Management Menu

The TDM Port Configurations selection appears in the menu only when the line card's UART setting is set to UART backplane mode.

4. From the TDM Management Menu, select **UART Configurations** to display the UART Configuration Menu, shown in Figure 84.

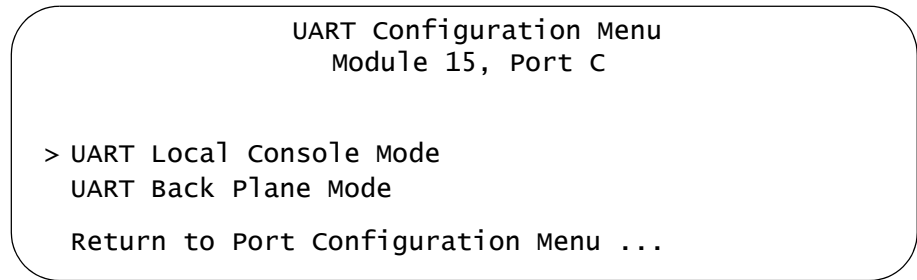


Figure 84. UART Configuration Menu

5. From the UART Configuration Menu, select one of the following options:
  - UART Local Console Mode - Select this setting to configure the T1/E1 ports from the Console port on the line card. This setting is appropriate for AT-CM70S Line Cards in chassis that do not have a management card. This is the default setting.
  - UART Back Plane Mode - Select this setting to configure the T1/E1 ports using a management card. Do not select this setting if the card will be deployed at a remote site in a chassis that does not have a management card.
6. At the confirmation prompt, type **Y** to implement your change or type **N** to cancel it.
7. To save your changes in the master configuration file, return to the Main Menu and select **Configuration** and **Save System and All Line Card Configurations**.

## Configuring the T1/E1 Ports from the AT-CV5M02 Management Card

To configure the T1/E1 ports on the AT-CM70S Line Card from the menus in the AT-CV5M02 Management Card:

1. From the Main Menu, select **Module Status and Configuration**. The Module Status and Configuration Menu is shown in Figure 48 on page 128.
2. Select the AT-CM70S Line Card you want to configure.
3. From the line card's Module Configuration Menu, select **TDM LIU (E1/T1) Configuration** to display the menu in Figure 83 on page 194.
4. From the TDM Management Menu, select **TDM Port Configurations** to display the LIU Mode and Channel Select Menu, shown in Figure 85.

---

### Note

If the TDM Port Configurations selection is not included in the TDM Management Menu, you need to set the card's UART setting to the backplane mode. For instructions, refer to "Selecting the Management Method for the T1/E1 Ports" on page 192.

---

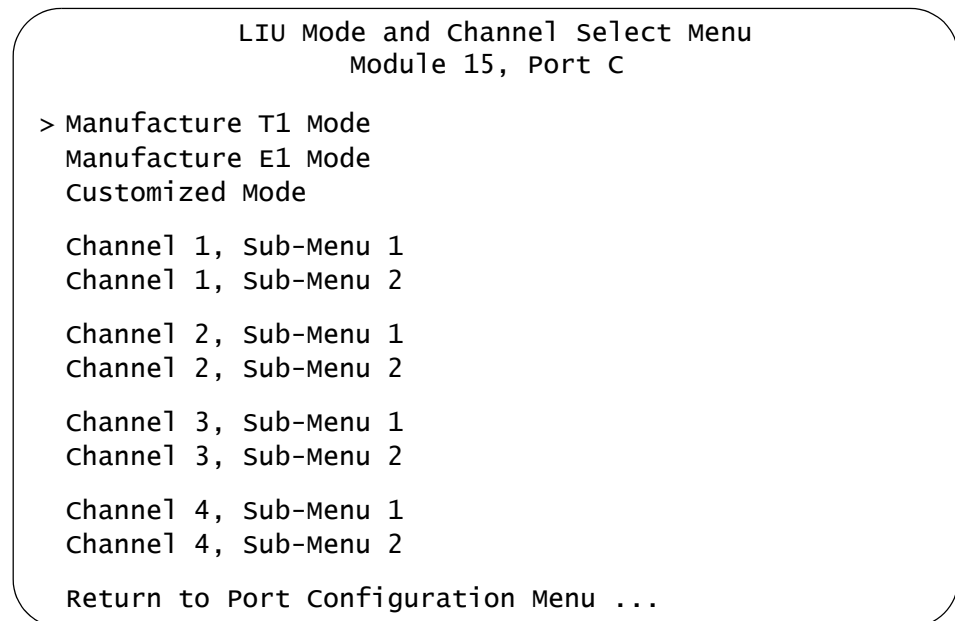


Figure 85. LIU Mode and Channel Select Menu

5. To designate the T1 or E1 carrier type for the line card, select **Manufacture T1 Mode** or **Manufacture E1 Mode**, respectively.

6. After you've designated the carrier type, configure the individual ports. Each channel in the menu represents a different port on the line card. Channel 1 represents T1/E1 port 1, channel 2 represents T1/E1 port 2, and so forth. Each port has a submenu 1, shown in Figure 86, and a submenu 2, shown in Figure 87. Some of the selections differ depending on the designated carrier type of the card.

```

TDM Channel Configuration Menu 1
Module 15, Port C

> Long Haul
  Limited Long Haul

> T1 DSX-1(0 to 133ft)/0dB CSU
  T1 DSX-1(133 to 266ft)
  T1 DSX-1(266 to 399ft)
  T1 DSX-1(399 to 533ft)
  T1 DSX-1(533 to 655ft)
  T1 -7.5dB CSU
  T1 -15dB CSU
  T1 -22.5dB CSU

Return to LIU Mode and Channel Select Menu ...

```

Figure 86. TDM Channel Configuration Menu 1

```

TDM Channel Configuration Menu 2
Module 15, Port C

Transmit All Ones
> Transmit Data Normally

> Transmit PRBS Disable
  Transmit PRBS Enable

> Remote Loopback Disable
  Remote Loopback Enable

> Local Loopback Disable
  Local Loopback Enable

Return to LIU Mode and Channel Select Menu ...

```

Figure 87. TDM Channel Configuration Menu 2

As you configure the ports, the top selection in the LIU Mode and Channel Select Menu changes to Customized Mode to indicate that the port settings have been changed from their default values.

7. Adjust the settings as needed. Refer to Table 24 for the possible settings.

Table 24. T1/E1 Port Settings

Parameter	T1 Settings	E1 Settings
Receiver Sensitivity Setting	<input type="checkbox"/> Limited Long Haul <input type="checkbox"/> Long Haul (default)	<input type="checkbox"/> Short Haul <input type="checkbox"/> Long Haul (default)
Line Build Out	<input type="checkbox"/> DSX-1 CSU (0 to 133ft) (default) <input type="checkbox"/> DSX-1 (133 to 266ft) <input type="checkbox"/> DSX-1 (266 to 399ft) <input type="checkbox"/> DSX-1 (399 to 533ft) <input type="checkbox"/> DSX-1 (533 to 655ft) <input type="checkbox"/> -7.5dB CSU <input type="checkbox"/> -15dB CSU <input type="checkbox"/> -22.5dB CSU	<input type="checkbox"/> 75 Ohm Normal <input type="checkbox"/> 120 Ohm Normal (default) <input type="checkbox"/> 75 Normal with High Return Loss <input type="checkbox"/> 120 Normal with High Return Loss
Transmit All Ones	Menu selections from the AT-CV5M02 Management Card: <input type="checkbox"/> Transmit Data Normally (default) <input type="checkbox"/> Transmit All Ones Menu selections from the Console Port on the AT-CM70S Line Card: <input type="checkbox"/> Normal (default) <input type="checkbox"/> Unframed All Ones	Menu selections from the AT-CV5M02 Management Card: <input type="checkbox"/> Transmit Data Normally (default) <input type="checkbox"/> Transmit All Ones Menu selections from the Console Port on the AT-CM70S Line Card: <input type="checkbox"/> Normal (default) <input type="checkbox"/> Unframed All Ones
PRBS	<input type="checkbox"/> Enable <input type="checkbox"/> Disable (default)	<input type="checkbox"/> Enable <input type="checkbox"/> Disable (default)
Remote Loopback	<input type="checkbox"/> Enable <input type="checkbox"/> Disable (default)	<input type="checkbox"/> Enable <input type="checkbox"/> Disable (default)

8. To save your changes in the master configuration file, return to the Module Configuration Menu and select **Line Card Configuration** and **Save Line Card Configuration**.

## Configuring the T1/E1 Ports from the Console Port on the Line Card

---

This procedure explains how to configure the settings on the T1/E1 ports on the AT-CM70S Line Card from the card's Console port. This is the appropriate procedure to perform when the card's UART setting is set to UART local console mode and the chassis containing the line card does not have a management card.



---

### Caution

The Console port on the AT-CM70S Line Card does not have any security features like logon usernames or passwords. Anyone with physical access to the location of the card may alter the configuration settings of the T1/E1 ports on the device. The card and its chassis should be installed in a secure location, such as a locked wiring closet, to protect against unauthorized changes to its operating parameters.

---

---

### Note

The parameter settings of the SFP slot and the 10/100/1000Base-T port on the line card cannot be set through the Console port.

---

To configure the T1/E1 ports from the Console port on the AT-CM70S Line Card:

1. Configure the settings on your terminal or terminal emulator program as follows:
    - Bits per second: 115200
    - Data bits: 8
    - Parity: None
    - Stop bits: 1
    - Flow control: None
    - Echo typed characters locally: Enabled
- 

### Note

The settings on the Console port on the line card are not adjustable.

---

2. Connect the management cable included with the AT-CM70S Line Card to the Console port on the card and to the RS-232 port on your terminal or computer.
3. If the card is already running, the terminal screen will be blank. To display the card's menu shown in Figure 88, type **m** for menu and press Return.

```

                                AT-CM70S Local Console Menu
-----
Boot Configuration:
<a> Boot Data From                : Customized in EEPROM
<b> LIU Mode                       : T1
-----

Current Status:
T1 with B8ZS Coding (All 4 Channels)

      Channel 1   Channel 2   Channel 3   Channel 4
<1> Rec Sens Set   : Long Haul  Long Haul  Long Haul  Long Haul
<2> Line Build Out : DSX-1/0 CSU DSX-1/0 CSU DSX-1/0 CSU DSX-1/0 CSU
<3> Transmit All Is : Normal    Normal    Normal    Normal
<4> PRBS           : Disabled   Disabled   Disabled   Disabled
<5> Remote Loopback : Disabled   Disabled   Disabled   Disabled

Enter <Item#><space><Channel#> to change each channel's config.
Change will be saved automatically if EEPROM data was used.

Command>

```

Figure 88. Local Console Menu on the AT-CM70S Line Card

The first selection in the menu, <a> Boot Data From, returns the parameter settings of the T1/E1 ports to the default values. This selection initially says Manufacture Default, which indicates that the parameter settings on the ports are at their default values. As you configure the ports, it automatically changes to Customized in EEPROM. If at a later time you want to discard all of your changes and return the ports to the default values, type **a** (lowercase) and respond to the confirmation prompt.

The second selection, <b> LIU Mode, toggles the line card between T1 or E1 support, as explained in step 4.

The main part of the menu is a table with the current settings of the T1/E1 ports (channels). To change a setting of a port, refer to step 5.

4. To toggle the line card between T1 or E1 support:

---

**Note**

Changing the T1/E1 mode of the line card returns the port settings to the default values. Any changes to the port settings are discarded.

---

- a. Type **b** (lowercase) to select LIU Mode and press Return.

- b. At the confirmation prompt, type **Y** and press Return to implement the change or **N** and Return to cancel it.
5. To configure the settings of a T1/E1 port, enter the number of the setting you want to change followed by the port (channel) number, separated by a space. For example, to change the remote loopback setting for port 2, you enter:

**5 2**

Table 24 on page 198 lists the possible settings.

6. When you finish managing the line card, simply disconnect the management cable from the Console port. The port doesn't have a logout command.



## Chapter 8

# Configuring the Operations, Administration, and Maintenance Client

---

The sections in this chapter are:

- “Configuring an OAM Client” on page 204
- “Performing an OAM Loopback Test” on page 209
- “Displaying OAM Information for Local OAM Clients” on page 214
- “Displaying OAM Information for Remote OAM Clients” on page 221
- “Displaying OAM Statistics” on page 223
- “Viewing MIB Variables with OAM Variable Requests” on page 225

---

**Note**

For background information, refer to “OAM-based Features” on page 46.

---

## Configuring an OAM Client

---

You should set the operating modes of the AT-CM Line Cards to the OAM visible mode before configuring the OAM parameters. For instructions, refer to “Setting the Operating Mode” on page 145.

**Menus** To configure the OAM clients on the line cards from the menus:

1. From the Main Menu, select **Module Status and Configuration** to display the Module Configuration Menu. An example of the menu is shown in Figure 53 on page 139.
2. From the Module Status and Configuration Menu, select the AT-CM Line Card you want to configure. This displays the Port Management Menu shown in Figure 54 on page 140. You can configure only one card at a time.
3. Select **Port A**, the fiber optic port, on the line card. The OAM client is supported only on Port A. An example of the Port Management Menu is shown in Figure 54 on page 140.
4. From the Port Management Menu, select **OAM Configurations** to display the OAM Configurations menu in Figure 89.

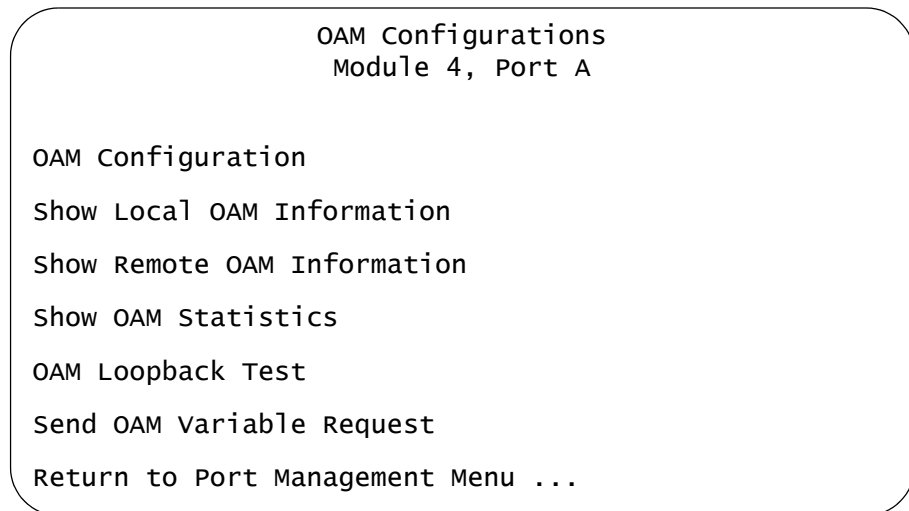


Figure 89. OAM Configurations Menu

5. From the OAM Configuration Menu, select **OAM Configuration** to display the OAM Configuration submenu, shown in Figure 90.

OAM Configuration Module 4, Port A	
Admin State	Enabled
Mode	Passive
Maximum OAMPDU Size	1518
Unidirectional Support	Yes
Loopback Support	Yes
Link Event Support	No
Variable Retrieval Support	Yes
Return to OAM Configurations ...	

Figure 90. OAM Configuration Submenu

The parameters in the OAM Configuration submenu are defined in Table 25. Your changes are immediately implemented by the line card.

Table 25. OAM Client Parameters

Parameter	Description
Admin State	<p>This parameter controls the state of the OAM client on the line card. The possible values are:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Enabled – This enables the OAM client. The line card can participate in the OAM Discovery process and perform other OAM functions. This is the appropriate setting for the OAM-based features on the AT-CM Line Cards. This is the default setting.</li> <li><input type="checkbox"/> Disabled – This disables the OAM client. The line card cannot participate in the OAM Discovery process because it will not generate or respond to OAMPDUs.</li> </ul>

Table 25. OAM Client Parameters

Parameter	Description
Mode	<p>This parameter specifies the mode of the OAM client on the line card. The possible values are:</p> <ul style="list-style-type: none"> <li data-bbox="683 405 1409 573">❑ Passive – This sets the client’s mode to Passive. Clients in the Passive mode can not initiate the Discovery process or send Loopback Control OAMPDUs or Variable Request OAMPDUs. This is the default setting.</li> <li data-bbox="683 590 1409 720">❑ Active – This setting sets the client’s mode to Active. Clients in this mode can initiate the Discovery process. This is the appropriate setting for the OAM-based features on the AT-CM Line Cards.</li> </ul>
Maximum OAMPDU Size	<p>This parameter specifies the maximum size in octets of the OAMPDUs. The OAM clients negotiate the maximum OAMPDU size during the discovery process. If a client receives an Information OAMPDU from its OAM counterpart with a different value for the maximum OAMPDU size, it uses the smaller value. For instance, if, during the Discovery process, a client receives an Information OAMPDU from its remote OAM counterpart that has a smaller value for the maximum OAMPDU size than its own value, the client uses the remote client’s value. The range of this value is 64 to 1518 octets. The default value is 1518 octets.</p>
Unidirectional Support	<p>This parameter controls whether or not the OAM client sends OAMPDUs if the receiver connector on the fiber optic port of Port A is not receiving a signal or network traffic. The possible values are:</p> <ul style="list-style-type: none"> <li data-bbox="683 1346 1409 1476">❑ Yes – The OAM client sends OAMPDUs even when the receive fiber optic connector on the fiber optic port on port A is not receiving a signal or network traffic. This is the default setting.</li> <li data-bbox="683 1493 1409 1661">❑ No – The OAM client sends OAMPDUs only when the receive fiber optic connector on the fiber optic port on port A is receiving a signal or network traffic, and the port has established a link with its remote counterpart.</li> </ul>

Table 25. OAM Client Parameters

Parameter	Description
Loopback Support	<p>This parameter controls whether or not the OAM client on the line card can participate in OAM loopback tests by returning test packets received on port A from another OAM client. This parameter applies only to OAM clients that return the test packets. It has no affect on OAM clients that generate the test packets. For information on this feature, refer to “Performing an OAM Loopback Test” on page 209. The possible values are:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Yes – The OAM client can return test packets from OAM loopback tests. This is the default setting.</li> <li><input type="checkbox"/> No – The OAM client cannot return test packets.</li> </ul>
Link Event Support	This parameter is not implemented in this release.
Variable Retrieval Support	<p>This parameter controls whether or not the OAM client on the line card can respond to variable retrieval requests from other OAM clients. A variable retrieval request is a query of an OAM client by another OAM client for the current value of a MIB object. The possible values are:</p> <p>Yes - The OAM client can respond to variable retrieval requests. This is the default setting.</p> <p>No - The OAM client cannot respond to variable retrieval requests.</p> <hr/> <p><b>Note</b> The AT-CM Line Cards do not support any of the MIB objects in the portion of the MIB tree that variable retrieval requests can access. As a result, the line cards will never return a MIB value in response to a variable retrieval request from an OAM client, such as another AT-CM Line Card.</p> <hr/>

6. To save your changes in the master configuration file, return to the Module Configuration Menu and select **Line Card Configuration** and **Save Line Card Configuration**. Alternatively, return to the Main Menu and select **Configuration** and **Save System and All Line Card Configurations**.

## Web Browser

To configure the OAM clients on the AT-CM Media Converter Line Cards from the web browser windows:

1. Select **Module Status & Configuration** from the menu bar.
2. From the Chassis View, click **Port A**, the fiber optic port, on the AT-CM Line Card you want to configure. The OAM client is only supported on Port A. Alternatively, select the Menu View and click the model name of the AT-CM Line Card.
3. If the **Port A** tab is not selected, select it.
4. Select the **OAM Configuration** tab to display the OAM Configuration window shown in Figure 91.

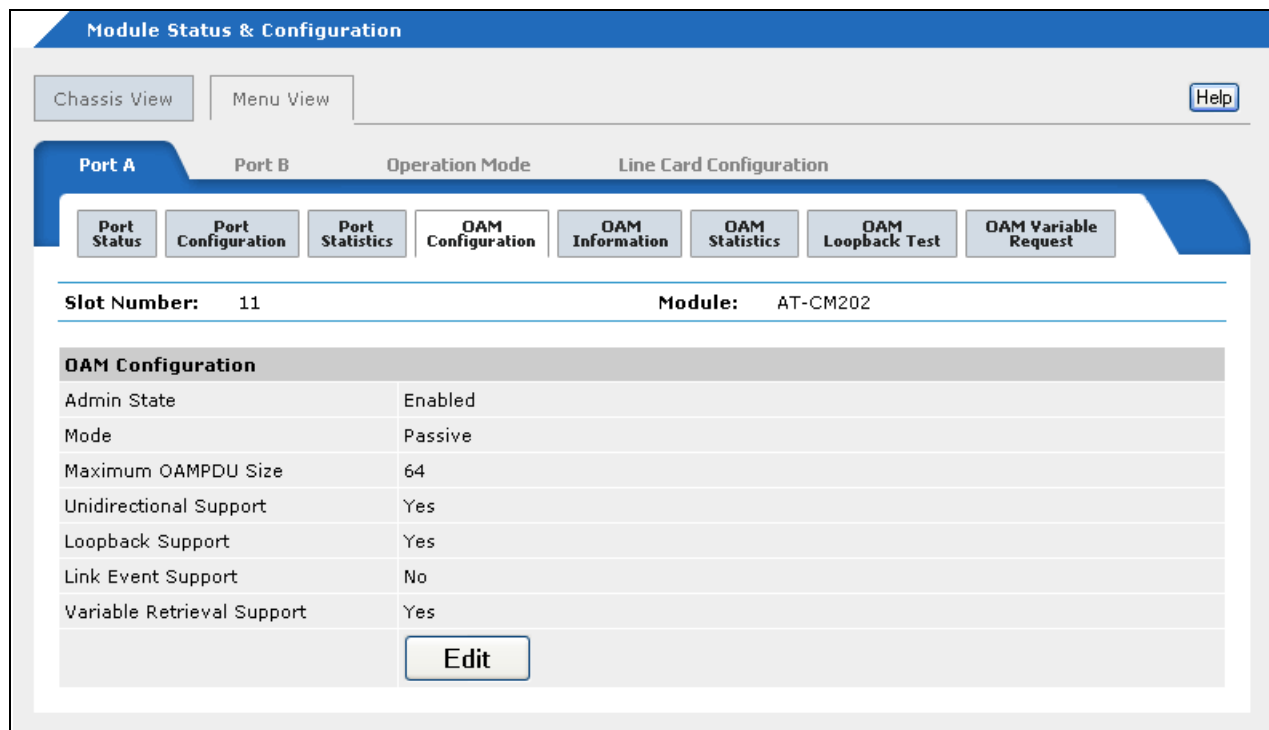


Figure 91. OAM Configuration Tab

If the OAM Configuration tab is not included in the window, either you did not select Port A or the line card is not set to the OAM visible mode or the OAM bypass mode.

5. To change the OAM settings, click **Edit** to display the OAM Configuration pop-up window and adjust the settings as needed. The parameters are defined in Table 25, "OAM Client Parameters" on page 205.
6. To save your changes in the master configuration file, click the **Line Card Configuration** tab, the **Current Configuration** tab, and the **Save Current Configuration** button.

## Performing an OAM Loopback Test

---

For background information, refer to “OAM Loopback Tests” on page 51.

**Menus** To perform the OAM loopback test from the menus:



---

**Caution**

This test is disruptive to network operations. Some network traffic may be lost. The local and remote media converter line cards do not forward network traffic during the test.

---

1. From the Main Menu, select **Module Status and Configuration** to display the Module Status and Configuration Menu. An example of the menu is shown in Figure 48 on page 128.
2. Select the local AT-CM Line Card you want to perform the loopback test. This displays the Module Configuration Menu for the line card. An example of the menu is shown in Figure 53 on page 139.
3. Select **Port A** to display the Port Management Menu, shown in Figure 54 on page 140.
4. From the Port Management Menu, select **OAM Configurations** to display the OAM Configuration Menu in Figure 89 on page 204.
5. From the OAM Configuration Menu, select **OAM Loopback Test** to display the OAM Loopback Test Menu, shown in Figure 92.

```
OAM Loopback Test
Module 11, Port = 1

Enable Remote Loopback
> Disable Remote Loopback

Start Loopback Test
> Stop Loopback Test

Show Loopback Test Statistics
Clear Loopback Test Statistics

Return to OAM Configurations ...
```

Figure 92. OAM Loopback Test Menu

6. From the OAM Loopback Test Menu, select **Enable Remote Loopback**.



---

**Caution**

The local media converter line card and its remote counterpart stop forwarding network traffic. Some network traffic may be lost.

---

---

**Note**

There may be a delay of several seconds before the menu reflects your selection.

---

If the line card is not configured correctly for the OAM loopback test, an error message is displayed. The messages are described here.

