



WaveRider®
The World's Wireless Web Company

LMS2000 User Guide

Version 0.3



WaveRider Communications Inc.

Software License Agreement

This is a legal agreement between you (either an individual or an entity) and WaveRider Communications Inc. for the use of WaveRider computer software, hereinafter the "LICENSED SOFTWARE".

By using the LICENSED SOFTWARE installed in this product, you acknowledge that you have read this license agreement, understand it, and agree to be bound by its terms. You further agree that it is the full and complete agreement between you and WaveRider Communications Inc., superseding all prior written or verbal agreements of any kind related to the LICENSED SOFTWARE. If you do not understand or do not agree to the terms of this agreement, you will cease using the LICENSED SOFTWARE immediately.

1. GRANT OF LICENSE—This License Agreement permits you to use one copy of the LICENSED SOFTWARE.
2. COPYRIGHT—The LICENSED SOFTWARE is owned by WaveRider Communications Inc. and is protected by copyright laws and international treaty provisions; therefore, you must treat the LICENSED SOFTWARE like any other copyrighted material (e.g., a book or magazine). You may not copy the written materials accompanying the LICENSED SOFTWARE.
3. OTHER RESTRICTIONS—You may not rent or lease the LICENSED SOFTWARE. You may not reverse engineer, decompile, or disassemble the LICENSED SOFTWARE.
4. LIMITED WARRANTY—The LICENSED SOFTWARE is provided "as is" without any warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The entire risk as to the quality and performance of the LICENSED SOFTWARE is with you, the licensee. If the LICENSED SOFTWARE is defective, you assume the risk and liability for the entire cost of all necessary repair, service, or correction.

Some states/jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you. This warranty gives you specific legal rights, and you may have other rights, which vary from state/jurisdiction to state/jurisdiction.

WaveRider Communications Inc. does not warrant that the functions contained in the LICENSED SOFTWARE will meet your requirements, or that the operation of the LICENSED SOFTWARE will be error-free or uninterrupted.

5. NO OTHER WARRANTIES—To the maximum extent permitted by applicable law, WaveRider Communications Inc. disclaims all other warranties, either express or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose, with regard to the LICENSED SOFTWARE and the accompanying written materials.
6. NO LIABILITY FOR CONSEQUENTIAL DAMAGES—To the maximum extent permitted by applicable law, in no event shall WaveRider Communications Inc. or its suppliers be liable for any damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, or any other pecuniary loss) arising from the use of or inability to use the LICENSED SOFTWARE, even if WaveRider Communications Inc. has been advised of the possibility of such damages, or for any claim by any other party.

Because some states/jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

In no event will WaveRider's liability exceed the amount paid for the LICENSED SOFTWARE.

The following are trademarks or registered trademarks of their respective companies or organizations:

Microsoft Windows NT 4.0 Workstation (with Service Pack 6a), Microsoft Windows NT Server 4.0, Microsoft Access, Microsoft SQL Server, Microsoft SQL Agent / Microsoft Corporation

Vircom VOP Radius Server / Vircom Inc.

Castlerock SNMPc Server / Castle Rock Computing

Tardis Timeserver / H.C. Mingham-Smith Ltd.

APS PowerChute PLUS / American Power Conversion

CD-Writer Plus / Hewlett Packard Company

3200 Color Jetprinter / Lexmark International Inc.

Veritas Backup Exec / VERITAS Software

© 2000, 2001 by WaveRider Communications Inc. All rights reserved. This manual may not be reproduced by any means in whole or in part without the express written permission of WaveRider Communications Canada Inc.

Version 0.3, February 2001

Warranty

In the following warranty text, "WaveRider®" shall mean WaveRider Communications Inc.

This WaveRider product is warranted against defects in material and workmanship for a period of **one (1) year** from the date of purchase. During this warranty period WaveRider will, at its option, either repair or replace products that prove to be defective.

For warranty service or repair, the product must be returned to a service facility designated by WaveRider. Authorization to return products must be obtained prior to shipment. The WaveRider RMA number must be on the shipping documentation so that the service facility will accept the product. The buyer shall pay all shipping charges to WaveRider and WaveRider shall pay shipping charges to return the product to the buyer within Canada or the USA. For all other countries, the buyer shall pay shipping charges as well as duties and taxes incurred in shipping products to or from WaveRider.

WaveRider warrants that the firmware designed by it for use with the unit will execute its programming instructions when properly installed on the unit. WaveRider does not warrant that the operation of the unit or firmware will be uninterrupted or error-free.

Limitation of Warranty

The foregoing warranty shall not apply to defects resulting from improper or inadequate maintenance by the buyer, buyer-supplied interfacing, unauthorized modification or misuse, operation outside the environmental specifications for the product, or improper site preparation or maintenance. No other warranty is expressed or implied. WaveRider specifically disclaims the implied warranties of merchantability and fitness for any particular purpose.

No Liability for Consequential Damages

To the maximum extent permitted by applicable law, in no event shall WaveRider or its suppliers be liable for any damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, or any other pecuniary loss) arising from the use of or inability to use the product, even if WaveRider has been advised of the possibility of such damages, or for any claim by any other party.

Because some states/jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

In no event will WaveRider's liability exceed the amount paid for the product.

Regulatory Notices

This equipment has been tested and found to comply with the limits for a Class A Intentional Radiator, pursuant to Part 15 of the FCC Regulations and RCC-210 of the IC Regulations. These limits are intended to provide protection against harmful interference when the equipment is operated in a commercial/business/industrial environment.

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

Notice to User

Any changes or modifications to equipment that are not expressly approved by the manufacturer may void the user's authority to operate the equipment.

Contents

1	Understanding the LMS2000	1
1.1	NAP	2
1.1.1	NAP Router	4
1.1.2	Ethernet Switch	4
1.1.3	NAP UPS	4
1.1.4	NMS Server	4
1.1.5	Advanced Bandwidth Manager (optional)	4
1.2	Network Management System (NMS)	5
1.2.1	Microsoft Windows NT	5
1.2.2	LMS Network Management System	5
1.2.3	LMS Network Management System Server Software	5
1.2.4	LMS Network Management System Client Software	5
1.2.5	Microsoft SQL Server	6
1.2.6	Vircom VOP RADIUS	6
1.2.7	Castlerock SNMPc Server	7
1.2.8	Veritas Backup Exec with Microsoft SQL Agent	7
1.2.9	Network/ISP Interface	7
1.3	CAP	7
1.3.1	CCU	8
1.3.2	CAP Ethernet Switch	8
1.3.3	CAP UPS	9
1.3.4	Radio Frequency Subsystem	9
1.3.5	Antenna Subsystem	9
1.3.6	Back Haul (Optional)	9
1.4	EUM	10
1.5	Data Flow	11
2	Installing the NAP and the CAP	13
2.1	Setting up the CAP Using the Default Configuration	14
2.1.1	Reconnecting the UPS Battery After Shipping	15
2.1.2	Setting up your Back Haul Equipment	17
2.2	Setting up the NAP Using the Default Configuration	18
2.3	Testing the NAP/CAP Connection	19
3	Getting Started with the NMS	21
3.1	Starting the NMS Workstation	21
3.2	Understanding Records Management	23
3.2.1	LMS2000 Branch	25
3.2.2	Inventory Branch	26
3.2.3	Accounts Branch	27
3.2.4	Shortcut Menus	28
3.2.5	Buttons	31

3.2.6	Icon Colors	32
3.3	Opening Records for Individual Devices	33
3.3.1	Understanding the Properties Screen	33
4	Setting Up SNMPc Server	35
4.1	Changing the SNMPc Server Password	36
4.2	Creating a Network Map	36
4.3	Adding SNMP Communities	39
4.4	Adding a Trend Report	40
5	Configuring the NAP and CAP	45
5.1	Configuring the NAP	45
5.1.1	Understanding NAP IP Address Defaults	46
5.1.2	Naming the NAP	47
5.1.3	Verifying the NAP Configuration	47
5.1.4	Configuring the NAP Ethernet Switch	52
5.1.5	Configuring the NAP Router	53
5.1.6	Configuring Router-based Bandwidth Management	55
5.1.7	Changing the IP Address of the NMS	58
5.1.8	Configuring Other NAP Components	62
5.2	Configuring the CAP	62
5.2.1	Understanding CAP IP Address Defaults	63
5.2.2	Naming the CAP	65
5.2.3	Verifying the CAP Configuration	65
5.2.4	Configuring the CAP Ethernet Switch	67
5.2.5	Configuring Other CAP Components	68
5.3	Connecting the NAP to the Internet	68
5.3.1	Testing the Internet Connection	69
6	Configuring a CCU	71
6.1	Assigning a Password to a CCU	72
6.2	Configuring the Ethernet and Radio Properties	73
6.2.1	Assigning a CCU ID	73
6.2.2	Adding EUMs to the CCU Record	73
6.2.3	Assigning a Radio Channel to the CCU	74
6.2.4	Enabling Radio Transmission	75
6.2.5	Verifying the Network IP Address	75
6.2.6	Verifying the Radio IP Address	75
6.3	Configuring the IP Routing Properties	76
6.3.1	Configuring Static Routing	76
6.3.2	Configuring RIP	78
6.4	Configuring the SNMP Properties	79
6.4.1	Defining SNMP Communities	80
6.4.2	Defining SNMP Trap Servers	81
6.5	Uploading the Configuration to the CCU	83
7	Adding an EUM	85
7.1	Connecting to an EUM	86

7.2	Creating a New EUM Record.	87
7.2.1	Adding a New EUM Record to the NMS	87
7.2.2	Importing a Saved EUM Configuration	88
7.2.3	Naming an EUM	89
7.2.4	Assigning a Password	89
7.3	Configuring the Ethernet and Radio Properties	91
7.4	Configuring the IP Routing Properties	93
7.4.1	Configuring Static Routing	93
7.4.2	Configuring RIP	95
7.4.3	Configuring DHCP Relay	96
7.5	Configuring SNMP and DNS Server Properties.	97
7.5.1	Configuring SNMP Properties	98
7.5.2	Configuring DNS Server Options	99
7.6	Saving the EUM Configuration to a File.	100
7.7	Uploading the Configuration to the EUM	101
7.8	Assigning a Subscriber and Service Level to an EUM.	101
7.9	Adding an EUM to a CCU Record	105
7.10	Changing the Ethernet IP Address	107
7.11	Deploying an EUM.	108
8	Configuring RFSM	109
8.1	Installing an RFSM into a CAP	112
8.1.1	Changing the IP Address of the RFSM	114
8.2	Configuring the RFSM	115
8.2.1	Changing the RFSM Password	117
8.3	Configuring CCU Connections to the RFSM	118
8.4	Starting the RFSM Service	121
8.5	Verifying the Polling Engine is Running.	123
8.6	Testing the Backup Antenna	125
9	Configuring the Advanced Bandwidth Manager	127
9.1	Installing iSurfRanger Hardware into the NAP.	130
9.1.1	Installing the iSurfRanger Controller	130
9.1.2	Initializing the iSurfRanger Controller	132
9.1.3	Connecting the Controller to the Network	134
9.1.4	Installing a Dual Controller	135
9.1.5	Installing Non-redundant Controllers	135
9.1.6	Cabling a Serial Redundant Controller	136
9.1.7	Cabling a Parallel Redundant Controller	137
9.2	Adding a Bandwidth Manager Record to the NMS	138
9.3	Defining Controller Properties	143
9.3.1	Configuring Redundancy	143
9.3.2	Configuring Bandwidth Controls	148
9.4	Defining System Security Parameters.	151
9.5	Configuring Bandwidth Sets.	153
9.5.1	Setting Priorities	153
9.5.2	Configuring a Bandwidth Set	155

9.6	Establishing Schedules	160
9.7	Setting a Traffic Policy	161
9.7.1	Adding a Policy	163
10	Testing Communications	167
10.1	Running the Continuous Transmit (Tx) Test	168
10.2	Running the Continuous Receive (Rx) Test	170
10.3	Running the Transmit/Receive Loopback Test	172
10.4	Performing a Ping Test	174
11	Backing up the System	177
11.1	Recommended Backup Schedule	177
11.2	Setting Backup Properties	178
11.3	Backing Up Manually	191
11.4	Checking the Backed-up Files	192
12	Restoring Backups	193
13	Operating RFSM	211
13.1	Monitoring CCU Status Using RFSM	211
13.1.1	Refreshing the Display	214
13.2	Monitoring CCUs with the RFSM Polling Engine	214
13.3	Replacing a CCU After Configuration has Switched to Backup	215
13.4	Switching CCU Antennas and Configurations Using RFSM	221
13.4.1	Switching CCU Configurations	222
13.4.2	Switching Antennas	223
13.5	Re-establishing RFSM Polling	225
14	Running Reports	229
14.1	Running a Report	229
14.1.1	Adding Your Logo to Reports	230
14.2	Accounts Report	231
14.3	CCU/EUM Firmware Report	233
14.4	Service Level Report	234
14.5	Network IP Address Report	235
14.6	SNMPc Trend Report	237
15	Monitoring Performance	239
15.1	Network Interface Statistics	239
15.2	IP Statistics	242
15.3	Radio Packet Error Rate	245
15.4	NMS Application Logs	246
15.5	NMS Transaction Logs	248
15.6	Setting RADIUS Log Parameters	250
15.7	RADIUS Server Error Log	251
15.8	RADIUS Server User Log	252
15.9	RADIUS Server Statistics	253

15.10	SNMPc Server Device Management Details	254
15.11	SNMPc Server Event Logs	258
16	Maintaining Hardware	261
16.1	Maintaining the LMS2000 Environment	261
16.1.1	Maintaining Temperature and Humidity	261
16.1.2	Cleaning the Equipment	262
16.1.3	Checking the Cooling Fans	262
16.2	Recovering From a Power Failure	262
16.2.1	Recovering from a Power Failure at the NMS Workstation	262
16.2.2	Recovering From a Power Failure at the NAP	263
16.2.3	Recovering From a Power Failure at the CAP	263
16.2.4	Recovering From a Power Failure at an EUM	263
16.3	Maintaining the ABWM Controller	264
16.3.1	Proper Use of a Module	264
16.3.2	Replacement or Disposal of Batteries	264
16.3.3	Removing and Replacing Modules	264
17	Removing Components from your Network	267
17.1	Removing an EUM.	267
17.1.1	Disabling an Account or Subscriber	267
17.1.2	Removing an EUM from the Field	268
17.1.3	Deleting an Account or Subscriber	269
17.2	Removing an RFSM.	270
18	Upgrading the System	275
18.1	Synchronizing Database Information	275
18.2	Updating EUM and CCU Firmware	276
18.2.1	Updating EUM or CCU Firmware Using Remote Connections	278
18.3	Updating RFSM Firmware	279
18.4	Replacing Hardware Components	280
18.5	Repairing the NMS Workstation.	281
19	Troubleshooting	283
19.1	Common Problems and Solutions	283
Appendix A	Device Configuration Defaults	291
Appendix B	Operating Channel Frequencies	297
Appendix C	Command-Line Syntax	299
Appendix D	SNMP MIB Definitions	315
	CCU2000 MIB Definitions	315
	EUM2000 MIB Definitions	318
Appendix E	LMS2000 Specifications	321
	NAP Specifications	321

ABWM Specifications	322
CAP Specifications	323
RFSM Specifications	324
CCU and EUM Specifications	325
Appendix F Acronyms and Glossary	327

Figures

Figure 1	LMS2000 System Components	2
Figure 2	NAP Cabinet	3
Figure 3	CAP Cabinet	8
Figure 4	End User Modem (EUM)	10
Figure 5	System Data Flow	11
Figure 6	CAP Default Configuration (CAP #1)	14
Figure 7	Exide 5119 UPS with Battery Disconnected	16
Figure 8	Exide 5119 UPS with Battery Connected	16
Figure 9	CAP to NAP Back Haul	17
Figure 10	NAP Configuration	18
Figure 11	LMS Network Management System Main Window	23
Figure 12	NMS Record Connections	24
Figure 13	LMS2000 Branch	25
Figure 14	Inventory Branch	26
Figure 15	Accounts Branch	27
Figure 16	NAP Shortcut Menu	29
Figure 17	Inventory Shortcut Menu	29
Figure 18	Accounts Shortcut Menu	30
Figure 19	Shortcut Menu from Right Frame	33
Figure 20	Typical Properties Screen	34
Figure 21	Seeds Tab—Discovery Agents Window	37
Figure 22	General Tab—Discovery Agents Window	38
Figure 23	Comm Tab—Discovery Agents Window	39
Figure 24	Example of the SNMPc Server Main Screen	40
Figure 25	SNMPc Server Network Map	41
Figure 26	Insert Trend Report—General Tab	42
Figure 27	Trend Report Properties—Export Destinations Tab	43
Figure 28	SNMPc Trend Report Menu	44
Figure 29	LMS2000 NAP Default IP Addresses	46
Figure 30	NAP Properties	47
Figure 31	NAP Router Configuration	48
Figure 32	NAP Ethernet Switch Properties	48
Figure 33	Router-Based Bandwidth Manager Properties	49

Figure 34	Advanced Bandwidth Manager Properties	49
Figure 35	NAP UPS Properties	50
Figure 36	RADIUS Server Properties	50
Figure 37	SNMP Manager Properties	51
Figure 38	NAP Ethernet Switch Properties	52
Figure 39	NAP Ethernet Switch Web Interface	53
Figure 40	NAP Router Configuration—SNMP Tab	54
Figure 41	Router Reboot Confirmation Dialog Box	54
Figure 42	TFTPD Window	55
Figure 43	Upload Complete Dialog Box	55
Figure 44	New Bandwidth Manager Definition Dialog Box	56
Figure 45	Bandwidth Manager Properties Screen	56
Figure 46	Router Name Drop-down List	57
Figure 47	Bandwidth Set Definition Dialog Box	57
Figure 48	Edit Service Set Dialog Box	58
Figure 49	Network Dialog Box—Protocols Tab	59
Figure 50	Microsoft TCP/IP Properties Dialog Box—IP Address Tab	60
Figure 51	ABWM Application Server Config Window	61
Figure 52	Application Server Config Window	62
Figure 53	LMS2000 CAP Default Configuration (CAP #1)	64
Figure 54	CAP Properties Dialog Box	65
Figure 55	CAP Ethernet Switch Properties	66
Figure 56	CAP UPS Properties	66
Figure 57	CAP Ethernet Switch Properties	67
Figure 58	CAP Switch Web Interface	68
Figure 59	IP/Network Access Tab—Router Configuration	69
Figure 60	Channel Unit Properties—Tools Tab	72
Figure 61	Channel Unit Properties—Ethernet/Radio Tab	73
Figure 62	Add Unit Dialog Box	74
Figure 63	Channel Unit Properties—IP Routing Tab	77
Figure 64	Add Network Routes Dialog Box	77
Figure 65	Channel Unit Properties—IP Routing—RIP	78
Figure 66	Channel Unit Properties—SNMP/RADIUS Tab	80
Figure 67	Add Community String	81
Figure 68	Channel Unit Properties—SNMP/RADIUS Tab	82
Figure 69	Add Trap Server	82
Figure 70	Device Reboot Confirmation Dialog Box	83
Figure 71	End User Modem Properties	88

Figure 72	Import Configuration From File	89
Figure 73	End User Modem Properties—Tools Tab	90
Figure 74	End User Modem Properties—Ethernet/Radio Tab	91
Figure 75	Add Unit	93
Figure 76	End User Modem Properties—IP Routing Tab	94
Figure 77	Add Network Routes	94
Figure 78	End User Modem Properties—IP Routing—RIP	95
Figure 79	Add DHCP Server Dialog Box	96
Figure 80	End User Modem Properties—SNMP/RADIUS Tab	97
Figure 81	Add Community String	98
Figure 82	Add Trap Server	98
Figure 83	End User Modem Properties—SNMP/RADIUS Tab	99
Figure 84	Add DNS Server	100
Figure 85	Device Reboot Confirmation Dialog Box	101
Figure 86	Account Properties	102
Figure 87	Subscriber Properties	103
Figure 88	End User Modem Properties—Subscriber Tab	104
Figure 89	Channel Unit Properties—Ethernet/Radio Tab	105
Figure 90	Add Unit Dialog Box	105
Figure 91	End User Modem Properties—IP Routing Tab	106
Figure 92	Add Network Routes Dialog Box	106
Figure 93	Device Reboot Confirmation Dialog Box	108
Figure 94	RFSM Connections Under Normal Conditions	110
Figure 95	RFSM Connections Under Switch Conditions	110
Figure 96	RFSM Front Plane	112
Figure 97	RFSM Back Plane	112
Figure 98	RF Cable Ports on RFSM Backplane	113
Figure 99	RFSM Properties—General Tab	116
Figure 100	RFSM Properties—General Tab	117
Figure 101	Password Change Dialog Box	118
Figure 102	RFSM CCU-Antenna Assignment	119
Figure 103	Activate CCU Shortcut Menu	120
Figure 104	Activate CCU Dialog Box	120
Figure 105	RFSM Backup Antenna Reminder	121
Figure 106	RFSM Service Manager in Services Window	122
Figure 107	Service Startup Dialog Box	122
Figure 108	RFSM Service Manager in Services Window	123
Figure 109	Service Control	123

Figure 110	RFSM Service Manager	124
Figure 111	RFSM Service Manager	125
Figure 112	PEngine Icon	125
Figure 113	Relationship Between ABWM Elements	129
Figure 114	Attaching the Mounting Brackets	131
Figure 115	Mounting the Controller	131
Figure 116	Cabling the iSurfRanger Controller to the NMS	132
Figure 117	ABWM Controller Cabling	134
Figure 118	ABWM Controller Lamp Activity	135
Figure 119	iSurfRanger Controller Configured for No Redundancy	136
Figure 120	iSurfRanger Controller Configured for Serial Redundancy	136
Figure 121	Cabling for Serial Redundancy	137
Figure 122	iSurfRanger Controller Configured for Parallel Redundancy	137
Figure 123	Cabling for Parallel Redundancy	138
Figure 124	Amplifynet Bandwidth Manager Login Dialog Box	139
Figure 125	Bandwidth Manager Properties—General Tab	139
Figure 126	Bandwidth Manager Shortcut Menu	140
Figure 127	Switch to ABWM Dialog Box	140
Figure 128	Amplifynet Bandwidth Manager Login Dialog Box	141
Figure 129	Bandwidth Manager Properties	141
Figure 130	BWM to ABWM Switch Success Dialog Box	142
Figure 131	Router Restart Dialog Box	142
Figure 132	Bandwidth Manager Login	142
Figure 133	Bandwidth Manager Properties—Controller Tab	143
Figure 134	Bandwidth Manager Properties—Controller Tab	145
Figure 135	Bandwidth Manager Properties—Controller Tab	146
Figure 136	Bandwidth Manager Properties—Controller Tab	147
Figure 137	Bandwidth Manager Properties—Controller Tab	149
Figure 138	Bandwidth Manager Properties—Controller Tab	150
Figure 139	Bandwidth Manager Properties—Controller Tab	151
Figure 140	Password Change Dialog Box	152
Figure 141	Bandwidth Manager Properties—System/Security Tab	152
Figure 142	Bandwidth Manager Properties—Bandwidth Sets Tab	154
Figure 143	Priority Edit Dialog Box	155
Figure 144	Bandwidth Set Edit Dialog Box	157
Figure 145	Bandwidth Set Edit Dialog Box	158
Figure 146	Bandwidth Manager Properties—Bandwidth Sets Tab	159
Figure 147	Schedule Edit Dialog Box—Edit Mode	160