OAM port is disconnected.

This message indicates that port A on the local line card has not established a link with its counterpart on the remote line card, possibly because the fiber optic cable is not connected to the ports.

OAM is not in active mode.

This message indicates that the OAM mode of the line card is set to the passive mode instead of the active mode. To correct the problem, perform the procedure “Configuring an OAM Client” on page 204 and change the Mode setting from Passive to Active in the OAM Configuration submenu.

Line card not in OAM visible mode.

This message indicates that the line card’s operational mode is set to the OAM bypass mode instead of the OAM visible mode. To correct the problem, perform the procedure “Setting the Operating Mode” on page 145 and select the OAM visible mode from the Operating Mode Config Menu.

If you select Enable Remote Loopback and, after several seconds, it remains unselected, it probably means that support for the loopback test is disabled on the remote line card.

7. To begin the test, select **Start Loopback Test** from the OAM Loopback Test Menu. The test starts immediately.

8. To view test statistics, select **Show Loopback Test Statistics**. The Show Loopback Test Statistics window is shown in Figure 93.

Show Loopback Test Statistics	
Module = 5, Port = 1	
Number of Seconds	71
Number of Tx Frames	71
Number of Rx Frames	71
Number of Rx Errored Frames	0
Number of Tx Bytes	4260
Number of Rx Bytes	4260
Number of Rx Errored Bytes	0
Number of Tx Bits	34080
Number of Rx Bits	34080
Number of Rx Errored Bits	0
Return to OAM Loopback Test...	

Figure 93. Show Loopback Test Statistics Window

The first line displays the duration of the test in seconds. The counters display the number of test packets the local OAM client transmitted to its remote counterpart over the fiber optic connection, and the number of packets the local client received back. The measurements are given in frames, bytes (octets) and bits. The local client should receive the same number of test frames, bytes, and bits as it transmitted. Test frames are sixty octets in length.

9. You can stop the test at any time by selecting **Stop Loopback Test** from the OAM Loopback Test Menu.
10. To resume normal network operations of the line card, select **Disable Remote Loopback**.
11. To clear the statistics counters, select **Clear Loopback Test Statistics**.

**Web Browser** To run the loopback test from the web browser windows:

---

**Caution**  
 This test is disruptive to network operations. Some network traffic may be lost. The local and remote media converter line cards do not forward network traffic during the test.

---

1. Select **Module Status & Configuration** from the menu bar.
2. From the Chassis View, click **Port A**, the fiber optic on the AT-CM Line Card you want to perform the loopback test. Alternatively, select the Menu View and click the model name of the AT-CM Line Card.
3. If the **Port A** tab is not selected, select it. The OAM client is only supported on Port A.
4. Click the **OAM Loopback Test** tab to display the OAM Loopback Test tab in Figure 94.

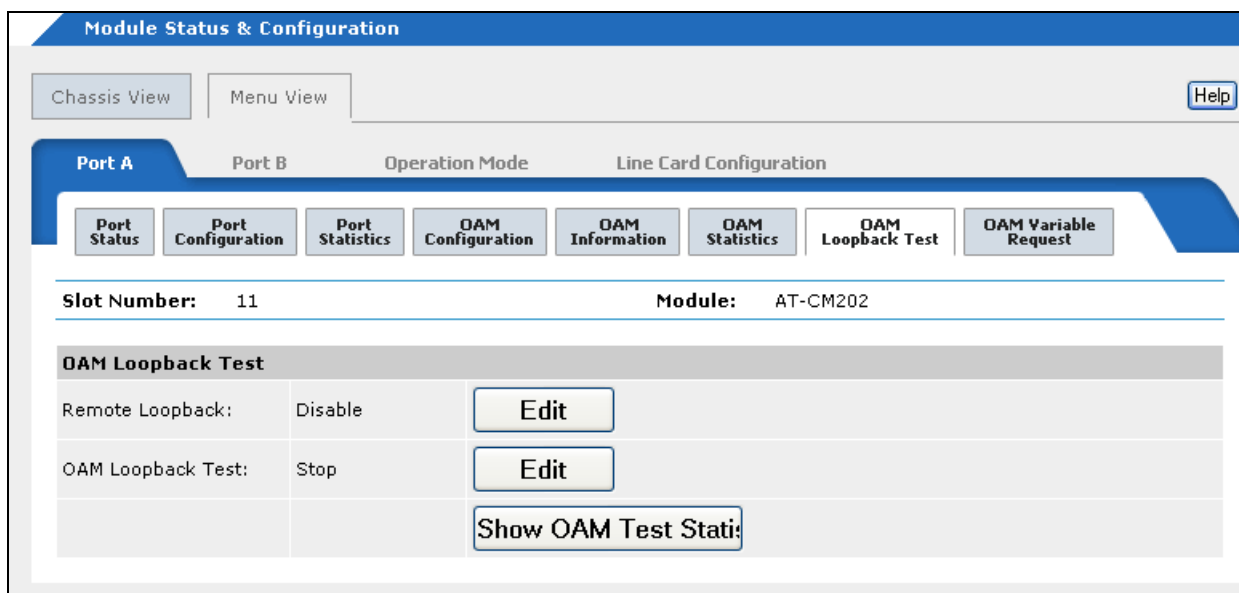


Figure 94. OAM Loopback Test Tab

5. To activate the loopback test on the local line card, click **Edit** in the Remote Loopback field to display a pop-up window and select **Enable** from the pull-down menu.

---

**Caution**  
 At this point the local media converter line card and its remote counterpart stop forwarding network traffic. Some network traffic may be lost.

---

6. To start the test, click **Edit** in the OAM Loopback Test field to display a pop-up window and select **Start** from the pull-down menu. The local line card begins to transmit test packets to the remote line card.
7. To view test statistics, click **Show OAM Test Statistics**. An example of the counters is shown in Figure 95.

OAM Test Statistics	
Number of Seconds	0
Number of Tx Frames	0
Number of Rx Frames	0
Number of Rx Errored Frames	0
Number of Tx Bytes	0
Number of Rx Bytes	0
Number of Erroed Bytes	0
Number of Tx Bits	0
Number of Rx Bits	0
Number of Rx Errored Bits	0

[Clear Loopback Statistics](#)

Figure 95. OAM Test Statistics

The first line displays the duration of the test in seconds. The counters display the number of test packets the local OAM client transmitted to its remote counterpart over the fiber optic connection, and the number of packets the local client received back. The measurements are given in frames, bytes (octets) and bits. Test frames are sixty octets in length.

To clear the counters, click **Clear Loopback Statistics**.

8. To stop the test, change the OAM Loopback Test field to Stop by clicking **Edit** and selecting **Stop** from the pull-down menu. The line card stops transmitting test packets.
9. To resume normal network operations on the line cards, change the Remote Loopback field to Disable by clicking **Edit** and selecting **Disable** from the pull-down menu. The local and remote line cards resume forwarding network traffic.

## Displaying OAM Information for Local OAM Clients

---

The procedures in this section explain how to view OAM status information on local OAM clients on the AT-CM Line Cards.

---

**Note**

For you to view OAM information, the AT-CM Line Cards have to be set to the OAM visible mode.

---

- Menus** To display status information for local OAM clients from the menus:
1. From the Main Menu, select **Module Status and Configuration** to display the Remote Module Status and Configuration Menu. An example of the menu is shown in Figure 48 on page 128.
  2. Select the local line card whose OAM information you want to view. This displays the Module Configuration Menu for the line card. An example is shown in Figure 53 on page 139.
  3. Select **Port A** to display the Port Management Menu shown in Figure 54 on page 140. OAM is only supported on port A of the line cards.
  4. From the Port Management Menu, select **OAM Configurations** to display the OAM Configuration Menu, An example of the menu is shown in Figure 89 on page 204.
  5. From the OAM Configuration Menu, select the **Show Local OAM Information** window to display the Show Local OAM Information Menu, shown in Figure 96 on page 215.

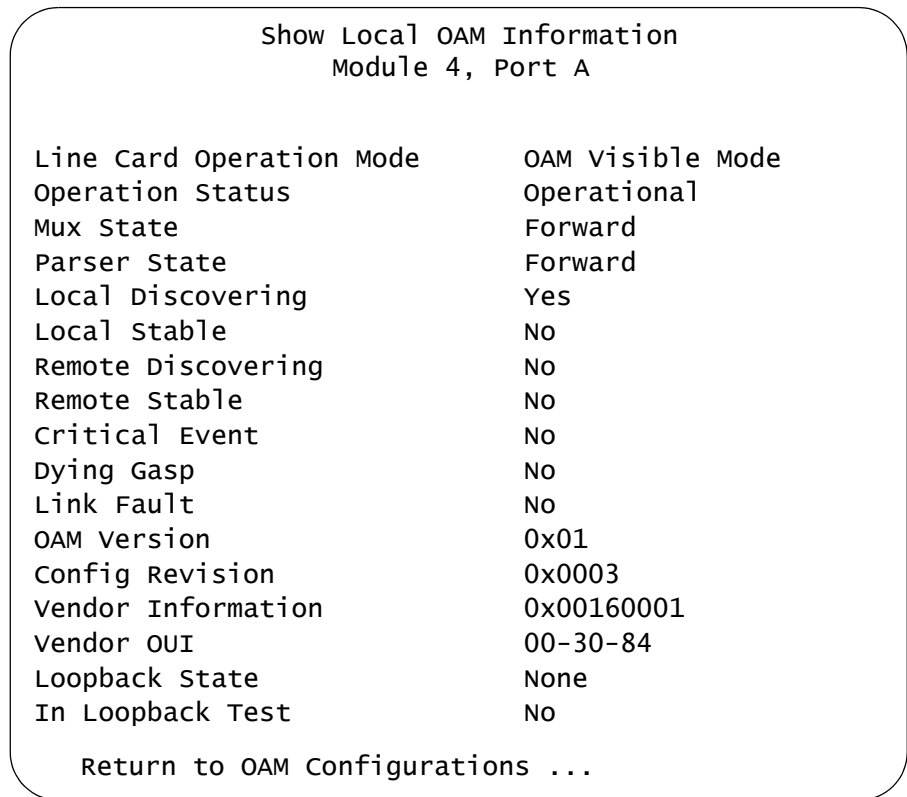


Figure 96. Show Local OAM Information Window

This window is for viewing purposes only. The items in the window are defined in Table 26.

Table 26. Show Local OAM Information Window

Column	Description
Line Card Operation Mode	<p>Displays the OAM operating mode of the line card. The possible values are:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> OAM Bypass Mode – In this mode the line card does not process any OAMPDU packets it receives. Rather, it handles them like normal network traffic forwarding them onto the other port. This allows the line card to be used in a network where the Converteon chassis is not part of the IEEE802.3ah end points. In this mode, the OAM function of the line card is disabled. The module will pass all OAMPDUs whose vendor OUI is not Allied Telesis.</li> </ul>

Table 26. Show Local OAM Information Window

Column	Description
Line Card Operation Mode (Continued)	<ul style="list-style-type: none"> <li><input type="checkbox"/> OAM Visible Mode – In this mode the line card generates and responds to OAMPDU packets. As such, it can initiate the OAM discovery process, participate in OAM loopback tests and send OAM variable requests.</li> </ul>
Operation Status	<p>Indicates the OAM operating status. The possible values are:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Disabled – The OAM client is disabled.</li> <li><input type="checkbox"/> Passive Wait – The OAM client is waiting for its remote OAM counterpart to initiate the OAM discovery process. The client cannot initiate the OAM discovery process because its mode has been set to passive.</li> <li><input type="checkbox"/> Active Send Local – The OAM client has initiated the OAM discovery process and is waiting for a response from the remote OAM client to its queries. The client is able to initiate the OAM discovery process because its mode has been set to active.</li> <li><input type="checkbox"/> Send Local and Remote – The local OAM client is sharing its OAM settings with the remote client by sending OAM Information OAMPDUs that contain its settings and the OAM settings received from the remote client.</li> <li><input type="checkbox"/> IOAM Peering Locally Rejected – The remote OAM client has rejected the OAM information from the local client.</li> </ul>
Operation Status (continued)	<ul style="list-style-type: none"> <li><input type="checkbox"/> OAM Peering Remotely Rejected – The local OAM client has rejected the OAM information from the remote client.</li> <li><input type="checkbox"/> Operational – The OAM client is in the operational state. The AT-CM Line Cards have to be in this state to support the OAM-based features.</li> </ul>
Mux State	<p>Displays the state of the multiplexer function, which governs the flow of frames from the MAC client. The possible values are:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Forward – Multiplexer passes MAC client frames to subordinate sublayer.</li> <li><input type="checkbox"/> Discard – Multiplexer discards MAC client frames.</li> </ul>

Table 26. Show Local OAM Information Window

Column	Description
Parser State	<p>Indicates the state of the parser function in the OAM peer as reflected in the latest OAMPDU. This value is changed based on loopback actions by either the local or remote station. The possible values are:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Forward – Parser passes received non-OAMPDUs to superior sublayer.</li> <li><input type="checkbox"/> Loopback – Parser passes received non-OAMPDUs to Multiplexer during remote loopback test.</li> <li><input type="checkbox"/> Discard – Parser discards received non-OAMPDUs.</li> </ul>
Local Discovering	<p>Indicates whether the local station can accept or reject the configuration of the peer OAM entity.</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Yes – Local station accepts the configuration of the peer OAM entity. (default)</li> <li><input type="checkbox"/> No – Local station rejects the configuration of the peer OAM entity.</li> </ul>
Local Stable	<p>Indicates whether or not the local OAM client is satisfied with the OAM information it received from the remote OAM client.</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Yes – Indicates that the local OAM client is satisfied with the OAM information from the remote OAM client.</li> <li><input type="checkbox"/> No – Indicates that the local OAM client has not received any OAM information or is not satisfied with the OAM information from the remote OAM client.</li> </ul>
Remote Discovering	<p>Indicates the remote station can accept or reject the configuration of the peer OAM entity.</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Yes – Remote station accepts the configuration of the peer OAM entity.</li> <li><input type="checkbox"/> No – Remote station rejects the configuration of the peer OAM entity.</li> </ul>

Table 26. Show Local OAM Information Window

Column	Description
Remote Stable	<p>Indicates whether or not the remote OAM client is satisfied with the OAM information it received from the local OAM client. Possible values are:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Yes – Indicates that the remote OAM client is satisfied with the information it received from the local OAM client.</li> <li><input type="checkbox"/> No – Indicates that the remote OAM client has not received any OAM information or is not satisfied with the information from the local OAM client.</li> </ul>
Critical Event	<p>Indicates whether or not the local OAM client received a critical event notification from the remote OAM client. A critical event notification indicates a severe error condition that does not result in a complete reset or reboot by the remote client.</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Yes – The local OAM client received a critical event notification from the remote OAM client.</li> <li><input type="checkbox"/> No – The local OAM client has not received a critical event notification.</li> </ul>
Dying Gasp	<p>Indicates whether or not the local OAM client received a dying gasp notification from the remote OAM client. A dying gasp notification indicates that the remote chassis with the remote OAM client experienced a power failure.</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Yes – The local OAM client received a dying gasp notification.</li> <li><input type="checkbox"/> No – The local OAM client has not received a dying gasp notification.</li> </ul> <p>For background information, refer to “Dying Gasp Feature” on page 52.</p>
Link Fault	<p>Indicates whether or not the receiver connector on the fiber optic port on port A is receiving a signal.</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Yes – The receiver connector is receiving a signal.</li> <li><input type="checkbox"/> No – received connector is not receiving a signal.</li> </ul>
OAM Version	<p>Indicates the version supported by the media converter line card. This field contains the value “0x01” to indicate compliance with Version 1 of this protocol.</p>

Table 26. Show Local OAM Information Window

Column	Description
Config Revision	Indicates the current revision of the Information TLV. The value of this field starts at zero and be incremented each time something in the Information TLV changes. Upon reception of an Information TLV from a peer, an OAM Client may use this field to decide if it needs to be processed (an Information TLV that is identical to the previous Information TLV doesn't need to be parsed as nothing in it has changed).
Vendor Information	Indicates the 32-bit identifier that may be used to differentiate a vendor's product models/versions.
Vendor OUI	Contains the Organizationally Unique Identifier (OUI) of 00-30-84 for Allied Telesis.
Loopback State	<p>Indicates the current loopback state of the OAM client.</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> None – No loopback initiated.</li> <li><input type="checkbox"/> Initiating Loopback – The local OAM client is initiating a loopback test with the remote client.</li> <li><input type="checkbox"/> Remote in Loopback – The remote OAM client has received the loopback command from the local client and is ready to participate or is already participating in the loopback test.</li> <li><input type="checkbox"/> Terminating Loopback – The local OAM client is ending the loopback test.</li> </ul>
In Loopback Test	<p>Indicates whether or not the OAM client is currently running a loopback test.</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Yes – The OAM client is running a loopback test.</li> <li><input type="checkbox"/> No – The OAM client is not running a loopback test.</li> </ul>

**Web Browser** To display status information for local OAM clients from the web browser windows:

1. Select **Module Status & Configuration** from the menu bar.
2. From the Chassis View, click **Port A**, the fiber optic port, on the AT-CM Line Card whose OAM information you want to view. Alternatively, select the Menu View and click the model name of the AT-CM Line Card.
3. If Port A is not selected, select it. The OAM client is only supported on Port A.
4. Click the **OAM Local Information** tab to display the window in Figure 97.

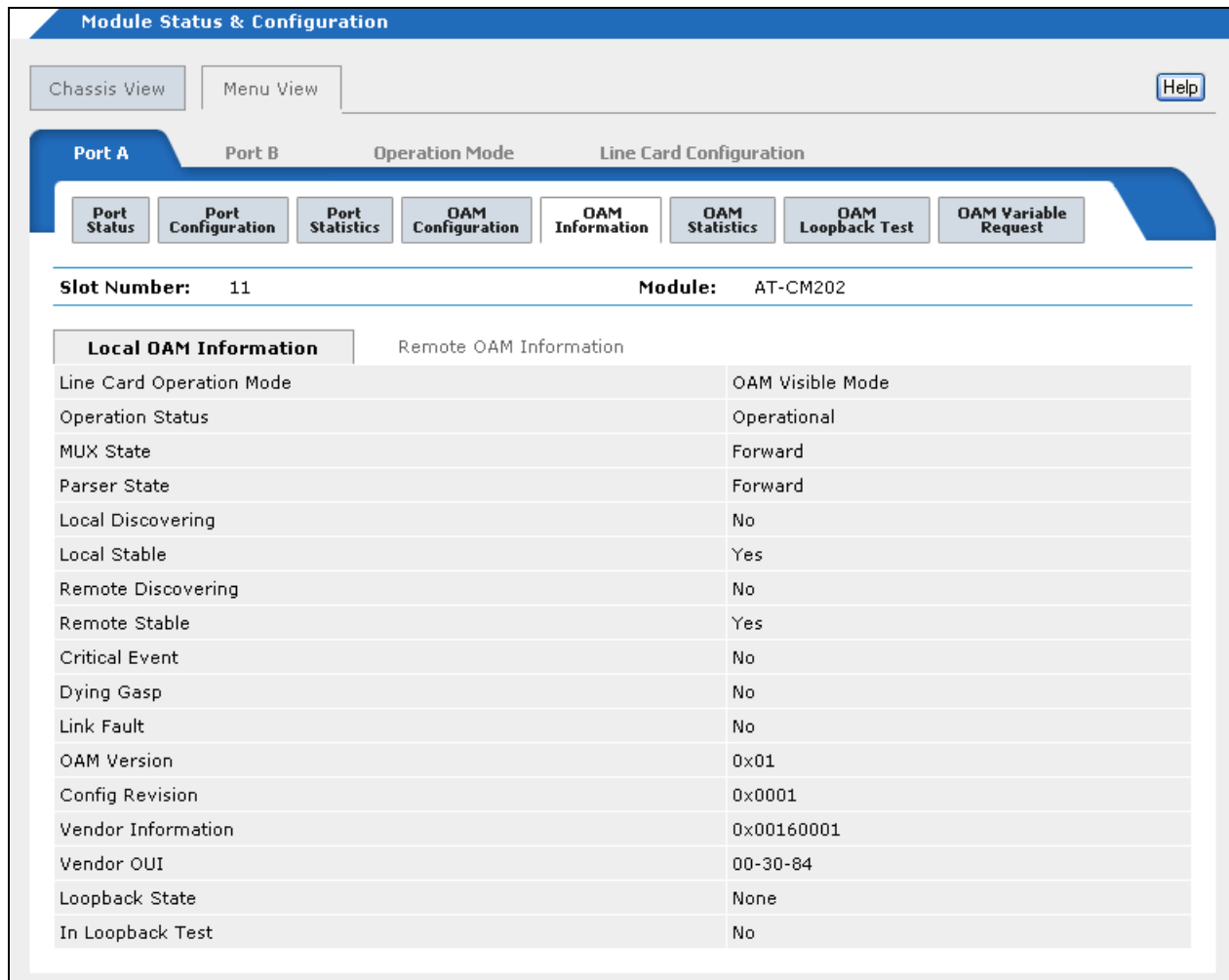


Figure 97. OAM Local Information Tab

This tab is for viewing purposes only. The items are defined in Table 26 on page 215.

## Displaying OAM Information for Remote OAM Clients

The procedures in this section are used to view OAM status information on remote OAM clients connected to local AT-CM Line Cards.

### Note

These procedures require that the local and remote AT-CM Line Cards be set to the OAM visible mode.

**Menus** To display status information for remote OAM clients from the menus:

1. From the Main Menu, select **Module Status and Configuration** to display the Module Status and Configuration Menu, shown in Figure 48 on page 128.
2. Select the local card that is connected to the remote OAM device whose status information you want to view. The Module Configuration Menu is shown in Figure 53 on page 139.
3. Select **Port A**, the fiber optic port, to display the Port Management Menu in Figure 54 on page 140. OAM is only supported on port A.
4. From the Port Management Menu, select **OAM Configurations** to display the OAM Configuration Menu, shown in Figure 89 on page 204.
5. From the OAM Configuration Menu, select **Show Remote OAM Information** to display the Show Remote OAM Information window, shown in Figure 98.

Show Remote OAM Information Module 11, Port A			
MAC Address	00:0c:46:9a:21:c9	Mux State	Forward
Parser State	Forward	Local Discovering	Yes
Local Stable	No	Remote Discovering	No
Remote Stable	No	Critical Event	No
Dying Gasp	No	Link Fault	No
OAM Version	0x01	Config Revision	0x0003
Vendor Info	0x00160001	Vendor OUI	00-30-84
Mode	Active	Max OAMPDU Size	1518
Loopback Support	Yes	Event Support	No
Variable Support	Yes	Unidirect Support	Yes
Return to OAM Configurations ...			

Figure 98. Show Remote OAM Information Window

This window is for viewing purposes only. Refer to Table 26 on page 215 for definitions of the items in the window.

### Web Browser

To display OAM status information about remote OAM clients from the web browser windows:

1. Select **Module Status & Configuration** from the menu bar.
2. From the Chassis View, click **Port A**, the fiber optic port, on the AT-CM Line Card that is connected to the remote OAM device whose status information you want to view. Alternatively, select the Menu View and click the model name of the AT-CM Line Card.
3. If the **Port A** tab is not selected, select it. The OAM client is only supported on Port A.
4. Click the **OAM Information** tab to display the tab in Figure 97 on page 220.
5. Click the **Remote OAM Information** tab to display the tab in Figure 99.

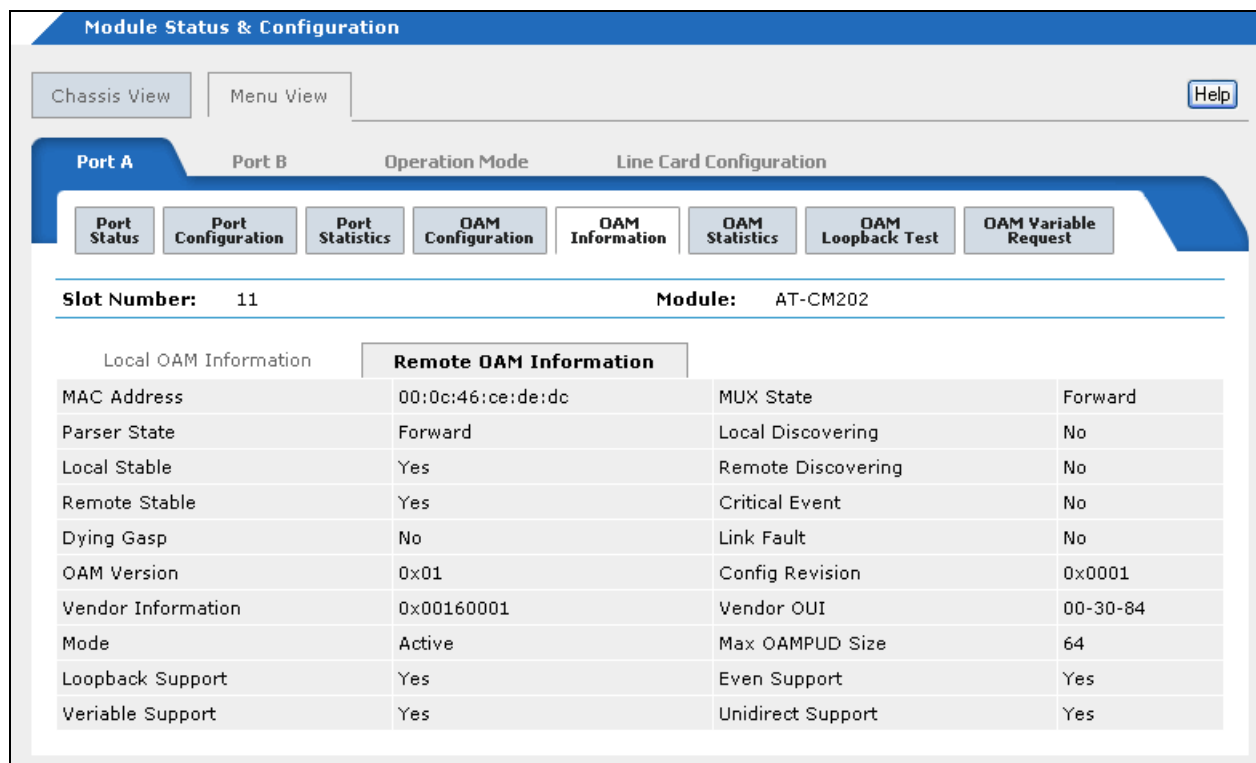


Figure 99. Remote OAM Information Tab

This tab is for viewing purposes only. Refer to Table 26 on page 215 for item definitions.

## Displaying OAM Statistics

### Note

These procedures require that the local and remote AT-CM Line Cards be set to the OAM visible mode.

**Menus** To display OAM statistics for local OAM clients from the menus:

1. From the Main Menu, select **Module Status and Configuration** to display the Module Status and Configuration Menu, shown in Figure 48 on page 128.
2. Select the AT-CM Line Card whose OAM statistics you want to view. The Module Configuration Menu is shown in Figure 53 on page 139.
3. Select **Port A** to display the Port Management Menu in Figure 54 on page 140.
4. From the Port Management Menu, select **OAM Configurations** to display the OAM Configuration Menu in Figure 89 on page 204.
5. From the OAM Configuration Menu, select **Show OAM Statistics** to display the Show OAM Statistics window in Figure 100.

Show OAM Statistics	
Module 11, Port = A	
Tx OAMPDUS	70917
Rx OAMPDUS	70918
Tx Information OAMPDUS	70917
Rx Information OAMPDUS	70918
Tx Event OAMPDUS	0
Rx Unique Event OAMPDUS	0
Rx Duplicate Event OAMPDUS	0
Tx Loopback Control OAMPDUS	0
Rx Loopback Control OAMPDUS	0
Tx Variable Request OAMPDUS	0
Rx Variable Request OAMPDUS	0
Tx Variable Response OAMPDUS	0
Rx Variable Response OAMPDUS	0
Tx Organizational Specific OAMPDUS	0
Rx Organizational Specific OAMPDUS	0
Rx Unsupported OAMPDUS	0
Return to OAM Configurations ...	

Figure 100. Show OAM Statistics Window

Refer to the IEEE 802.3ah standard for definitions of the different types of OAMPDUs.

### Web Browser

To display OAM statistics for local OAM clients from the web browser windows:

1. Select **Module Status & Configuration** from the menu bar.
2. From the Chassis View, click **Port A** on the AT-CM Line Card whose OAM statistics you want to view. Alternatively, select the Menu View and click the model name of the AT-CM Line Card.
3. If the **Port A** tab is not selected, select it. The OAM client is only supported on Port A.
4. Click the **OAM Statistics** tab to display the window in Figure 101.

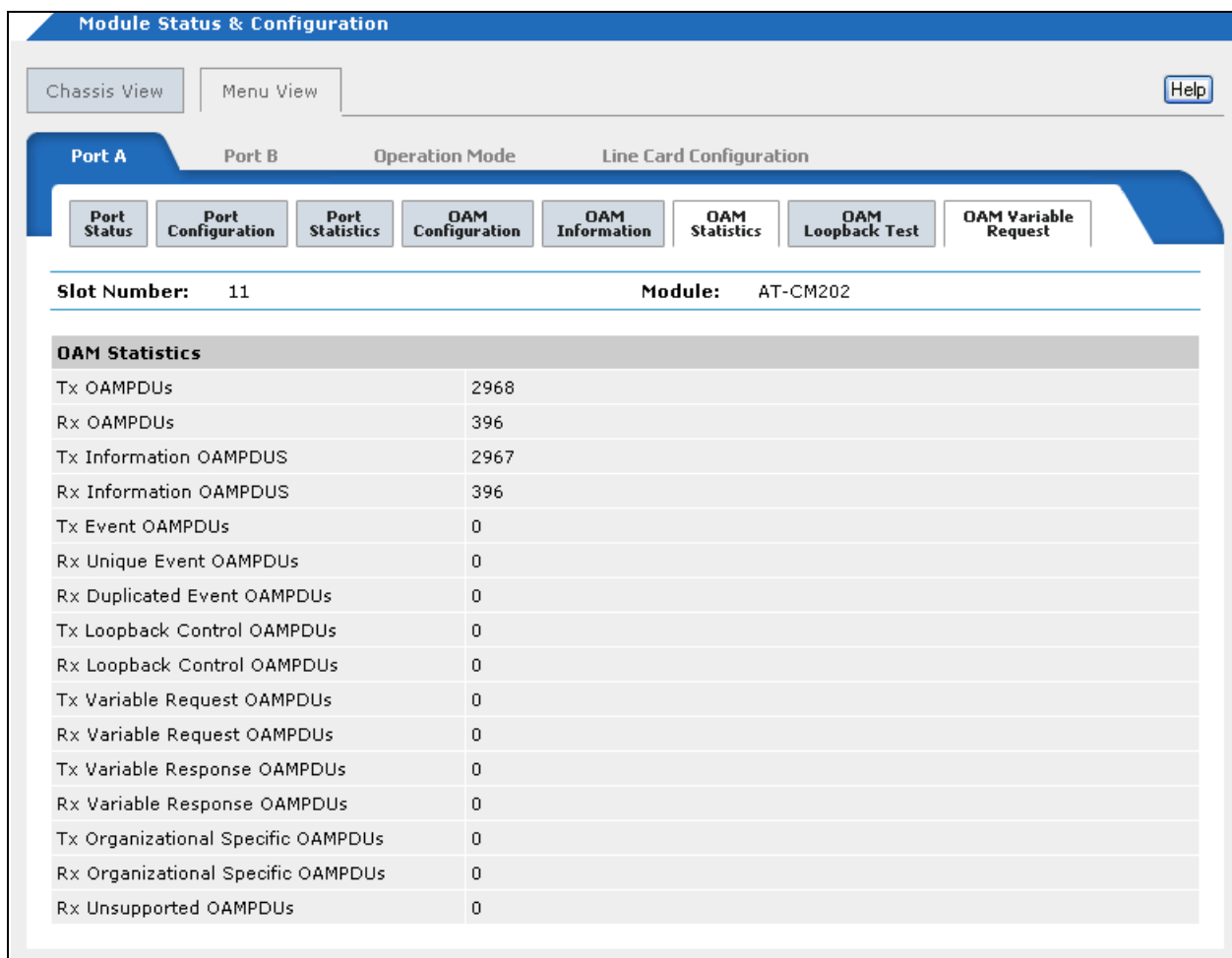


Figure 101. OAM Statistics Tab\*

Refer to the IEEE 802.3ah standard for definitions of the different types of OAMPDUs.

## Viewing MIB Variables with OAM Variable Requests

---

These procedures are used to send OAM variable requests from the fiber optic ports on local AT-CM Line Cards to remote OAM-compatible devices. OAM variable requests are used to view the values of MIB objects on remote devices. For background information, refer to “OAM Variable Requests” on page 55.

---

### Note

These procedures require that the local and remote AT-CM Line Cards be set to the OAM visible mode.

---



---

### Note

The AT-CM Line Cards do not support any of the MIB objects in the portion of the MIB tree that variable requests can access. So although the line cards can be used to send variable requests to query other OAM-compatible devices for MIB values, they do not respond to variable requests.

---

**Menus** To send MIB variable requests from the menus:

1. From the Main Menu, select **Module Status and Configuration** to display the Module Status and Configuration Menu shown in Figure 48 on page 128.
2. Select the local AT-CM Line Card whose remote OAM counterpart you want to query with an OAM variable request. The Module Configuration Menu is shown in Figure 53 on page 139.
3. Select **Port A**, the fiber optic port, on the line card to display the Port Management Menu shown in Figure 54 on page 140.
4. From the Port Management Menu, select **OAM Configurations** to display the OAM Configuration Menu shown in Figure 89 on page 204.
5. From the OAM Configuration Menu, select **Send OAM Variable Request**. The prompt in Figure 102 is displayed.

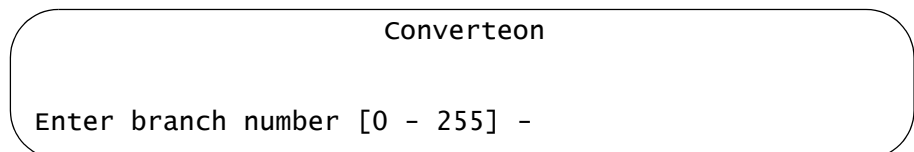


Figure 102. Enter Branch Number Prompt

6. Enter the branch number of the MIB package or object to be returned. The range is 0 to 255. The prompt in Figure 103 is displayed.

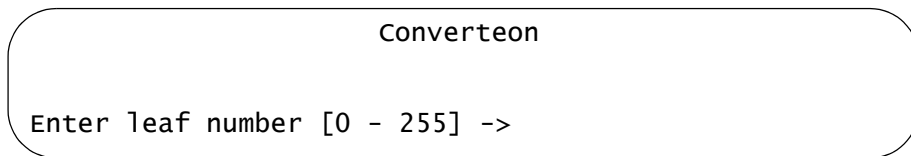


Figure 103. Enter Leaf Number Prompt

7. Enter the leaf number of the package or object to be returned. The range is 0 to 255.

If the remote OAM device has a value for the corresponding MIB object, the value is displayed on the screen.

### Web Browser

To send MIB variable requests from the web browser windows:

1. Select **Module Status & Configuration** from the menu bar.
2. From the Chassis View, click **Port A**, the fiber optic port, on the AT-CM Line Card whose remote counterpart you want to query with an OAM variable request. Alternatively, select the Menu View and click the model name of the AT-CM Line Card.
3. If the **Port A** tab is not selected, select it.
4. Click the **OAM Variable Request** tab to display the window in Figure 104.

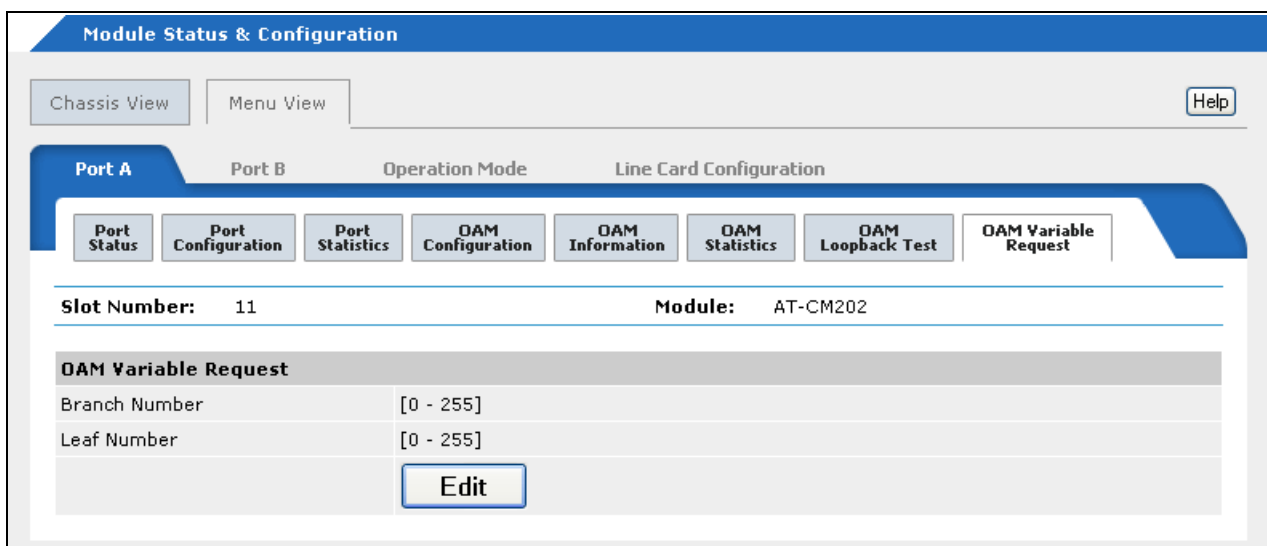


Figure 104. OAM Variable Request Tab

5. Click **Edit** to display the OAM Variable Request pop-up window.
6. Select the **Branch Number** field and enter the branch number of the MIB package or object to be returned. The range is 0 to 255.
7. Select the **Leaf Number** field and enter the leaf number of the package or object to be returned. The range is 0 to 255.
8. Click **Send**.

If the remote OAM device has a value for the corresponding MIB object, the value is displayed on the screen.



## Chapter 9

# Configuring AT-CM Line Cards for Dying Gasp

---

The sections in this chapter are:

- “Configuring the AT-CM Line Cards” on page 230
- “Testing the Feature” on page 235

For background information, refer to “Dying Gasp Feature” on page 52.

## Configuring the AT-CM Line Cards

---

This procedure explains how to configure the settings of the AT-CM Line Cards for the dying gasp feature. The procedure has you do the following:

- ❑ Verify the hardware version numbers of the line cards.
- ❑ Verify the version numbers of the AT-S73 Management Software on the line cards.
- ❑ Set the operating modes of the line cards to OAM visible.
- ❑ Set the OAM operating mode of the fiber optic ports on the line cards to active.

You have to perform this procedure at a managed Converteon chassis that has the AT-CV5M02 Management Card. The AT-CM Line Cards that will be deployed in the unmanaged AT-CV1203 Chassis at the remote sites have to be configured in a managed chassis before they are installed in the AT-CV1203 Chassis.

The following procedure uses the menus to configure the line cards. You can also perform the procedure from the web browser windows.

To verify and configure the AT-CM Line Card for the dying gasp feature from the menus:

1. Install the AT-CM Line Card in the AT-CV5000 Chassis that has the AT-CV5M02 Management Card.
2. Start a local management session on the chassis.
3. From the Main Menu select **Administration -> Diagnostics -> Line Card Image Version**.
4. Examine the hardware version number of the AT-CM Line Card. The version numbers are displayed as extensions of the model names, like "-v2." Refer to Table 27 for the supported hardware versions. Line cards without a version number do not support the dying gasp feature.

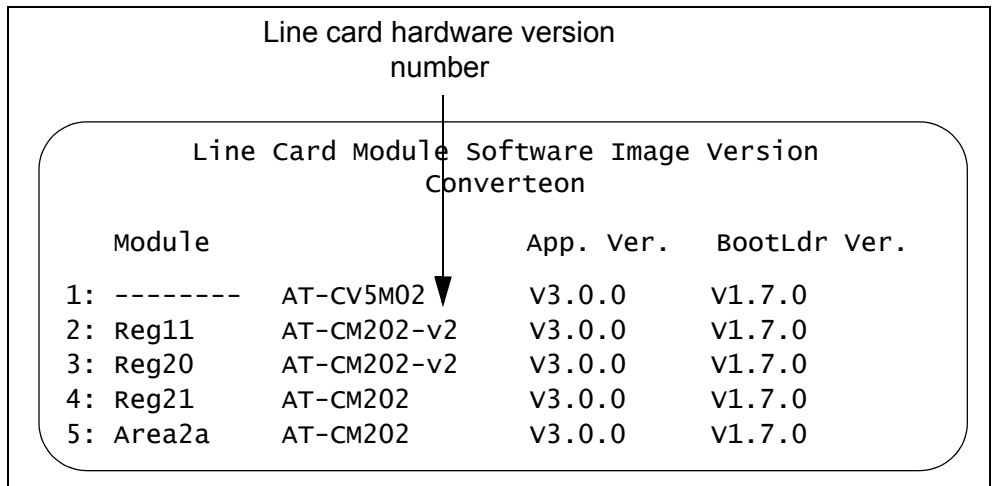


Figure 105. Line Card Module Software Image Version - Hardware Version Numbers

Table 27. Version Numbers of AT-CM Line Cards that Support the Dying Gasp Feature

Media Converter Line Card	New Hardware Version
AT-CM201	Version 2
AT-CM202	Version 2
AT-CM202/1	Version 2
AT-CM202/2	Version 2
AT-CM212A/1	Version 2
AT-CM212B/1	Version 2
AT-CM70S	Version 2
AT-CM2KOS	Version 3

- In the same window, check the version number of the AT-S73 Management Software on the AT-CM Line Card. It should be Version 2.0.1 or later. Earlier versions do not support this feature.

AT-S73 Management Software  
Version Number

Line Card Module Software Image Version  
Conversion

	Module	App. Ver.	BootLdr Ver.
1:	----- AT-CV5M02	V3.0.0	v1.7.0
2:	Reg11 AT-CM202-v2	V3.0.0	v1.7.0
3:	Reg20 AT-CM202-v2	V3.0.0	v1.7.0
4:	Reg21 AT-CM202	V3.0.0	v1.7.0
5:	Area2a AT-CM202	V3.0.0	v1.7.0

Figure 106. Line Card Module Software Image Version - AT-S73 Version Numbers

6. Return to the Main Menu.
7. Select **Module Status and Configuration**.
8. In the Module Status and Configuration window, verify that the operating mode of the line card is set to OAM visible mode (OamVisib).

Line card operating modes

Module Status and Configuration  
Conversion

MODULE INFO				FIBER PORT				COPPER PORT											
Mod_Name	CardType	Ver	ST	OperMode	IPC	AC	VER	ST	SP	FC	IngRL	EgrRL	OAM	ST	SP	FC	IngRL	EgrRL	AN
1	-----	AT-CV5M02	*	-----	800		V300	-	---	-	---	---	*	100	-	---	---	---	-
2	Reg11	AT-CM202-v2	*	OamVisib	o**	N	V300	*	100	N	0	0	A	*	100	N	0	0	Y
3	Reg20	AT-CM202-v2	*	OamVisib	o*o	N	V300	*	100	N	0	0	*oo	*	100	N	0	0	Y
4	Reg21	AT-CM202-v2	*	OamVisib	o*o	N	V300	*	100	N	0	0	*oo	*	100	N	0	0	Y
5	Area2a	AT-CM202-v2	*	OamVisib	o*o	N	V300	*	100	N	0	0	*oo	*	100	N	0	0	Y
6	Area2b	AT-CM202-v2	*	OamVisib	o*o	N	V300	*	100	N	0	0	*oo	*	100	N	0	0	Y
7	a121	AT-CM202-v2	*	OamVisib	o*o	N	V300	*	100	N	0	0	*oo	*	100	N	0	0	Y
8	Reg12	AT-CM202-v2	*	OamVisib	o*o	N	V300	*	100	N	0	0	+oo	*	100	N	0	0	Y
9		AT-CM202-v2	*	OamVisib	o*o	N	V300	*	100	N	0	0	*oo	*	100	N	0	0	Y
10		AT-CM202-v2	*	OamVisib	o*o	N	V300	*	100	N	0	0	*oo	*	100	N	0	0	Y
11		AT-CV102	*	LinkTest				*	100	N	---	---	---	*	100	-	---	---	-
12		AT-CV102	*	LinkTest				*	100	N	---	---	---	*	100	-	---	---	-
13		AT-CV102	*	LinkTest				*	100	N	---	---	---	*	100	-	---	---	-
14		AT-CV102	*	LinkTest				*	100	N	---	---	---	*	100	-	---	---	-
15		AT-CV102	*	LinkTest				*	100	N	---	---	---	*	100	-	---	---	-

More ...  
Return to Main Menu ...

Figure 107. Module Status and Configuration Menu

9. Highlight the line card you want to configure and press Return to display the Module Configuration Menu for the card. The menu is shown in Figure 53 on page 139.

---

**Note**

If the line card is already set to the OAM visible mode, go to step 11. Otherwise, continue to the next step.

---

10. Select **Configure Operating Mode** to display the Operating Mode Config Menu for the line card.
11. From the Operating Mode Config Menu, select **OAM Visible Mode**. This confirmation prompt is displayed:  
  
warning: Changing the Operation Mode will reset the line card.  
Change operation mode now? (Yes or No):
12. Type **Y**. This prompt is displayed:  
  
If auto-copy is enable, operation mode change need to be saved to take affect.  
Save line card configuration before rebooting? (Yes or No):
13. Type **Y** for yes to update the master configuration file on the management card with the new setting for the card's operating mode. This step is especially important if the auto-copy feature is activated on the card's slot. If the card's operating mode isn't saved in the master configuration file, the new setting will not take affect because the card, after resetting, will revert to its previous operating mode. If you are not sure whether or not the auto-copy feature is enabled on the slot, select Yes anyway. In fact, there is little likelihood you would ever respond with No to this prompt. (This step isn't applicable to the AT-CM70S Line Card because it doesn't support the auto-copy feature.)  
  
The operating mode on the line card changes to OAM visible and the card resets.
14. Wait approximately one minute for the line card to initialize its management software and then select it again from the Module Status and Configuration Menu:
15. From the Module Configuration Menu, select **Port A**, the fiber optic port on the line card, to display the Port Management Menu, shown in Figure 54 on page 140.
16. Select **OAM Configurations** to display the OAM Configuration menu, shown in Figure 89 on page 204.
17. Select **OAM Configuration** to display the OAM Configuration submenu, shown in Figure 90 on page 205.
18. If the Admin State is set to Disabled, select **Admin State** and press Return to toggle the parameter to **Enabled**.

19. If the Mode parameter is set to Passive, highlight **Mode** and press Return to toggle the parameter to **Active**.

---

**Note**

The Admin State and the Mode parameters are the only OAM variables you have to configure for the dying gasp feature. For information on the other parameters in this window, refer to “Configuring an OAM Client” on page 204.

---

20. Return to the Main Menu.
21. Select **Configuration**.
22. Select **Save System and All Line Card Configurations**.
23. Return to the Main Menu.

This completes the procedure for configuring the AT-CM Media Converter Line Card for the dying gasp feature. Repeat this procedure on all of the line cards that will send or receive the signal in the AT-CV1203 and AT-CV5000 Chassis. Afterwards, for those line cards intended for the AT-CV1203 Chassis, install the line cards in the units and deploy the units at the remote sites.

## Testing the Feature

---

To test the feature:

1. Verify that the AT-CV1203 and AT-CV5000 Chassis are powered on and the fiber optic ports on the AT-CM Line Cards are cabled correctly. For installation and cabling instructions, refer to the chassis and line card installation guides.
2. Start a management session on the AT-CV5M02 Management Card in the AT-CV5000 Chassis.
3. From the Main Menu select **Remote Module Status and Configuration** to display the Remote Peer on Fiber Connection window, which is used to configure remote AT-CM Line Cards. The remote peer management feature has nearly the same configuration requirements as the dying gasp feature. So if the remote peer management feature is working between two line cards, one local to the AT-CV5000 Chassis and the other remote, the dying gasp feature should be working, too. For information on this window, refer to “Configuring Remote AT-CM Line Cards from the Menus” on page 174.

---

### Note

The AT-CM Line Cards have to be in the OAM operational state to send or receive the dying gasp signal. The cards may take up to two minutes to achieve this state when a chassis is powered on or the cards are reset. They have to Initialize its management software and negotiate the OAM state.

---

4. Power off the AT-CV1203 Chassis. If the chassis has two power supplies, disconnect one of the supplies, wait a second or two and power off the second supply.
5. From the Main Menu, select **Administration**.
6. From the Administration Menu, select **Event Log** and **Display Event Log**. If the AT-CV1203 Chassis has just one power supply or if it has two power supplies but not a management card, you should see this message in the event log:

Dying Gasp has occurred on remote linecard *number*.

*Number* is the slot number of the line card in the AT-CV5000 Chassis that received the dying gasp signal from the remote line card in the AT-CV1203 Chassis.

If the remote AT-CV1203 Chassis has two power supplies and the AT-CV5M02 Management Card, the event log should also contain this message, logged when the first power supply on the remote chassis lost power.