Figure 148	Schedule Edit Dialog Box—Add Mode	161
Figure 149	Two Different Bandwidth Policy Scenarios	163
Figure 150	New Policy Definition Dialog Box	164
Figure 151	Add/Edit Account/User Group	165
Figure 152	Add IP Group	165
Figure 153	New Policy Definition Dialog Box	166
Figure 154	Suggested Backup Process	178
Figure 155	Progress Indicator	179
Figure 156	Backup Exec Assistant	179
Figure 157	Options - Set Application Defaults—Media Overwrite	180
Figure 158	Options - Set Application Defaults—Backup Tab	181
Figure 159	Options - Set Application Defaults—SQL Tab	182
Figure 160	Options - Set Application Defaults—Job History	183
Figure 161	Backup SNMPc Files	184
Figure 162	SNMPc Backup Confirmation Dialog Box	184
Figure 163	Backup Job Properties—Selections Tab—C Drive Backup	185
Figure 164	SQL Database Profile Information Dialog Box	186
Figure 165	Backup Job Properties—Microsoft SQL Server Backup	186
Figure 166	Backup Job Properties—General Tab	187
Figure 167	Backup Job Properties—Advanced Tab	188
Figure 168	Schedule Options	189
Figure 169	Media Request Dialog Box	190
Figure 170	Backup Exec Job Monitor with Completed Job	191
Figure 171	Job Monitor	192
Figure 172	RFSM Service Manager in Services Window	194
Figure 173	Service Control	194
Figure 174	Restore SNMP Files Dialog Box	195
Figure 175	SNMPc File Restoration Dialog Box	195
Figure 176	MSSQLServer Icon in Windows System Tray	196
Figure 177	SQL Server Service Manager	196
Figure 178	Stop Database Confirmation Dialog Box	196
Figure 179	Stopping SQLServerAgent Confirmation Dialog Box	197
Figure 180	SQL Server Service Manager—SQLServerAgent Stopped	197
Figure 181	SQL Server Group Started	198
Figure 182	Microsoft SQL Server Enterprise Manager	198
Figure 183	Connect to SQL Server Dialog Box	199
Figure 184	LMS2000_v6 Properties Dialog Box	199
Figure 185	Microsoft SQL Server Enterprise Manager	200

Figure 186	AMP Properties Dialog Box	201
Figure 187	MSSQL Server Icon in Windows System Tray	201
Figure 188	SQL Server Service Manager	202
Figure 189	Stop Database Confirmation Dialog Box	202
Figure 190	Restore Job Properties—Selections Tab	203
Figure 191	Restore Job Properties—SQL Tab	204
Figure 192	SQL Server Group Started	205
Figure 193	Microsoft SQL Server Enterprise Manager	206
Figure 194	Connect to SQL Server Dialog Box	206
Figure 195	LMS2000_v6 Properties Dialog Box	207
Figure 196	Microsoft SQL Server Enterprise Manager	208
Figure 197	AMP Properties Dialog Box	209
Figure 198	MSSQL Server Icon in Windows System Tray	209
Figure 199	SQL Server Service Manager	210
Figure 200	RFSM Control	212
Figure 201	Switch Control	213
Figure 202	RFSM Polling Engine Window	214
Figure 203	RFSM Service Manager	216
Figure 204	RFSM Service Manager	218
Figure 205	RFSM Switch Control Shortcut Menu—Restore Configuration	219
Figure 206	RFSM Service Manager	220
Figure 207	RFSM Service Manager in Services Window	221
Figure 208	Service Control	221
Figure 209	RFSM Switch Control Shortcut Menu—Switch Configuration	222
Figure 210	RFSM Switch Control Shortcut Menu—Switch Antenna	223
Figure 211	RFSM Switch Control Shortcut Menu—Restore Antenna	224
Figure 212	RFSM Control Shortcut Menu	225
Figure 213	Activate CCU Shortcut Menu	226
Figure 214	Activate CCU Dialog Box	226
Figure 215	RFSM Backup Antenna Reminder	227
Figure 216	NMS Reports Menu	230
Figure 217	Sample Accounts Report	232
Figure 218	Sample Accounts Report with Report Window	232
Figure 219	Sample Firmware Report	233
Figure 220	Sample Service Level Report	234
Figure 221	Sample Network IP Address Report	236
Figure 222	Sample SNMPc Trend Report—Daily	238
Figure 223	Sample SNMPc Trend Report—Weekly	238

Figure 224	Channel Unit Properties—Network Interface Statistics	241
Figure 225	End User Modem Properties—Network Interface Statistics	242
Figure 226	Channel Unit Properties—IP Statistics	244
Figure 227	End User Modem Properties—IP Statistics	244
Figure 228	Channel Unit Properties—Diagnostics	246
Figure 229	Application Log File	247
Figure 230	Event Detail	248
Figure 231	Sample NMS Transaction Log File	249
Figure 232	RADIUS Server Properties Screen	250
Figure 233	Sample RADIUS Server Error Log File	251
Figure 234	File Not Found Dialog Box	251
Figure 235	Sample RADIUS Server User Log File	253
Figure 236	VPRStat.log File	254
Figure 237	SNMPc Main Screen	258
Figure 238	SNMPc Server Main Screen	259
Figure 239	RFSM Service Manager	270
Figure 240	RFSM Service Manager in Services Window	271
Figure 241	Service Control	271
Figure 242	RFSM Maintenance—RFSM Control Tab	272
Figure 243	RFSM Delete Confirmation Dialog Box	273
Figure 244	Firmware Download—Connect	276
Figure 245	Firmware Download—Success	277

— This page is intentionally left blank —

Tables

Table 1	NMS Workstation Default User Names and Passwords	22
Table 2	Icon Buttons	31
Table 3	CCU and EUM Icon Colors in NMS	32
Table 4	Subscriber Icons	32
Table 5	RFSM Symbols—Front Plane	111
Table 6	RFSM Symbols—Back Plane	111
Table 7	Radio Packet Error Rate Definitions	167
Table 8	CCU LED Colors	212
Table 9	Switch Control Icon Colors	213
Table 10	Network Interface Statistics	240
Table 11	IP Statistics	242
Table 12	Radio Packet Error Rate Definitions	245
Table 13	Fields in the NMS Application Log File	246
Table 14	Fields in the NMS Transaction Log File	249
Table 15	RADIUS Server User Log Fields	252
Table 16	VPRStat.log File Fields	253
Table 17	CCU and EUM Monitoring Reports	255
Table 18	Ethernet Switch Monitoring Reports	255
Table 19	Router Monitoring Reports	255
Table 20	UPS Monitoring Reports	256
Table 21	Recommended Temperature and Humidity for NAP and CAP	261
Table 22	NAP Device Defaults	291
Table 23	CAP Device Defaults	292
Table 24	Command-Line Syntax Conventions	299
Table 25	Command-Line Shortcuts and Getting Help	300
Table 26	EUM Command-Line Syntax	300
Table 27	CCU Command-Line Syntax	306
Table 28	RFSM Command Line Syntax	312
Table 29	CCU2000 WaveRider Enterprise MIBs	315
Table 30	CCU2000 RFC MIB-II Traps	317
Table 31	EUM2000 WaveRider Enterprise MIBs	318
Table 32	EUM2000 RFC MIB-II Traps	319
Table 33	CAP-NAP Back Haul Interface Specifications	321

Table 34	NAP-Internet Interface Specifications	321
Table 35	Power Supply Specifications	321
Table 36	Environmental Specifications	322
Table 37	NAP Physical Specifications	322
Table 38	iSurfRanger Environmental Specifications	322
Table 39	iSurfRanger Physical Specifications	322
Table 40	Other iSurfRanger Specifications	323
Table 41	CAP Radio Specifications	323
Table 42	Ethernet Back Haul Interface Specifications	323
Table 43	Power Supply Specifications	323
Table 44	Environmental Specifications	324
Table 45	CAP Physical Specifications	324
Table 46	RFSM Radio Specifications	324
Table 47	RFSM Ethernet Interface Specifications	325
Table 48	RFSM Physical Specifications	325
Table 49	CCU and EUM Radio Specifications	325
Table 50	Ethernet Interface Specifications	326
Table 51	Power Supply Specifications	326
Table 52	Environmental Specifications	326
Table 53	Acronyms and Abbreviations	327
Table 54	LMS Network Glossary	329

Preface

About this Manual

WaveRider recommends that you read the following sections before you install and operate the LMS2000:

- *Software License Agreement*, on page 2
- *Warranty*, on page 4
- [Warnings and Advisories](#), on page xix
- [Regulatory Notices](#), on page xvii

NOTE: The information contained in this manual is subject to change without notice.

Regulatory Notices

Industry Canada

The LMS2000 complies with IC RSS-210.

Operators must be familiar with IC RSS-210 and RSS-102.

The IC certification number for the LMS2000 EUM and CCU is 32251032130.

Federal Communications Commission

The transmitter of this device complies with Part 15.247 of the FCC Rules.

The LMS2000 complies with FCC Part 15 Regulations.

The FCC ID for the LMS2000 EUM and CCU is OOX-WRM1151.

WARNING!



Operators must be familiar with the requirements of the FCC Part 15 regulations prior to operating any link using this equipment. For installations outside the United States, contact local authorities for applicable regulations.

WARNING!



This system must be professionally installed.

Operational Conditions

Three conditions pertaining to the operation, in the USA, of spread-spectrum devices employing high-gain, directional antennas are:

1. The applications must be fixed, point-to-point; they cannot be roaming.
2. Point-to-multipoint systems, omni-directional applications, and multiple co-located transmitters transmitting the same information are prohibited (that is, you cannot sum the bandwidth of each unit).
3. The operator of a spread-spectrum system is responsible for ensuring that the system is operated in the manner outlined in [Operational Conditions](#), on page xviii and [Operational Requirements](#), on page xviii.

Operational Requirements

In accordance with the FCC Part 15 regulations:

1. The maximum peak power output of the intentional radiator shall not exceed one (1) watt for all spread-spectrum systems operating in the 2.4000-2.4835 GHz band.
2. Systems operating in the 2.4000-2.4835 GHz band that are used exclusively for fixed, point-to-point operations may employ transmitting antennas with directional gain greater than 6 dBi, provided the maximum peak output power of the intentional radiator is reduced by 1 dB for every 3 dB that the directional gain of the antenna exceeds 6 dBi.
3. Stations operating in the 2.4000-2.4835 GHz band that are used for fixed, point-to-multipoint operations may employ transmitting antennas with directional gain greater than 6 dBi, provided the peak output power from the intentional radiator is reduced by the amount in dB that the directional gain of the antenna exceeds 6 dBi.
4. Fixed, point-to-point operation, as used in Point 2, excludes the use of point-to-multipoint systems, omni-directional applications, and multiple co-located intentional radiators transmitting the same information. The operator of the spread-spectrum intentional radiator or, if the equipment is professionally installed, the installer is responsible for ensuring that the system is used exclusively for fixed, point-to-point operations.
5. The operator of a spread-spectrum system is responsible for ensuring that the system is operated in the manner outlined in [Operational Requirements](#), on page xviii and [Interference Environment](#), on page xix.
6. The EUM is considered to be a point-to-point transmitter. The CCU is considered to be a point-to-multipoint transmitter.

Interference Environment

Manufacturers and operators of spread-spectrum devices are reminded that the operation of these devices is subject to the conditions that:

- any received interference, including interference from industrial, scientific, and medical (ISM) operations, must be accepted; and
- these devices are not permitted to cause harmful interference to other radio services.

If the operation of these systems does cause harmful interference, the operator of the spread-spectrum system must correct the interference problem, even if such correction requires the Part 15 transmitter to cease operation. The FCC does not exempt spread-spectrum devices from this latter requirement regardless of the application. The FCC strongly recommends that utilities, cellular stations, public safety services, government agencies, and others that provide critical communication services exercise due caution to determine if there are any nearby radio services that can be affected by their communications.

Warnings and Advisories

General Advisory

Operator and maintenance personnel must be familiar with the related safety requirements before they attempt to install or operate the LMS2000 equipment.

It is the responsibility of the operator to ensure that the public is not exposed to excessive Radio Frequency (RF) levels. The applicable regulations can be obtained from local authorities.

WARNING!



This system must be professionally installed. Antennas and associated transmission cable must be installed by qualified personnel. WaveRider assumes no liability for failure to adhere to this recommendation or to recognized general safety precautions.

WARNING!



To comply with FCC RF exposure limits, the antenna for this transmitter must be fix-mounted on outdoor permanent structures to provide a separation distance of 2 meters or more from all persons to satisfy RF exposure requirements. The distance is measured from the front of the antenna and the human body. It is recommended that the antenna be installed in a location with minimal pathway disruption by nearby personnel.

WARNING!



Do not operate the LMS2000 CCU or EUM without connecting a 50-ohm termination to the antenna port. This termination can be a 50-ohm antenna or a 50-ohm resistive load capable of absorbing the full RF output power of the transceiver. Failure to terminate the antenna port properly may cause permanent damage to the device.

Customer Support

If you have any problems with the hardware or software, please contact WaveRider Communications Inc.

Telephone: +1 416-502-3161

Fax: +1 416-502-2968

Email: techsupport@waverider.com

URL: www.waverider.com

WaveRider offers a complete training program. Please contact your sales representative for training information.

1

Understanding the LMS2000

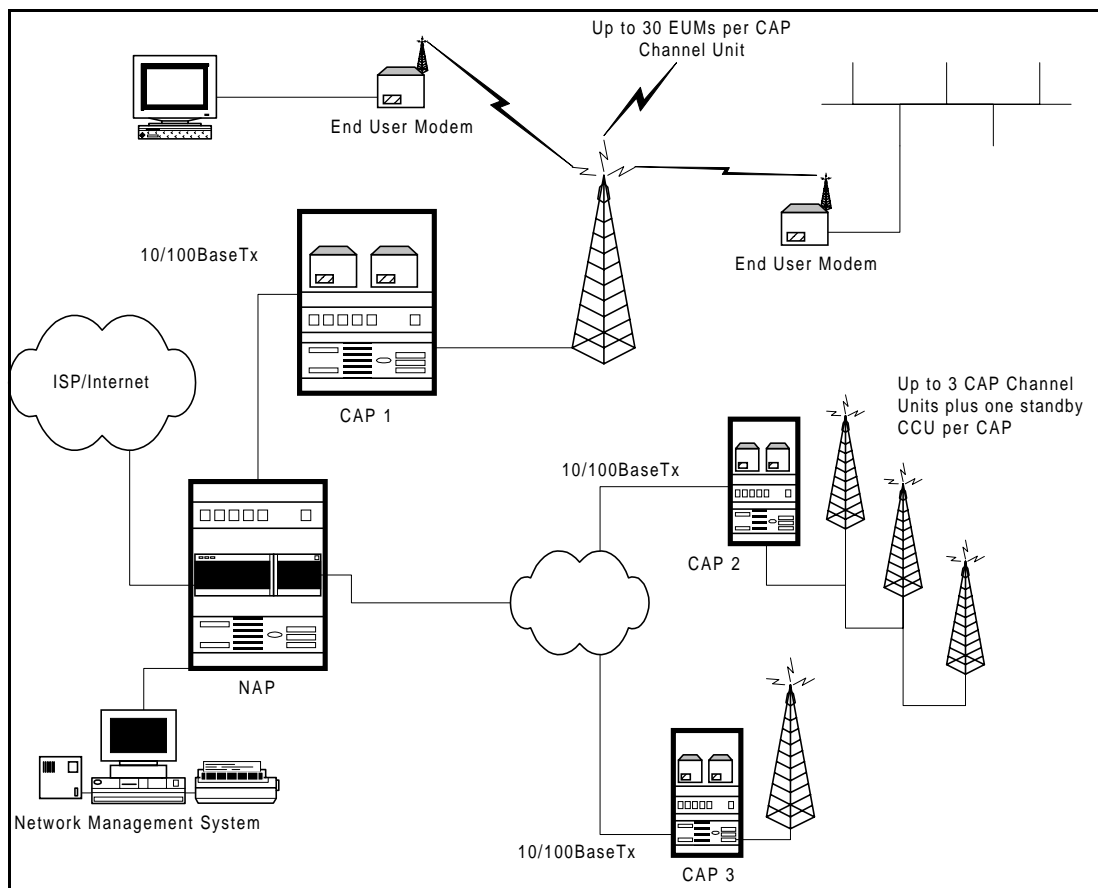
The LMS2000 is part of WaveRider Communication Inc.'s Last Mile Solution (LMS) product line. The LMS2000 provides the end user with wireless Internet connectivity in the 2.4 GHz unlicensed radio band and uses direct-sequence spread spectrum (DSSS) access technology with a raw data rate of up to 11 Mbps.

The LMS2000 is a Point-to-Multipoint (PMP) wireless system designed to fulfill the data traffic requirements of multiple business or small office/home office (SOHO) subscribers for high quality access to information services. The services can encompass simple Internet access to business-related multimedia capability that includes simultaneous voice telephony, video, audio, and file transfers.

The purpose of the LMS2000 system is to provide end users with wireless (RF) connection to the Internet. Applications supported by the network include e-mail, file transfer, web browsing, and limited streaming video and audio.

[Figure 1](#) shows the connections between the components of the LMS2000 system, the Internet, and the customer's PC or network.

Figure 1 LMS2000 System Components



The LMS2000 system consists of three main components:

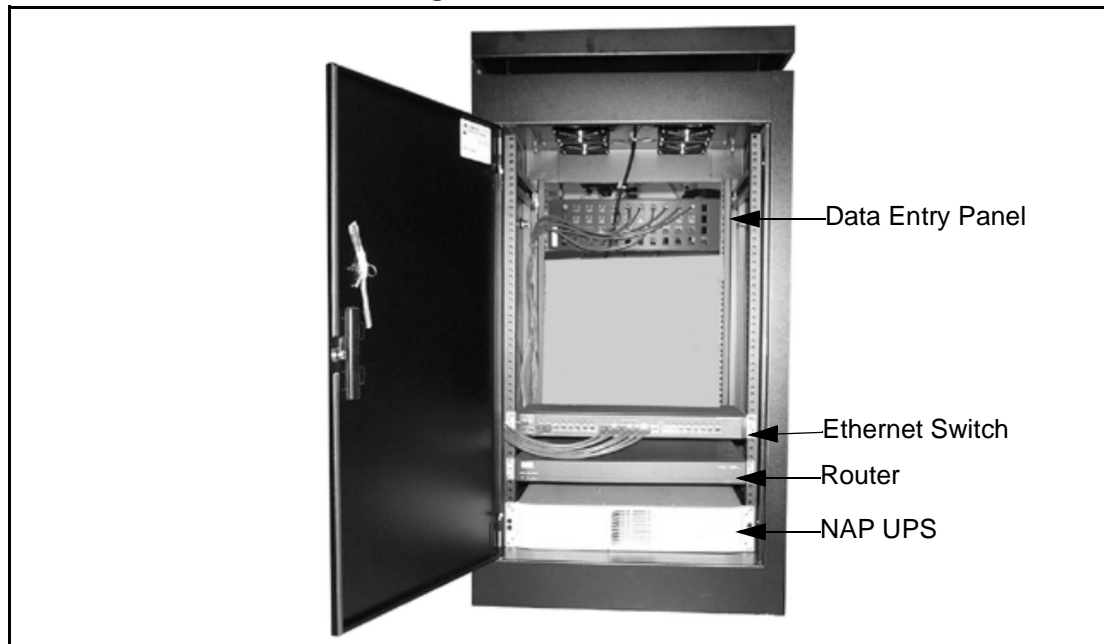
- Network Access Point (NAP)
- Communications Access Point (CAP)
- End User Modem (EUM)

Each of these components is introduced below.

1.1 NAP

The NAP provides the ISP with the necessary hardware and software to operate and maintain the LMS2000 system. It provides the following services for the LMS2000 system:

- Network security
- Subscriber management
- Data distribution and bandwidth management
- Operations alarms and maintenance
- Interface to the ISP network

Figure 2 NAP Cabinet

The NAP equipment includes the following components:

- Data-entry panel
- Ethernet switch
- Router
- Uninterruptible power supply (UPS)
- Advanced bandwidth manager (ABWM) (optional)

These components are enclosed within a free-standing equipment cabinet. The NMS workstation is located near the cabinet and is connected to it by an Ethernet network cable.

The NAP hardware consists of a half height indoor free-standing equipment cabinet containing a 19" wide equipment rack. This cabinet provides mounting space for the NAP equipment, as well as providing room for internal cable routing. In addition to the hardware located within the NAP cabinet, the NAP hardware includes the NMS hardware. The NAP equipment includes the following:

- High speed router that provides the interconnection between the CAPs and the ISP, and performs basic bandwidth management for up to 350 EUMs
- Ethernet switch, which connects with the router, NMS, UPS, and CAP back haul
- Uninterruptible power supply (UPS)
- Rack mounted network management server
- Advanced bandwidth manager (optional)
- NAP equipment cabinet and rack, complete with cooling fans

1.1.1 NAP Router

The NAP router acts as the directional gateway between the LMS2000 network and the Internet connection, and may provide a simple bandwidth management function. The router is configured through the Network Management Server.

1.1.2 Ethernet Switch

The Ethernet switch is the gateway that moves data between the CAP and the NAP, and provided connectivity for the UPS and the NMS server located in the NAP cabinet. The NAP Ethernet switch may connect to up to 15 CAPs.

1.1.3 NAP UPS

In the event of a power outage, the NAP UPS provides the NAP hardware and software with extended operating time so that the NAP may continue to operate during brief power outages. For longer power outages, the network operator can remotely command the devices connected to the UPS to shut down gracefully, before the UPS loses all of its battery power. Once power is restored, the router, switch, and Advanced Bandwidth Manager should reboot automatically.

1.1.4 NMS Server

The NMS server consists of a computer equipped with a backup tape drive. The NMS server contains the software for managing the LMS2000 system. The UPS provides power for the NMS workstation in case the main power is lost, allowing the operator to backup the current data. If the power outage is a long one, the operator can power down the NMS server without loss of data.

1.1.5 Advanced Bandwidth Manager (optional)

LMS2000 systems that have several CAPs and many EUMs may use an Advanced Bandwidth Manager. This reduces the workload on the router, so that it can provide greater utilization of the available bandwidth in the system. It also provides more flexibility in setting and controlling grades of services to each EUM.

1.2 Network Management System (NMS)

The NMS contains all the pre-loaded software to manage the LMS2000 system. The software that comes loaded on the NMS includes the following:

- Microsoft Windows NT 4.0 Server (with Service Pack 6a)
- WaveRider LMS Network Management System Server Software
- WaveRider LMS Network Management System Client Access Software
- Microsoft SQL Server 7.0 (with Service Pack 2.0)
- Vircom VOP RADIUS
- Castlerock SNMPc Server
- Veritas Backup Exec with Microsoft SQL Agent

1.2.1 Microsoft Windows NT

Microsoft Windows NT with Service Pack 6a provides the operating environment for the NMS software.

1.2.2 LMS Network Management System

The Network Management System software application is a three-tiered distributed network architecture application consisting of a set of software services residing on the NMS server and a thin-shell client application providing network management access to the NMS Server

1.2.3 LMS Network Management System Server Software

This WaveRider-developed software provides the control processing engine and data storage associated with the Subscriber Management functions of the LMS2000. These functions include customer account and subscriber definitions, equipment inventory, equipment configuration, network device monitoring, alarm generation, and bandwidth service level settings. The Network Management System software is a three-tiered communication process with all administrative functions residing on the NAP NMS server. Access to the NMS server software functions is handled by requests from the LMS Network Management System client software.

1.2.4 LMS Network Management System Client Software

This WaveRider-developed software provides the WISP network operator with a graphical user interface enabling customer entry, equipment configuration, and service level settings by establishing a remote connection with the NMS server. Customer and equipment reports are generated from the Network Management System directly from the NMS application software.

The NMS application supports the Graphical User Interface to fulfill the following operations processes:

- Set up or remove CCU or EUM access to the network
- Configure router parameters
- Configure bandwidth management
- Display alarm log and equipment database
- Monitor system operations and alarms
- Monitor system usage
- Configure CCUs
- Configure EUMs
- Setup or remove subscribers
- EUM authentication
- Generate reports
- Visual indication and alarm generation of the RFSM switchover during a CCU failure

1.2.5 Microsoft SQL Server

The Microsoft SQL Sever database contains all the supported customer, equipment, and supported billing information. Microsoft SQL Server resides on the NMS server and is accessed through the NMS client application. Reports generated through the Microsoft SQL Server software are accessed through the NMS Client Application.

SQL Server features and extension include support for the following:

- CCU and EUM communication links (a possible total of 15 CAPs and 15,000 EUMs)
- Frequency channel of operation for each EUM and CCU
- Single point of access to the EUM subscriber information
- Class of service
- Billing support

1.2.6 Vircom VOP RADIUS

The RADIUS server controls the logon and authentication access for the EUMs. Each EUM has a coded ID/password combination that RADIUS uses to recognize the modem. The RADIUS server software resides on the NMS server. The RADIUS software is programmed through an API directly from the NMS server software.

1.2.7 Castlerock SNMPc Server

The SNMPc software provides a visual map of the system and monitors it for operations and failures. This includes using SNMP traps to provide alarm indications within the system.

SNMPc alarms are generated for the following:

- Detected failures of CAP channel units
- Lost communications to any network device
- Power failure at the CAP or NAP
- Test alarms generated by the NMS real-time monitoring or system usage
- Lost communications to an EUM
- Alarms received from any device managed by SNMPc (e.g., routers, switches, UPS, etc.)

1.2.8 Veritas Backup Exec with Microsoft SQL Agent

Veritas Backup Exec software enables backup of the SQL Server while SQL is running.

1.2.9 Network/ISP Interface

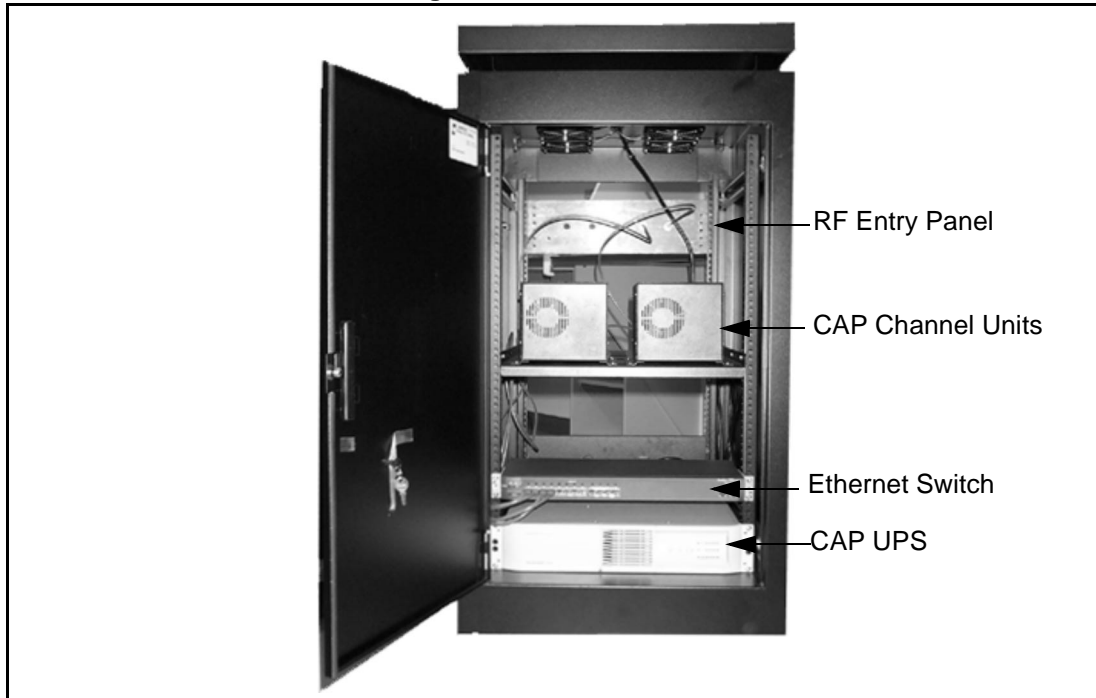
The interface from the LMS2000 NAP to the WISP's system is a 10/100BaseT connection. It is the responsibility of the WISP to provide any firewalls between the system, the Internet, and the LMS2000.

1.3 CAP

The CAP is the distributed collection point for communication in the LMS2000 system. The CAP is the central radio access point for EUMs to obtain wireless connectivity to the system, providing a path for Internet data to travel between the EUM and the NAP for routing to the Internet.

The LMS2000 CAP supports up to three channels operating simultaneously, with each unit operating on non-overlapping channels. The WISP operator selects frequency channels during system commissioning. Note that the normal CAP configuration is for 1, 2, or 3 active channels.

Figure 3 CAP Cabinet



CAP hardware consists of an indoor, free-standing, half-height cabinet containing a 19" wide equipment rack. The cabinet provides mounting space for the CAP equipment, including the following:

- One to three active CAP channel units (CCUs), complete with AC/DC power supplies
- Ethernet switch
- Uninterruptible power supply (UPS)
- Space for a back haul, such as an NCL1155
- Additional RF equipment, including bulkhead connector plate, cavity filters, lightning arrestors, cabling, and connectors
- Additional CCU and RF switch matrix (RFSM) for CAP redundancy (optional)

1.3.1 CCU

The CCU is the communications access point for up to 30 EUMs. It routes IP packets received from the EUM to its Ethernet port, for further transfer to the NAP and the Internet. The CCU processes received Ethernet packets or routes them to the appropriate EUM.

The CCU operates as a stand-alone unit that connects to the Ethernet switch in the CAP. You can remove a CCU from the CAP without having to power down the complete CAP.

1.3.2 CAP Ethernet Switch

The CAP Ethernet switch is the gateway that moves data between the CCUs and the back haul interface equipment. The Ethernet switch collects data from multiple CCUs, directs all the data into a single stream, and then sends the aggregated data to the external back haul. In the

other direction, the Ethernet switch collects data from the back haul and fans it out to multiple CCUs.

1.3.3 CAP UPS

The CAP UPS is a 10-minute backup power supply that ensures the continuous operation of the CCUs, Ethernet switch, and RF subsystem during brief power outages or sags. The UPS and CAP operate in an in-line configuration, which means power must first travel through the UPS before reaching the CAP. All input power from the AC source is regulated by the UPS to provide a seamless switchover from the mains power to the UPS battery backup when the primary power source fails. By switching over seamlessly, the UPS protects the system from unexpected power surges, spikes, or sags.

The UPS also notifies the NMS about the mains power loss, and the NMS records the event. If the mains power remains out for an extended period of time, the UPS notifies the operator that the remaining backup power will only last for a few more minutes. The operator has a minimum of ten minutes to close all active sessions and perform a graceful shutdown. When power returns, the CAP equipment automatically restarts and sends a confirmation to the NMS.

1.3.4 Radio Frequency Subsystem

The CAP Radio Frequency subsystem acts as the wireless access infrastructure for the network. This subsystem consists of the following main components:

- one to three CAP Channel Units
- a lightning arrestor for each antenna system
- RF cabling
- optional RFSM with backup CCU

1.3.5 Antenna Subsystem

The antenna system includes the antenna, antenna transmission line, and mounting hardware. Each active CCU requires a transmission line and antenna.

The installer of the antenna system must connect each antenna to a lightning arrestor, which is part of the RF subsystem. If a lightning strike occurs, the lightning arrestor diverts the bulk of the energy away from the RF transmission line and equipment to a bonded ground point.

WaveRider is your source for all antenna and lightning arrestor equipment. For more information, contact your WaveRider Sales Representative.

1.3.6 Back Haul (Optional)

You will require back haul equipment to link NAPs and CAPs that are not co-located. The equipment type depends on the configured size of the CAP, the available back haul

infrastructure and spectrum in the service area, and the distance between the CAP and the NAP. A large number of variables come into play when provisioning back haul equipment, so application engineering is necessary.

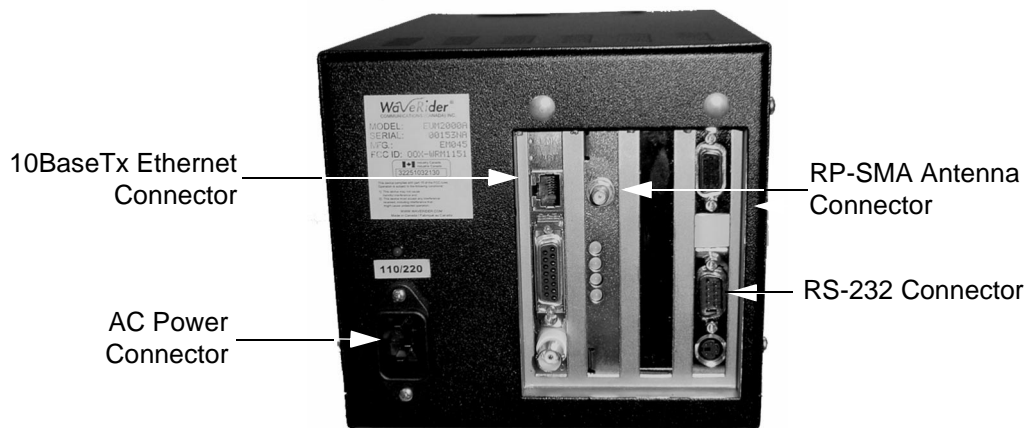
If the appropriate RF channels are available, WaveRider NCL wireless routers can provide a wireless back haul. Contact your WaveRider sales representative for more information.

1.4 EUM

The EUM is a self-contained wireless router that connects directly to a subscriber's network or computer. The EUM provides raw data of up to 11 Mbps between the EUM and a CCU using wireless IP routing to create a direct high-speed Internet access gateway to and from a local area network (LAN).

The EUM functions as a wireless router that transmits or receives data from a local network through an Ethernet connection, then transmits or receives the coded data through a radio link to the CCU radio on the CAP.

Figure 4 End User Modem (EUM)



The EUM equipment includes the following components:

- Wireless EUM unit with serial, Ethernet, and radio frequency (RF) connections
- Outdoor antenna
- Supporting equipment, including a power cord and cables

1.5 Data Flow

Data transfer in the LMS2000 network is controlled by routers, of which there are three:

- The NAP contains a router.
- The CAP contains CCUs, which act as routers, with the following exception. The CCU will route all traffic from its EUMs to the NAP router and traffic from the NAP router to the appropriate EUMs.
- The EUM is a router.

Each router has two (or more) connections on it.

- The NAP router connects to the WISP's Internet Point of Presence and the CCU in the CAP.
- The CCU connects to the NAP (Ethernet) and to multiple EUMs (radio).
- The EUM connects to the CCU (radio) and the subscriber's PC or network (Ethernet).

Figure 5 further illustrates the connections between the Internet, the LMS2000 equipment, and the subscriber's computer or LAN. It also identifies typical default IP addresses for each router.

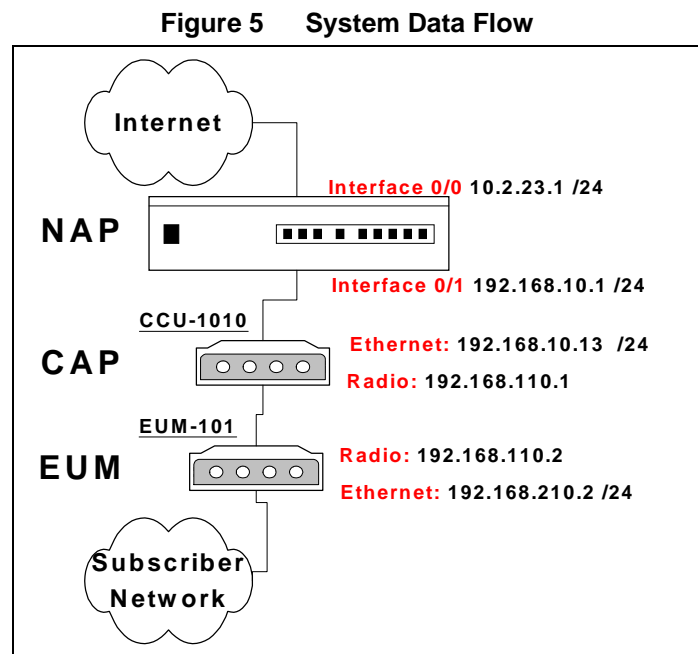


Figure 5 shows the default IP addresses for the NAP router, CCU, and EUM. The Internet interface IP address for the NAP router will change to reflect the subnetwork of the ISP. The EUM Ethernet IP will also change to reflect the subscriber's subnetwork address.

— This page is intentionally left blank —

2

Installing the NAP and the CAP

The first step in setting up your LMS2000 network is to link the NAP to the CAP. WaveRider recommends that you set up the NAP and CAP using the default settings initially. After the network is operational, you can optionally change the network addresses to suit your needs using the LMS Network Management System (NMS) software.

The basic procedure for setting up the LMS2000 system, including the CAP to NAP link, is as follows:

1. Set up the CAP.
2. Set up the back haul for the CAP to NAP link.
3. Set up the NAP.
4. Set up the NMS Workstation.
5. Configure SNMPc Server.
6. Initialize and configure the NMS software.
7. Verify the CAP to NAP link is operational.
8. Configure CCUs.
9. Configure and deploy EUMs in your network.

This chapter describes the procedures to set up the LMS2000 CAP and NAP components.

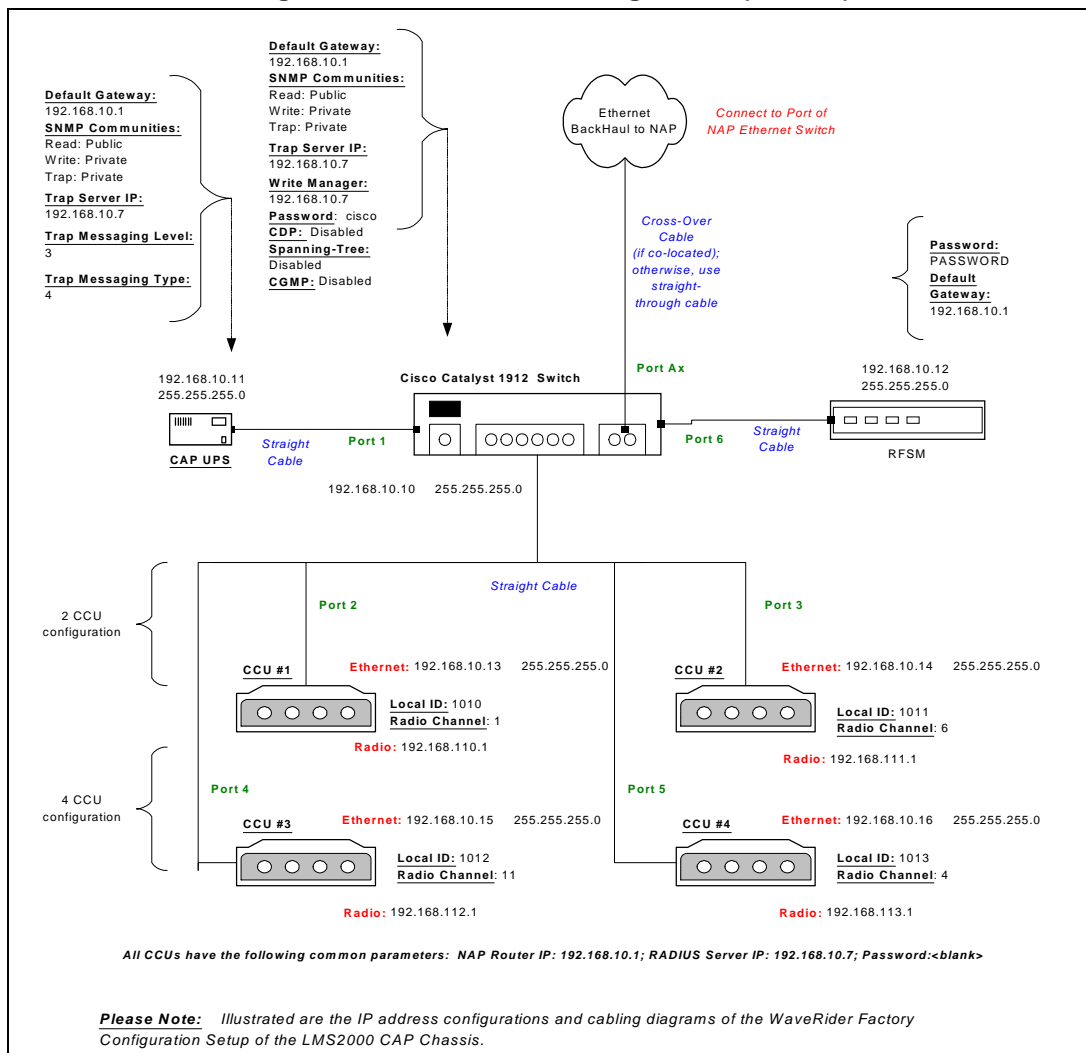
2.1 Setting up the CAP Using the Default Configuration

The CAP is the first component that you should set up. It consists of the following factory configured components:

- Cabinet with power bar and fans
- Exide 5119 Uninterruptible Power Supply (UPS)
- Cisco Catalyst 1912 Switch
- CAP Channel Units (CCUs) complete with cables, bulkhead lightning arrestor, power cords, antennas, and cables
- Radio frequency switching matrix (RFSM) (optional)

The CAP configuration can include up to 4 CCUs, depending on your requirements. Refer to [Figure 6](#) for the default configuration for the CAP components. It shows both a 2- and 4-CCU configuration.

Figure 6 CAP Default Configuration (CAP #1)



To set up the CAP with the default configuration, use the steps described below:

1. Ensure that your CAP site has been prepared to support the CAP requirements, including CCU antenna structures, power, grounding, and radio frequency (RF) lightning protection.

WARNING!



This system must be professionally installed. Antennas and associated transmission cable must be installed by qualified personnel. WaveRider assumes no liability for failure to adhere to this recommendation or to recognized general safety precautions.

2. Reconnect the Exide 5119 UPS battery. Refer to [section 2.1.1](#), Reconnecting the UPS Battery After Shipping.
3. Plug the CAP UPS power cable into a 110 or 220 V AC power source using the provided cable.
4. Set up your back haul equipment and connect to the CAP. Refer to [Setting up your Back Haul Equipment](#), on page 17 for more information.

After you have set up the CAP, the next step is to set up the NAP. Refer to [Setting up the NAP Using the Default Configuration](#), on page 18.

2.1.1 Reconnecting the UPS Battery After Shipping

The Exide 5119 UPS is shipped with the battery bank disconnected and the rear breaker on the rear power distribution bar in the “OFF” position. Reconnect the battery and place the power switch to the “ON” position. Complete the following instructions before powering up the unit.

WARNING!

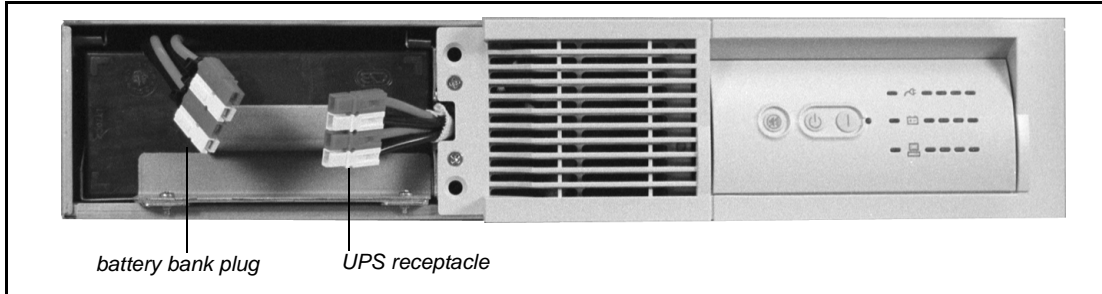


The UPS is capable of generating sufficient voltage to cause bodily harm. Use extreme caution when working with high voltage equipment.

To Reconnect the UPS Battery

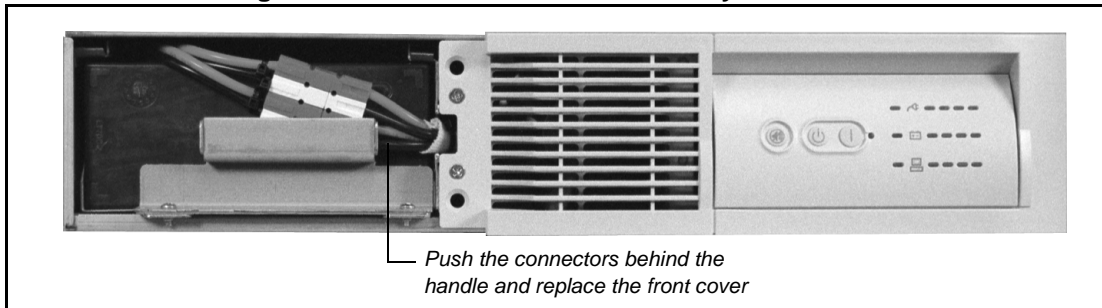
1. Open or remove the front and rear doors on the cabinet.
2. Pull the front cover off the UPS to expose the battery connection.

Figure 7 Exide 5119 UPS with Battery Disconnected



3. To reconnect the battery, plug the battery bank plug into the UPS receptacle.

Figure 8 Exide 5119 UPS with Battery Connected



4. Align the front cover in position and snap it back in place.
 5. Place the breaker on the rear power distribution bar of the UPS in the "ON" position.
- The UPS battery is fully charged before shipping.
6. Plug the UPS into the power source to maintain the charge in the battery.

2.1.2 Setting up your Back Haul Equipment

The type of back haul equipment for your site depends on the following conditions:

- Expected traffic load
- Available back haul infrastructure
- Distance between the CAP and the NAP

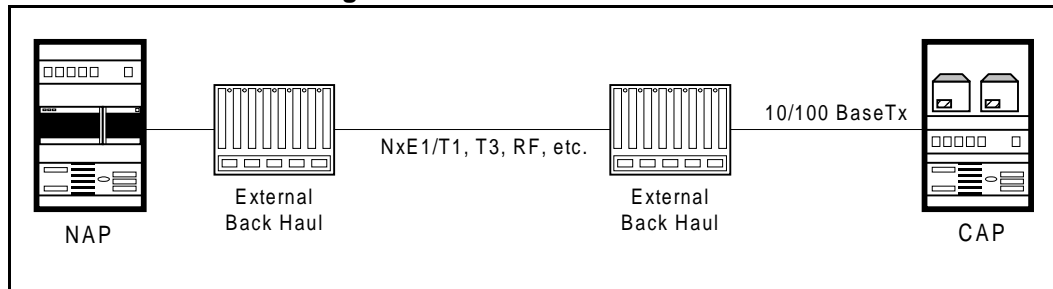
The back haul can be either a wired connection to the NAP or a connection through an external unit that provides a transparent connection at the Ethernet Layer 2 transport.



TIP: The WaveRider NCL line of wireless routers provides a cost-effective solution to establish a wireless back haul solution.

Figure 9 shows a simple back haul configuration for the CAP to NAP back haul.

Figure 9 CAP to NAP Back Haul



NOTE: Because the back haul can be configured in many different ways, provisioning a back haul interface for the LMS2000 requires application engineering. For information on WaveRider back haul equipment, contact your **WaveRider Sales Representative**.