CV1203 RPS Failure on Remote Line Card *n*

## Chapter 10

# Configuring SNMPv3

---

This chapter provides a description of the AT-S99 implementation of the SNMPv3 protocol. In addition, the chapter contains procedures that allow you to create and modify SNMPv3 entities. The following sections are provided:

- ❑ “SNMPv3 Overview” on page 238
- ❑ “Configuring SNMPv3 Entities” on page 247
- ❑ “Configuring the SNMPv3 User Table” on page 248
- ❑ “Configuring the SNMPv3 View Table” on page 251
- ❑ “Configuring the SNMPv3 Access Table” on page 254
- ❑ “Configuring the SNMPv3 Group Table” on page 258
- ❑ “Configuring the SNMPv3 Notify Table” on page 261
- ❑ “Configuring the SNMPv3 Target Address Table” on page 264
- ❑ “Configuring the SNMPv3 Target Parameters Table” on page 267

## SNMPv3 Overview

---

The SNMPv3 protocol builds on the existing SNMPv1 and SNMPv2c protocol implementation. In SNMPv3, User-based Security Model (USM) authentication is implemented along with encryption, allowing you to configure a secure SNMP environment.

In addition, SNMP terminology changes in the SNMPv3 protocol. In the SNMPv1 and SNMPv2c protocols, the terms *agent* and *manager* are used. An agent is an SNMP user while a manager is an SNMP host. In the SNMPv3 protocol, agents and managers are called *entities*. In any SNMPv3 communication, there is an authoritative entity and a non-authoritative entity. The authoritative entity checks the authenticity of the non-authoritative entity. And, the non-authoritative entity checks the authenticity of the authoritative entity.

With the SNMPv3 protocol, you create users, determine the protocol used for message authentication as well as determine if data transmitted between two SNMP entities is encrypted. In addition, you can restrict user privileges by determining the user's view of the Management Information Bases (MIB). In this way, you restrict which MIBs the user can display and modify. In addition, you can restrict the types of messages, or traps, the user can send. (A trap is a type of SNMP message.)

After you have created a user, you define SNMPv3 message notification. This consists of determining where messages are sent and what types of messages can be sent. This configuration is similar to the SNMPv1 and SNMPv2c configuration because you configure IP addresses of trap receivers, or hosts. In addition, with the SNMPv3 implementation you decide what types of messages are sent.

This section further describes the features of the SNMPv3 protocol. The following subsections are included:

- ❑ “SNMPv3 Authentication Protocols” on page 239
- ❑ “SNMPv3 Privacy Protocol” on page 239
- ❑ “SNMPv3 MIB Views” on page 239
- ❑ “SNMPv3 Storage Types” on page 241
- ❑ “SNMPv3 Message Notification” on page 241
- ❑ “SNMPv3 Tables” on page 242
- ❑ “SNMPv3 Configuration Example” on page 246

## **SNMPv3 Authentication Protocols**

The SNMPv3 protocol supports two authentication protocols—HMAC-MD5-96 (MD5) and HMAC-SHA-96 (SHA). Both MD5 and SHA use an algorithm to generate a message digest. Each authentication protocol authenticates a user by checking the message digest. In addition, both protocols use keys to perform authentication. The keys for both protocols are generated locally using the Engine ID, a unique identifier that is assigned to the switch automatically, and the user password. You modify a key only by modifying the user password.

In addition, you have the option of assigning no user authentication. In this case, no authentication is performed for this user. You may want to make this configuration for someone with super-user capabilities.

---

### **Note**

The keys generated by the MD5 and SHA protocols are specific to the SNMPv3 protocol. They have no relation to the SSL and SSH keys for encryption.

---

## **SNMPv3 Privacy Protocol**

After you have configured an authentication protocol, you have the option of assigning a privacy protocol. In SNMPv3 protocol terminology, privacy is equivalent to encryption. Currently, the DES protocol is the only encryption protocol supported. The DES privacy protocol requires the authentication protocol to be configured as either MD5 or SHA.

If you assign a DES privacy protocol to a user, then you are also required to assign a privacy password. If you choose to not assign a privacy value, then SNMPv3 messages are sent in plain text format.

## **SNMPv3 MIB Views**

The SNMPv3 protocol allows you to configure MIB views for users and groups. The MIB tree is defined by RFC 1155 (Structure of Management Information), as illustrated in Figure 108 on page 240.

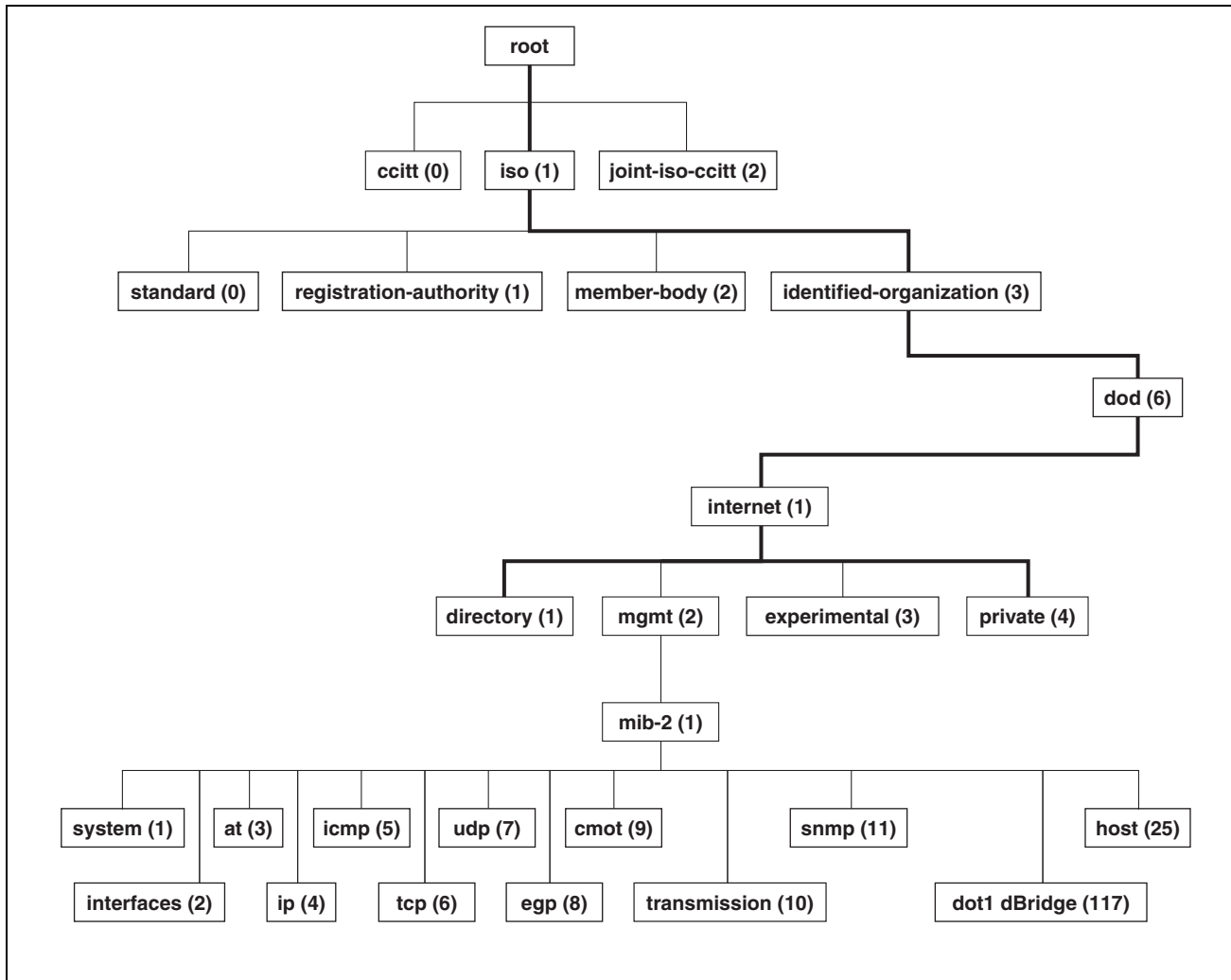


Figure 108. MIB Tree

The management software supports the MIB tree, starting with the Internet MIBs, as defined by 1.3.6.1. There are two ways to specify a MIB view. You can enter the OID number of the MIB view or its equivalent text name. For example, to specify MIBs in the Internet view, you can enter the OID format “1.3.6.1” or the text name “internet.”

In addition, you can define a MIB view that the user can access or a MIB view that the user cannot access. When you want to permit a user to access a MIB view, you include a particular view. When you want to deny a user access to a MIB view, you exclude a particular view.

After you specify a MIB subtree view you have the option of further restricting a view by defining a subtree mask. The relationship between a MIB subtree view and a subtree mask is analogous to the relationship between an IP address and a subnet mask. The switch uses the subnet mask to determine which portion of an IP address represents the network

address and which portion represents the node address. In a similar way, the subtree mask further refines the subtree view and enables you to restrict a MIB view to a specific row of the OID MIB table. You need a thorough understanding of the OID MIB table to define a subtree mask.

## **SNMPv3 Storage Types**

Each SNMPv3 table entry has its own storage type. You can choose between nonvolatile storage which allows you to save the table entry or volatile storage which does not allow you to save an entry. If you select the volatile storage type, when you power off the switch your SNMPv3 configuration is lost and cannot be recovered.

At each SNMPv3 menu, you are prompted to configure a storage type. You do not have to configure the same storage type value for each table entry.

## **SNMPv3 Message Notification**

When you generate an SNMPv3 message from the switch, there are three basic pieces of information included in the message:

- The type of message
- The destination of the message
- SNMP security information

To configure the type of message, you need to define if you are sending a Trap or Inform message. Basically, the switch expects a response to an Inform message and the switch does not expect a response to a Trap message. These two message types are defined in the SNMPv3 (RFC 2571-6).

To determine the destination of the message, you configure the IP address of the host. This configuration is similar to the SNMPv1 and SNMPv2c configuration.

The SNMP security information consists of information about the following:

- User
- View of the MIB Tree
- Security Level
- Security Model
- Authentication Level
- Privacy Protocol
- Group

To configure the SNMP security information, you associate a user and its related information—View, Security Level, Security Model, Authentication Level, Privacy Protocol and Group—with the type of message and the host IP address.

### SNMPv3 Tables

The SNMPv3 configuration is neatly divided into configuring SNMPv3 user information and configuring the message notification. You must configure all seven tables to successfully configure the SNMPv3 protocol. You use the following tables for user configuration:

- ❑ Configure SNMPv3 User Table
- ❑ Configure SNMPv3 View Table
- ❑ Configure SNMPv3 Access Table
- ❑ Configure SNMPv3 Group Table

First, you create a user in the Configure SNMPv3 User Table. Then you define the MIB view this user has access to in the Configure SNMPv3 View Table. To configure a security group and associate a MIB view to a security group, you configure the Configure SNMPv3 Access Table. Finally, configure the Configure SNMPv3 Group menu to associate a user to a security group. Figure 109 illustrates of how the user configuration tables are linked.

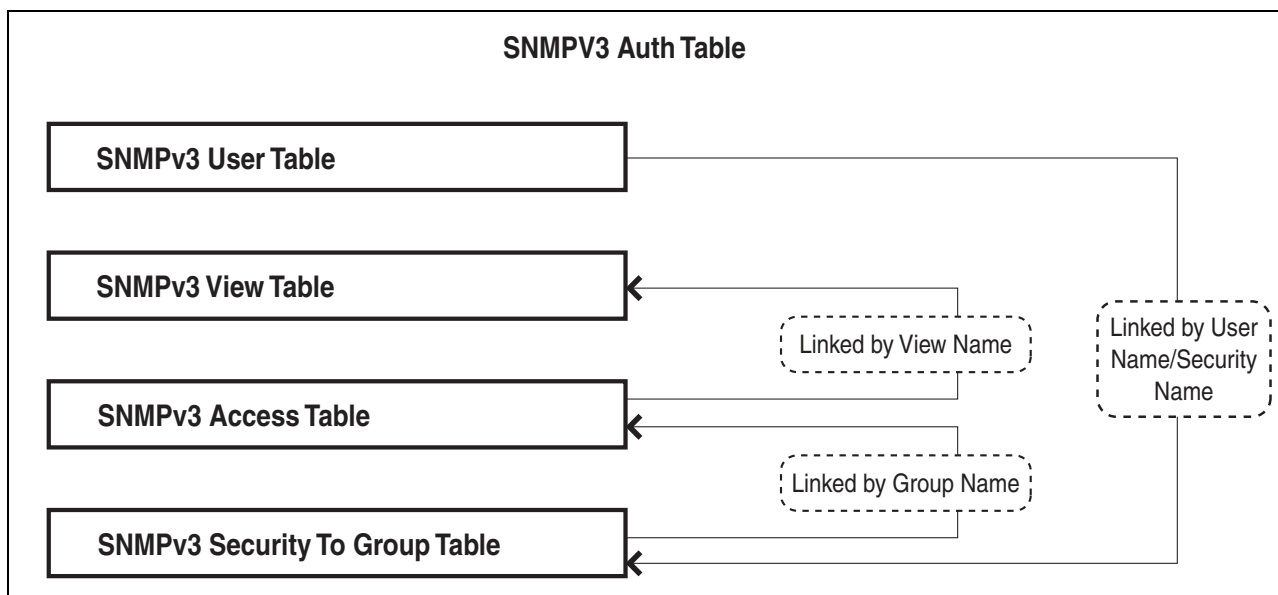


Figure 109. SNMPv3 User Configuration Process

In general, you focus on configuring security groups and then add and delete users from the groups as needed. For example, you may want to have two groups—one for manager privileges and a second one for operator privileges. Refer to Appendix B, "SNMPv3 Configuration Examples" on page 291 for an example of manager and operator configurations.

After you configure an SNMPv3 user, you need to configure SNMPv3 message notification. This configuration is accomplished with the following tables:

- ❑ Configure SNMPv3 Notify Table
- ❑ Configure SNMPv3 Target Address Table
- ❑ Configure SNMPv3 Target Parameters Table

You start the message notification configuration by defining the type of message you want to send with the SNMPv3 Notify Table. Then you define a IP address that is used for notification in the Configure SNMPv3 Target Address Table. This is the IP address of the SNMPv3 host. Finally, you associate the trap information with a user by configuring the Configure SNMPv3 Target Parameters Table.

Figure 110 illustrates of how the message notification tables are linked.

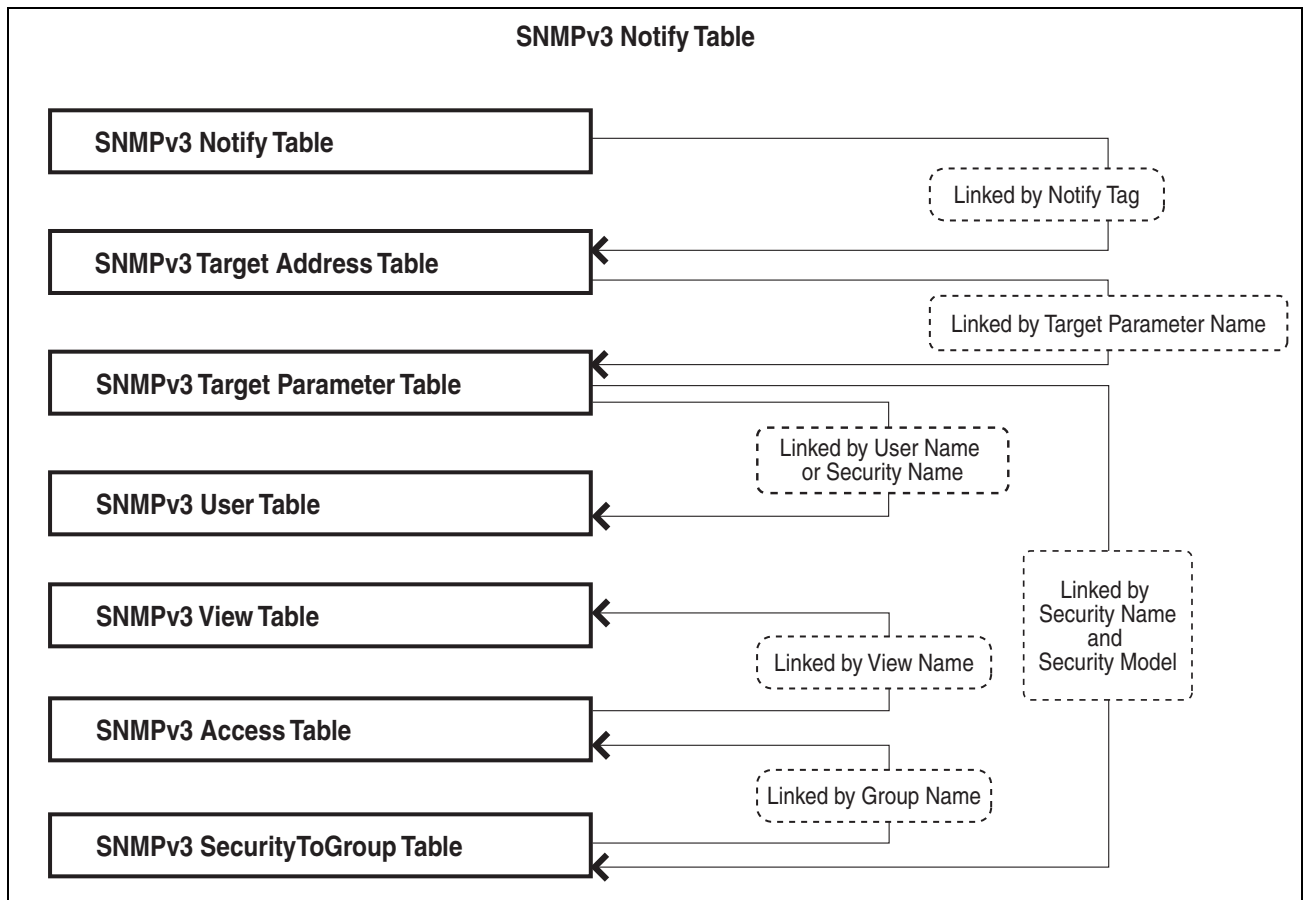


Figure 110. SNMPv3 Message Notification Process

For a more detailed description of the SNMPv3 Tables, see the following subsections:

- ❑ “SNMPv3 User Table” on page 244
- ❑ “SNMPv3 View Table” on page 244
- ❑ “SNMPv3 Access Table” on page 244
- ❑ “SNMPv3 Group Table” on page 245
- ❑ “SNMPv3 Notify Table” on page 245
- ❑ “SNMPv3 Target Address Table” on page 245
- ❑ “SNMPv3 Target Parameters Table” on page 245

### **SNMPv3 User Table**

The Configure SNMPv3 User Table menu allows you to create an SNMPv3 user and provides the options of configuring authentication and privacy protocols. With the SNMPv3 protocol, users are authenticated when they send and receive messages. In addition, you can configure a privacy protocol and password so messages a user sends and receives are encrypted. The DES privacy algorithm uses the privacy password and the Engine ID to generate a key that is used for encryption. Lastly, you can configure a storage type for this table entry which allows you to save this user and its related configuration to flash memory.

### **SNMPv3 View Table**

The Configure SNMPv3 View Table menu allows you to create a view of the MIB OID Table. First, you configure a view of a subtree. Then you have the option of configuring a Subtree Mask that further refines the subtree view. For example, you can use a Subtree Mask to restrict a user’s view to one row of the MIB OID Table. In addition, you can chose to include or exclude a view. As a result, you can let a user see a particular view or prevent a user from seeing a particular view. Lastly, you can configure a storage type for this table entry which allows you to save this view to flash memory.

### **SNMPv3 Access Table**

The Configure SNMPv3 Access Table menu allows you to configure a security group. After you create a security group, you assign a set of users with the same access privileges to this group using the SNMPv3 Group Table. Consider the types of groups you want to create and the types of access privileges each group will have. In this way, you can more easily keep track of your users as belonging to one or two groups.

For each group, you can assign read, write, and notify views of the MIB table. The views you assign here have been previously defined in the Configure SNMPv3 View Table menu. For example, the Read View allows

group members to view the specified portion of the OID MIB table. The Write View allows group members to write to, or modify, the MIBs in the specified MIB view. The Notify View allows group members to send trap messages defined by the MIB view. Lastly, you can configure a storage type for this table entry which allows you to save this view to flash memory.

### **SNMPv3 Group Table**

The Configure SNMPv3 Group Table menu allows you to associate a User Name with a security group called a Group Name. The User Name is previously configured with the Configure SNMPv3 User Table menu. The security group is previously configured with the Configure SNMPv3 Access Table menu. Lastly, you can configure a storage type for this table entry which allows you to save the entry to flash memory.

### **SNMPv3 Notify Table**

The Configure SNMPv3 Notify Table menu allows you to define the type of message that is sent from the switch to the SNMP host. In addition, you have the option of defining the message type as either an Inform or a Trap message. The difference between these two types of messages is that when a switch sends an Inform message, the switch expects a response from the host. In comparison, the switch does not expect the host to respond to Trap messages.

In addition, you define a Notify Tag that links an SNMPv3 Notify Table entry to the host IP address defined in the Configure SNMPv3 Target Address Table menu. Lastly, you can configure a storage type for this table entry which allows you to save the entry to flash memory.

### **SNMPv3 Target Address Table**

The Configure SNMPv3 Target Address Table menu allows you to configure the host IP address. Also, in the same table, you configure the values of the Tag List parameter with the previously defined Notify Tag parameter values. The Notify Tag parameter is configured in the Configure SNMPv3 Notify Table. In this way, the Notify and Target Address tables are linked. Lastly, you can configure a storage type for this table entry which allows you to save the entry to flash memory.

### **SNMPv3 Target Parameters Table**

The Configure SNMPv3 Target Parameters Table menu allows you to define which user can send messages to the host IP address defined in the Configure SNMPv3 Target Address Table. The user and its associated information is previously configured in the Configure SNMPv3 User Table, SNMPv3 View Table, SNMPv3 Access Table, and SNMPv3 Group Table. Lastly, you can configure a storage type for this table entry which allows you to save the entry to flash memory.

**SNMPv3  
Configuration  
Example**

You may want to have two classes of SNMPv3 users—Managers and Operators. In this scenario, you would configure one group, called Managers, with full access privileges. Then you would configure a second group, called Operators, with monitoring privileges only. For a detailed example of this configuration, see Appendix B, "SNMPv3 Configuration Examples" on page 291.

## Configuring SNMPv3 Entities

---

The following sections describe how to configure SNMPv3 entities using the SNMPv3 Tables. To successfully configure this protocol, you must perform the procedures in the order given here. For overview information about SNMPv3, see the “SNMPv3 Overview” on page 238.

The following SNMPv3 tables are described:

- ❑ “Configuring the SNMPv3 User Table,” next
- ❑ “Configuring the SNMPv3 View Table” on page 251
- ❑ “Configuring the SNMPv3 Access Table” on page 254
- ❑ “Configuring the SNMPv3 Group Table” on page 258
- ❑ “Configuring the SNMPv3 Notify Table” on page 261
- ❑ “Configuring the SNMPv3 Target Address Table” on page 264
- ❑ “Configuring the SNMPv3 Target Parameters Table” on page 267

The SNMPv3 User, View, Access, and Group tables are concerned with setting up a user, determining authentication and privacy, and associating a user to a security group. The SNMPv3 Notify, Target Address, and Target Parameters tables are concerned with message notification. You use the SNMPv3 Community Table to configure SNMPv1 and SNMPv2 communities.

Due to the complexity of the SNMPv3 configuration, Allied Telesis recommends that you configure the SNMPv3 protocol with the procedures listed above, in the order they are listed. However, you can configure the SNMPv3 protocol using the above procedures in any order.

## Configuring the SNMPv3 User Table

---

This section describes the parameters for SNMPv3 User Table entries. The parameters are:

- User Name
- Authentication protocol
- Authentication password
- Privacy protocol
- Privacy password

To manage the SNMPv3 User Table from the menus:

- From the Main Menu, select **Configuration -> System Configuration -> SNMPv3 Configurations -> Configure SNMPv3 User Table**. The Configure SNMPv3 User Table menu is shown in Figure 111.