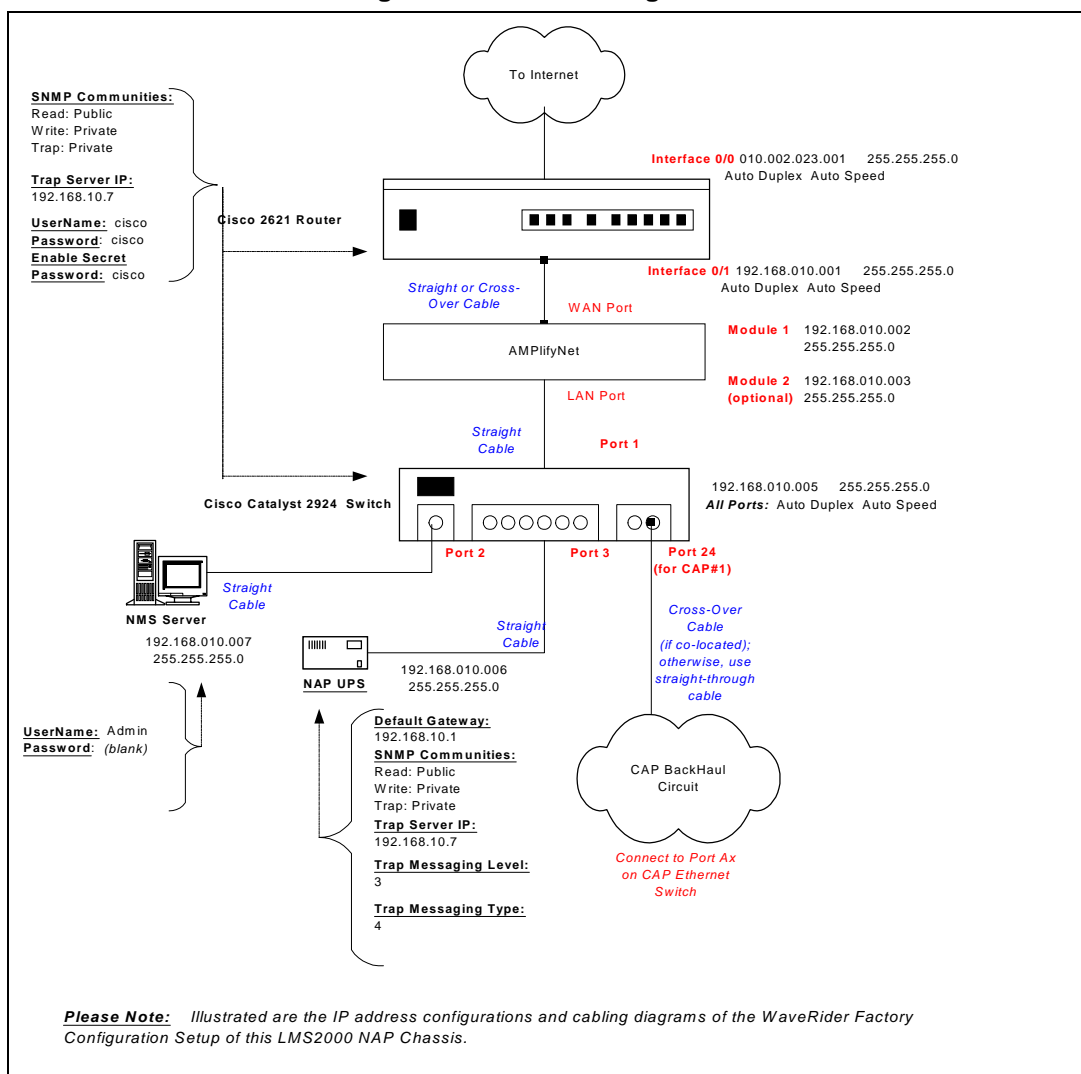
2.2 Setting up the NAP Using the Default Configuration

After you have set up the CAP, the next step is to set up the NAP. The NAP consists of the following factory configured components:

- Cabinet complete with power bar and fans
- Cisco Catalyst 2924 Switch
- Cisco 2621 Router
- Exide 5119 Uninterruptible Power Supply (UPS)
- NMS Workstation complete with monitor, keyboard, mouse, internal backup tape unit, printer, and cables
- APC Back-UPS PRO 650 (NMS Workstation UPS)

The NAP components all use the default configuration shown in [Figure 10](#).

Figure 10 NAP Configuration



Use the following procedure to set up a NAP:

1. Ensure that your NAP site has been prepared to support the NAP requirements, including power and grounding.
2. Reconnect the Exide 5119 UPS battery. Refer to [Reconnecting the UPS Battery After Shipping](#), on page 15.
3. Plug the NAP UPS power cable into a 110 or 220 V AC power source using the provided cable.
4. Connect the back haul equipment to a free RJ-45 Ethernet port on the front panel of the NAP switch. Back haul equipment must provide transparent Ethernet Layer 2 transport between the NAP and CAP. Refer to [Setting up your Back Haul Equipment](#), on page 17 for more information.
5. Power up the NAP.

2.3 Testing the NAP/CAP Connection

After the NAP and CAP are installed and connected, test the network connections between both the NAP and CAP.

1. At the NMS Workstation, click **Start > Programs > Command Prompt** to open a Command Prompt window.
2. At the DOS prompt, type `<ping ip_address_of_CAP_switch>`.

If the connection is established, you will see the following message:

```
Reply from 192.168.10.10: bytes = 32    time<10ms    TTL=64
Reply from 192.168.10.10: bytes = 32    time<10ms    TTL=64
Reply from 192.168.10.10: bytes = 32    time<10ms    TTL=64
Reply from 192.168.10.10: bytes = 32    time<10ms    TTL=64
```

If the connection is down, you will see the following message:

```
Request timed out.
```

If there is a configuration problem with the network routes defined in the router, you will see the following message:

```
Reply from 192.168.10.10: Destination host unreachable
```

3. Repeat this test for each piece of equipment in the network, from the NAP router to each CCU in the CAP. If you receive a bad connection message, note where the connection failed. You should be able to determine the origin of the problem in the network. Correct it by checking the configuration of the attached equipment or software.

— This page is intentionally left blank —

3

Getting Started with the NMS

Once you have installed the CAP and the NAP, you will use the Network Management System (NMS) to configure the NAP, CAP, CCUs, EUMs, and other components of your LMS2000 system. This chapter helps you set up the NMS workstation and helps familiarize you with its interface.

3.1 Starting the NMS Workstation

The NMS Workstation includes the following components installed and configured for use.

Hardware

- PC, including mirrored hard drives and 4mm tape drive
- APC UPS

Software

- Microsoft Windows NT 4.0 (with Service Pack 6a)
- WaveRider LMS Network Management System (NMS software)
- Microsoft SQL Server
- Vircom VOP RADIUS
- Castle Rock SNMPc Server—Enterprise Edition
- APC PowerChute PLUS
- VERITAS Backup Exec

When you log on to the NMS workstation for the first time, it will ask you for the following default user names and passwords.

Table 1 NMS Workstation Default User Names and Passwords

Windows NT Login User Name	Administrator
Windows NT Login Password	<blank>
SNMPc Server User Name	Administrator
SNMPc Server Password	<blank>

To Log on to the NMS Workstation for the First Time

1. Plug the UPS cable for the NMS Workstation into a 110- or 220-volt AC power source.
2. Connect the NMS Workstation to the NAP switch using the provided straight-through Ethernet cable.
3. Power on the NMS Workstation.

The Windows NT login process begins.

4. At the **Begin Login** screen, press **Ctrl+Alt+Delete**.
5. In the **Login Information** dialog box, type the Windows NT User Name and Password, and press **Enter**.

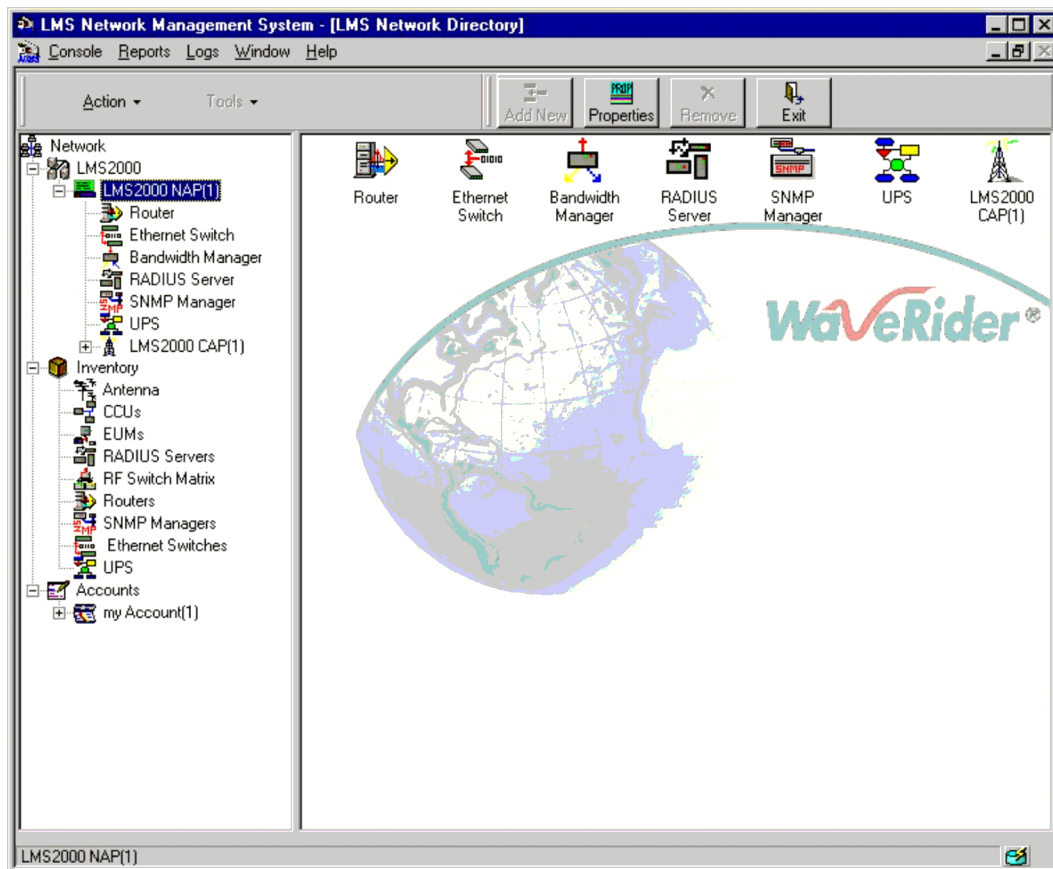
Windows NT is pre-configured with no password.

NOTE: For security, WaveRider recommends that you change the password for Windows NT as soon as possible. For instructions on changing the password, refer to the [Microsoft Windows NT Server](#) documentation provided with this system.

The LMS2000 **Network Management System** (NMS) launches automatically, and the LMS2000 tree structure is collapsed when the NMS software first opens.

6. Click the plus-sign next to a component to expand the contents and view the LMS2000 tree structure.

[Figure 11](#) shows the LMS2000 tree structure.

Figure 11 LMS Network Management System Main Window

3.2 Understanding Records Management

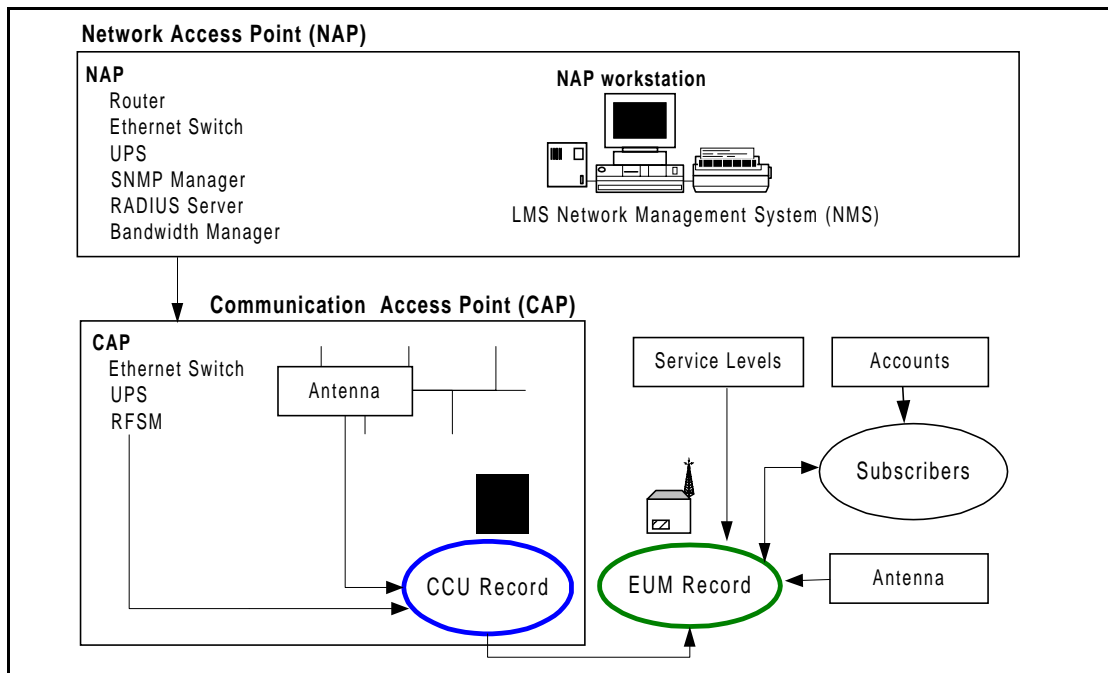
The tree structure in the NMS software is divided into three primary branches: LMS2000, Inventory, and Accounts.

- The **LMS2000** branch contains records for active network components.
- The **Inventory** branch contains records for all network components, both active and inactive.
- The **Accounts** branch contains records for accounts and their subscribers.

When you click a tree element, the records associated with that element on the next level appear in the right panel. They may also appear beneath the element in the tree structure itself. [Figure 11](#) shows the expanded branches in the tree.

[Figure 12](#) shows how the records connect within the NMS program.

Figure 12 NMS Record Connections

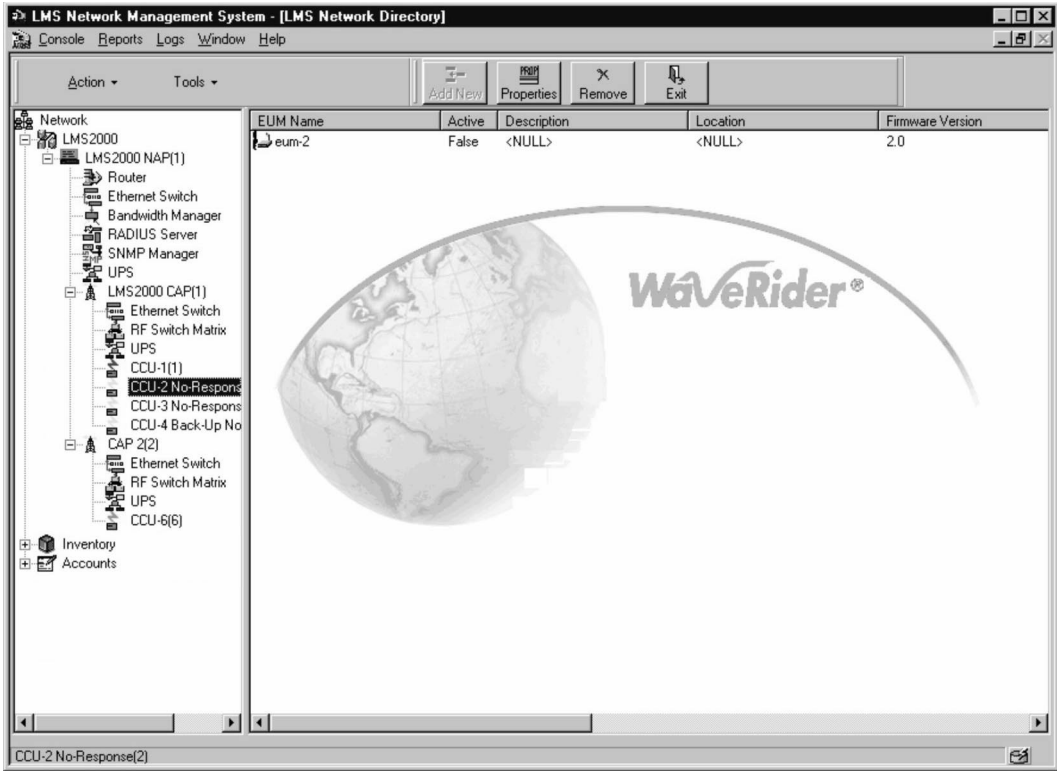


3.2.1 LMS2000 Branch

You can right-click any of the items in the tree structure to open a shortcut menu of commands specifically related to that item. For example, you can use the shortcut menu to add new device records or open the Properties dialog box for the record.

NOTE: Once they have been added, the devices appear both in the tree structure and in the right panel, when the parent record is selected.

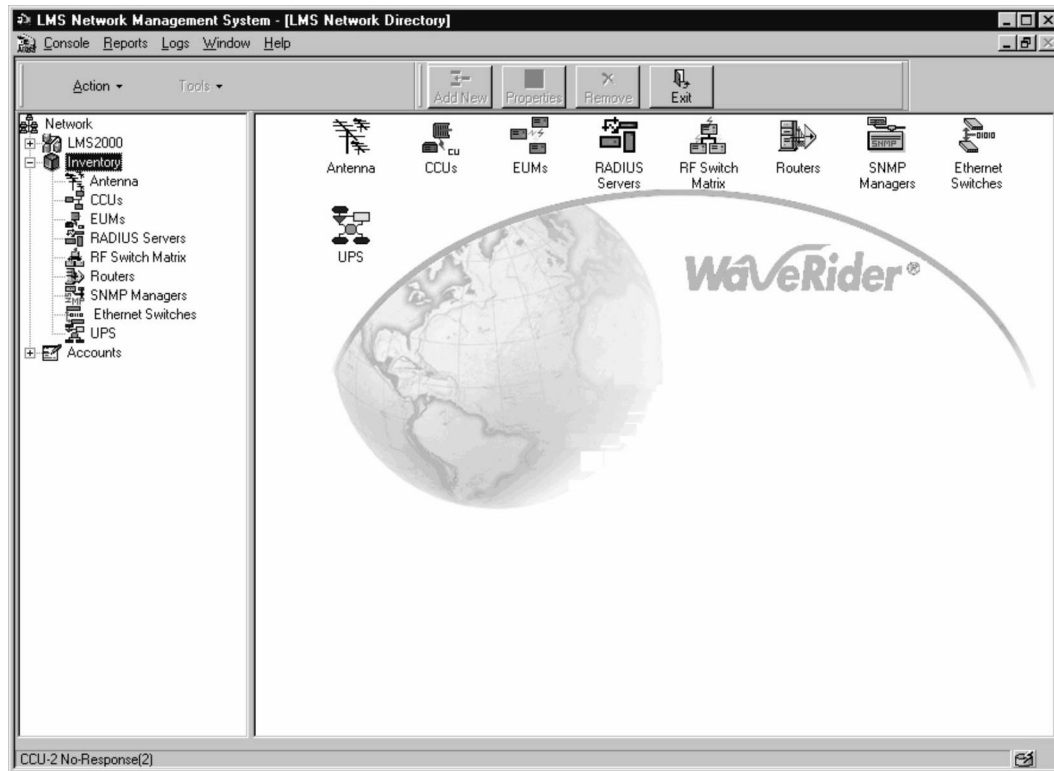
Figure 13 LMS2000 Branch



3.2.2 Inventory Branch

The Inventory branch includes records for all the equipment in the network, including those assigned to the network. You can pre-configure equipment and keep it in inventory, so you can deploy it more quickly later. Records that have not been assigned to the network have blue icons and record names.

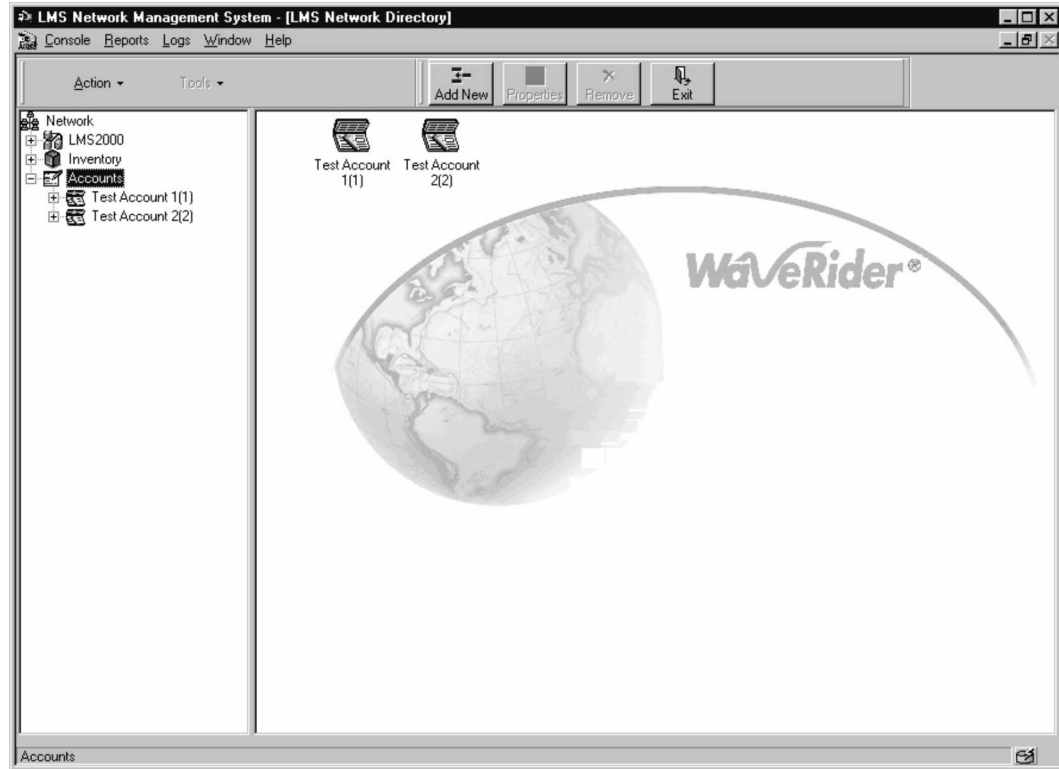
Figure 14 Inventory Branch



3.2.3 Accounts Branch

The Accounts branch contains records for accounts and subscribers. Use the records in this branch to represent accounts and subscribers and to associate subscribers with EUMs.

Figure 15 Accounts Branch



3.2.4 Shortcut Menus

When you right-click an icon in the menu tree or main window, a shortcut menu opens and provides you with a series of actions related to that device or type of device. The shortcut menu enables you to complete the following actions:

- Add a new device
- Access the Properties screen for the device
- Link the record to other records
- Connect to the device through Telnet, Serial Interface, or Download new firmware (CCU/EUM only)
- Enable or disable the record (This option applies to accounts, subscribers, CCU/EUM radios.)
- Remove or delete the device
 - **Remove** appears if the record has links to other records.
 - **Delete** appears if the record has no associations.

The following graphics show the shortcut menus available from each of the three branches.

Figure 16 NAP Shortcut Menu

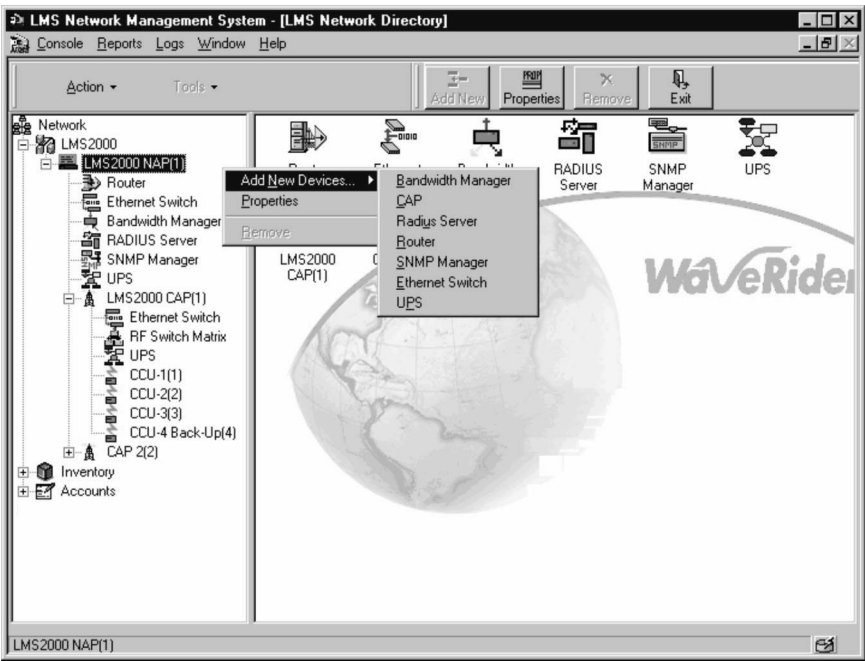


Figure 17 Inventory Shortcut Menu

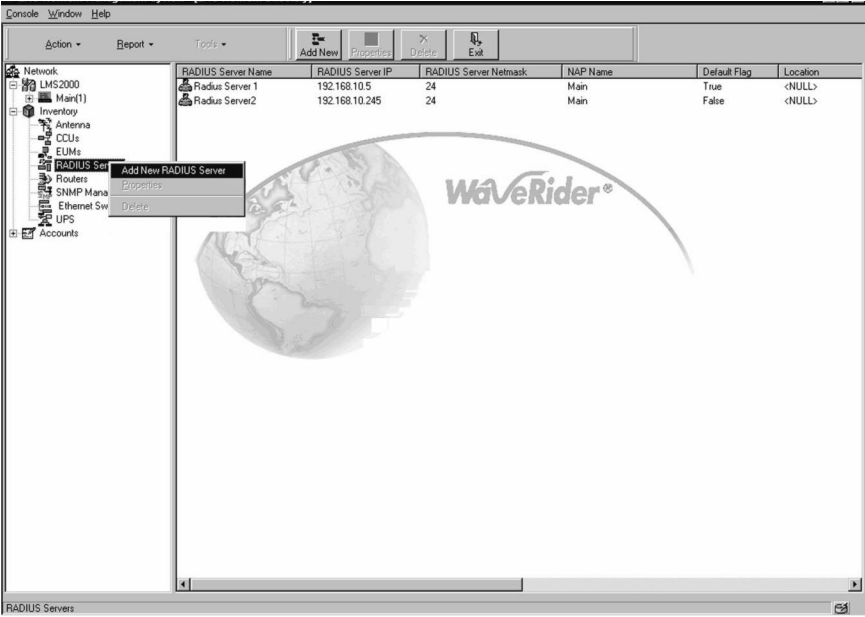
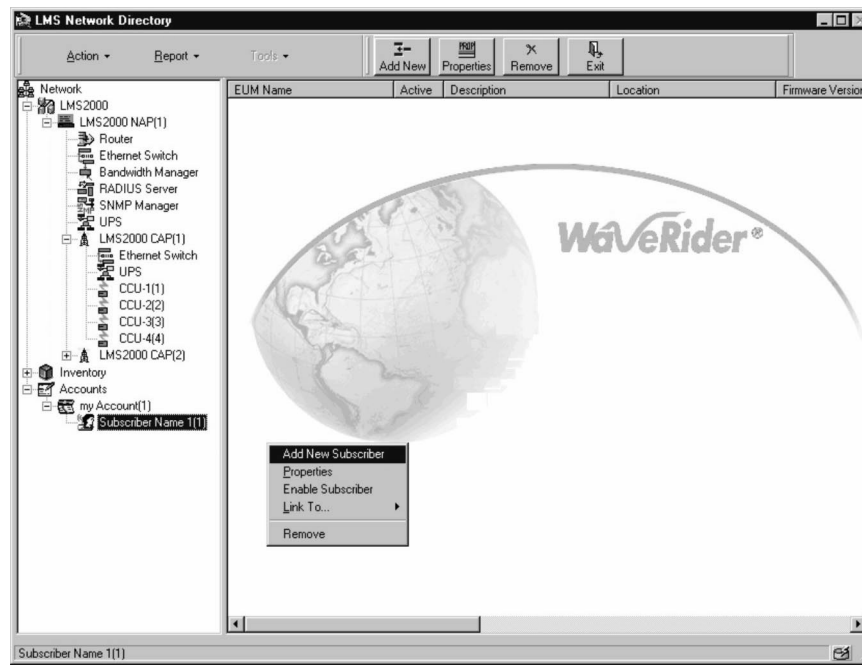











Figure 18 Accounts Shortcut Menu



3.2.5 Buttons

Many of the buttons in the NMS software include words and are self-explanatory. The following list describes the icon buttons and their functions.