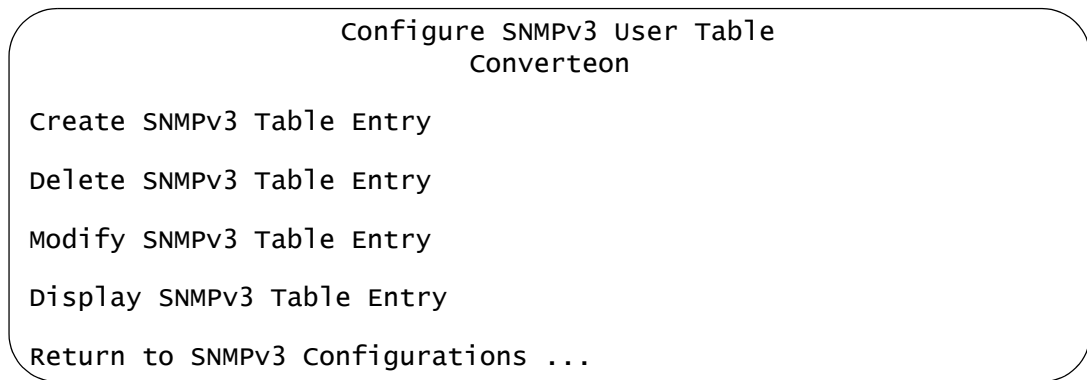


Figure 111. Configure SNMPv3 User Table Menu

To manage the SNMPv3 User Table from the web browser windows:

- :Click the **Configuration** button in the menu bar and then select the **SNMPv3** tab and the **User Table** tab. The SNMPv3 User Table tab is shown in Figure 112.

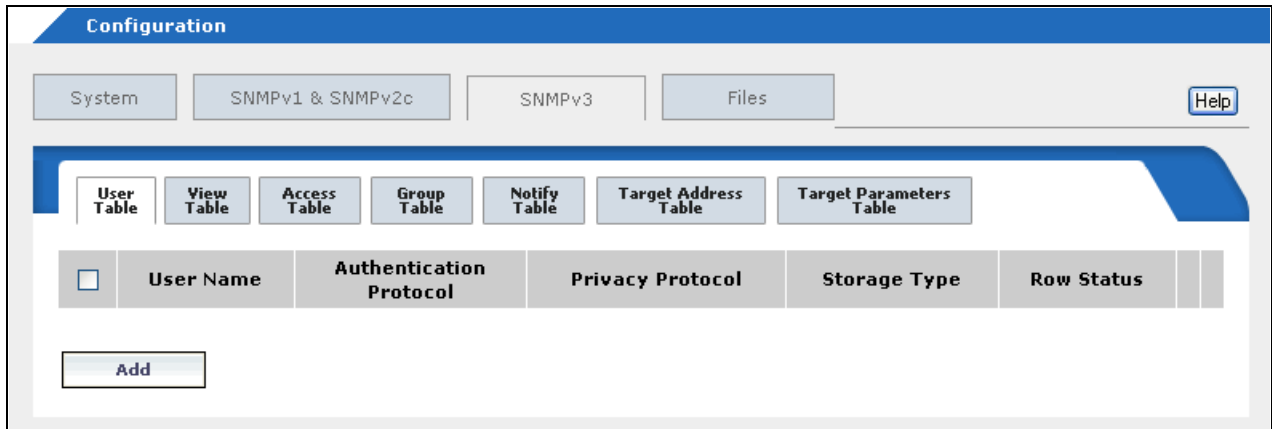


Figure 112. SNMPv3 User Table Tab

The parameters for SNMPv3 User Table entries are defined in Table 28.

Table 28. SNMPv3 User Table Parameters

Parameter	Description
User (Security) Name	A descriptive name for the user of up to 32 alphanumeric characters.
Authentication Protocol	<p>The user's authentication protocol. The possible values are:</p> <p><b>M-MD5</b>                      This value represents the MD5 authentication protocol. Users (SNMP entities) are authenticated with the MD5 authentication protocol after a message is received. This algorithm generates the message digest. The user is authenticated when the authentication protocol checks the message digest. With the MD5 selection, you can configure a Privacy Protocol.</p> <p><b>S-SHA</b>                      This value represents the SHA authentication protocol. With this selection, users are authenticated with the SHA authentication protocol after a message is received. This algorithm generates the message digest. The user is authenticated when the authentication protocol checks the message digest. With the SHA selection, you can configure a Privacy Protocol.</p>

Table 28. SNMPv3 User Table Parameters

Parameter	Description
Authentication Protocol (continued)	<p>N-None This value represents no authentication protocol. When messages are received, users are not authenticated. This selection does not support a Privacy Protocol.</p> <hr/> <p><b>Note</b> You may want to assign NONE to a super user.</p> <hr/>
Authentication Password	An authentication password of 8 to 32 alphanumeric characters. Applies only to MD5 and SHA authentication protocols.
Privacy Protocol	<p>Applies only to MD5 and SHA authentication protocols. The possible values are:</p> <p>D-DES This value makes the DES privacy (or encryption) protocol the privacy protocol for this User Table entry. With this selection, messages transmitted between the host and the device are encrypted with the DES protocol.</p> <p>N-None Select this value if you do not want a privacy protocol for this User Table entry. With this selection, messages transmitted between the host and the switch are not encrypted.</p>
Privacy Password	A privacy password of 8 to 32 alphanumeric characters. Applies only to DES privacy protocol.
Storage Type	<p>The possible values are:</p> <p>V-Volatile This selection blocks the management card from saving the entry in the master configuration file.</p> <p>N-NonVolatile This selection allows the management card to save the entry in the master configuration file when a save command is issued. Allied Telesis recommends this storage type.</p>
Row Status	This parameter appears only when you display the SNMPv3 User Table. The Active value indicates the entry takes effect immediately.

## Configuring the SNMPv3 View Table

---

This section describes the parameters for SNMPv3 View Table entries. The parameters are:

- ❑ View Name
- ❑ Subtree OID
- ❑ Subtree Mask
- ❑ MIB OID Table View

To access the SNMPv3 View Table from the menus:

- ❑ From the Main Menu, select **Configuration** -> **System Configuration** -> **SNMPv3 Configurations** -> **Configure SNMPv3 View Table**. The Configure SNMPv3 View Table menu is shown in Figure 113.

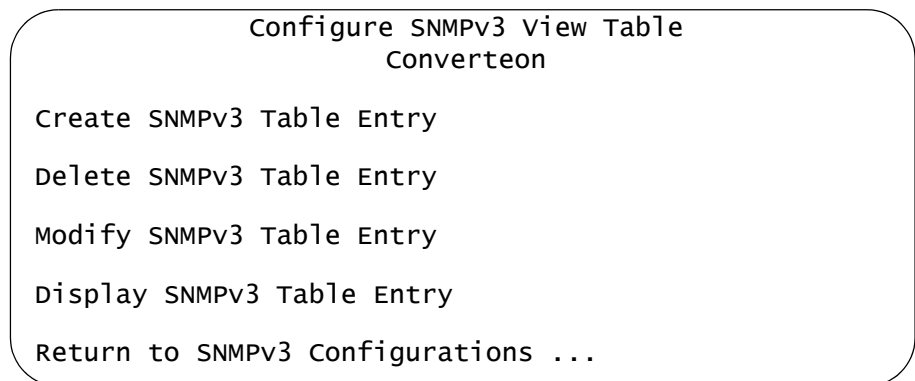


Figure 113. Configure SNMPv3 View Table Menu

To manage the SNMPv3 View Table from the web browser windows:

- ❑ :Click the **Configuration** button in the menu bar and then select the **SNMPv3** tab and the **View Table** tab. The SNMPv3 View Table tab is shown in Figure 114.

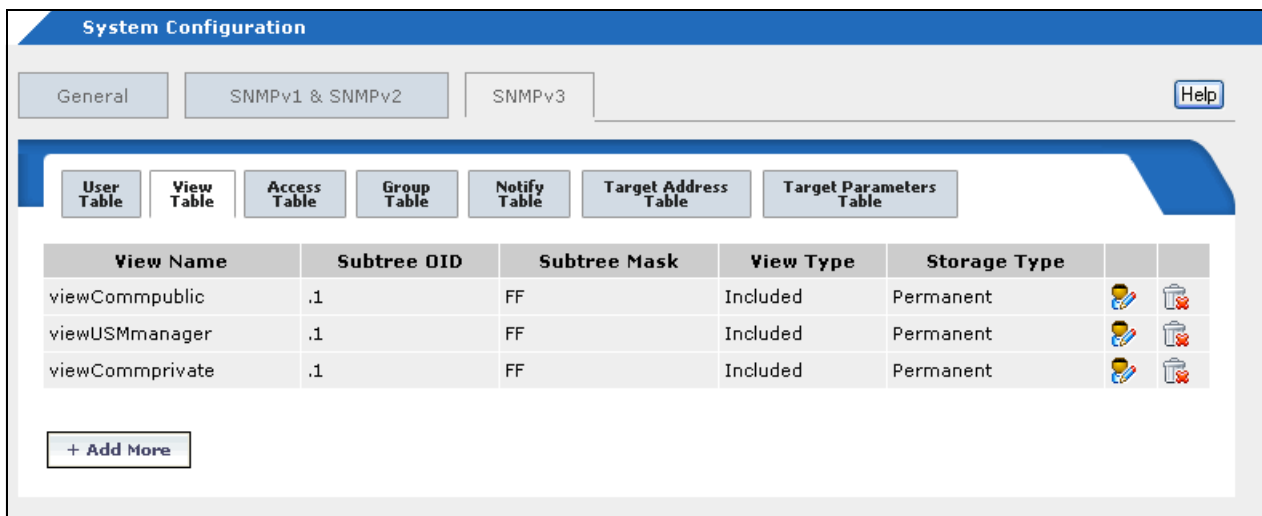


Figure 114. SNMPv3 View Table Tab

A knowledge of the OID table is required to create view entities. You can be very specific about the view a user can or cannot access—down to a column or row of the table. The AT-S99 Management Software program of the AT-CV5M02 Management Card supports the Internet subtree of the OID table.

The parameters for SNMPv3 View Table entries are defined in Table 29.

Table 29. SNMPv3 View Table Parameters

Parameter	Description
View Name	A descriptive name for this view of up to 32 alphanumeric characters. <hr/> <p><b>Note</b> The “defaultViewAll” value is the default entry for the SNMPv1 and SNMPv2c configuration. You cannot use this default value for an SNMPv3 View Table entry.</p>
View Subtree	The subtree that this view will or will not be permitted to display. You can enter either a numeric value in hex format or the equivalent text name. For example, the OID hex format for TCP/IP is:  1.3.6.1.2.1.6  The text format is for TCP/IP is:  tcp

Table 29. SNMPv3 View Table Parameters

Parameter	Description
Subtree Mask	<p>A subtree mask in hexadecimal format. This is an optional parameter used to further refine the value in the View Subtree parameter. This parameter is in binary format.</p> <p>The relationship between a subtree mask and a subtree is similar to the relationship between an IP address and a subnet mask. The subnet mask further refines the IP address. In the same way, the OID table entry defines a MIB View and the subtree mask further restricts a user's view to a specific the column and row of the MIB View. The value of the Subnet Mask parameter is dependent on the subtree you select. For example, if you configure the View Subtree parameter as MIB, ifEntry.0.3 has the following value:</p> <p>1.3.6.1.2.1.2.2.1.0.3</p> <p>To restrict the user's view to the third row (all columns) of the ifEntry MIB, enter the following value for the Subtree Mask parameter</p> <p>ff:bf</p>
View Type	<p>The possible values are:</p> <p>I-Included Enter this value to permit the View Name to see the subtree specified above.</p> <p>E-Excluded Enter this value to not permit the View Name to see the subtree specified above.</p>
Storage Type	<p>The possible values are:</p> <p>V-Volatile This selection blocks the management card from saving the entry in the master configuration file.</p> <p>N-NonVolatile This selection allows the management card to save the entry in the master configuration file when a save command is issued. Allied Telesis recommends this storage type.</p>
Row Status	<p>This parameter appears only when you display the SNMPv3 View Table. The Active value indicates the entry takes effect immediately.</p>

## Configuring the SNMPv3 Access Table

---

This section describes the parameters for SNMPv3 Access Table entries. The SNMPv3 Access Table is used to configure security groups. Each user must belong to a security group. After you have configured a security group, use the Group Table to assign users to security groups.

The parameters are:

- Group Name
- Security Model
- Security Level
- Read View Name
- Write View Name
- Notify View Name
- Storage Type

Before adding entries to the Access Table, you should configure entries in the View Table. These values are used to configure the Read, Write, and Notify View parameters. Refer to “Configuring the SNMPv3 View Table” on page 251.

To access the SNMPv3 Access Table from the menus.

- From the Main Menu, select **Configuration -> System Configuration -> SNMPv3 Configurations -> Configure SNMPv3 Access Table**. The Configure SNMPv3 Access Table menu is shown in Figure 115.

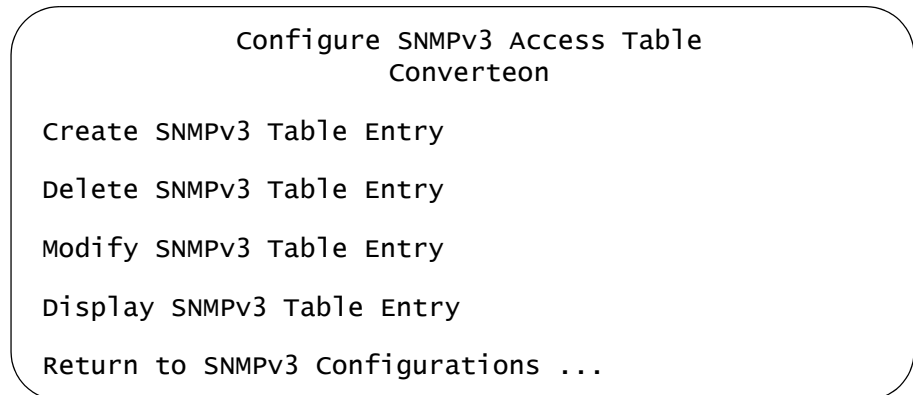


Figure 115. Configure SNMPv3 Access Table Menu

To manage the SNMPv3 View Table from the web browser windows:

- :Click the **Configuration** button in the menu bar and then select the **SNMPv3** tab and the **Access Table** tab. The SNMPv3 Access Table tab is shown in Figure 116.

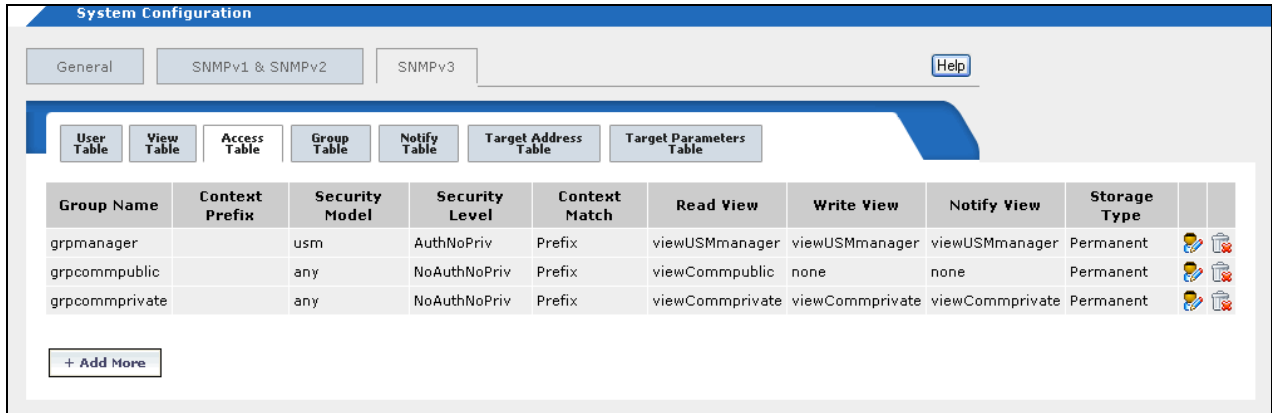


Figure 116. SNMPv3 Access Table Tab

The parameters for SNMPv3 Access Table entries are defined in Table 30.

Table 30. SNMPv3 Access Table Parameters

Parameter	Description
Group Name	<p>A descriptive name for the group of up to 32 alphanumeric characters. You are not required to enter a unique value here because the SNMPv3 Access Table entry is indexed with the Group Name, Security Model, and Security Level parameter values. However, unique group names allow you to more easily distinguish the difference groups.</p> <p>There are four default values for this field:</p> <ul style="list-style-type: none"> <li>□ defaultV1GroupReadOnly</li> <li>□ defaultV1GroupReadWrite</li> <li>□ defaultV2cGroupReadOnly</li> <li>□ defaultV2cGroupReadWrite</li> </ul> <p>These values are reserved for SNMPv1 and SNMPv2c implementations.</p>

Table 30. SNMPv3 Access Table Parameters

Parameter	Description
Security Model	<p>The possible values are:</p> <p>Select one of the following SNMP protocols as the Security Model for this Group Name.</p> <p><b>1-v1</b> Select this value to associate the Group Name with the SNMPv1 protocol.</p> <p><b>2-v2c</b> Select this value to associate the Group Name with the SNMPv2c protocol.</p> <p><b>3-v3</b> Select this value to associate the Group Name with the SNMPv3 protocol. The SNMPv3 protocol allows you to configure the group to authenticate SNMPv3 entities (users) and encrypt messages.</p>
Security Level	<p>The possible values are:</p> <p><b>A-AuthNoPriv</b> This option represents authentication, but no privacy protocol. Select this security level if you want to authenticate SNMP users, but you do not want to encrypt messages using a privacy protocol. You can select this value if you configured the Security Model parameter with the SNMPv3 protocol.</p> <p><b>P-AuthPriv</b> This option represents authentication and the privacy protocol. Select this security level to encrypt messages using a privacy protocol and authenticate SNMP entities. This level provides the greatest level of security. You can select this value if you configured the Security Model parameter with the SNMPv3 protocol.</p> <p><b>N-NoauthNoPriv</b> This option represents no authentication and no privacy protocol. Select this security level if you do not want to authenticate SNMP entities and you do not want to encrypt messages using a privacy protocol. This security level provides the least security.</p> <hr/> <p><b>Note</b> The only security level for SNMPv1 and SNMPv2c is N-NoauthNoPriv.</p> <hr/>

Table 30. SNMPv3 Access Table Parameters

Parameter	Description
Read View Name	The value that you configured with the View Name parameter in the SNMPv3 View Table. A Read View Name allows the users assigned to this Group Name to view the information specified by the View Table entry. This value does not need to be unique.
Write View Name	The value that you configured with the View Name parameter in the SNMPv3 View Table.  A Write View Name allows the users assigned to this Security Group to write, or modify, the information in the specified View Table. This value does not need to be unique.
Notify View Name	The value that you configured with the View Name parameter in the SNMPv3 View Table.  A Notify View Name allows the users assigned to this Group Name to send traps permitted in the specified View. This value does not need to be unique.
Storage Type	The possible values are:  V-Volatile This selection blocks the management card from saving the entry in the master configuration file.  N-NonVolatile This selection allows the management card to save the entry in the master configuration file when a save command is issued. Allied Telesis recommends this storage type.
Context Prefix	This parameter appears only when you display the SNMPv3 Access Table and is set to null.
Context Match	This parameter appears only when you display the SNMPv3 Access Table and is set to exact.
Row Status	This parameter appears only when you display the SNMPv3 Access Table. The Active value indicates the entry takes effect immediately.

## Configuring the SNMPv3 Group Table

---

This section contains a description of the SNMPv3 Group Table and how to create, delete, and modify table entries. The SNMPv3 Group Table allows you to associate a User Name with a Group Name. The User Name is configured in the Configure SNMPv3 User Table menu while the Group Name is configured in the Configure SNMPv3 Access Table menu. In addition, the configuration in the Configure SNMPv3 Access Table menu defines which MIB views this User can read, write (modify), and send traps from. For each User Name, you can assign:

- ❑ A Security Model (SNMPv1, SNMPv2c, SNMPv3)
- ❑ A Group Name
- ❑ A Storage Type

To access the SNBMPv3 Group Table from the menus:

- ❑ From the Main Menu, select **Configuration -> System Configuration -> SNMPv3 Configurations -> Configure SNMPv3 Group Table**. The Configure SNMPv3 Group Table menu is shown in Figure 117.

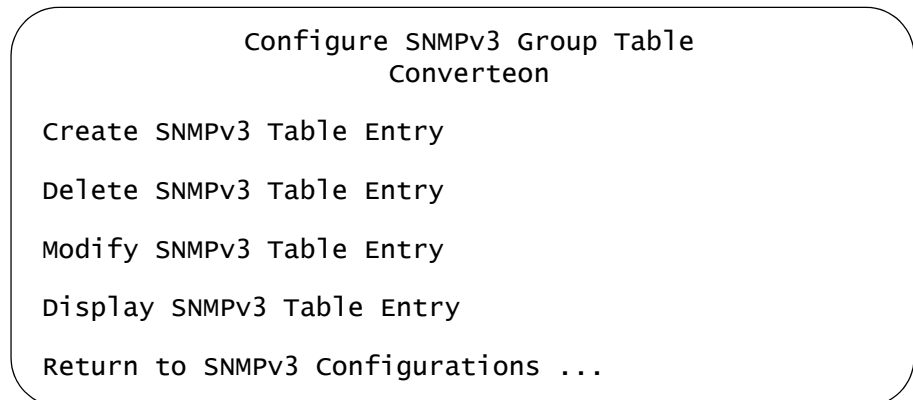


Figure 117. Configure SNMPv3 Group Table Menu

To access the SNMPv3 Group Table from the web browser windows:

- ❑ :Click the **Configuration** button in the menu bar and then select the **SNMPv3** tab and the **Group Table** tab. The tab is shown in Figure 118.

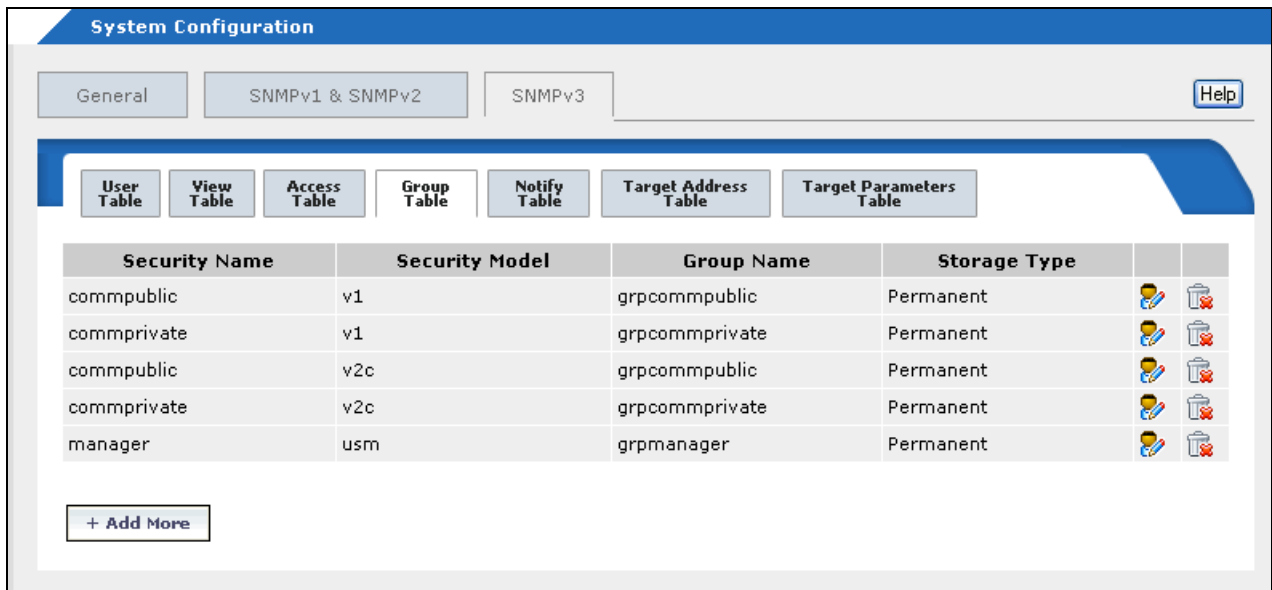


Figure 118. SNMPv3 Group Table Tab

The parameters for SNMPv3 Group Table entries are defined in Table 31.

Table 31. SNMPv3 Group Table Parameters

Parameter	Description
Security Name	The Security Name that you want to associate with a group. Enter a Security Name that you configured in “Configuring the SNMPv3 User Table” on page 248.
Security Model	The corresponding SNMP protocol of the User Name. The possible values are:  1-v1 Select this value to associate the Group Name with the SNMPv1 protocol.  2-v2c Select this value to associate the Group Name with the SNMPv2c protocol.  3-v3 Select this value to associate the Group Name with the SNMPv3 protocol.