Table 2 Icon Buttons

Icon	Screens where it appears	Function
	<ul style="list-style-type: none"> Channel Unit Properties EUM Properties 	If you have a saved configuration file, you can import that configuration into the current record using this button.
	<ul style="list-style-type: none"> NAP Router Configuration NAP Ethernet Switch Properties CAP Ethernet Switch Properties Channel Unit Properties EUM Properties 	It saves the configuration of the current record to a file.
	<ul style="list-style-type: none"> NAP Router Configuration NAP Ethernet Switch Properties CAP Ethernet Switch Properties Channel Unit Properties EUM Properties 	It establishes a remote connection to the device.
	<ul style="list-style-type: none"> NAP Router Configuration NAP Ethernet Switch Properties CAP Ethernet Switch Properties Channel Unit Properties EUM Properties 	It is only available while you are connected to a device. Clicking this button closes the connection.
	<ul style="list-style-type: none"> NAP Router Configuration NAP Ethernet Switch Properties CAP Ethernet Switch Properties Channel Unit Properties EUM Properties 	It uploads the configuration of the current record to the device.
	<ul style="list-style-type: none"> Channel Unit Properties EUM Properties 	Use this button to set the time interval for recording device statistics.
	<ul style="list-style-type: none"> Channel Unit Properties EUM Properties 	Closes the record.
	<ul style="list-style-type: none"> LMS2000 Main Screen 	Starts and stops the Database Synchronization Manager.
	<ul style="list-style-type: none"> Windows System Tray 	Icon for the RFSM Service, which controls the RFSM polling engine.

3.2.6 Icon Colors

In the main NMS screen, icons and icon names change color to reflect the status of the device.

The following devices show a black icon if they are assigned to a NAP or a CAP, and they show a blue icon if they are not assigned:

- RADIUS Server
- RFSM
- Router
- SNMP Manager
- Ethernet Switch




[Table 3](#) summarizes the icon colors for CCUs and EUMs and the states they reflect. CCUs that are connected to a radio frequency switching matrix may exhibit additional colors. For further information about CCU icon colors, please refer to [Table 9, on page 213](#).

Table 3 CCU and EUM Icon Colors in NMS

Device	Icon Color	Text Color	State
CCU	Green	Black	Assigned to CAP
CCU	Red	Blue	Not assigned to CAP
EUM	Green	Black	Assigned to CCU
EUM	Red	Blue	Not assigned to CCU

In the main NMS screen, when you select an account in the Accounts tree, icons for each of the subscribers associated with that account appear in the left pane. There are three possible icons associated with a subscriber record. [Table 4](#) identifies and describes these icons.

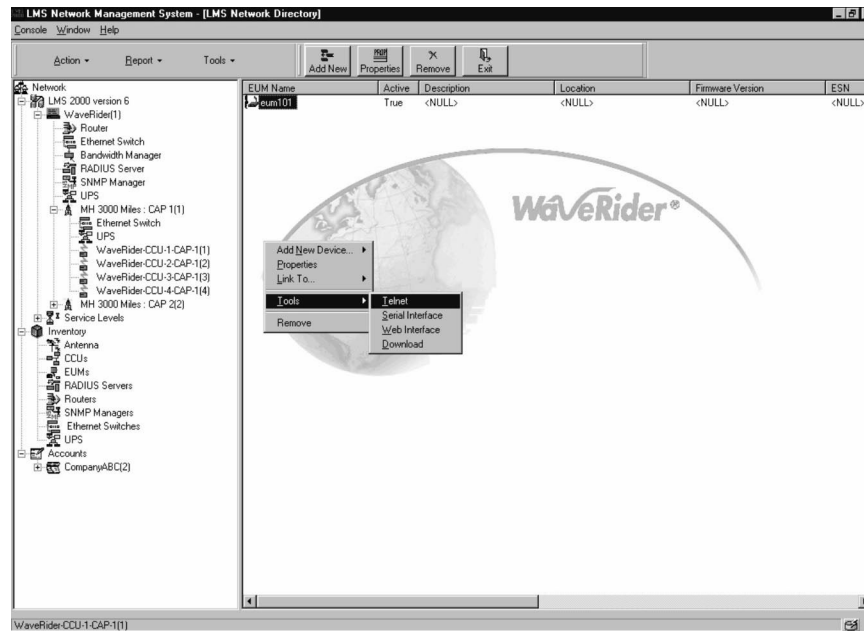
Table 4 Subscriber Icons

Icon	Associated with EUM?	Radio Enabled?
 ABC Supply(1)	No	No
 ABC Supply(1)	Yes	Yes
 ABC Supply(1)	Yes	No

3.3 Opening Records for Individual Devices

When you click an item in the menu tree on the left, the records assigned to that item appear in the right frame of the main screen. Use the shortcut menus from these right-frame items to open the **Properties** dialog box for individual records.

Figure 19 Shortcut Menu from Right Frame



3.3.1 Understanding the Properties Screen

When you select **Properties** from the shortcut menu for any component, the **Properties** screen for that component opens. Use this screen to configure elements.

Figure 20 Typical Properties Screen

End User Modem Properties: EUM1

Statistics Diagnostics Tools Subscriber

General Ethernet/Radio IP Routing SNMP/RADIUS

CCU
CCU-1

General Information:

EUM ID: [Grayed out]

* EUM Name: EUM1

Location: Calgary

Description: EUM 1 of CCU 1

System Information:

Unit:

Model: EUM20006

Software Version: EUM20006

Serial #: EUM2000_V0_00072NA

Radio:

MAC Address: Unknown

Antenna:

Antenna ID: 2

Antenna Type: Antenna for EUM1

Date Entered: 19-Jun-00 Date Updated: 19-Jun-00

Close Restore Apply

Status: Settings:

The following points describe the Properties screen:

- Red asterisk indicates a mandatory field
- Grayed-out entries are populated from the database and cannot be changed OR they are optional features not available on the current system.
- **Date Entered** appears automatically on the creation of a new record
- **Date Updated** appears when an existing record has been changed
- **Description/Comment** fields can be used to enter special information about the device or to record problems encountered during operation.
- **Close** button exits the screen without saving. If you did not click **Apply** first, a system message prompts you to save.
- **Restore** button reverts to the original record information, if you have not yet clicked the **Apply** button.
- **Apply** button saves any changes, and the screen remains open.

4

Setting Up SNMPc Server

SNMP enables a network management station to monitor, control, and remotely configure network devices called agents.

SNMP allows you to look at SNMP variables using READ communities and to set SNMP variables using WRITE communities. Communities are optional on LMS2000 devices, and they can support a maximum of five communities. EUMs, CCUs, routers, Ethernet switches, UPSs, and SNMP Managers are factory configured with two SNMP communities:

- READ community called “public”
- WRITE community called “private”

SNMP also provides a mechanism called trap, which notifies a network management station of significant events. A significant event can be an interface going down or coming up, a unit performing a cold or warm start, or an authentication failure. LMS2000 devices are factory configured with one SNMP trap community called “private”. Refer to RFC 1157 for details.

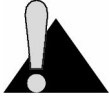
Associated with SNMP are Management Information Bases (MIBs). These specify a collection of management information available from the agent. This information can be controlled and monitored from a network management station.

The NMS implements SNMPv2c and includes a number of standard SNMP MIBs:

- RFC1157 (MIB-II)
- RFC1493 (bridging)

It also includes two custom MIBs, called Enterprise MIBs, for the EUM and CCU. For definitions of the LMS2000 MIBs, please refer to [D, *SNMP MIB Definitions*](#), on page 315.

The LMS2000 system comes with all required MIBs pre-compiled. Upgrades to WaveRider MIBs can be downloaded from the Technical Support page at www.waverider.com. The following procedure describes how to configure standard SNMP security for read/write access to the SNMP agent and to specify a server IP address to which trap messages are sent.



CAUTION: Do not close SNMPc while the system is running. Closing SNMPc stops SNMP monitoring of the system. When you are finished with the screen, minimize it until you need it again.

4.1 Changing the SNMPc Server Password

The SNMPc Server application comes pre-configured with no password. WaveRider recommends that you change the password as soon as possible for network security.

To Change the Password

1. Open SNMPc Server.
2. Select **User Profiles** from the **Config** menu.
3. In the **Setup Users** dialog box, select **Administrator** and click **Modify**.
4. In the **Edit Users Properties** dialog box, type your new password in the **Password** and **Re-enter Password** text boxes.
5. Click **OK** to exit the dialog box.
6. Click **Done** to return to the **SNMPc Server** main window.

NOTE: Refer to the SNMPc Server online help for more information about changing passwords.

4.2 Creating a Network Map

SNMPc Server creates a map of your LMS2000 network. First, you must supply SNMPc Server with the IP addresses of all the routing devices in the network. SNMPc will then use that information to automatically discover all the devices connected to those routers. As SNMPc discovers the devices, it creates a network map to graphically represent the devices and the connections between them.

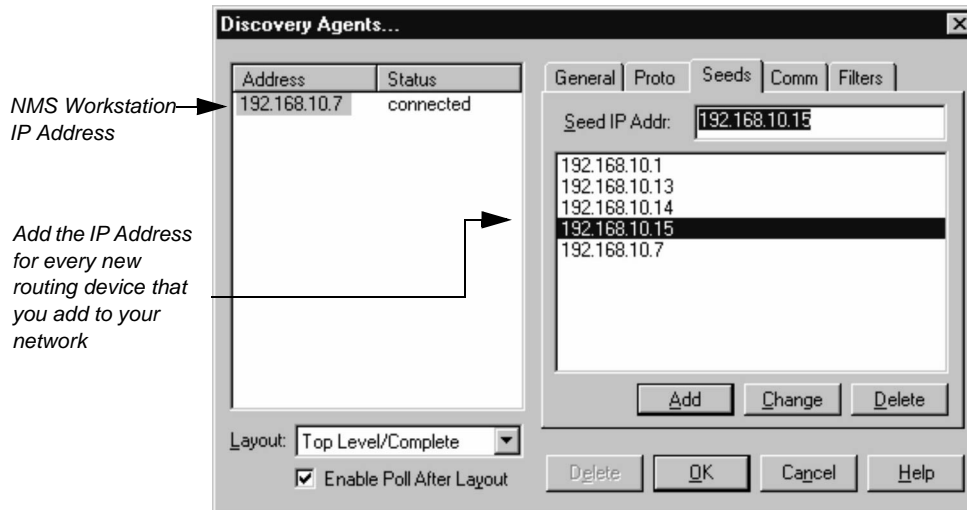


CAUTION: It can take several hours for SNMPc to automatically discover all devices in the network.

To Add Router IP Addresses

1. In the **SNMPc Server** main window, select **Discovery Agents** from the **Config** menu.
2. In the **Discovery Agents** window, click the **Seeds** tab.

Figure 21 Seeds Tab—Discovery Agents Window



3. In the **Seed IP Addr** box, verify the IP Address for the NAP Router and the CCUs that are pre-configured for your network.
4. Type the IP address for any new routing device that you add to your network in the **Seed IP Addr** box.
5. Click **Add**.

The IP address for the routing device is added to the **Seed IP Addr** list.

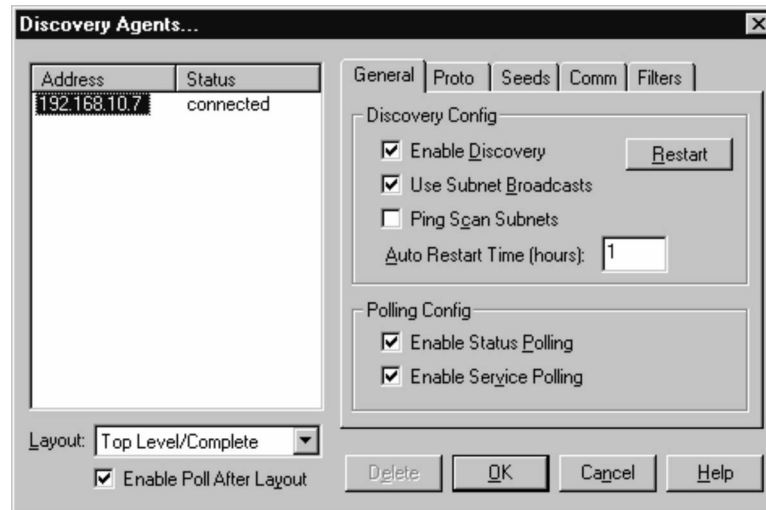
6. Repeat [step 4](#) and [step 5](#) to add any back haul routing devices and any additional CCUs in your network to the SNMPc Server list of routers.
7. Click **OK** to return to the **SNMPc Server** main window.

NOTE: After you have added a device, you must perform a discovery to create a network map, so SNMPc Server is aware of the device.

To Create a Network Map

1. In the **SNMPc Server** main window, select **Discovery Agents** from the **Config** menu.
2. In the **Discovery Agents** window, click the **General** tab.

Figure 22 General Tab—Discovery Agents Window



3. Select **Enable Discovery** in the **Discovery Config** group to set automatic discovery in SNMPc Server.
4. Click **Restart** to begin the discovery process.
5. When the process is complete, click **OK** to return to the **SNMPc Server** main window.

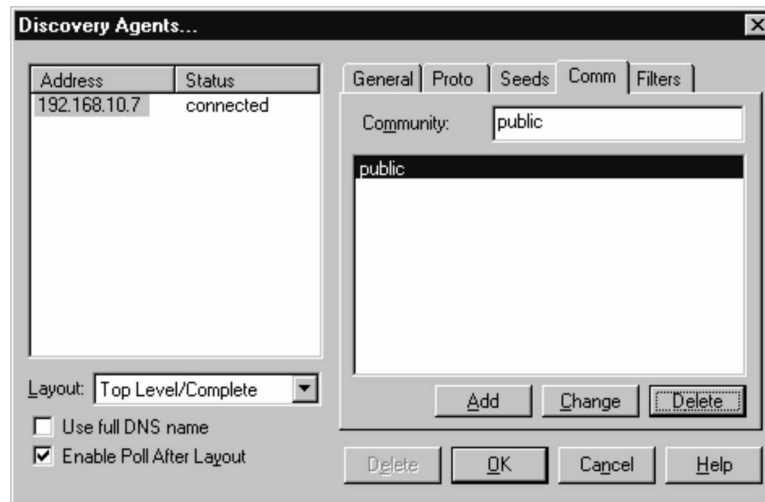
4.3 Adding SNMP Communities

To Add an SNMP Community

1. In the **SNMPc Server** main window, click the **Config** menu and then select **Discovery Agents**.
2. In the **Discovery Agents . . .** window, click the **Comm** tab.

One default **public** community appears in the **Community** list box.

Figure 23 Comm Tab—Discovery Agents Window



3. Modify the community properties to match the communities that you set for your network devices.
4. To add a new community, type a name in the **Community** box and click **Add**.
5. Repeat step 4 for each community that you want to add.

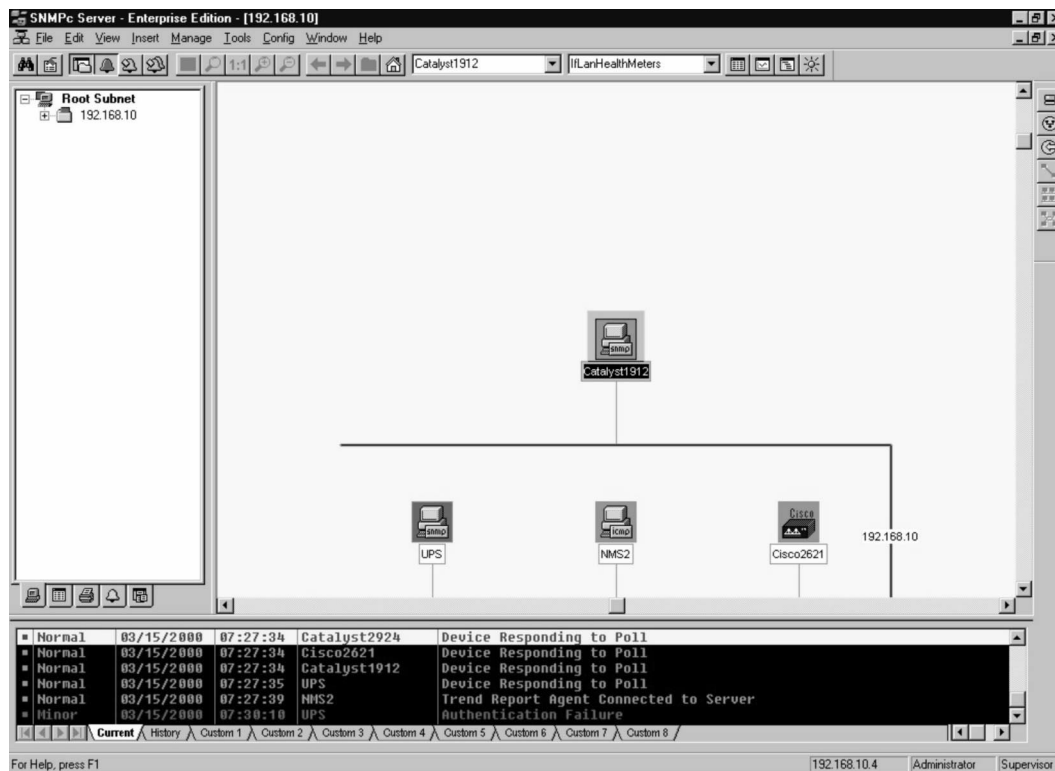
4.4 Adding a Trend Report

SNMPc frequently polls the network devices and automatically discovers new devices. Once the new device appears on the network map, you can add a **Trend Report**.

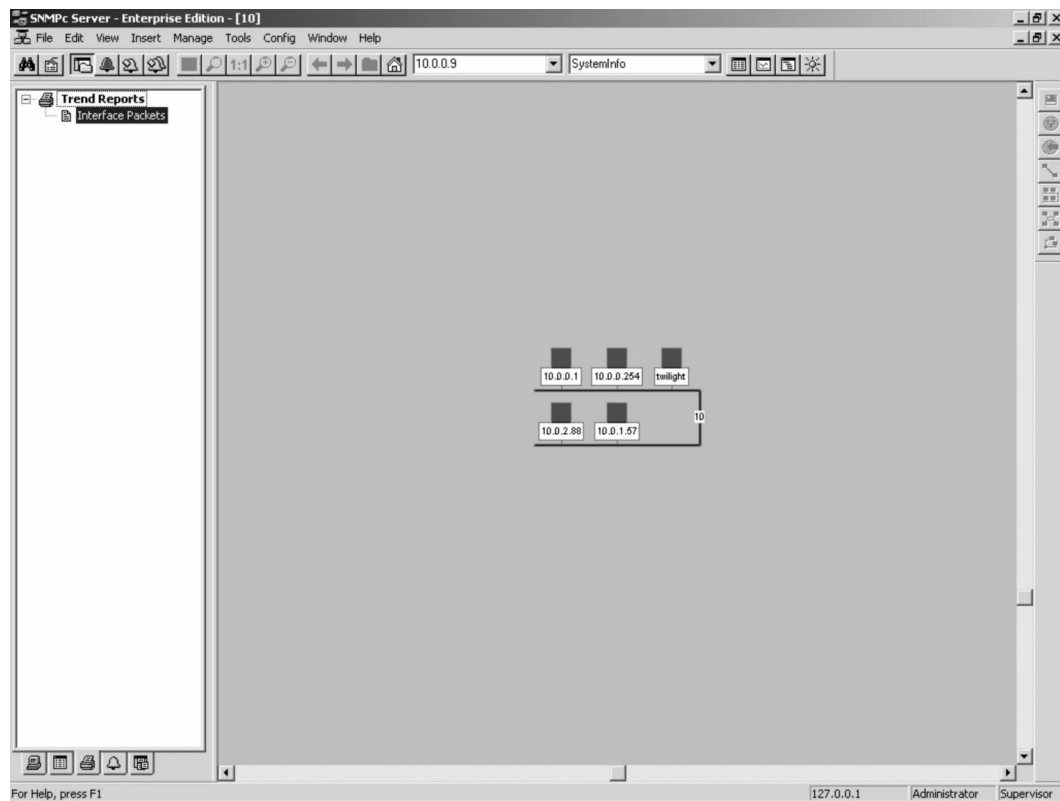
To Add a Trend Report

1. Maximize SNMPc Server.

Figure 24 Example of the SNMPc Server Main Screen



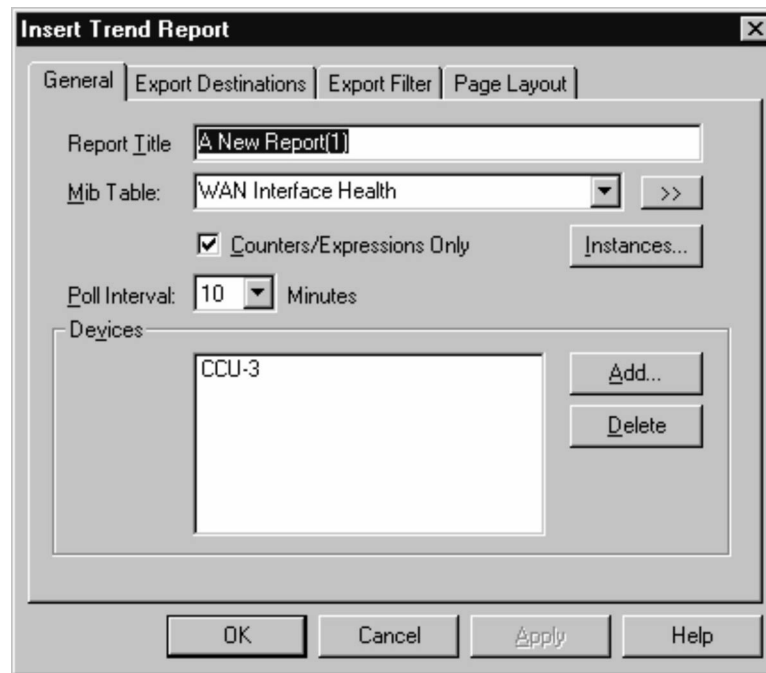
2. On the main SNMPc screen, click the icon for the device.

Figure 25 SNMPc Server Network Map

3. Click the **Insert** menu and select **Trend Report**.

The **Insert Trend Report** screen appears with the **General** tab displayed.

Figure 26 Insert Trend Report—General Tab

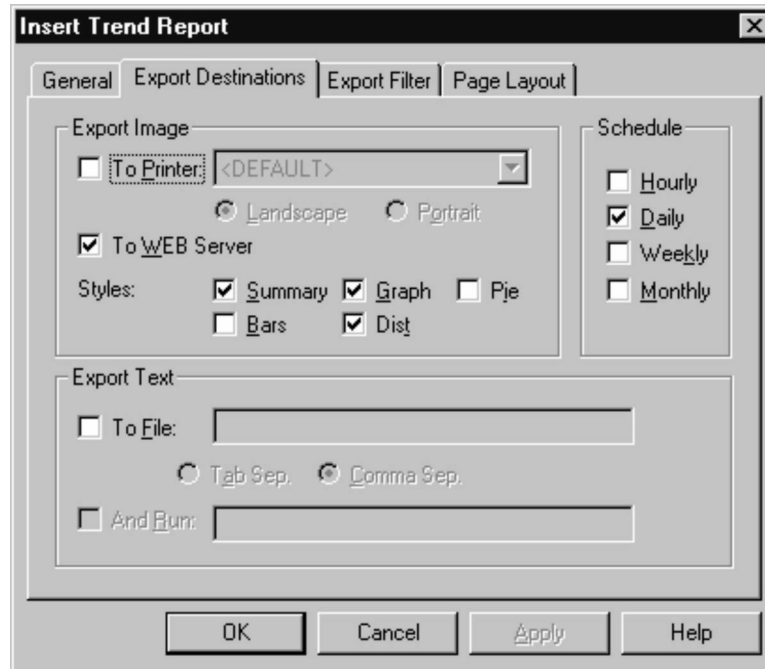


4. Click **>>** to browse for the MIB file.
5. Find the path, and highlight the folder name.
`C:/Program Files/SNMPc 5.0/mibfiles/`
6. Click **OK**.
7. From the **MIB Table** drop-down list, choose the entry that you want to graph and then name the report in the **Report Title** to reflect the MIB Table choice.

To Set Export Destinations

1. In SNMPc Server, click the **Insert** menu and select **Trend Report**.
2. Click the **Export Destinations** tab.

Figure 27 Trend Report Properties—Export Destinations Tab



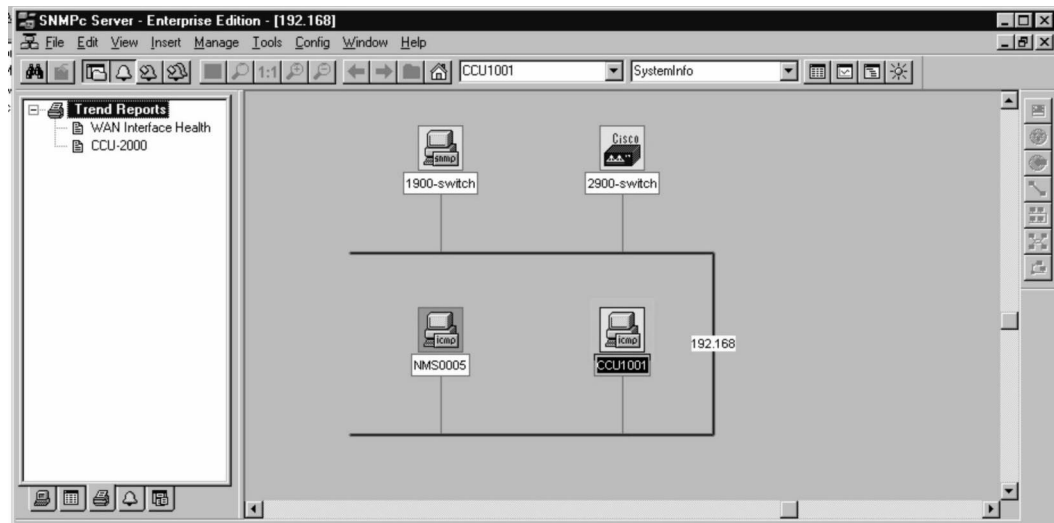
WARNING!



Hourly and Daily monitoring consumes system space and slows the system. Use only for detailed troubleshooting for specific devices.

3. Configure the screen with the settings you require.
4. Click **OK**.

Figure 28 SNMPc Trend Report Menu



5. To see which reports have been defined, click the **Trend Reports icon** on the task bar at the bottom of the left frame.

Note that the **Trend Report** list appears at the top of the left frame.

5

Configuring the NAP and CAP

The NAP and CAP are the first components you will configure in your network. Many of the settings are default and are best left as default. When you configure the NAP and CAP, you will need to verify the default properties and define others as necessary.

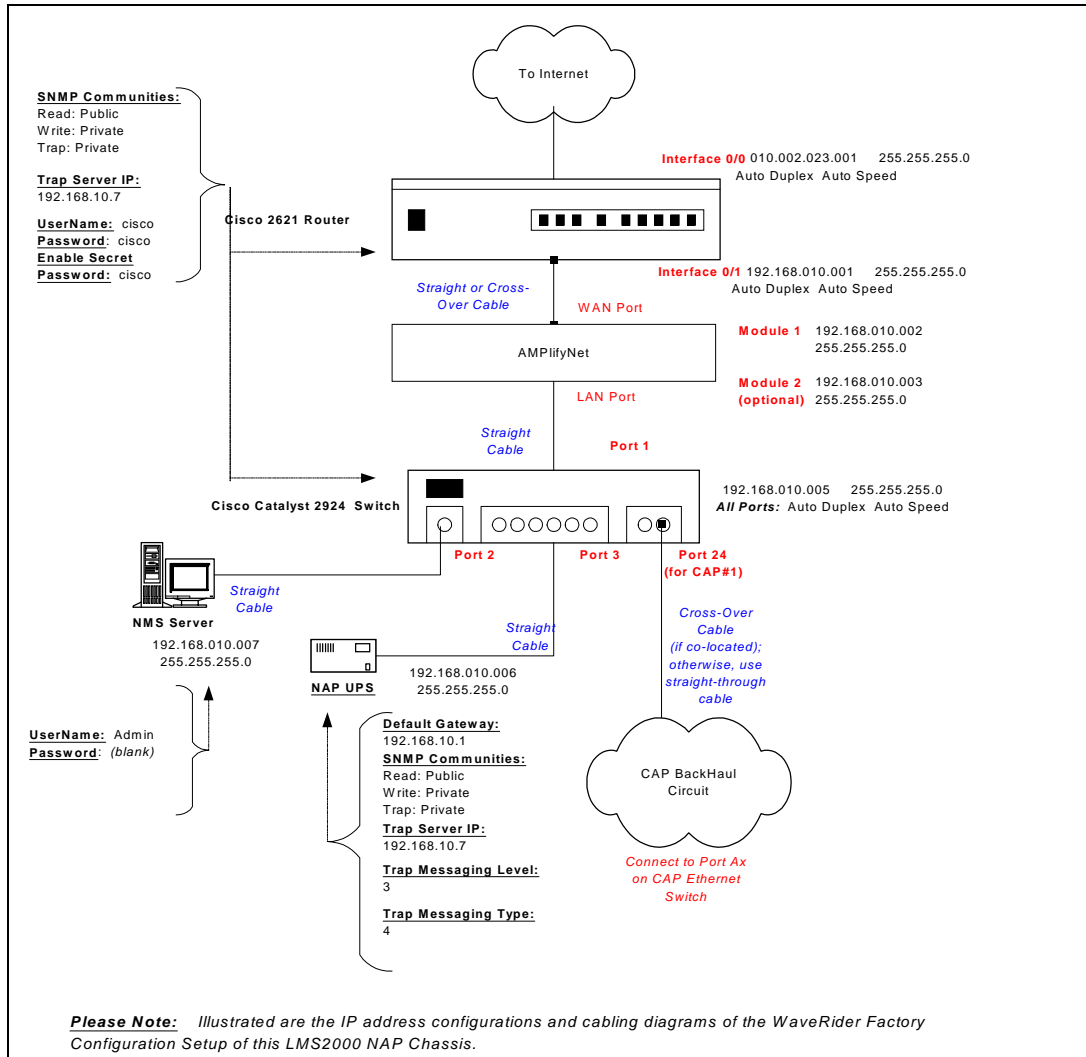
5.1 Configuring the NAP

The NAP is pre-configured using factory defaults. For a listing of default configuration settings, please refer to [Device Configuration Defaults](#), on page 291. You should open the database records for the NAP components in the NMS software to verify that they are configured correctly. Also, assign a unique name to the NAP.

5.1.1 Understanding NAP IP Address Defaults

Each new LMS system comes with default IP addresses for all NAP and CAP components, which are listed in [Device Configuration Defaults](#), on page 291. If you are unable to connect to a new device through the NMS, check the IP addresses on the related records.

Figure 29 LMS2000 NAP Default IP Addresses



5.1.2 Naming the NAP

To Name the NAP

1. In the NMS software, under the LMS2000 tree, right-click the NAP name.
A shortcut menu opens.
2. Select **Properties**.

Figure 30 NAP Properties

The screenshot shows a window titled "NAP Properties: WaveRider(1)". Inside, there are several fields and buttons. At the top, "Network: LMS2000" and "NAP ID: 1" are displayed. Below these, there is a field for "NAP Name" containing "WaveRider". Underneath is a "Description" field with the text "Description of NAP". Below that is a "Comments" field. At the bottom of the window, it shows "Date Entered: 25-Apr-00" and "Date Updated: 26-May-00". Three buttons are at the very bottom: "Close", "Restore", and "Apply".

3. Ensure the **NAP Name** field has been completed.

5.1.3 Verifying the NAP Configuration

For each NAP device, verify the default configuration according to the list in [Device Configuration Defaults](#), on page 291. The screen captures on the following pages also show the defaults.

To Verify NAP Device Defaults

1. In the NMS software, under the LMS2000 tree, right-click the device and select **Properties**.
2. Verify the properties.

Figure 31 NAP Router Configuration

Router Configuration

NAP
LMS2000 NAP

General | **IP/Network Access** | SNMP | IP Routing

Internet (WAN) Port:
 Interface Port: Interface F0/0
 IP Address: 10 . 2 . 23 . 1
 NetMask: 24 255.255.255.0

LMS (LAN) Port:
 * Interface Port: Interface F0/1
 * IP Address: 192 . 168 . 10 . 1
 * NetMask: 24 255.255.255.0

Network Information:
 Host Name:

Login Information:
 UserName: cisco
 Password:
 Enable Password:
☐ Enable HTTP Access

Date Entered: 25-Jul-00 Date Updated:

Close Restore Apply

Status: Settings:

Figure 32 NAP Ethernet Switch Properties

Ethernet Switch Properties

Web Interface | SwitchForm | Exit

NAP
LMS2000 NAP

General

General Information:
 Ethernet Switch ID: 1
 * IP Address: 192 . 168 . 10 . 5

Trap Servers:
 Trap Server IP: 192 . 168 . 10 . 7
 NetMask: 24 255.255.255.0

SNMP Communities:
 Read Community String: public
 Write Community String: private
 Trap Community String: private

Date Entered: 21-Nov-00 Date Updated:

Close Restore Apply

Status: Settings:

Figure 33 Router-Based Bandwidth Manager Properties

Bandwidth Manager Properties: BWM1 (3)

NAP
LMS2000 NAP

General
Bandwidth Manager ID: 3
* Name: BWM1
Location:
Description:
Date Entered: 18-Dec-00 Date Updated: 18-Dec-00

Router
* Router Name: 2600

Service Sets

Set Name	CIR
Copper	128
Fire	512
Bronze	1024
Silver	1600
Gold	3200
Diamond	6400

Add Delete Edit

Close Restore Apply

Figure 34 Advanced Bandwidth Manager Properties

Bandwidth Manager Properties

NAP
LMS2000 NAP

General **Controller** Bandwidth Sets Schedules Policies System/Security

Redundancy Mode
☒ None ☐ Serial ☐ Parallel

IP Addressing
* Primary: 192.168.10.2
* Secondary: N/A

Parallel Redundancy
* Default Router IP:
Keep Alive Port: ☐ A ☐ B ☒ Both
* Keep Alive Interval (sec): 0
* Number of Packets before Switch-Over: 0

Physical Connection Capacity
* Pipe In Size (Kbps): 100000
* Pipe Out Size (Kbps): 100000

CIR Thresholds
* Activity Reset Timer(sec): 10
* Max Burst Rate In (Kbps): 15000
* Max Burst Rate Out (Kbps): 15000
* Reserved Margin In (Kbps): 15000
* Reserved Margin Out (Kbps): 15000

Alert Thresholds
* Soft: 1 * Hard: 5

Update Close

Figure 35 NAP UPS Properties

UPS Properties: NAP UPS

General

Network Addressing

* UPS IP Address: 192 . 168 . 10 . 6

* Netmask: 24 255.255.255.0

* Default Gateway: 192 . 168 . 10 . 1

SNMP

System Name: GET SET

System Contact: GET SET

System Location: GET SET

Attached Devices: SNMP Device GET SET

Read Community String: public

Write Community String: private

Trap Server

Trap Server IP: 192 . 168 . 10 . 7

Trap Community String: private

Trapping Type

☐ Standard MIB

☐ Exclude MIB

☐ Standard MIB and Messages

☒ Exclude MIB and Messages SET

Trapping Level

☐ No Traps

☐ Critical Traps and Messages

☒ All Traps and Messages SET

Close Restore Apply

Figure 36 RADIUS Server Properties

RADIUS Server Properties: Radius Server 1 (1)

NAP

LMS2000 NAP

General

RADIUS Server ID: 1 ☒ Set For Default Configuration?

* RADIUS Server Name: Radius Server 1

Location:

Description:

Comments:

IP

* RADIUS Server IP Address: 192 . 168 . 10 . 7

* RADIUS Server Netmask: 24 255.255.255.0

Date Entered: 25-Jul-00 Date Updated:

Close Restore Apply

Figure 37 SNMP Manager Properties

SNMP Manager Properties: SNMP Server 1 (1)

NAP
LMS2000 NAP

General
SNMP Manager ID: 1 ☒ Set For Default Configuration?
* SNMP Manager Name: SNMP Server 1
Comments:

IP
* Trap Server IP Address: 192 . 168 . 10 . 7
* Trap Server Netmask: 24 255.255.255.0

Default
* Trap Community Name: private
* Read Community Name: public
* Write Community Name: private

Date Entered: 25-Jul-00 Date Updated:

Close Restore Apply

5.1.4 Configuring the NAP Ethernet Switch

The NAP Ethernet switch uses a web interface for configuration. The following procedure explains how to access the configuration interface. For detailed instructions on configuring the switch, please refer to the following URL:

- **Cisco IOS Desktop Switching Software Configuration Guide:** http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/29_35sa6/scg/

NOTE: The default user name and password for the NAP Ethernet switch are both **cisco**, all lowercase.



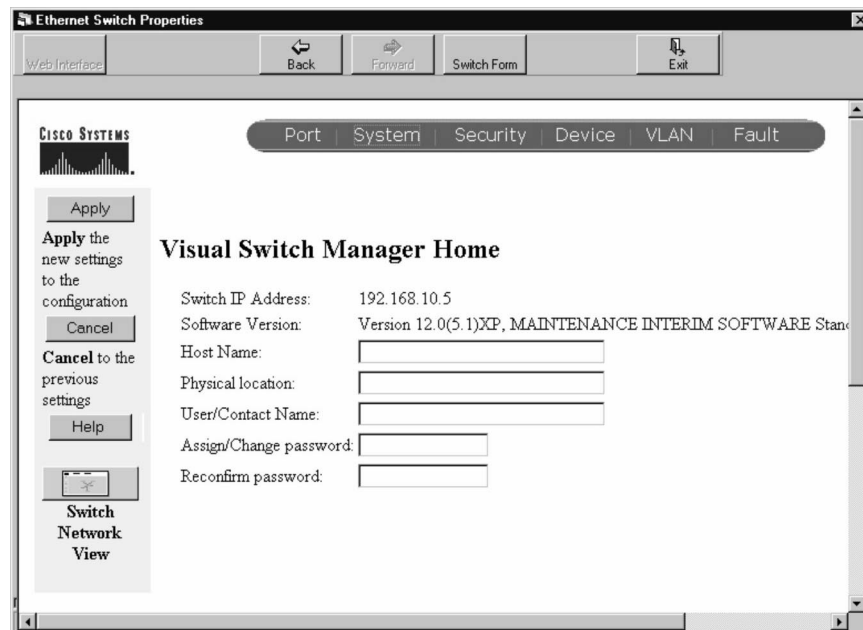
CAUTION: Changing Ethernet Switch variables on the Cisco web interface requires that you also change these values manually on the NMS screens. Changing the values on the web interface only, without changing them on the NMS screens, will prevent you from connecting to the switch.

To Access the NAP Switch Configuration Interface

1. In the NMS software, open the screen for the **NAP Ethernet Switch**.

Figure 38 NAP Ethernet Switch Properties

2. Click the **Web Interface** button.
3. On the web interface, click the **Virtual Switch Manager** link.

Figure 39 NAP Ethernet Switch Web Interface

4. Click the **Port**, **System**, **Security**, **Device**, **VLAN**, or **Fault** menu links to access the various configuration screens.
5. Click **Apply**.
6. Click **Switch Form** when you have completed your configuration.

The Ethernet Switch Properties screen switches from the web interface to the NMS interface.

7. Update the Ethernet Switch Properties screen to reflect any changes you made on the web interface.
8. Click **Apply** to save the changes to the database.

5.1.5 Configuring the NAP Router

The SNMP tab of the NAP Router Configuration screen contains a field for TFTP Server IP, shown in [Figure 40](#). This is a calculated address of the workstation where the NMS is currently installed. If you have a dedicated TFTP server, you can type its IP address in this field. However, the NMS will not save the IP address.

NOTE: In future versions, the TFTP IP address will be permanently stored in the database.



CAUTION: The NAP Router retains all user-defined access lists manually entered in the router's configuration. However, extended access list number definitions, in the range of 2000-2750, are reserved for WaveRider use if the router is used as the primary means of bandwidth management. It is recommended that you do not use


access lists defined in this range because the router will overwrite all user settings from 2000-2750.

To Update the NAP Router Configuration Using TFTP

1. In the NMS software, open the NAP Router Configuration screen.

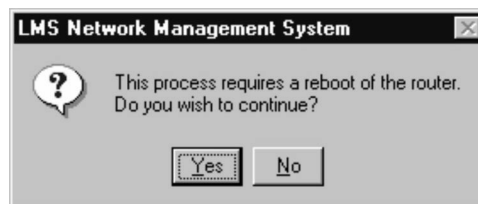
Figure 40 NAP Router Configuration—SNMP Tab

The screenshot shows the 'Router Configuration' window with the 'SNMP' tab selected. The 'General SNMP Information' section includes fields for 'System Name', 'System Contact', and 'System Location'. The 'SNMP Communities' section includes fields for 'Read Community String' (public), 'Write Community String' (private), and 'Trap Community String' (private). The 'Trap Servers' section includes a field for 'Trap Server IP' (192.168.10.7). The 'Trtp Server' section includes a field for 'Trtp Server IP' (192.168.10.7) and a note 'This address is not stored in the database'. The window also shows 'Date Entered: 31-Oct-00' and 'Date Updated: 15-Nov-00'. Buttons for 'Close', 'Restore', and 'Apply' are at the bottom.

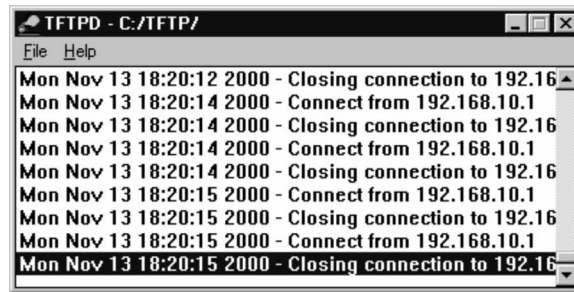
2. Change the device configuration as necessary.
3. Click **Apply** to save changes to the database.
4. Click  to upload the changes.

The Router Reboot Confirmation dialog box opens.

Figure 41 Router Reboot Confirmation Dialog Box



5. Click **Yes** to continue.
6. [Optional] Click the **TFTP** icon on the Windows task bar to monitor the connections.

Figure 42 TFTP Window

As TFTP uploads the configuration, status messages appear in the status bar on the NAP Router Configuration screen. When it has finished, the Upload Complete dialog box opens.

Figure 43 Upload Complete Dialog Box

7. Click **OK** to restart the router.

The configuration has been successfully updated.

5.1.6 Configuring Router-based Bandwidth Management

The LMS2000 system uses either router-based bandwidth management or advanced bandwidth management (ABWM). Advanced bandwidth management is optional and requires iSurfRanger hardware. If you configure your system to use router-based bandwidth management, you can convert it to ABWM using the procedures described in this section. Refer to [Configuring the Advanced Bandwidth Manager](#), on page 127 for instructions on ABWM.

Router-based bandwidth management includes six pre-configured service sets, each with a different maximum data rate:

- Copper (128 Kbps)
- Fire (512 Kbps)
- Bronze (1024 Kbps)
- Silver (1600 Kbps)
- Gold (3200 Kbps)
- Diamond (6400 Kbps)

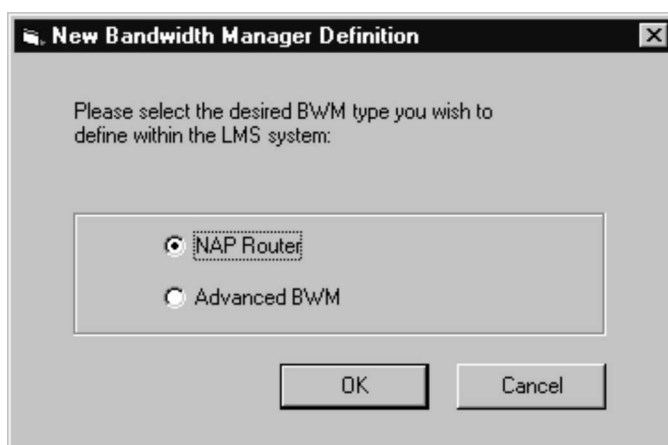
When you add subscribers and assign them EUMs, you will also associate a service level with that EUM. You may use the pre-configured service sets, or you may add your own.

To Add a Router-based Bandwidth Manager to the NMS

1. In the NMS software, right-click the **LMS2000 NAP** branch.
2. From the shortcut menu, select **Add New Device > Bandwidth Manager**.

The New Bandwidth Manager Definition dialog box opens.

Figure 44 New Bandwidth Manager Definition Dialog Box



3. Select the **NAP Router** option and click **OK**.

A new bandwidth manager record opens.

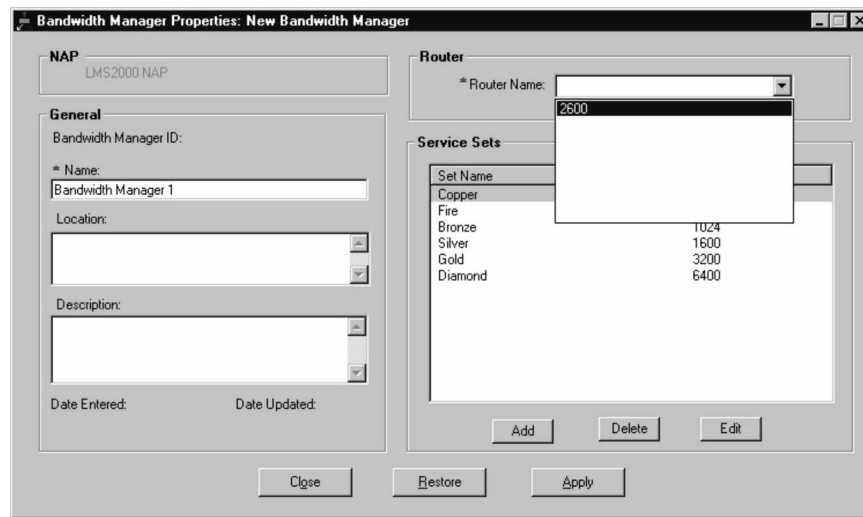
Figure 45 Bandwidth Manager Properties Screen

 A window titled "Bandwidth Manager Properties: New Bandwidth Manager". It has a tab labeled "NAP" with "LMS2000 NAP" below it. The window is divided into two main sections. The left section is labeled "General" and contains fields for "Bandwidth Manager ID:", "Name:" (with a text input field), "Location:" (with a text input field and a dropdown arrow), "Description:" (with a text input field and a dropdown arrow), "Date Entered:", and "Date Updated:". The right section is labeled "Router" and contains a dropdown menu for "* Router Name:". Below the "Router" section is a "Service Sets" table. The table has two columns: "Set Name" and "CIR". It lists five service sets: Copper (128), Fire (512), Bronze (1024), Silver (1600), and Gold (3200). Below the table are buttons for "Add", "Delete", and "Edit". At the bottom of the window are buttons for "Close", "Restore", and "Apply".