Table 31. SNMPv3 Group Table Parameters

Parameter	Description
Group Name	<p>a Group Name that you configured in the SNMPv3 Access Table. Refer to “Configuring the SNMPv3 Access Table” on page 254.</p> <p>There are four default values for this field:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> defaultV1GroupReadOnly</li> <li><input type="checkbox"/> defaultV1GroupReadWrite</li> <li><input type="checkbox"/> defaultV2cGroupReadOnly</li> <li><input type="checkbox"/> defaultV2cGroupReadWrite</li> </ul> <p>These values are reserved for SNMPv1 and SNMPv2c implementations.</p>
Storage Type	<p>The possible values are:</p> <p>V-Volatile This selection blocks the management card from saving the entry in the master configuration file.</p> <p>N-NonVolatile This selection allows the management card to save the entry in the master configuration file when a save command is issued. Allied Telesis recommends this storage type.</p>
Row Status	<p>This parameter appears only when you display the SNMPv3 Group Table. The Active value indicates the entry takes effect immediately.</p>

## Configuring the SNMPv3 Notify Table

---

The SNMPv3 Notify Table is used to create names for sending traps or inform messages. The entry parameters in the SNMPv3 Notify Table are:

- Notify Name
- Notify Tag
- Notify Type
- Storage Type

The parameters are defined in Table 32 on page 262.

To access the Configure SNMPv3 Notify Table from the menus:

- From the Main Menu, select **Configuration -> System Configuration -> SNMPv3 Configurations -> Configure SNMPv3 Notify Table**. The Configure SNMPv3 Notify Table menu is shown in Figure 119.

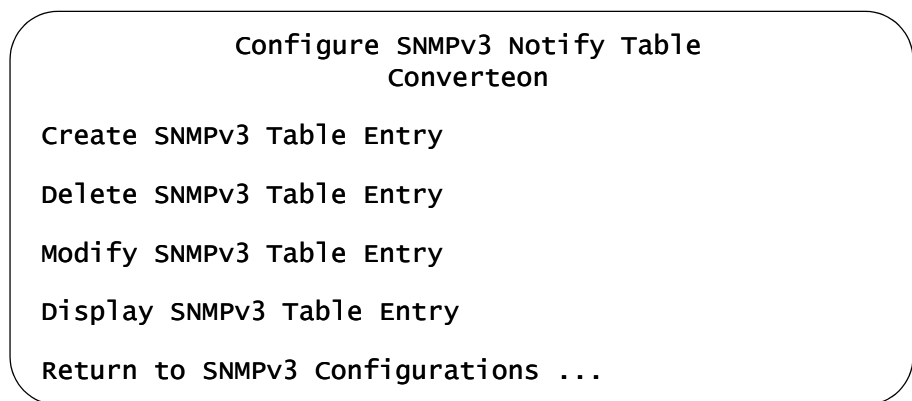


Figure 119. Configure SNMPv3 Notify Table Menu

To access the SNMPv3 Notify Table from the web browser windows:

- :Click the **Configuration** button in the menu bar and then select the **SNMPv3** tab and the **Notify Table** tab. The tab is shown in Figure 122.

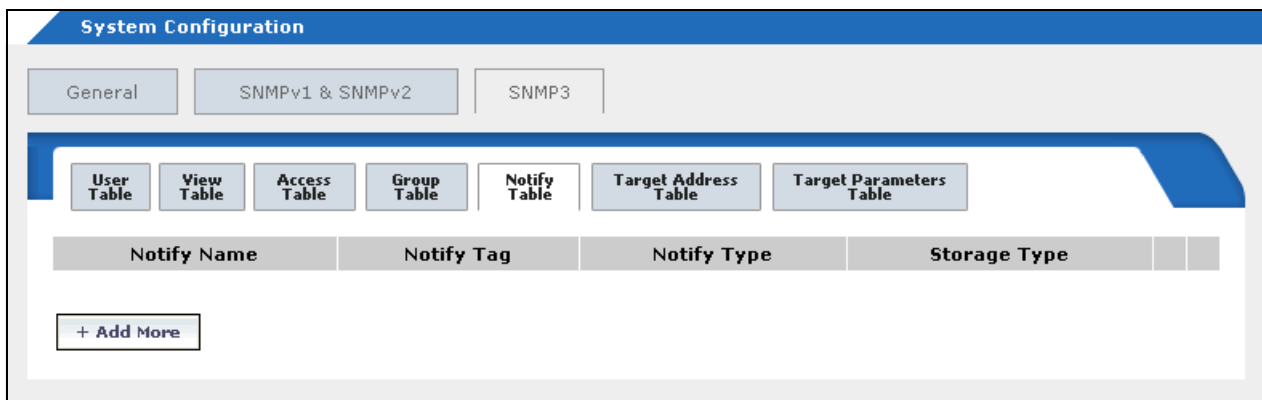


Figure 120. SNMPv3 Notify Table Tab

The parameters for SNMPv3 Notify Table entries are defined in Table 32.

Table 32. SNMPv3 Notify Table Parameters

Parameter	Description
Notify Name	The name to be associated with this trap message. The name can be up to 32 alphanumeric characters. For example, you might define a trap message for hardware engineering and enter a value of “hardwareengineeringtrap” for the Notify Name.
Notify Tag	The name of a Notify Tag. The name can be up to 32 alphanumeric characters. This parameter is added to the Tag List parameter in the SNMPv3 Target Address Table, which defines the IP addresses of the devices to receive the traps or inform messages.
Notify Type	<p>The possible values are:</p> <p>T-Trap This option sends traps. SNMPv3 does not expect hosts to respond to traps.</p> <p>I-Inform This option sends inform messages. SNMPv3 expects hosts to respond to inform messages.</p>
Storage Type	<p>The possible values are:</p> <p>V-Volatile This selection blocks the management card from saving the entry in the master configuration file.</p>

Table 32. SNMPv3 Notify Table Parameters

<b>Parameter</b>	<b>Description</b>
Storage Type (Continued)	N-NonVolatile This selection allows the management card to save the entry in the master configuration file when a save command is issued. Allied Telesis recommends this storage type.
Row Status	This parameter appears only when you display the SNMPv3 Notify Table. The Active value indicates the entry takes effect immediately.

## Configuring the SNMPv3 Target Address Table

---

The SNMPv3 Target Address Table is used to designate the IP addresses of hosts to receive notifications. The SNMPv3 Target Address Table is linked internally to the SNMPv3 Notify Table through the Tag List parameter. The entries in the SNMPv3 Notify Table receive the host IP addresses from the entries in the SNMPv3 Target Address Table.

The parameters of the entries in the SNMPv3 Target Address Table are:

- Target Address Name
- Target IP Address
- UDP Port
- Timeout Value
- Number of Retries
- Tag List
- Target Parameters
- Storage Type

The parameters are defined in Table 33 on page 265.

To access the Configure SNMPv3 Target Address Table from the menus:

- From the Main Menu, select **Configuration -> System Configuration -> SNMPv3 Configurations -> Configure SNMPv3 Target Address Table**. The Configure SNMPv3 Target Address Table menu is shown in Figure 121.

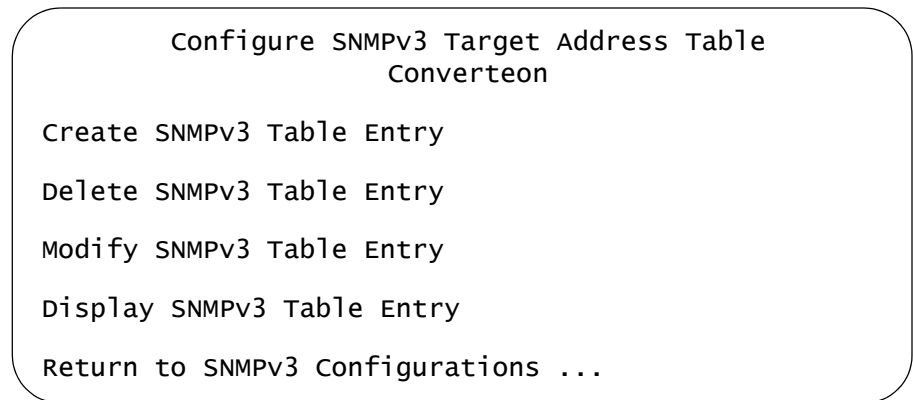


Figure 121. Configure SNMPv3 Target Address Table Menu

To access the Configure SNMPv3 Target Address Table from the web browser windows:

- :Click the **Configuration** button in the menu bar and then select the **SNMPv3** tab and the **Target Address Table** tab. The Target Address Table tab is shown in Figure 122.

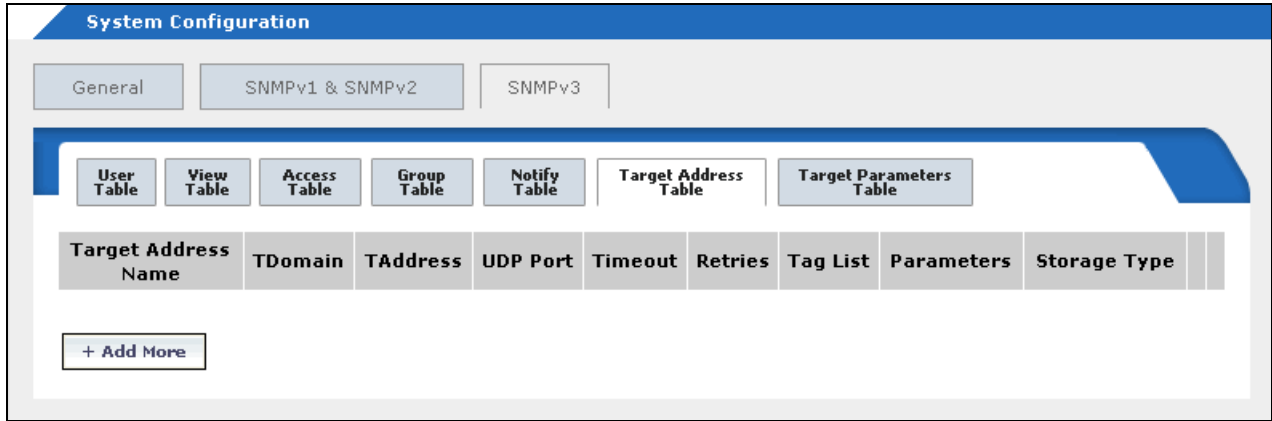


Figure 122. SNMPv3 Target Address Table Tab

Table 33. SNMPv3 Target Address Table Parameters

Parameter	Description
Target Address Name	The name of the SNMP manager, or host, that manages the SNMP activity on your switch. The name can be up to 32 alphanumeric characters.
IP Address (TAddress)	The IP address of the host. The IP address is entered in this format:  XXX.XXX.XXX.XXX
UDP Port#:	The UDP port. The range is 0 to 65,535. The default port is 162.
Timeout (10mS)]	The timeout value in milliseconds. When an Inform message is generated, a response from the device is required. The timeout value determines how long SNMPv3 considers the Inform message as an active message. This parameter applies to Inform messages only. The range is from 0 to 2,147,483,647 milliseconds. The default value is 1500 milliseconds.

Table 33. SNMPv3 Target Address Table Parameters

Parameter	Description
Retries	The number of times the switch retrles, or resends, an Inform message. When an Inform message is generated, a response from the switch is required. This parameter determines how many times the switch resends an Inform message. The Retries parameter applies to Inform messages only. The range is 0 to 255 retries. The default is 3 retries.
Tag List	The tag or list of tags defined by the Notify Tag parameter in the corresponding entry in the SNMPv3 Notify Table. The tag list can be up to 256 alphanumeric characters. Separate entries with a space, for example:  hwengtag swengtag testengtag
Target Parameters	The corresponding Target Parameters name. This value has to match the name of the corresponding entry in the SNMPv3 Target Parameters Table.
Storage Type	The possible values are:  V-Volatile This selection blocks the management card from saving the entry in the master configuration file.  N-NonVolatile This selection allows the management card to save the entry in the master configuration file when a save command is issued. Allied Telesis recommends this storage type.
Row Status	This parameter appears only when you display the SNMPv3 Target Address Table. The Active value indicates the entry takes effect immediately.

## Configuring the SNMPv3 Target Parameters Table

---

This section describes the parameters for entries in the SNMPv3 Target Parameters Table, which links the user security information with the message notification information in the SNMPv3 Notify Table and the SNMPv3 Target Address Table.

In the SNMPv3 Target Parameters Table, you specify the SNMP parameters that are used when a message is generated to a target, or host, IP address. The SNMPv3 Target Parameters Table also links a User Name and its related security information, called *user security information*, with a host. The user security information consists of the following parameters listed in the SNMPv3 tables where they are configured:

- User Name parameter configured in the SNMPv3 User Table menu
- View Name parameter configured in the SNMPv3 View Table menu
- Group Name, Security Model, and Security Level parameters configured in the SNMPv3 Access Table
- User Name, Security Model, and Group Name configured in the SNMPv3 Group Table

When you enter user security information in an SNMPv3 Target Parameters Table entry, the information must match the configuration in the SNMPv3 tables listed above. If the user security information in the SNMPv3 Target Parameters Table entry does not match the configuration in the tables listed above, messages are not sent on behalf of the user.

---

**Note**

In the SNMPv3 Target Parameters Table, the Security Name parameter is the equivalent to the User Name parameter in the SNMPv3 User Table.

---

The parameters for the entries in the SNMPv3 Target Parameters Table are:

- Target Parameters Name
- Security Name (User Name)
- Security Model
- Security Level
- Storage Type

To access the SNMPv3 Target Parameters Table from the menus:

- From the Main Menu, select **Configuration -> System Configuration -> SNMPv3 Configurations -> Configure SNMPv3 Target Parameters Table**. The Configure SNMPv3 Target Parameters Table menu is shown in Figure 123.

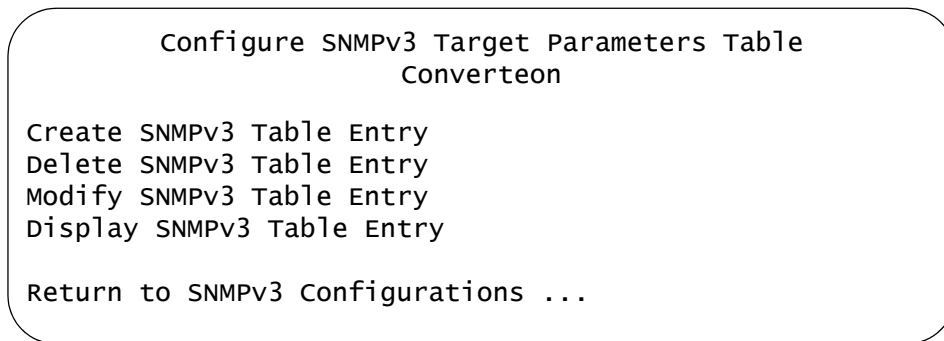


Figure 123. Configure SNMPv3 Target Parameters Table Menu

To access the Configure SNMPv3 Target Parameters Table from the web browser windows:

- Click the **Configuration** button in the menu bar and then select the **SNMPv3** tab and the **Target Parameters Table** tab. The Target Address Table tab is shown in Figure 122.

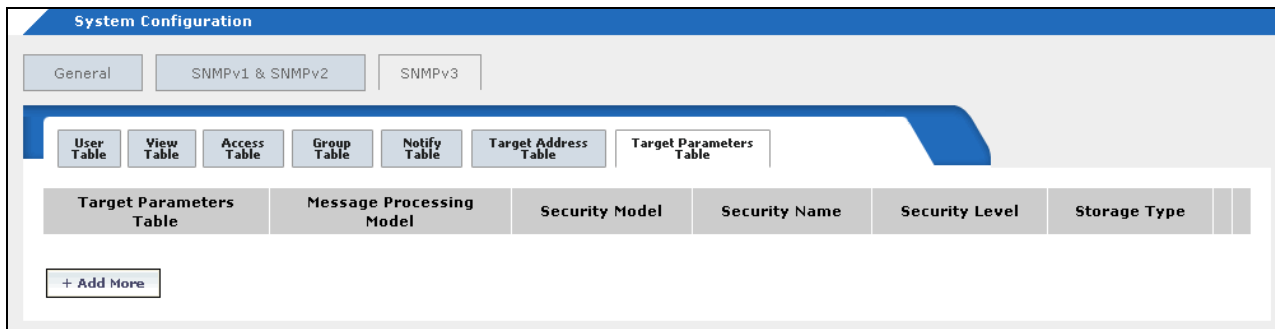


Figure 124. SNMPv3 Target Parameters Table Tab

The paramters are defined in Figure 33 on page 265.

Table 34. SNMPv3 Target Parameters Table Parameters

Parameter	Description
Target Parameters Name	A name for the entry of up to 32 alphanumeric characters.
User (Security) Name	The user name of the appropriate entry in the SNMPv3 User Table.

Table 34. SNMPv3 Target Parameters Table Parameters

Parameter	Description
Security Model [1-v1, 2-v2c, 3-v3]	<p>The Security Model for this Security Name or User Name. The possible values are</p> <p>1-v1 This value associates the Security Name or User Name with the SNMPv1 protocol.</p> <p>2-v2c This value associates the Security Name or User Name with the SNMPv2c protocol.</p> <p>3-v3 This value associates the Security Name or User Name with the SNMPv3 protocol. The SNMPv3 protocol allows you to configure the group to authenticate SNMPv3 entities (users) and to encrypt messages.</p>
Security Level [A-AuthNoPriv, P-AuthPriv, N-NoauthNoPriv]	<p>The possible values are:</p> <hr/> <p><b>Note</b> This value must match the security level of the corresponding user name in the SNMPv3 User Table.</p> <hr/> <p>A-AuthNoPriv This option provides authentication, but no privacy protocol. The SNMP user is authenticated, but without encryption. You can select this value if you configured the Security Model parameter with the SNMPv3 protocol.</p> <p>P-AuthPriv This option provides authentication and the privacy protocol. This security level encrypts messages using a privacy protocol and authenticates SNMP entities. This level provides the greatest level of security. You can select this value if you configured the Security Model parameter with the SNMPv3 protocol.</p> <p>N-NoauthNoPriv This option provides no authentication and no privacy protocol. This security level is appropriate if you do not want authentication of SNMP entities or encryption. This security level provides the least security.</p> <hr/> <p><b>Note</b> The only security level for SNMPv1 and SNMPv2c is N-NoauthNoPriv.</p> <hr/>

Table 34. SNMPv3 Target Parameters Table Parameters

Parameter	Description
Storage Type [V-Volatile, N-NonVolatile]	<p>The possible values are:</p> <p>V-Volatile This selection blocks the management card from saving the entry in the master configuration file.</p> <p>N-NonVolatile This selection allows the management card to save the entry in the master configuration file when a save command is issued. Allied Telesis recommends this storage type.</p>
Row Status	This parameter appears only when you display the SNMPv3 Target Parameters Table. The Active value indicates the entry takes effect immediately.

In an SNMPv3 Target Parameters Table entry, the Security Name parameter is linked to the User Name parameter on the SNMPv3 User Table. In an SNMPv3 User Table entry, the User Name parameter is used as an index for the entry. Because the User Name and Security Name parameters are linked, the information you configure that relates to a User Table entry must match the information you configure in the SNMPv3 Target Parameters Table entry. In addition, the values configured for the following parameters in an SNMPv3 Target Parameters Table entry must match those configured in the corresponding table entry:

- User Name parameter in the SNMPv3 User Table
- View Name parameter in the SNMPv3 View Table
- Group Name, Security Model, and Security Level parameters in the SNMPv3 Access Table
- User Name, Security Model, Group Name parameters in the SNMPv3 Group Table




---

**Caution**

If the values of the Security Model parameter in the SNMPv3 User Table and the SNMPv3 Target Parameter Table entry do not match, notification messages are not generated on behalf of this User (Security) Name.

---

## Chapter 11

# Uploading and Downloading Files

---

The procedures in this chapter explain how to update the management software on the AT-CV5M02 Management Card and the AT-CM Media Converter Line Cards. The sections in the chapter include:

- ❑ “Overview” on page 272
- ❑ “Configuring the TFTP Client” on page 273
- ❑ “Downloading New Management Software Using TFTP” on page 275
- ❑ “Downloading New Management Software Using XMODEM” on page 279
- ❑ “Uploading the Master Configuration File from a Management Card” on page 281
- ❑ “Downloading the Master Configuration File to a Management Card” on page 284

## Overview

---

Allied Telesis may periodically release new versions of the management software for the Converteon management cards and line cards. New releases are available from the company's web site.

---

**Note**

Before installing new software, read the software release notes that are included with a new release to determine whether there are any special restrictions or guidelines.

---

The cards in the Converteon product line use the following management software programs:

- ❑ The AT-CV5M02 Management Card uses the AT-S99 Management Software.
- ❑ The AT-CM Media Converter Line Cards use the AT-S73 Management Software and bootloader file.
- ❑ The AT-CV Media Converter Line Cards do not use management software.

You can use XMODEM or TFTP to download new management software. Downloads using XMODEM have to be performed from a local management session at the chassis. Downloads using TFTP can be performed from local management sessions or remote Telnet or web browser management sessions.

## Configuring the TFTP Client

---

The procedure in this section explains how to configure the TFTP client. This is the first step to using TFTP to download new versions of the management software programs to the AT-CV5M02 Management Card or the AT-CM Line Cards. This procedure has to be performed from the menus. After you've configured the client, go to "Downloading New Management Software Using TFTP" on page 275.

To configure the TFTP client:

1. From the Main Menu, select **Configuration** to display the Configuration Menu shown in Figure 20 on page 80.
2. From the Configuration Menu, select **System Configuration** to display the menu in Figure 21 on page 80.
3. From the System Configuration Menu, select **TFTP Image Download Configuration** to display the menu in Figure 125.

TFTP Image Download Configuration

TFTP Server IP Address:

Management Card:

AT-CM2x2 Image File Name:

AT-CM2Kx Image File Name:

AT-CM70x Image File Name:

Line Card Bootloader Image File Name:

Return to System Configuration Menu ...

Figure 125. TFTP Image Download Configuration

4. To enter or edit the IP address of the TFTP server on your network, select the **TFTP Server IP Address** field and enter the IP address.
5. In the File Name fields, enter the filenames of the new image files of the management software that you obtained from the Allied Telesis web site and stored on your TFTP server. You do not have to enter filenames for all of the fields. Rather, enter the filenames for just those line cards you want to upgrade. The fields are defined here:

**Management Card Image File Name** - This field is for the image filename of the AT-S99 Management Software for the AT-CV5M02 Management Card. Be sure to include the ".img" extension.

**AT-CM2x2 Image File Name** - This field is for the image filename of the AT-S73 Management Software for the following line cards: AT-CM201, AT-CM202, AT-CM202/1, AT-CM202/2, AT-CM212A/1, and AT-CM212B/1. All of these line cards use the same image file. Be sure to include the ".img" extension.

**AT-CM2Kx Image File Name** - This field is for the image filename of the AT-S73 Management Software for the AT-CM2KOS Line Card. Be sure to include the ".img" extension.

**AT-CM70x Image File Name** - This field is for the image filename of the AT-S73 Management Software for the AT-CM7OS Line Card. Be sure to include the ".img" extension.

**Linecard Bootloader Image File Name** - This field is for the filename of the bootloader for the AT-CM Line Cards. All of the AT-CM Line Cards use the same bootloader. Be sure to include the ".bin" extension. Not all new releases of the AT-S73 Management Software for the AT-CM Line Cards include a new bootloader file. Refer to the software release notes for information.

6. After entering the appropriate information in the fields, click **Update**.
7. To save this information in the master configuration file, select the **Files** tab, choose **Save System Configuration and All Card Configurations** and click **Apply**.

To perform the actual upgrade, go to "Downloading New Management Software Using TFTP" on page 275.

## Downloading New Management Software Using TFTP

---

The procedure in this section explains how to use TFTP to download new versions of the management software programs to the AT-CV5M02 Management Card or the AT-CM Line Cards. The procedure has the following requirements:

- ❑ There has to be a node with TFTP server software on your network.
- ❑ The management card must have an IP address configuration. For instructions, refer to “Assigning an IP Address Configuration” on page 80.
- ❑ The management card should reside on the same subnet as the TFTP server or should have access to its subnet through routers or other Layer 3 routing devices.
- ❑ If the management card resides on a different subnet from the TFTP server, the card’s IP address configuration has to include the default gateway address that identifies the IP address of the router interface of the first hop to reaching the server.
- ❑ The 10/100Base-TX port on the card has to be connected to a device on your network, such as an Ethernet switch. The management card communicates with your network through that port.
- ❑ You should start the TFTP server before you begin the download procedure.
- ❑ Store the new image files on the TFTP server.
- ❑ You have to configure the TFTP client before you can download new management software. For instructions, refer to “Configuring the TFTP Client” on page 273.

---

### Note

Allied Telesis recommends that you update the master configuration file on the management card with the current configurations of all the AT-CM Line Cards in the chassis before performing this procedure. For instructions, refer to “Saving Your Configuration Changes” on page 64.