Set Name	CIR
Copper	128
Fire	512
Bronze	1024
Silver	1600
Gold	3200

4. In the Name field, type a name to uniquely identify the bandwidth manager.
5. Click the **Router Name** drop-down arrow.

A list of available routers appears in the list.

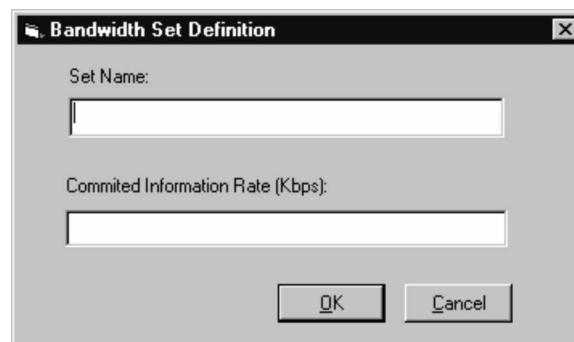
Figure 46 Router Name Drop-down List

6. Select the NAP router, **2600**, from the list.
7. Click **Apply** to save the changes to the database.
8. Click **Close**.

To Add a New Service Set

1. Open the Bandwidth Manager Properties screen.
2. Click **Add**.

The Bandwidth Set Definition dialog box opens.

Figure 47 Bandwidth Set Definition Dialog Box

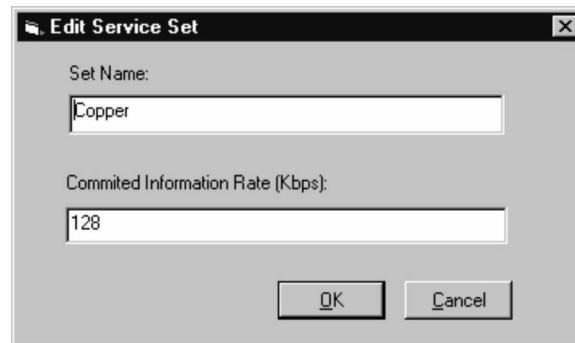
3. In the **Set Name** box, type a name for the service set (e.g., Platinum).
4. In the **Committed Information Rate (Kbps)** box, type the bit rate in Kbps at which EUMs using this service set will be able to connect to the network.
5. Click **OK** to close the dialog box.
6. Click **Apply** to save the changes to the database.

To Edit an Existing Service Set

1. Open the Bandwidth Manager Properties screen.
2. Select an existing service set.
3. Click **Edit**.

The Edit Service Set dialog box opens.

Figure 48 Edit Service Set Dialog Box



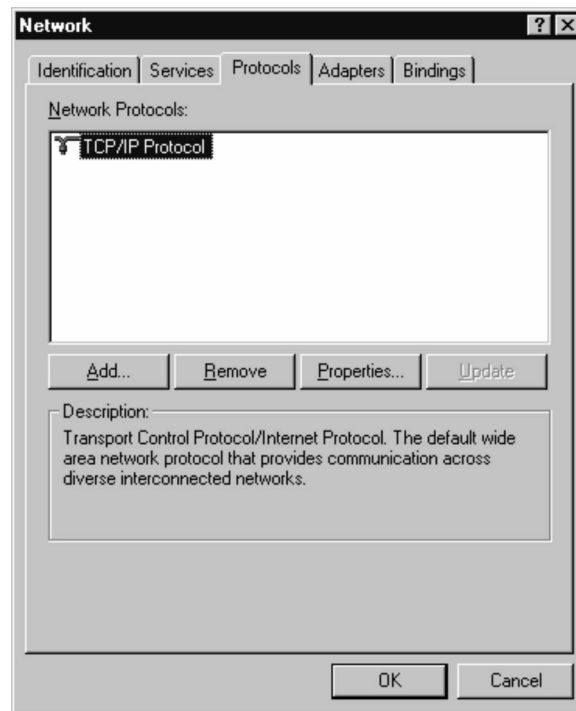
4. Update the **Set Name** and/or **Committed Information Rate (Kbps)** boxes to reflect the desired values.
5. Click **OK** to close the dialog box.
6. Click Apply to save the changes to the database.

5.1.7 Changing the IP Address of the NMS

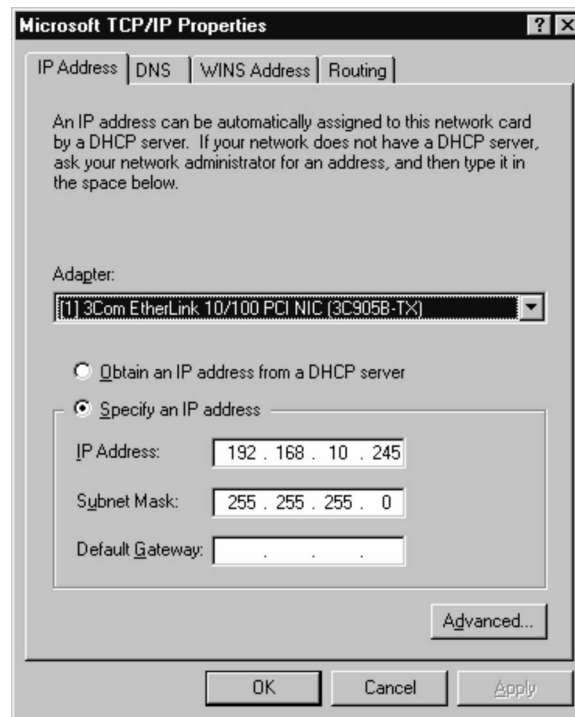
If your network uses private network addressing (an address other than 192.168.10.7), then you will have to change the NMS server IP to match your network. If you use a non-default IP address for the NMS server, the ABWM NMS control no longer transposes the IP address to the NMS server name. As a result, you must change the server settings to identify the NMS server by name rather than by IP address. The procedures for changing the IP address of the NMS server and changing the IP connection parameters of the ABWM NMS control are both described on the following pages.

To Change the IP Address of the NMS Server

1. On your Windows desktop, right-click the **Network Neighborhood** icon.
2. On the drop-down list, click **Properties**.
3. Click the **Protocols** tab.

Figure 49 Network Dialog Box—Protocols Tab

4. If it is not already selected, select the **TCP/IP Protocol**.
5. Click **Properties**.
6. Click the **IP Address** tab.

Figure 50 Microsoft TCP/IP Properties Dialog Box—IP Address Tab

7. Select the correct adapter from the **Adapter** drop-down list.
8. Specify the new IP address.
9. Click **OK** to close the Microsoft TCP/IP Properties dialog box.
10. Click **OK** to close the Network dialog box.
11. If you have an iSurfRanger box in your NAP, change the IP connection parameters of the ABWM NMS control, as described below.

To Change the IP Connection Parameters of the ABWM NMS Control

1. From the Windows **Start** menu, open the **Windows Explorer** application.
2. Navigate to the **Program Files\AmplifyNet\iSurfCommander\bin** directory.
3. Double-click **AppSetup.exe** to open the Application Server Config window.

Figure 51 ABWM Application Server Config Window



The image shows a Windows-style dialog box titled "Application Server Config". It has three tabs: "General", "Database", and "JDBC Drivers". The "General" tab is selected. Inside the dialog, there are three sections: "Server Setting", "Log Setting", and "Applet Setting". In the "Server Setting" section, the "Server Name" field contains "192.168.10.27" and the "Use IP Address" checkbox is checked. The "Server Port" field contains "1099". In the "Log Setting" section, both the "Event Log" and "Error Log" checkboxes are checked. In the "Applet Setting" section, the "Enable Applet" checkbox is checked, and the "Applet Directory" field contains "C:\inetPub\wwwroot\iSurfCommand", with a "Browse" button next to it. At the bottom right of the dialog are "Ok" and "Cancel" buttons.

Application Server Config

General Database JDBC Drivers

Server Setting

Server Name: 192.168.10.27 ☒ Use IP Address

Server Port: 1099

Log Setting

☒ Event Log ☒ Error Log

Applet Setting

☒ Enable Applet

Applet Directory: C:\inetPub\wwwroot\iSurfCommand **Browse**

Ok **Cancel**

4. On the **General** tab, clear the **Use IP Address** check box.

The name of the computer should appear in the **Server Name** field.

Figure 52 Application Server Config Window

The screenshot shows the 'Application Server Config' window with the 'General' tab selected. The window has three tabs: 'General', 'Database', and 'JDBC Drivers'. The 'General' tab contains three sections: 'Server Setting', 'Log Setting', and 'Applet Setting'. In the 'Server Setting' section, 'Server Name' is 'nms0005' and 'Server Port' is '1099'. There is an unchecked checkbox for 'Use IP Address'. In the 'Log Setting' section, both 'Event Log' and 'Error Log' are checked. In the 'Applet Setting' section, 'Enable Applet' is checked, and 'Applet Directory' is 'C:\inetPub\wwwroot\SurfCommand', with a 'Browse' button next to it. At the bottom right are 'Ok' and 'Cancel' buttons.

5. Click **OK**.

The NMS Application will now function properly when connecting to the AMP database.

5.1.8 Configuring Other NAP Components

Configure the NAP UPS on-site from the serial console to give it its network parameters. The only parameters to set for the UPS are the SNMP parameters on the UPS Properties screen.

For instructions on configuring the Advanced Bandwidth Manager, please refer to [Configuring the Advanced Bandwidth Manager](#), on page 127.

5.2 Configuring the CAP

Like the NAP, the CAP is pre-configured using factory defaults. For a listing of default configuration settings, please refer to [Device Configuration Defaults](#), on page 291. You should open the database records for the CAP components in the NMS software to verify that they are configured correctly. Also, assign a unique name to the CAP.

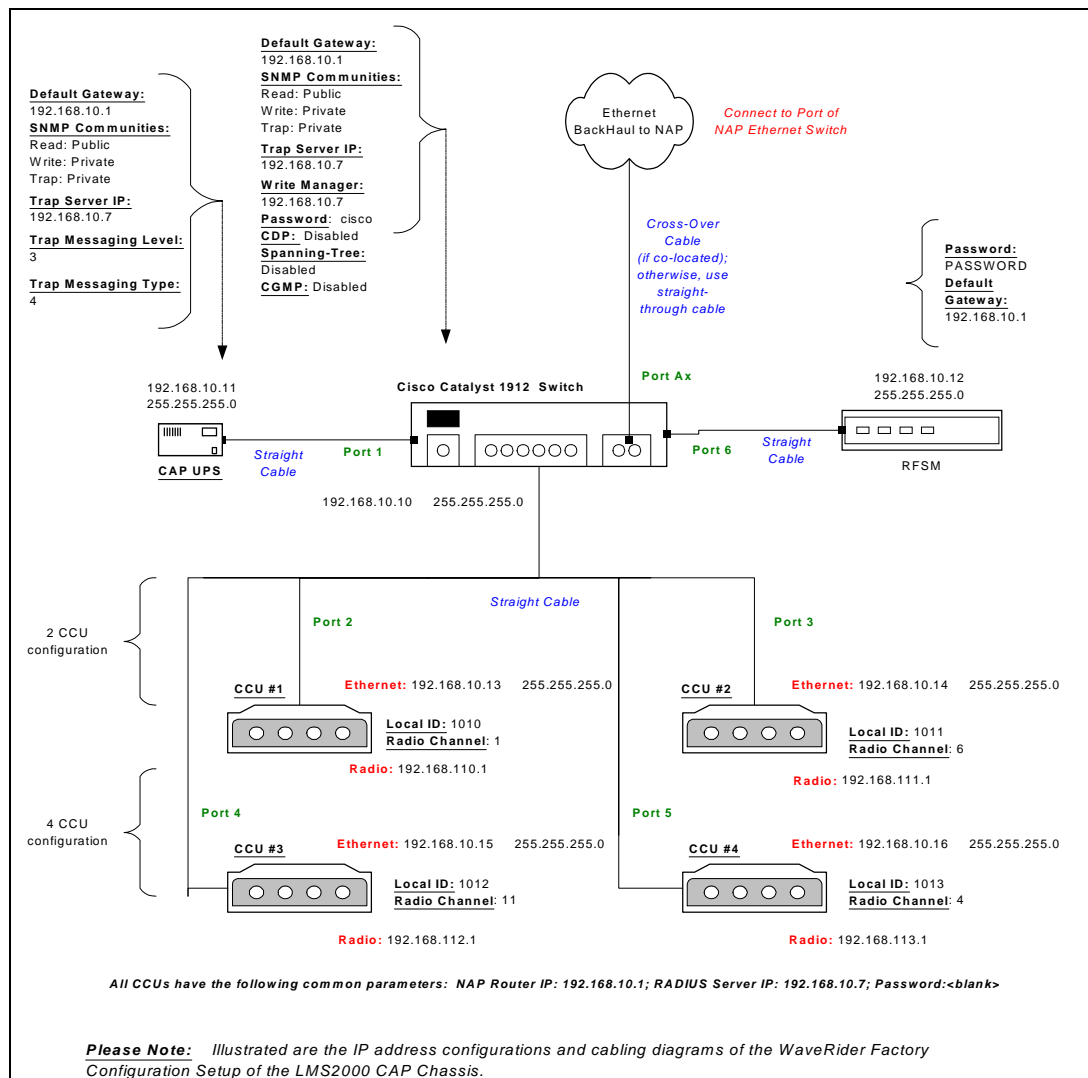
5.2.1 Understanding CAP IP Address Defaults

If a new installation has more than one CAP, the component defaults are set so that all CAPs can be connected and commissioned without changing IP addresses. [Device Configuration Defaults](#), on page 291 lists the default IPs for seven CAPs and the replacement CCUs.

NOTE: The table shows four CCUs per CAP. Not all systems have this option. Contact your **WaveRider Sales Representative** for details on availability.

New CAPs and CCUs that get added after the initial installation of the system also have pre-configured IP addresses. However, since all replacement devices have the same IP addresses, these addresses must be changed using the NMS as soon as the system connects to the devices.

Figure 53 LMS2000 CAP Default Configuration (CAP #1)



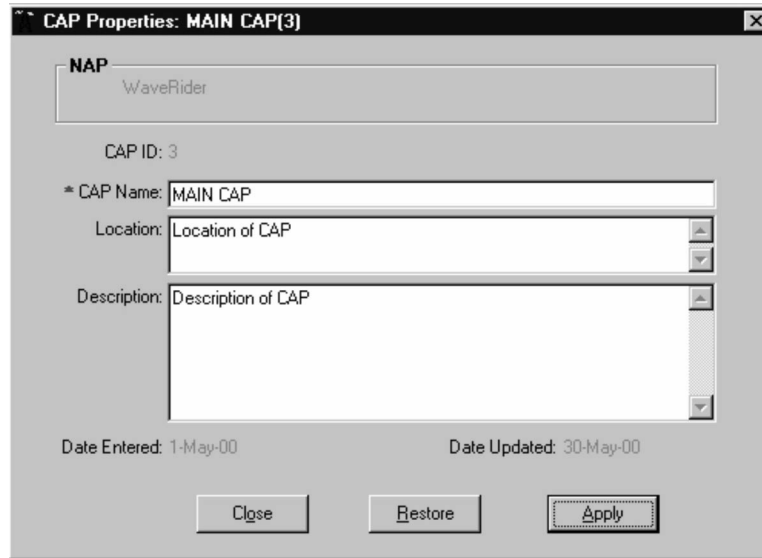
CAUTION: If you add a new CAP or CCU after the initial installation, you must change the default IP addresses of the new equipment once you establish a connection to the device.

5.2.2 Naming the CAP

To Name the CAP

1. Open the CAP record.

Figure 54 CAP Properties Dialog Box



The screenshot shows a dialog box titled "CAP Properties: MAIN CAP(3)". It contains the following fields and controls:

- NAP:** A text box containing "WaveRider".
- CAP ID:** A label showing "3".
- * CAP Name:** A text box containing "MAIN CAP".
- Location:** A text box containing "Location of CAP" with a dropdown arrow on the right.
- Description:** A large text area containing "Description of CAP" with a scrollbar on the right.
- Date Entered:** A label showing "1-May-00".
- Date Updated:** A label showing "30-May-00".
- Buttons:** "Close", "Restore", and "Apply" buttons at the bottom.

2. Confirm the identity and location of the CAP.

5.2.3 Verifying the CAP Configuration

For each CAP that you have, verify the CAP UPS and Ethernet switch to the default values shown in [Device Configuration Defaults](#), on page 291. If you have more than one CAP, refer to the default configuration provided with each CAP. If the IP addresses are incorrect in any of the devices, update the correct value to the device.

To Verify CAP Device Configurations

1. In the NMS software, right-click the device and select **Properties**.
2. Verify the configuration.

The following screen captures show the device configuration defaults for each.

Figure 55 CAP Ethernet Switch Properties

Ethernet Switch Properties

Web Interface SwitchForm Exit

CAP
LMS2000 CAP

General

General Information:
 Ethernet Switch ID: 2
 * IP Address: 192 . 168 . 10 . 10

Trap Servers:
 Trap Server IP: 192 . 168 . 10 . 7
 NetMask: 24 255.255.255.0

SNMP Communities:
 Read Community String: public
 Write Community String: private
 Trap Community String: private

Date Entered: 21-Nov-00 Date Updated:

Close Restore Apply

Status: Settings:

Figure 56 CAP UPS Properties

UPS Properties: CAP 1 UPS

General Network/SNMP

Network Addressing
 *UPS IP Address: 192 . 168 . 10 . 11
 *Netmask: 24 255.255.255.0
 *Default Gateway: 192 . 168 . 10 . 1

SNMP
 System Name: GET SET
 System Contact: GET SET
 System Location: GET SET
 Attached Devices: SNMP Device GET SET
 Read Community String: public
 Write Community String: private

Trap Server
 Trap Server IP: 192 . 168 . 10 . 7
 Trap Community String: private

Trapping Type
☐ Standard MIB
☐ Exide MIB
☐ Standard MIB and Messages
☒ Exide MIB and Messages SET

Trapping Level
☐ No Traps
☐ Critical Traps and Messages
☒ All Traps and Messages SET

Close Restore Apply

5.2.4 Configuring the CAP Ethernet Switch

The CAP switch uses a web interface for configuration. The following procedure explains how to access the configuration interface. For detailed instructions on configuring the switch, please refer to the following URL:

- **Catalyst 1900 Series Installation and Configuration Guide:** <http://www.cisco.com/univercd/cc/td/doc/product/lan/28201900/1928v8x/19icg8x/index.htm>

NOTE: The default user name and password for the CAP Ethernet switch are both **cisco**, all lowercase.



CAUTION: Changing Ethernet Switch variables on the Cisco web interface requires that you also change these values manually on the NMS screens. Changing the values on the web interface only, without changing them on the NMS screens, will prevent you from connecting to the switch.

To Access the CAP Switch Configuration Interface

1. In the NMS software, open the screen for the **CAP Ethernet Switch**.

Figure 57 CAP Ethernet Switch Properties

Ethernet Switch Properties

Web Interface SwitchForm Exit

CAP
LMS2000 CAP

General

General Information:
Ethernet Switch ID: 2
* IP Address: 192 . 168 . 10 . 10

Trap Servers:
Trap Server IP: 192 . 168 . 10 . 7
NetMask: 24 255.255.255.0

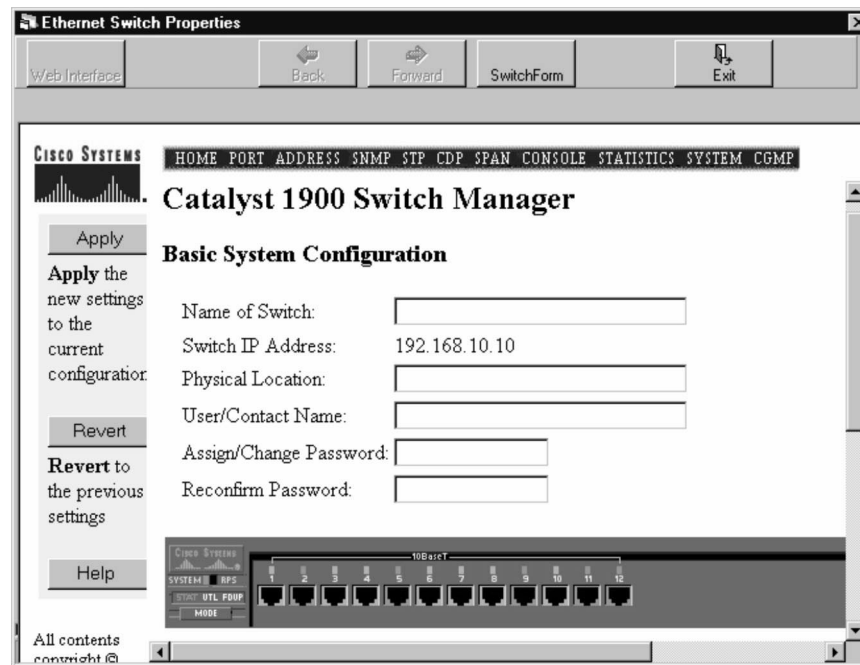
SNMP Communities:
Read Community String: public
Write Community String: private
Trap Community String: private

Date Entered: 21-Nov-00 Date Updated:

Close Restore Apply

Status: Settings:

2. Click the **Web Interface** button.

Figure 58 CAP Switch Web Interface

3. Click the **Port**, **Address**, **SNMP**, **STP**, **CDP**, **SPAN**, **Console**, **Statistics**, **System**, or **CGMP** menu links to access the various configuration screens.
4. Click **Switch Form** when you have completed your configuration.
5. Click **Apply** to save the changes to the database.

5.2.5 Configuring Other CAP Components

For instructions on configuring other CAP components, please refer to the following sections:

- [Configuring a CCU](#), on page 71
- [Configuring RFSM](#), on page 109

5.3 Connecting the NAP to the Internet


You can now connect to the Internet through the LMS2000 NAP Router. Refer to your Internet Point-Of-Presence (POP) Provider for specifications on your IP address and netmask.

To Connect to the Internet

1. In the NMS application, right-click the router for your network to open the Router Configuration dialog box.

Figure 59 IP/Network Access Tab—Router Configuration

The screenshot shows the 'Router Configuration' dialog box with the 'IP/Network Access' tab selected. The 'NAP' section at the top indicates 'LMS2000 NAP'. The 'General' tab is also visible. The 'Internet (WAN) Port' section has 'Interface Port' set to 'Interface F0/0', 'IP Address' set to '10 . 2 . 23 . 1', and 'NetMask' set to '24' with a dropdown showing '255.255.255.0'. The 'LMS (LAN) Port' section has 'Interface Port' set to 'Interface F0/1', 'IP Address' set to '192 . 168 . 10 . 1', and 'NetMask' set to '24' with a dropdown showing '255.255.255.0'. The 'Network Information' section has 'Host Name' as an empty field. The 'Login Information' section has 'UserName' set to 'cisco', 'Password' as an empty field with a masked password indicator, and 'Enable Password' as an empty field with a masked password indicator. The 'HTTP Interface' section has an 'Enable HTTP Access' checkbox that is unchecked. The 'Date Entered' is '25-Jul-00' and 'Date Updated' is empty. The 'Close', 'Restore', and 'Apply' buttons are at the bottom right. The status bar at the bottom shows 'Status:' and 'Settings:'.