---

---

### Note

Updating the AT-S99 Management Software on the AT-CV5M02 Management Card interrupts the card's operations. The card will be unresponsive for approximately two minutes as it downloads and initializes the new software. Your management session ends and you have to start a new management session to continue managing the unit.

---



**Caution**

Updating the AT-S73 Management Software on the AT-CM Line Cards interrupts the cards' network operations. Some network traffic may be lost. The line cards stop forwarding network traffic for approximately two minutes while they receive and initialize the new software.

This procedure has to be performed from the menus.

To upgrade the management software from the menus:

1. From the Main Menu, select **Image Download** to display the menu in Figure 126.

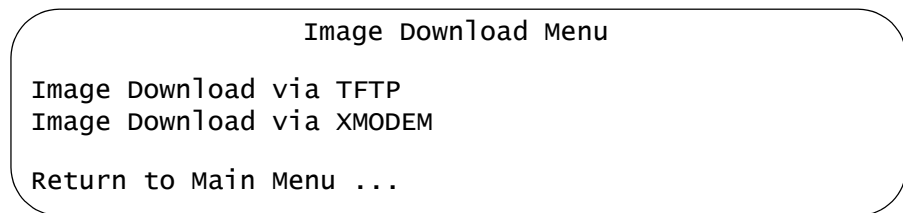


Figure 126. Image Download Menu

2. Select **Image Download via TFTP**. This displays the menu in Figure 127.

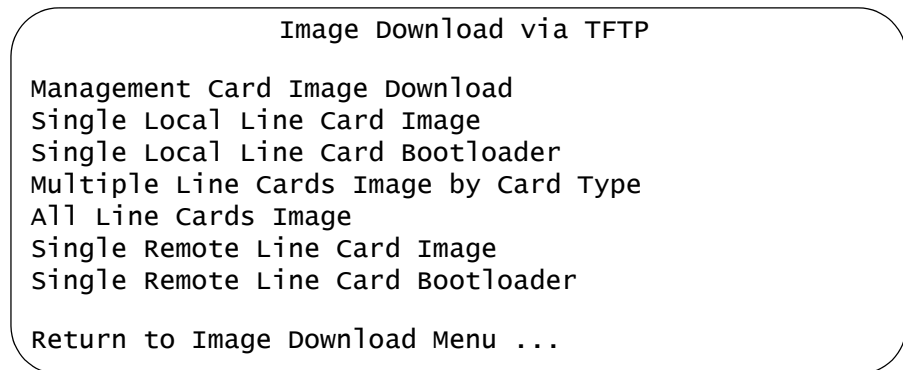


Figure 127. Image Download via TFTP Menu

3. Select one of the following menu options:

**Management Card Image Download** - Select this option to upgrade the AT-S99 Management Software on the AT-CV5M02 Management Card.

**Single Local Line Card Image** - Select this option to upgrade the AT-S73 Management Software on a single local AT-CM Line Card in the chassis. After you select this option, a prompt is displayed for the

slot number of the line card you want to upgrade. You can specify only one slot number.

**Single Local Line Card Bootloader** - Select this option to upgrade the bootloader file on a single local AT-CM Line Card in the chassis. After you select this option, a prompt is displayed for the slot number of the line card you want to upgrade. You can specify only one slot number.

**Multiple Line Card Images by Card Type** - Select this option to upgrade the AT-S73 Management Software on multiple local and remote AT-CM Line Cards. When you select this option, the following prompt is displayed:

- 1) AT-CM2x2
- 2) AT-CM2Kx
- 3) AT-CM70x

Enter card type group: ->

To update the AT-S73 Management Software on the local or remote AT-CM201, AT-CM202, AT-CM202/1, AT-CM202/2, AT-CM212A/1, and AT-CM212B/1 Line Cards, enter **1** to select **AT-CM2x2**. All of these line cards use the same image file. To update the management software on the AT-CM2KOS Line Cards, enter **2** for **AT-CM2Kx**. Finally, to update the AT-CM70S Line Cards, enter **3** for **AT-CM70x**.

The following prompt is displayed:

- 1) Local Line Cards Only
- 2) Remote Line Cards Only
- 3) Both Local and Remote Line Cards

Enter card type group: ->

Use this prompt to specify whether you want to upgrade the local line cards of the selected card type, the remote line cards, or both.

**Single Remote Line Card Image** - Select this option to upgrade the AT-S73 Management Software on a single remote AT-CM Line Card through the remote peer management feature. After you select this option, you are prompted for the slot number of the local line card that is connected to the remote line card you want to upgrade. You can specify only one slot number.

**Single Remote Line Card Bootloader** - Select this option to upgrade the bootloader on a single remote AT-CM Line Card through the remote peer management feature. After you select this option, you are prompted for the slot number of the local line card that is connected to the remote line card you want to upgrade. You can specify only one slot number.

After you've selected a download and provided the necessary information, the management card begins to download the file(s) by using the information in the TFTP Image Download tab to contact the TFTP server.

---

**Note**

To prevent damaging a management card or a line card, do not power off the chassis or remove a card while it is writing the file to flash memory.

---

## Downloading New Management Software Using XMODEM

---

The procedure in this section explains how to use XMODEM to download new versions of the management software programs to the AT-CV5M02 Management Card and the AT-CM Line Cards. Unlike TFTP downloads, which allow you to update multiple line cards at the same time, XMODEM downloads can only update one card at a time.

---

### Note

Allied Telesis recommends that you save the current configurations of all the AT-CM Line Cards in the master configuration file before performing these procedures. For instructions, refer to “Saving Your Configuration Changes” on page 64.

---



---

### Note

Updating the AT-S99 Management Software on the AT-CV5M02 Management Card interrupts the card's operations. The card will be unresponsive for approximately two minutes while it downloads and initializes the new software. Your management session ends. To resume managing the unit, you have to start a new management session.

---




---

### Caution

Updating the AT-S73 Management Software on the AT-CM Line Cards interrupts the cards' network operations. Some network traffic may be lost. The line cards stop forwarding network traffic for approximately two minutes while they store and initialize the new software.

---

This procedure has the following requirements:

- ❑ The procedure has to be performed from a local management session using the menus. For instructions, refer to “Starting a Local Management Session” on page 58.
- ❑ You need to store the new management software programs on your computer or terminal used to perform the local management session.

To download new management software using XMODEM:

1. From the Main Menu, select **Image Download** to display the menu in Figure 126 on page 276.
2. Select **Image Download via XMODEM**. This displays the menu in Figure 127.

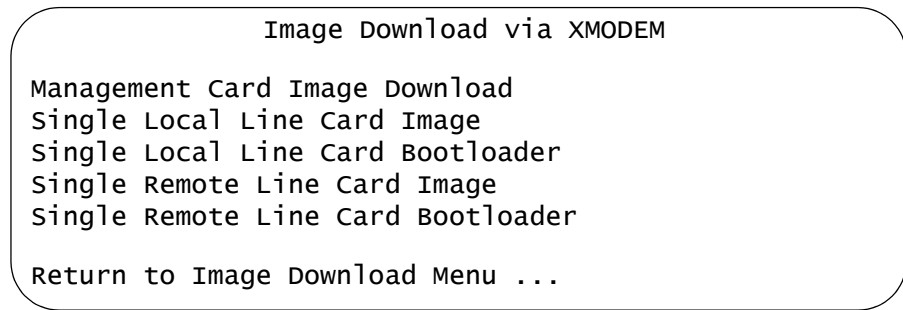


Figure 128. Image Download via TFTP Menu

3. Select one of the following menu options:

**Management Card Image Download** - Select this option to download a new version of the AT-S99 Management Software to the AT-CV5M02 Management Card.

**Single Local Line Card Image** - Select this option to download a new version of the AT-S73 Management Software to a single local AT-CM Line Card in the chassis. When you select this option, a prompt is displayed for the slot number of the line card you want to upgrade. You can enter only one slot number.

**Single Local Line Card Bootloader** - Select this option to upgrade the bootloader file on a single local AT-CM Line Card in the chassis. When prompted, enter the slot number of the line card you want to upgrade. You can specify only one slot number.

**Single Remote Line Card Image** - Select this option to upgrade the AT-S73 Management Software on a single remote AT-CM Line Card through the remote peer management feature. When prompted, enter the slot number of the local line card counterpart of the remote line card you want to upgrade. You can specify only one slot number.

**Single Remote Line Card Bootloader** - Select this option to upgrade the bootloader on a single remote AT-CM Line Card through the remote peer management feature. When prompted, enter the slot number of the local line card counterpart of the remote line card you want to upgrade. You can specify only one slot number.

4. After selecting a download and responding to the prompts, begin the file transfer with your terminal program.

---

**Note**

To prevent damaging a management card or a line card, do not power off the chassis or remove the card while the card is writing the file to flash memory.

---

## Uploading the Master Configuration File from a Management Card

---

You can upload the master configuration file from a management card to a TFTP server on your network. You might do this to maintain a history of the configurations of a chassis or to transfer the file to another management card.

---

### Note

The network operations of the media converter line cards in the chassis are not affected by this procedure.

---

**Menus** To upload the master configuration file to a TFTP server from the menus:

1. From the Main Menu, select **Configuration**. The Configuration Menu is shown in Figure 20 on page 80.

---

### Note

If you want to update the master configuration file before uploading it to the TFTP server, select **Save System and All Line Card Configurations** from the Configuration Menu.

---

2. From the Configuration Menu, select **Configuration File Upload/Download with TFTP** to display the menu in Figure 129.

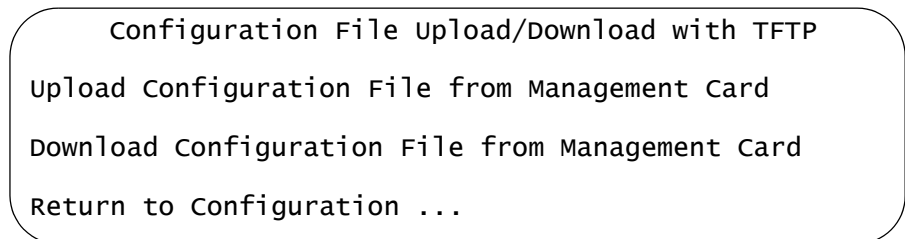


Figure 129. Configuration File Upload/Download with TFTP

3. Select **Upload Configuration File from Management Card**. This prompt is displayed:

```
TFTP Server IP Address-> _
```

4. Enter the IP address of the TFTP server. This prompt is displayed:

```
Configuration File Name-> _
```

5. Enter a filename for the configuration file. The file will be given this name on the TFTP server. The extension should be ".cfg". This prompt is displayed:

Ready to upload Configuration file through TFTP.

Warning: During Upload Configuration Management activity is disabled.

Do TFTP upload now? (Yes or No):

6. Type **Y** for to start the download. This prompt is displayed:

uploading configuration file through TFTP, please wait ...

TFTP upload Configuration file successfully

The management card displays the Configuration File Upload/Download with TFTP menu again when the upload is finished.

### Web Browser

To upload the master configuration file to a TFTP server from the web browser windows:

1. Click **Configuration** from the menus bar.
2. Click the **Files** tab. The tab is shown in Figure 130.

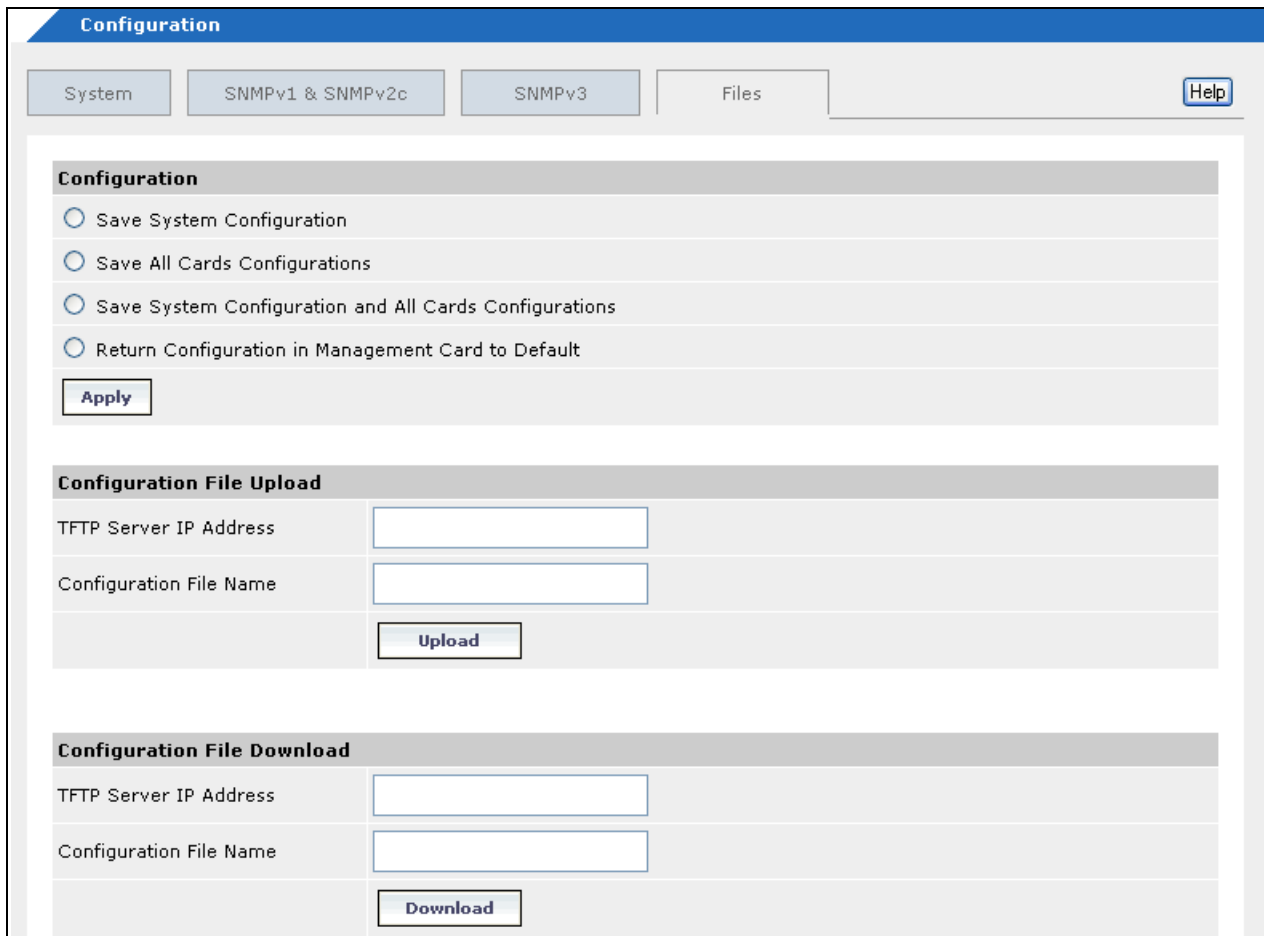


Figure 130. Files Tab

---

**Note**

If you want to update the master configuration file before uploading it to the TFTP server, click the radio button for **Save System Configuration and All Card Configurations** and click **Apply** in the Files tab.

---

3. In the Configuration File Upload section of the tab, select the **TFTP Server IP Address** field and enter the IP address of the TFTP server on your network.
4. Select the **Configuration File Name** field and enter a filename for the configuration file. The file will be stored with this name on the TFTP server. The extension should be “.cfg”.
5. Click **Upload**. The management card sends the its configuration file to the TFTP server.

## Downloading the Master Configuration File to a Management Card

---

These procedures are used to download a master configuration file to a management card: This procedures use TFTP and can be performed from either a local management session or a remote Telnet or web browser management session of the management card.

---

### Note

The current configuration settings of the management card will be overwritten by the configuration settings contained in the downloaded file. This includes the IP address, subnet mask, and DHCP status.

---



---

### Caution

These procedures may disrupt the network operations of the AT-CM Line Cards in the chassis. The parameter settings may change for those line cards that reside in chassis slots where the auto-copy feature is activated in the new master configuration file.

---

### Menus

To download the master configuration file to a management card from the menus:

1. If the chassis has two AT-CV5M02 Management Cards, remove the standby card.
1. From the Main Menu, select **Configuration**. The Configuration Menu is shown in Figure 20 on page 80.
2. From the Configuration Menu, select **Configuration File Upload/Download with TFTP** to display the menu in Figure 129 on page 281.
3. Select **Download Configuration File to Management Card**. This prompt is displayed:

```
TFTP Server IP Address-> _
```

4. Enter the IP address of the TFTP server. This prompt is displayed:

```
Configuration File Name-> _
```

5. Enter the filename of the configuration file on the TFTP server. Be sure to include the extension “.cfg”. This prompt is displayed:

```
Ready to download configuration file through TFTP.
```

```
warning: During Download Configuration Management activity is disabled.
```

Do TFTP download now? (Yes or No):

6. Type **Y** to start the download. This prompt is displayed:

```
Downloading configuration file through TFTP, please wait
...
```

After receiving the new file, the management card does the following:

- Writes the file to flash memory.
- Reboots and initializes its management software.
- Examines the new master configuration file for the auto-copy settings for the chassis slots and sends the configuration settings to those AT-CM Line Card that are installed in slots where auto-copy is enabled.

During this process, which takes about two minutes to complete, the management card will be unresponsive to commands.

7. To resume managing the chassis, start a new management session.
8. If the chassis has two management cards, reinstall the standby card. After the standby card has initialized its management software, the active management card automatically sends the new master configuration file to the standby card over the backplane of the chassis.

## Web Browser

To download the master configuration file to the management card from the web browser windows:

1. Click **Configuration** from the menus bar.
2. Click the **Files** tab. The tab is shown in Figure 130 on page 282.
3. In the Configuration File Download section of the tab, select the **TFTP Server IP Address** field and enter the IP address of the TFTP server on your network.
4. Select the **Configuration File Name** field and enter a filename of the configuration file on the TFTP server. The extension should be “.cfg”.
5. Click **Download**. After receiving the new file, the management card does the following:
  - Writes the file to flash memory.
  - Reboots and initializes its management software.
  - Examines the new master configuration file for the auto-copy settings for the chassis slots and sends the configuration settings to those AT-CM Line Card that are installed in slots where auto-copy is enabled.

During this process, which takes about two minutes to complete, the management card will be unresponsive to commands.

6. To resume managing the chassis, start a new management session.
7. If the chassis has two management cards, reinstall the standby card. After the standby card has initialized its management software, the active management card automatically sends the new master configuration file to the standby card over the backplane of the chassis.

## Appendix A

# Default Settings for the Management Software Programs

---

The following table lists the factory default settings for the AT-S99 Management Software on the AT-CV5M02 Management Card.

Table 35. Default Settings for the AT-S99 Management Software

<b>Settings</b>	<b>Default</b>
IP Address	10.0.0.1
Subnet Mask	255.255.252.0
Gateway Address	0.0.0.0
DHCP Client	Disabled
Name	None
Contact	None
Location	None
10/100Base-TX Port	Auto-Negotiation
Activity Monitor	Disabled
Network Time Protocol Client	Disabled
Maximum Temperature Threshold	60° C
Auto-copy (Set Per Slot)	Disabled
<b>Community Strings</b>	
Get Community String	public
Set Community String	private
Trap Community String	public
<b>Omega</b>	
Manager Password	friend
Operator Password	operator
Time Out Value	10 minutes
Local Access	Enabled

Table 35. Default Settings for the AT-S99 Management Software

<b>Settings</b>	<b>Default</b>
Remote Access (Telnet)	Enabled
<b>Console Port</b>	
Data Rate	115200
Terminal mode	VT-100-compatible / ANSI
Data Bits	8
Stop Bits	1
Parity	None
Flow control	None

This table lists the factory default settings for the AT-S73 Management Software on the AT-CM Media Converter Line Cards.

Table 36. Default Settings for the AT-S73 Management Software

<b>Settings</b>	<b>Default</b>
Default Operating Mode	OAM Visible
Name	None
<b>Port A (Fiber Optic Port)</b>	
State	Enabled
Flow Control	Enabled
Ingress Rate Limit	No Limit
Egress Rate Limit	No Limit
<b>Port B (Twisted Pair Port)</b>	
State	Enabled
Flow Control	Enabled
Speed and Duplex Mode	Auto-Negotiation
Ingress Rate Limit	No Limit
Egress Rate Limit	No Limit
<b>OAM</b>	
Admin State	Enabled
Mode	Passive

Table 36. Default Settings for the AT-S73 Management Software

<b>Settings</b>	<b>Default</b>
Maximum OAMPDU Size	1518 octets
Unidirectional Support	Yes
Loopback Support	Yes
Event Support	No
Variable Retrieval Support	Yes
<b>T1/E1 Ports (AT-CM70S Line Card)</b>	
Carrier Type	T1
Receiver Sensitivity	Long Haul
Line Build Out	DSX-1 (0 to 133ft)/0dB CSU
Test or Normal Transmission	Normal
PRBS	Disabled
Remote Loopback	Disabled



## Appendix B

# SNMPv3 Configuration Examples

---

This appendix provides two examples of SNMPv3 configurations using the SNMPv3 Table menus. In addition, a worksheet is provided which you can use as an aid when configuring the SNMPv3 protocol. This appendix includes the following sections:

- ❑ “SNMPv3 Manager Configuration” on page 291
- ❑ “SNMPv3 Operator Configuration” on page 293
- ❑ “SNMPv3 Worksheet” on page 294

## SNMPv3 Configuration Examples

---

This appendix provides SNMPv3 configuration examples for the following types of users:

- ❑ Manager
- ❑ Operator

In addition an SNMPv3 Configuration Table is provided to record your SNMPv3 configuration.

For more information about the SNMPv3 protocol, see Chapter 10, “Configuring SNMPv3” on page 237.

### **SNMPv3 Manager Configuration**

This section provides a sample configuration for a Manager with a User Name of systemadmin24. Each table is listed with its parameters.

#### **Configure SNMPv3 User Table Menu**

User Name: manager

Authentication Protocol: MD5

Privacy Protocol: DES

Storage Type: NonVolatile

### **Configure SNMPv3 View Table Menu**

View Name: internet

View Subtree OID: .1.3.6.1.2.1.6

Subtree Mask: ff

View Type: Included

Storage Type: NonVolatile

### **Configure SNMPv3 Access Table**

Group Name: grpmanager

Context Prefix:

Security Model: usm

Security Level: AuthNoPriv

Context Match: Prefix

Read View Name: viewUSMmanager

Write View Name: viewUSMmanager

Notify View Name: viewUSMmanager

Storage Type: NonVolatile

### **Configure SNMPv3 Group Table**

Security Name: commpublic

Security Model: v1

Group Name: grpcommpublic

Storage Type: NonVolatile

### **Configure SNMPv3 Notify Table**

Notify Name: sysadminTrap

Notify Tag: sysadminTag

Notify Type: Trap

Storage Type: NonVolatile

**Configure SNMPv3 Target Address Table**

Target Address Name: host408

Ip Address: 198.35.11.1

UDP Port#: 162

Timeout: 1500

Retries: 3

Tag List: sysadminTag

Target Parameters: SNMPmgrPC

Storage Type: NonVolatile

**Configure SNMPv3 Target Parameters Table**

Target Parameters Name: SNMPmanagerPC

User (Security) Name: systemadmin24

Security Model: v3

Security Level: P-AuthPriv

Storage Type: NonVolatile

**SNMPv3  
Operator  
Configuration**

This section provides a sample configuration for an Operator with a User Name of atiengr77. Since this user will only send messages to a group and not an SNMP host, you do not need to configure message notification for this user.

**Configure SNMPv3 User Table Menu**

User Name: atiengr77

Authentication Protocol: MD5

Privacy Protocol: None

Storage Type: NonVolatile

**Configure SNMPv3 View Table Menu**

View Name: internet

View subtree OID: 1.3.6.1 (or internet)

Subtree Mask:

View Type: Included

Storage Type: NonVolatile

**Configure SNMPv3 Access Table**

Group Name: Operators

Security Model: SNMPv3

Security Level: Authentication

Read View Name: internet

Write View Name:

Notify View Name:

**SNMPv3  
Worksheet**

This section provides a table that you can use as a worksheet when configuring SNMPv3. Each SNMPv3 Table is listed with its associated parameters.

<b>SNMPv3 Parameters</b>	
<b>SNMPv3 User Table</b>	
User (Security) Name	
Authentication Protocol	
Authentication Password	
Privacy Protocol	
Privacy Password	
Storage Type	
<b>SNMPv3 View Table Menu</b>	
View Name	
View Subtree (OID format/Text Name)	
Subtree Mask (Hex format)	
View Type	
Storage Type	
<b>SNMPv3 Access Table Menu</b>	
Group Name	
Security Model	
Security Level	
Read View Name	

<b>SNMPv3 Parameters (Continued)</b>	
Write View Name	
Notify View Name	
Storage Type	
<b>SNMPv3 Group Table Menu</b>	
Security Name	
Security Model	
Group Name	
Storage Type	
<b>SNMPv3 Notify Table Menu</b>	
Notify Name	
Notify Tag	
Notify Type	
Storage Type	
<b>SNMPv3 Target Address Table Menu</b>	
Target Address Name	
Ip Address	
UDP Port#	
Timeout (10ms)	
Retries	
Tag List	
Target Parameters	
Storage Type	
<b>SNMPv3 Target Parameters Table Menu</b>	
Target Parameters Name	
User (Security) Name	
Security Model	
Security Level	
Storage Type	



## Appendix C

# Packet Rate Limiting on the AT-CM2K0S Line Card

---

Because of the component design on the AT-CM2K0S Line Card, the actual performance of packet rate limiting on the two ports may not correspond with the value you specify. The graph in Figure 131 shows the correlation between the permitted ingress and egress rate limit values and the actual average rate limits. For example, the actual packet rate limit for any value between 150,000 and 250,000 is 285,714 packets. To set packet rate limiting, refer to “Configuring the Port Parameters on AT-CM Line Cards” on page 139.

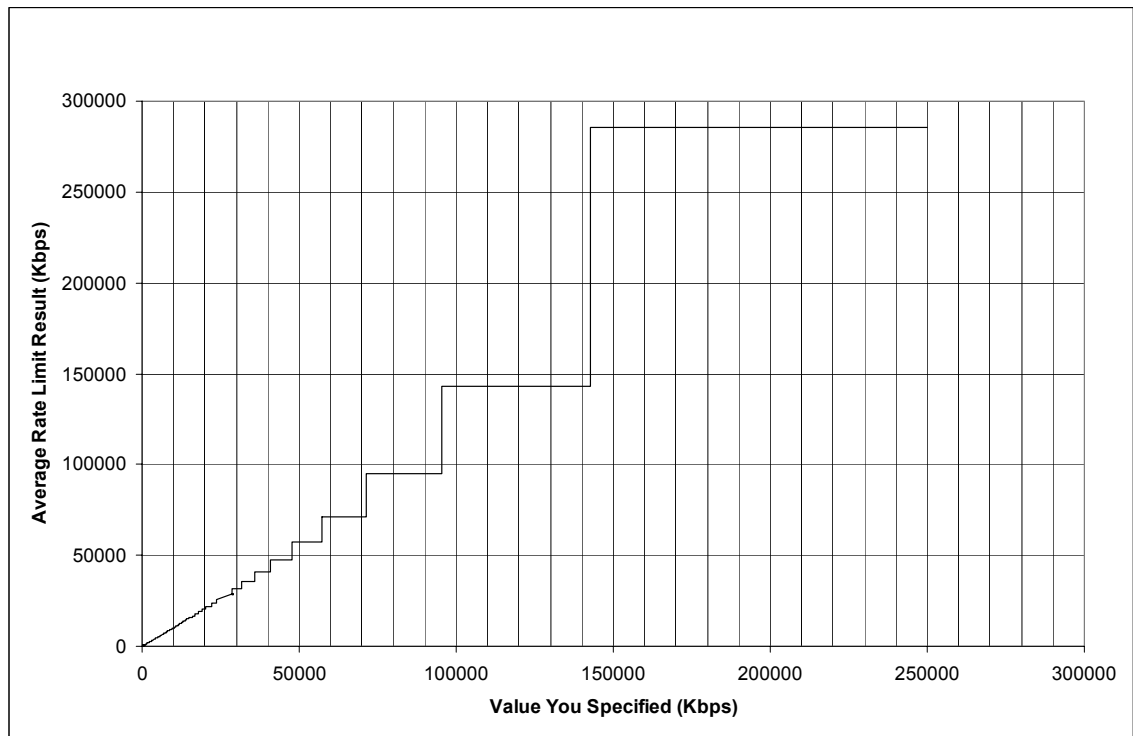


Figure 131. Rate Limit Input vs. Hardware Configured Values

Table 37 lists the values in table format. When you see multiple values in the “Specified Rate Limit (Kbps)” column and “Same” in the “Average Rate Limit (Kbps)” column, the average rate limit value equals the specified rate limit. When you see multiple values in the “Specified Rate Limit (Kbps)” column and one value in the “Average Rate Limit (Kbps)” column, all of the specified values result in the same average rate limit.

Table 37. Rate Limits Equivalents

<b>Specified Rate Limit (Kbps)</b>	<b>Average Rate Limit Result (Kbps)</b>
70 through 556	Same
557 and 558	558
559 through 566	Same
567 and 568	568
569 through 574	Same
575 and 576	576
577 through 581	Same
582 and 583	583
584 through 587	Same
588 and 589	589
590 through 592	Same
593 and 594	594
595 through 598	Same
599 and 600	600
601 through 602	Same
604 and 604	604
605 through 607	607
608 and 609	609
610 through 611	Same
612 and 613	613
614 through 615	Same
616 and 617	617
618 through 619	Same
620 and 621	621
622 through 623	Same
624 and 625	625
626 through 627	Same

Table 37. Rate Limits Equivalents (Continued)

<b>Specified Rate Limit (Kbps)</b>	<b>Average Rate Limit Result (Kbps)</b>
628 and 629	629
630	Same
631 and 632	632
633 through 634	Same
635 and 636	636
637	Same
638 and 639	639
640	Same
641 and 642	642
643 through 644	Same
645 and 646	646
647	Same
648 and 649	649
650	Same
651 and 652	652
653	Same
654 and 655	655
656	Same
657 and 658	658
659	659
660 and 661	661
662	662
663 and 664	664
665 and 666	666
667	667
668 and 669	669
670	670
671 and 672	672

Table 37. Rate Limits Equivalents (Continued)

<b>Specified Rate Limit (Kbps)</b>	<b>Average Rate Limit Result (Kbps)</b>
673	673
674 and 675	675
676 and 677	677
678	678
679 and 680	680
681	681
682 and 683	683
684 and 685	685
686	686
687 and 688	688
689 and 690	690
691	691
692 and 693	693
694 and 695	695
696	696
697 and 698	698
699 and 700	700
710 and 702	702
703	703
705 and 705	705
706 and 707	707
708	708
709 and 710	710
711 and 712	712
713 and 714	714
715 and 716	716
718 and 719	719
720 and 721	721

Table 37. Rate Limits Equivalents (Continued)

<b>Specified Rate Limit (Kbps)</b>	<b>Average Rate Limit Result (Kbps)</b>
722 and 723	723
724 and 725	725
726 and 727	727
728	728
729 and 730	730
731 and 732	732
733 and 734	734
735 and 736	736
737 and 738	738
739 and 740	740
741 and 742	742
743 and 744	744
745	745
746 and 747	747
748 and 749	749
750 and 751	751
752 and 753	753
754 and 755	755
756 and 757	757
758 and 759	759
760 and 761	761
762 and 763	763
764 and 765	765
766 and 767	767
768 through 768	768
769 and 770	770
771 and 772	772
773 and 774	774

Table 37. Rate Limits Equivalents (Continued)

<b>Specified Rate Limit (Kbps)</b>	<b>Average Rate Limit Result (Kbps)</b>
775 and 776	776
777 and 778	778
779 and 780	780
781 and 782	782
783 and 784	784
785 through 787	787
788 and 789	789
790 and 791	791
792 and 793	793
794 and 795	795
796 through 798	798
799 and 800	800
801 and 802	802
803 and 804	804
805 through 807	807
808 and 809	809
810 and 811	811
812 through 814	814
815 and 816	816
817 and 818	818
819 through 821	821
822 and 823	823
824 and 825	825
826 through 828	828
829 and 830	830
831 and 832	832
833 through 835	835
836 and 837	837

Table 37. Rate Limits Equivalents (Continued)

<b>Specified Rate Limit (Kbps)</b>	<b>Average Rate Limit Result (Kbps)</b>
838 to 840	840
841 and 842	842
843 through 845	845
846 and 847	847
851 and 852	852
853 through 855	855
856 through 858	858
859 and 860	860
861 through 863	863
864 and 865	865
866 through 868	868
869 through 871	871
872 and 873	873
874 through 876	876
877 through 879	879
880 and 881	881
882 through 884	884
885 through 887	887
888 through 890	890
891 and 892	892
893 through 895	895
896 through 898	898
899 through 901	901
902 through 904	904
905 through 907	907
908 and 909	909
910 through 912	912
913 through 915	915

Table 37. Rate Limits Equivalents (Continued)

<b>Specified Rate Limit (Kbps)</b>	<b>Average Rate Limit Result (Kbps)</b>
916 through 918	918
919 through 921	921
922 through 924	924
925 through 927	927
928 through 930	930
931 through 933	933
934 through 936	936
937 through 939	939
940 through 942	942
943 through 946	946
947 through 949	949
950 through 952	952
953 through 955	955
956 through 958	958
959 through 962	962
963 through 965	965
966 through 968	968
969 through 971	971
972 through 975	975
976 through 978	978
979 through 981	981
982 through 985	985
986 through 988	988
989 through 992	992
993 through 995	995
996 through 999	999
1000 through 1002	1002
1003 through 1006	1006

Table 37. Rate Limits Equivalentents (Continued)

<b>Specified Rate Limit (Kbps)</b>	<b>Average Rate Limit Result (Kbps)</b>
1007 through 1009	1009
1010 through 1013	1013
1014 through 1016	1016
1017 through 1020	1020
1021 through 1024	1024
1025 through 1027	1027
1028 through 1031	1031
1032 through 1035	1035
1036 through 1038	1038
1039 through 1042	1042
1043 through 1046	1046
1047 through 1050	1050
1051 through 1054	1054
1055 through 1058	1058
1059 through 1062	1062
1063 through 1066	1066
1067 through 1070	1070
1071 through 1074	1074
1075 through 1078	1078
1079 through 1082	1082
1083 through 1086	1086
1087 through 1090	1090
1091 through 1094	1094
1095 through 1098	1098
1099 through 1103	1103
1104 through 1107	1107
1108 through 1111	1111
1112 through 1116	1116

Table 37. Rate Limits Equivalents (Continued)

<b>Specified Rate Limit (Kbps)</b>	<b>Average Rate Limit Result (Kbps)</b>
1117 through 1120	1120
1121 through 1124	1124
1125 through 1129	1129
1130 through 1133	1133
1134 through 1138	1138
1139 through 1142	1142
1143 through 1147	1147
1148 through 1152	1152
1153 through 1156	1156
1157 through 1161	1161
1162 through 1166	1166
1167 through 1170	1170
1171 through 1175	1175
1176 through 1180	1180
1181 through 1185	1185
1186 through 1190	1190
1191 through 1195	1195
1196 through 1200	1200
1201 through 1205	1205
1206 through 1210	1210
1211 through 1215	1215
1216 through 1221	1221
1222 through 1226	1226
1227 through 1231	1231
1232 through 1236	1236
1237 through 1242	1242
1243 through 1247	1247
1248 through 1253	1253

Table 37. Rate Limits Equivalentents (Continued)

<b>Specified Rate Limit (Kbps)</b>	<b>Average Rate Limit Result (Kbps)</b>
1259 through 1264	1264
1265 through 1269	1269
1270 through 1275	1275
1276 through 1281	1281
1282 through 1287	1287
1288 through 1292	1292
1293 through 1298	1298
1299 through 1304	1304
1305 through 1310	1310
1311 through 1316	1316
1317 through 1322	1322
1323 through 1328	1328
1329 through 1335	1335
1336 through 1341	1341
1342 through 1347	1347
1348 through 1354	1354
1355 through 1360	1360
1361 through 1367	1367
1368 through 1373	1373
1374 through 1380	1380
1381 through 1386	1386
1387 through 1393	1393
1394 through 1400	1400
1401 through 1407	1407
1408 through 1414	1414
1415 through 1421	1421
1422 through 1428	1428
1429 through 1435	1435

Table 37. Rate Limits Equivalents (Continued)

<b>Specified Rate Limit (Kbps)</b>	<b>Average Rate Limit Result (Kbps)</b>
1436 through 1443	1443
1444 through 1450	1450
1451 through 1457	1457
1458 through 1465	1465
1466 through 1472	1472
1473 through 1480	1480
1481 through 1488	1488
1489 through 1495	1495
1496 through 1503	1503
1504 through 1511	1511
1512 through 1519	1519
1520 through 1527	1527
1528 through 1536	1536
1537 through 1544	1544
1545 through 1552	1552
1553 through 1561	1561
1562 through 1569	1569
1570 through 1578	1578
1579 through 1587	1587
1588 through 1596	1596
1597 through 1605	1605
1606 through 1614	1614
1615 through 1623	1623
1624 through 1632	1632
1633 through 1642	1642
1643 through 1651	1651
1652 through 1661	1661
1662 through 1670	1670

Table 37. Rate Limits Equivalents (Continued)

<b>Specified Rate Limit (Kbps)</b>	<b>Average Rate Limit Result (Kbps)</b>
1671 through 1680	1680
1681 through 1690	1690
1691 through 1700	1700
1701 through 1710	1710
1711 through 1721	1721
1722 through 1731	1731
1732 through 1742	1742
1743 through 1752	1752
1753 through 1763	1763
1764 through 1774	1774
1775 through 1785	1785
1786 through 1796	1796
1797 through 1808	1808
1809 through 1819	1819
1820 through 1831	1831
1832 through 1843	1843
1844 through 1855	1855
1856 through 1867	1867
1868 through 1879	1879
1880 through 1892	1892
1893 through 1904	1904
1905 through 1917	1917
1918 through 1930	1930
1931 through 1943	1943
1944 through 1956	1956
1957 through 1970	1970
1971 through 1984	1984
1985 through 1998	1998

Table 37. Rate Limits Equivalents (Continued)

<b>Specified Rate Limit (Kbps)</b>	<b>Average Rate Limit Result (Kbps)</b>
1999 through 2012	2012
2013 through 2026	2026
2027 through 2040	2040
2041 through 2055	2055
2056 through 2070	2070
2071 through 2085	2085
2086 through 2100	2100
2101 through 2116	2116
2117 through 2132	2132
2133 through 2148	2148
2149 through 2164	2164'
2165 through 2181	2181
2182 through 2197	2197
2198 through 2214	2214
2215 through 2232	2232
2233 through 2249	2249
2250 through 2267	2267
2268 through 2285	2285
2286 through 2304	2304
2305 through 2322	2322
2323 through 2341	2341
2342 through 2361	2361
2362 through 2380	2380
2381 through 2400	2400
2401 through 2421	2421'
2422 through 2442	2442
2443 through 2463	2463
2464 through 2484	2484

Table 37. Rate Limits Equivalentents (Continued)

<b>Specified Rate Limit (Kbps)</b>	<b>Average Rate Limit Result (Kbps)</b>
2485 through 2506	2506
2507 through 2528	2528
2529 through 2551	2551
2552 through 2574	2574
2575 through 2597	2597
2598 through 2621	2621
2622 through 2645	2645
2646 through 2670	2670
2671 through 2695	2695
2696 through 2721	2721
2722 through 2747	2747
2748 through 2773	2773
2774 through 2801	2801
2802 through 2828	2828
2829 through 2857	2857
2858 through 2886	2886
2887 through 2915	2915
2916 through 2945	2945
2946 through 2976	2976
2977 through 3007	3007
3008 through 3039	3039
3040 through 3072	3072
3073 through 3105	3105
3106 through 3139	3139
3140 through 3174	3174
3175 through 3210	3210
3211 through 3246	3246
3247 through 3284	3284

Table 37. Rate Limits Equivalents (Continued)

<b>Specified Rate Limit (Kbps)</b>	<b>Average Rate Limit Result (Kbps)</b>
3285 through 3322	3322
3323 through 3361	3361
3362 through 3401	3401
3402 through 3442	3442
3443 through 3484	3844
3485 through 3527	3527
3528 through 3571	3571
3572 through 3616	3616
3617 through 3663	3663
3664 through 3710	3710
3711 through 3759	3759
3760 through 3809	3809
3810 through 3861	3861
3862 through 3913	3913
3914 through 3968	3968
3969 through 4024	4024
4025 through 4081	4081
4082 through 4140	4140
4141 through 4201	4201
4202 through 4264	4264
4265 through 4329	4329
4330 through 4395	4395
4396 through 4464	4464
4465 through 4535	4535
4536 through 4608	4608
4609 through 4683	4683
4684 through 4761	4761
4762 through 4842	4842

Table 37. Rate Limits Equivalents (Continued)

<b>Specified Rate Limit (Kbps)</b>	<b>Average Rate Limit Result (Kbps)</b>
4843 through 4926	4926
4927 through 5012	5012
5013 through 5102	5102
5103 through 5194	5194
5195 through 5291	5291
5292 through 5390	5390
5391 through 5494	5494
5495 through 5602	5602
5603 through 5714	5714
5715 through 5830	5830
5831 through 5952	5952
5953 through 6079	6079
6080 through 6211	6211
6212 through 6349	6349
6350 through 6493	6493
6494 through 6644	6644
6645 through 6802	6802
6803 through 6968	5958
6969 through 7142	7142
7143 through 7326	7326
7327 through 7518	7518
7519 through 7722	7722
7723 through 7936	7936
7937 through 8163	8163
8164 through 8403	8403
8404 through 8658	8658
8659 through 8928	8928
8929 through 9216	9216

Table 37. Rate Limits Equivalents (Continued)

<b>Specified Rate Limit (Kbps)</b>	<b>Average Rate Limit Result (Kbps)</b>
9217 through 9523	9523
9524 through 9852	9852
9853 through 10204	10204
10205 through 10582	10582
10583 through 10989	10989
10990 through 11428	11428
11429 through 11904	11904
11905 through 12422	12422
12423 through 12987	12987
12988 through 13605	13605
13606 through 14285	14285
14286 through 15037	15037
15038 through 15873	15873
15874 through 16806	16806
16807 through 17857	17857
17858 through 19047	19047
19048 through 20408	20408
20409 through 21978	21978
21979 through 23809	23809
23810 through 25974	25974
25975 through 28571	28571
28572 through 31746	31746
31747 through 35714	35714
35715 through 40816	40816
40817 through 47619	47619
47620 through 57142	57142
57143 through 71428	71428
71429 through 95238	95238

Table 37. Rate Limits Equivalents (Continued)

<b>Specified Rate Limit (Kbps)</b>	<b>Average Rate Limit Result (Kbps)</b>
142858 through 250000	285714



# Index

---

## Numerics

- 10/100Base-TX port
  - configuring 107
  - described 22
  - restoring default settings 112

## A

- activity monitor
  - described 23
  - displaying 104
- AT-CM Line Cards
  - configuration files 29
  - configuring for dying gasp 230
  - configuring port settings 139
  - configuring remote port settings 180, 184
  - configuring, with remote peer management 174, 182
  - default settings 288
  - described 36
  - displaying port settings 136
  - displaying remote port settings 180, 184
  - downloading software with TFTP 275
  - downloading software with XMODEM 279
  - MAC addresses 167
  - naming 149
  - port statistics 160
  - remote version numbers 187
  - resetting 162
  - restoring configurations 30
  - restoring default settings 153
  - restoring last saved configuration 157, 181
  - restoring last saved remote configuration 185
  - restoring remote default settings 180, 185
  - serial numbers 167
  - status 128
  - version numbers 164
- AT-CM2KOS Line Card, maximum frame size 150
- AT-CM70S Line Card
  - Console port settings 199
  - T1/E1 ports 192
- AT-CV Line Cards
  - configuration files 29
  - described 40
  - serial numbers 167
  - status 128
- AT-CV5M01 Management Card 21
- AT-CV5M02 Management Card
  - activating standby card 117
  - default settings 287
  - described 21

- downloading master configuration files 284
  - downloading software with TFTP 275
  - downloading software with XMODEM 279
  - MAC addresses 121
  - master configuration files 29
  - naming 72, 85, 90
  - redundant cards 26
  - resetting 96
  - restoring default settings 113
  - serial number 167
  - uploading master configuration files 281
- AT-S73 Management Software
    - default settings 288
    - described 38
    - downloading, with TFTP 275
    - downloading, with XMODEM 279
    - remote version numbers 187
    - version numbers 164
  - AT-S99 Management Software
    - default settings 287
    - described 22
    - downloading master configuration files 284
    - downloading, with TFTP 275
    - downloading, with XMODEM 279
    - uploading master configuration files 281
  - auto-copy
    - described 30
    - setting 151
  - Auto-Negotiation
    - AT-CM Line Cards 139
    - AT-CV5M02 Management Card 107

## C

- configuration files 29, 64
  - See also *master configuration files*
- Console port
  - default settings 58, 288
  - described 22
  - setting baud rate 119
- console timeout 90
- contact 86
- Converteon chassis 34

## D

- date and time
  - setting 71, 93
- default settings
  - AT-CM Line Cards 288
  - AT-CV5M02 Management Card 287

dying gasp  
 configuring AT-CM Line Cards for 230  
 described 52  
 testing 235

**E**

event log  
 described 23  
 displaying 98

**F**

flow control 139

**I**

IP address configuration  
 described 23  
 setting 70, 80

**L**

Link Test operating mode  
 described 42  
 selecting 145  
 local management  
 described 25  
 enabling or disabling 90  
 starting 58  
 location 86

**M**

MAC addresses  
 AT-CM and AT-CV Line Cards 167  
 AT-CV5M02 Management Card 121  
 manager account  
 changing password 69, 90  
 described 24  
 master configuration files  
 described 29  
 downloading 284  
 redundant management cards 32  
 saving parameter settings 64  
 uploading 281  
 MDI, MDIX  
 AT-CM Line Cards 139  
 AT-CV5M02 Management Card 107  
 menus navigation 60  
 MissingLink operating mode  
 described 43  
 selecting 145

**N**

naming  
 AT-CM Line Cards 149  
 AT-CV5M02 Management Card 85  
 remote AT-CM Line Cards 179  
 Network Time Protocol (NTP) client  
 configuring 71, 95  
 described 24  
 requirements 28

**O**

OAM Bypass operating mode  
 described 45  
 selecting 145  
 OAM clients  
 configuring 204  
 default settings 288  
 local status 214  
 remote status 221  
 statistics 223  
 OAM loopback tests  
 configuring AT-CM Line Cards for 74  
 described 51  
 performing 209  
 OAM variable requests  
 configuring AT-CM Line Cards for 74  
 described 55  
 performing 225  
 OAM Visible operating mode  
 described 45  
 selecting 145  
 OAM-based features  
 configuring, on AT-CM Line Cards 74  
 described 46  
 settings 56  
 OAMPDUs, setting maximum size 206  
 operating modes  
 configuring 45  
 described 42  
 displaying 128  
 selecting 145  
 operator account  
 changing password 69, 90  
 described 24

**P**

passwords, setting 69, 90  
 pinging network devices  
 performing 125  
 requirements 28  
 ports, configuring 139

**R**

redundant management cards  
 activating 117  
 described 26  
 master configuration files 32  
 status messages 27  
 remote management software updates  
 configuring AT-CM Line Cards for 74  
 described 50  
 remote peer management  
 configuring AT-CM Line Cards for 74  
 described 46  
 using menus 174  
 using web browser windows 182  
 remote peer management updates  
 with TFTP 275  
 with XMODEM 279

- resetting
  - AT-CM Line Cards 162
  - AT-CV5M02 Management Card 96

## S

- serial numbers 167
- SFP information 170
- Smart MissingLink operating mode
  - described 44
  - selecting 145
- SNMP community strings
  - configuring 70, 88
  - default settings 287
- SNMP management
  - described 25
  - requirements 28
- SNMP traps
  - adding IP addresses of receivers 89
  - requirements 28
- SNMPv3
  - described 238
  - examples 291
- SNMPv3 Access Table
  - configuring 254
  - described 244
- SNMPv3 Group Table
  - configuring 258
  - described 245
- SNMPv3 Notify Table
  - configuring 261
  - described 245
- SNMPv3 Target Address Table
  - configuring 264
  - described 245
- SNMPv3 Target Parameters Table
  - configuring 267
  - described 245
- SNMPv3 User Table
  - configuring 248
  - described 244
- SNMPv3 View Table
  - configuring 251
  - described 244
- standby management card
  - activating 117
- standby management cards
  - described 26
- statistics 160
- syslog client
  - configuring 105
  - described 23
  - requirements 28

## T

- T1/E1 ports
  - configuring, from Console port 199
  - configuring, with AT-CV5M02 Management Card 196
  - default settings 289
  - selecting management method 192

- Telnet management
  - described 25
  - enabling or disabling 90
  - requirements 28
  - starting 61
- temperature threshold 115
- TFTP client
  - configuring 273
  - downloading management software 275
  - downloading master configuration files 284
  - requirements 28
  - uploading master configuration files 281

## U

- unidirectional support 206

## W

- web browser management
  - described 25
  - requirements 28
  - starting 62

## X

- XMODEM, downloading management software 279