2. Click the **IP/Network Access** tab.
3. Type the public **IP Address** and **Netmask** in the **Internet (WAN) Port** group.
4. Ensure that the **Interface Port** corresponds to the Ethernet ports used to connect your network.
5. Type the **Password** and **Enable Password** in the **Login Information** group.
6. Select **Enable HTTP Access** to allow the router to be configured via web access.
7. Click **Apply** to save the changes to the database.
8. Click  to upload the changes to the router.

5.3.1 Testing the Internet Connection

After the NAP is installed and connected, test the network connection to the Internet.

1. From the NMS Workstation, start your Telnet application.
2. Initiate a remote connection using the NAP router IP address.
3. Type the User Name and Password at the prompts.
4. Enter ENABLE mode in the router.

5. At the prompt, type `<ping internet_ip_address>` where *internet_ip_address* is a network destination located on the Internet, such as the IP address of your POP Provider.

If the connection is successful, you will see the following message:

```
Type escape sequence to abort
Sending 5, 100-byte ICMP echo to 193.165.10.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round trip min/ave/max = 4/4/4 ms
```

If the connection is unsuccessful, you will see the following message:

```
Type escape sequence to abort
Sending 5, 100-byte ICMP echo to 193.165.10.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Verify that your router tables and all connections to your POP Provider are valid. If they are correct, and you are unable to establish a connection, contact your POP Provider for assistance.

6

Configuring a CCU

A CCU is pre-configured with default network and radio IP addresses and radio channels for your network. See [Device Configuration Defaults](#), on page 291 for the default IP addresses. You must, however, set the password and enable the radio transmission. You can optionally configure various other properties of the CCU.

The following list identifies the high level steps in configuring a CCU. The remainder of this chapter outlines each of these steps in detail.

1. [Assigning a Password to a CCU](#), on page 72
2. [Configuring the Ethernet and Radio Properties](#), on page 73
 - [Assigning a CCU ID](#), on page 73
 - [Adding EUMs to the CCU Record](#), on page 73
 - [Assigning a Radio Channel to the CCU](#), on page 74
 - [Enabling Radio Transmission](#), on page 75
 - [Verifying the Network IP Address](#), on page 75
 - [Verifying the Radio IP Address](#), on page 75
3. [Configuring the IP Routing Properties](#), on page 76
 - [Configuring Static Routing](#), on page 76
 - [Configuring RIP](#), on page 78
4. [Configuring the SNMP Properties](#), on page 79
 - [Defining SNMP Communities](#), on page 80
 - [Defining SNMP Trap Servers](#), on page 81
5. [Uploading the Configuration to the CCU](#), on page 83

6.1 Assigning a Password to a CCU

The CCU is factory configured with no password. To properly secure your network, use a different password for each CCU in your network. Set the password in the Tools tab of the Channel Unit Properties screen. Record the password in a secure location for future reference. The NMS stores the password in a hidden field in the database. When you connect to the CCU from the NMS database, it uses the password from this hidden field. Remember to upload the password change to the CCU before you close the Properties screen.



CAUTION: For security, WaveRider recommends that you change the password in the CCU before you enable the radio transmission.

To Set the CCU Password

1. In the **Channel Unit Properties** dialog box, click the **Tools** tab.

Figure 60 Channel Unit Properties—Tools Tab

The screenshot shows the 'Channel Unit Properties: CCU-1' dialog box with the 'Tools' tab selected. The 'Change Password' section contains three text input fields: 'Current Password:', 'New Password:', and 'Retype:'. Below these fields are 'Apply' and 'Clear' buttons. The 'System' section below contains 'Load Defaults' and 'Reboot' buttons. At the bottom of the dialog, there are 'Date Entered: 31-Oct-00' and 'Date Updated: 10-Nov-0' labels, and 'Close', 'Restore', and 'Apply' buttons.

2. Type your new password in the **New Password** box.



TIP: Use a maximum of sixteen (16) alphanumeric, ASCII characters. Passwords are case-sensitive. For example, "abc" is not the same as "aBc".

3. Type the password again in the **Retype** box.
4. Record the password in a secure location.
5. Click **Apply** in the **Change Password** group to accept the new password.
6. Click **Apply** in the bottom-right corner of the screen to save to the database.

6.2 Configuring the Ethernet and Radio Properties

The Ethernet/Radio tab contains properties for enabling communications between the CCU, the NAP, and the EUMs.

Figure 61 Channel Unit Properties—Ethernet/Radio Tab

The screenshot shows the 'Channel Unit Properties: CCU-1' dialog box with the 'Ethernet/Radio' tab selected. The dialog is divided into several sections:

- Network Addressing:** IP Address: 192 . 168 . 10 . 13, Netmask: 24 (dropdown), 255.255.255.0
- Radio Addressing:** IP Address: 192 . 168 . 110 . 1
- Radio Parameters:**
 - Regulatory Domain: FCC (dropdown)
 - Radio Channel Parameters: Radio Enabled (checkbox), Radio Channel: 3 (dropdown), 2422 MHz
 - Local CCU ID: * Local ID: 1010 (dropdown)
 - EUM ID List: A table with columns 'Unit ID' and 'Destination Radio IP'. It contains one entry: Unit ID 101, Destination Radio IP 192.168.110.2. Buttons 'Add', 'Edit', and 'Delete' are to the right.

At the bottom, there are fields for 'Date Entered: 25-Jul-00' and 'Date Updated:', and buttons for 'Close', 'Restore', and 'Apply'. A 'Status' and 'Settings' section is at the very bottom.

6.2.1 Assigning a CCU ID

Every CCU and EUM in your network will have a Local ID number. You can choose any Local ID number as long as it is between 1 and 16,384 and is unique within your network.

To Assign a CCU ID

1. In the **Channel Unit Properties** dialog box, click the **Ethernet/Radio** tab.
2. In the **Local ID** box, type the ID number for the CCU.
3. Click **Apply** to save the changes to the database.

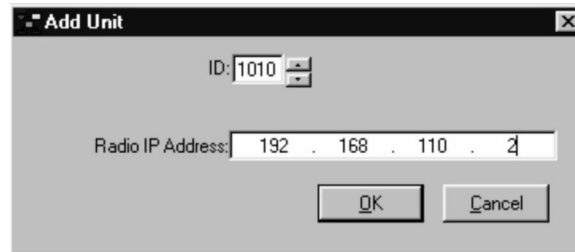
6.2.2 Adding EUMs to the CCU Record

The EUM ID list in the Channel Unit Properties dialog box must contain a list of the Unit ID and Radio IP addresses of every EUM connected to that CCU. You can find this information about the EUMs on the Ethernet/Radio tab of each EUM record. If you do not yet have any EUMs deployed on your network, you will have to add them to the CCU record as you deploy them.

To Add an EUM to a CCU Record

1. In the **Channel Unit Properties** dialog box, click the **Ethernet/Radio** tab.
2. In the **EUM ID** group, click the **Add** button.

Figure 62 Add Unit Dialog Box



3. In the **ID** box, type the EUM ID.
4. In the **Radio IP Address** box, type the Radio IP Address for the EUM.
5. Click **OK**.

You have successfully added the EUM to the CCU record.

6. Repeat steps 2 through 5 for every EUM that will communicate with this CCU.

6.2.3 Assigning a Radio Channel to the CCU

Each CCU in a CAP must use a different radio channel. By default, the Radio Channel is set according to the [Device Configuration Defaults](#), on page 291. Typically, every CCU in the network will use a different radio channel, and all EUMs associated with that CCU must use the same radio channel.

To Assign a Radio Channel

1. In the **Channel Unit Properties** dialog box, click the **Ethernet/Radio** tab.
2. In the **Radio Channel** drop-down list, select the channel for the CCU as determined by the site survey.
3. Click **Apply** to save the changes to the database.

6.2.4 Enabling Radio Transmission

You **MUST** enable radio transmission on both the CCU and a connected EUM to enable communications between them.

To Enable Radio Transmission

1. Click the **Ethernet/Radio** tab.
2. In the **Radio Channel Parameters** group, select **Radio Enabled**.
3. Click **Apply** to save the changes to the database.

6.2.5 Verifying the Network IP Address

The CCU is pre-configured with a default Network IP address, which enables the CCU to communicate with the NAP. If you decide to use a non-default IP address, you must ensure that it uses the same host ID as identified in the **LMS (LAN) Port** of the **NAP Router** record.

To Verify the Network IP Address

1. In the **Channel Unit Properties** dialog box, click the **Ethernet/Radio** tab.
2. In the **Network Addressing** group, verify that the **IP Address** and **Netmask** match the defaults listed in [Device Configuration Defaults](#), on page 291.

6.2.6 Verifying the Radio IP Address

The CCU is also pre-configured with a default Radio IP address, which enables it to communicate with the EUM. If you decide to use a non-default IP address, you must ensure that it uses the same host ID as the Radio IP address for the EUMs that are attached to it.

To Verify the Radio IP Address

1. In the **Channel Unit Properties** dialog box, click the **Ethernet/Radio** tab.
2. In the **Radio Addressing** group, verify that the **IP Address** matches the default listed in [Device Configuration Defaults](#), on page 291.

6.3 Configuring the IP Routing Properties

Use the **IP Routing** tab to set up the routing tables for the CCU. Routing tables define the gateways available from the CCUs. The LMS2000 currently supports static routing and RIP.

The CCU routing table should include IP addresses for the following devices, which are gateways for the CCU:

- NAP router
- Every EUM on the subnetwork of the CCU

NOTE: Routing Information Protocol (RIP) may not be configured in some LMS2000 releases. Contact your WaveRider Sales Representative for details on availability.

6.3.1 Configuring Static Routing

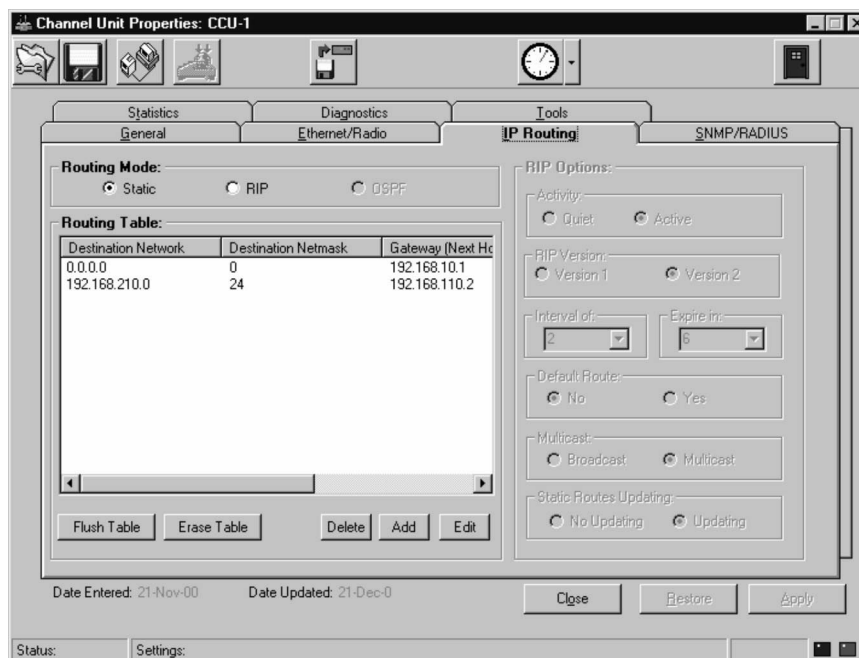
The buttons in the static routing table perform the following functions:

- The **Flush Table** button removes all dynamic entries from the Routing Table.
- The **Erase Table** button removes all static and dynamic entries from the Routing Table. This command cannot be undone.
- The **Delete** button removes a selected entry from the Routing Table.
- The **Add** button adds a static route to the Routing Table.
- The **Edit** button displays the current IP address, subnet, and Gateway IP address and lets you modify the information for that static route entry.

To Add a Default Static Route

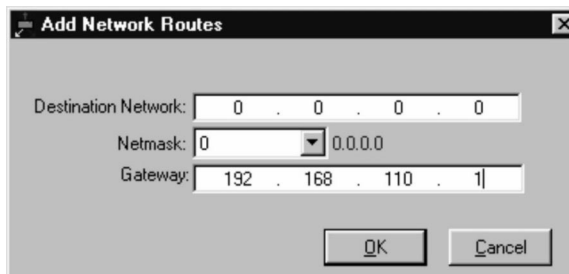
1. Click the **IP Routing** tab.

Figure 63 Channel Unit Properties—IP Routing Tab



2. Select **Static** in the **Routing Mode** group.
3. Click **Add** in the **Routing Table** group.

Figure 64 Add Network Routes Dialog Box



4. In the **Add Network Routes** dialog box, type an IP address in the **Destination Network** box to define a static route.
5. Select the appropriate **Netmask** for the destination from the drop-down list.
6. Type an IP address for the Gateway in the **Gateway** box.



TIP: To add the NAP router as a Gateway, use its LAN Ethernet IP address. To add each of the EUMs on the network as a Gateway, use its radio IP address.

7. Click **OK**.

You have successfully added the route to the routing table.

8. Repeat steps 3 through 7 until you have added the NAP Router and every EUM on the CCU's network as a gateway in the routing table.
9. Click **Apply** to save the changes to the database.

6.3.2 Configuring RIP

RIP is the routing information protocol. It is an alternate method of configuring routing for the CCUs, which dynamically updates the routing tables for the device.

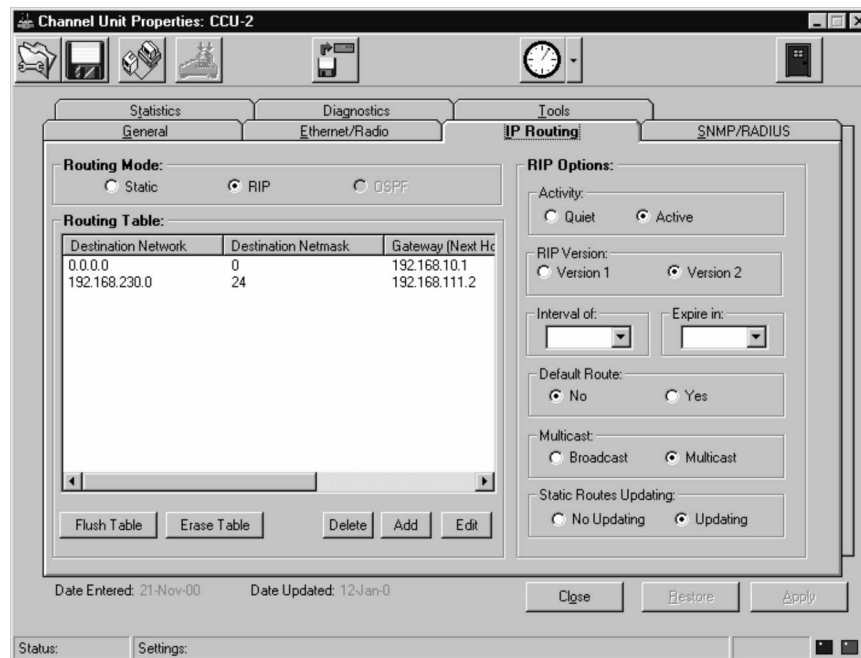
Some of the configuration parameters for RIP are dependent on which version of the protocol you are running. Specifically, the Multicast option is only available if you are running RIP Version 2. Version 1 of RIP supports only the Broadcast option.

NOTE: LMS2000 R6 does not support RIP version 1.

To Configure the CCU for RIP

1. In the **Channel Unit Properties** dialog box, click the **IP Routing** tab.
2. In the **Routing Mode** group, select **RIP** to activate the RIP Options group.

Figure 65 Channel Unit Properties—IP Routing—RIP



3. In the **Activity** group, select **Active** unless you want only to receive RIP packets and not broadcast them.
4. In the **RIP Version** group, select the version of **RIP** your network is using.

NOTE: LMS2000 R6 does not support RIP version 1.

5. In the **Default Route** group, select **Yes** or **No** to indicate whether a default route exists for the subnetwork.
6. In the **Multicast** group, select **Broadcast** if you want the CCU to send routing information packets to everyone on the subnetwork or **Multicast** to send packets to select devices on the subnetwork.

NOTE: The **Multicast** option is only available if you are using RIP Version 2.

7. In the **Static Routes Updating** group, select one of the following options:
 - **No Updating** if you do not want the static routes to update dynamically
 - **Updating** to dynamically update the all routes

6.4 Configuring the SNMP Properties

The LMS2000 network uses SNMPc Server to monitor network devices and determine when and why a device stops passing traffic.

SNMPc Server and network devices use community strings to authenticate messages between them. Each LMS2000 network device must have three types of community strings defined:

- Read community string
- Read/write community string
- Trap community string

These community strings are essentially passwords to verify that messages are from an authorized source.

If SNMPc Server sends a message to a device using a read community string, it can read information regarding the status of a device but not change the configuration.

If SNMPc Server sends a message using a read/write community string, it can read information about the status of the device and request the device to change a configuration parameter.

Network devices send messages to the SNMPc Server using the trap community string. These messages provide status information about the operation of the device.

Devices in the LMS2000 network are pre-configured with one of each type of community string:

- The community string for read is "public".
- The community string for read/write is "private".
- The community string for trap is "private".



CAUTION: Since these default community strings are commonly used by other systems, you should change them to prevent unauthorized access to your network devices.

6.4.1 Defining SNMP Communities

The SNMP Communities group defines the read and read/write community strings for the CCU. Confirm that SNMP Communities lists at least one community with write privileges and one with read privileges. If not, you must define the communities for the device. You can define up to five community strings.

NOTE: Community String fields are case-sensitive.

To Set CCU Communities

1. In the **Channel Unit Properties** dialog box, click the **SNMP/RADIUS** tab.

Figure 66 Channel Unit Properties—SNMP/RADIUS Tab

Channel Unit Properties: CCU-1

Statistics | Diagnostics | Tools | **SNMP/RADIUS**

General SNMP Information:

System Name: CCU2000
 System Contact: www.WaveRider.com
 System Location: Toronto, Ontario, Canada

SNMP Communities:

Community String	Properties
private	read/write
public	read

Buttons: Add, Edit, Delete

Trap Servers:

Trap Server IP Address	Trap Community String
------------------------	-----------------------

Buttons: Add, Edit, Delete

DNS Servers:

DNS Domain Name:

Buttons: Add, Edit, Delete

NAP Router:

IP Address: 192.168.10.1
 Netmask: 24 255.255.255.0

RADIUS Server:

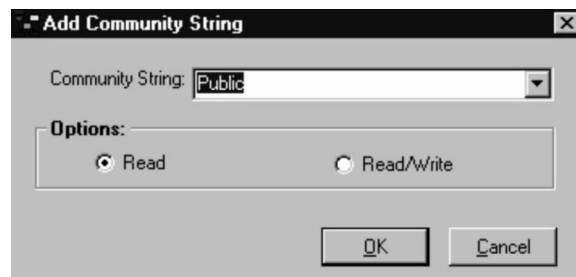
IP Address: 192.168.10.5
 Netmask: 24 255.255.255.0

Date Entered: 19-Jun-00 Date Updated: 19-Jun-00

Buttons: Close, Restore, Apply

Status: Settings:

2. In the **SNMP Communities** group, click the **Add** button.

Figure 67 Add Community String

3. In the **Community String** field, type the password for the SNMPc Server to gain access to the device.
4. In the **Options** group, select **Read** if the password should grant read-only access, or select **Read/Write** if the password should grant both read and write privileges.
5. Click **OK**.
6. Click **Apply** to save the changes to the database.

6.4.2 Defining SNMP Trap Servers

The Trap Servers group defines the trap community string for the CCU. You can define up to five different trap servers.

NOTE: Community String fields are case-sensitive.

To Set CCU Trap Servers

1. In the **Channel Unit Properties** dialog box, click the **SNMP/RADIUS** tab.

Figure 68 Channel Unit Properties—SNMP/RADIUS Tab

2. In the **Trap Servers** group, click the **Add** button.

Figure 69 Add Trap Server


3. In the **Trap Server IP Address** box, type the IP Address for the NMS Workstation where the SNMPc Server is installed.
4. In the **Trap Community String** box, type the password for the CCU to enable device information to write to the SNMPc Server.
5. Click **OK**.
6. Click **Apply** to save the changes to the database.

6.5 Uploading the Configuration to the CCU

Use this procedure every time you make any change to the CCU configuration in the NMS software.

NOTE: After you configure the CCU in the Channel Unit Properties dialog box, you must upload the configuration to the CCU for it to take effect.

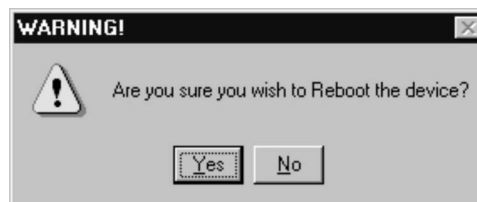
To Upload CCU Configurations to the Device

1. In the NMS software, open the Properties screen for the CCU.
2. Change the device configuration as necessary.
3. Click **Apply** to save changes to the database.
4. Click  to upload the changes.

As FTP uploads the configuration, status messages appear in the status bar on the Properties screen.

After the upload is complete, the Device Reboot Confirmation dialog box opens.

Figure 70 Device Reboot Confirmation Dialog Box



5. Click **Yes** to reboot the device.

The configuration is successfully updated.

— This page is intentionally left blank —

7

Adding an EUM

An EUM is an End User Modem, and it routes traffic between the CCU and the subscriber's network or PC. Before an EUM can pass traffic, you must configure it through the NMS and deploy it to the subscriber's site.

The following list identifies the high level steps in configuring an EUM. The remainder of this chapter outlines each of these steps in detail.

1. [Connecting to an EUM](#), on page 86
2. [Creating a New EUM Record](#), on page 87
3. [Configuring the Ethernet and Radio Properties](#), on page 91
4. [Configuring the IP Routing Properties](#), on page 93
5. [Configuring SNMP and DNS Server Properties](#), on page 97
6. [Saving the EUM Configuration to a File](#), on page 100
7. [Uploading the Configuration to the EUM](#), on page 101
8. [Assigning a Subscriber and Service Level to an EUM](#), on page 101
9. [Adding an EUM to a CCU Record](#), on page 105
10. [Changing the Ethernet IP Address](#), on page 107
11. [Deploying an EUM](#), on page 108

7.1 Connecting to an EUM

Before you configure the EUM through the NMS, you should establish a physical connection to the device.

To Connect to the EUM

1. Connect one end of the RJ-45 cable to the Ethernet port on the EUM.
2. Plug the other end of the cable into any available Ethernet connection on the NAP switch.
3. Terminate the antenna lead of the EUM by attaching a 50-ohm RF load.

NOTE: The EUM radio transmission capabilities are disabled prior to shipment to prevent equipment damage. However, as a general precaution, WaveRider recommends that you always connect the antenna or load before connecting to a power source.

WARNING!



Antennas and associated transmission cable must be installed by qualified personnel. Failure to terminate the antenna port correctly can permanently damage the EUM. WaveRider assumes no liability for failure to adhere to this recommendation or to recognized general safety precautions.

4. Plug the EUM into an AC power source.
5. Confirm the following conditions:
 - Red power LED is on.
 - Green network link LED is on.
 - Cooling fan is operating.

7.2 Creating a New EUM Record

The first time you create a new EUM record, you will have to configure many of the properties.



TIP: Once you have configured the first EUM, you can save that configuration to a file and use it as a basis for configuring additional EUMs. For instructions on saving a configuration to a file, refer to [Saving the EUM Configuration to a File](#), on page 100.

7.2.1 Adding a New EUM Record to the NMS

There are two methods for creating a new EUM record:

- Add a new device to a CCU.
- Add a new EUM to inventory.

If you know the CCU to which the EUM will connect, you should add the new device directly to the CCU. Otherwise, add it to inventory.

When you add a new EUM record by adding a new device to the CCU, the following fields are defined automatically:

- The **Radio Channel** field is automatically defined to be the same as the CCU radio channel.
- The **Unit ID** and **Destination Radio IP** of the CCU automatically appear in the EUM IDs list.

When you create a new EUM record by adding it to inventory, these fields are not automatically defined, so you will have to define them later when you associate the EUM with a CCU.

To Add a New EUM to a CCU

1. In the **CAP** branch of the LMS2000 tree, right-click the **CCU** to which you want to add an EUM.
2. From the pop-up menu, select **Add New Device**, then **EUM**.

To Add a New EUM to Inventory


- In the **Inventory** branch, right-click **EUMs** and select **Add New EUM**.

Figure 71 End User Modem Properties

7.2.2 Importing a Saved EUM Configuration

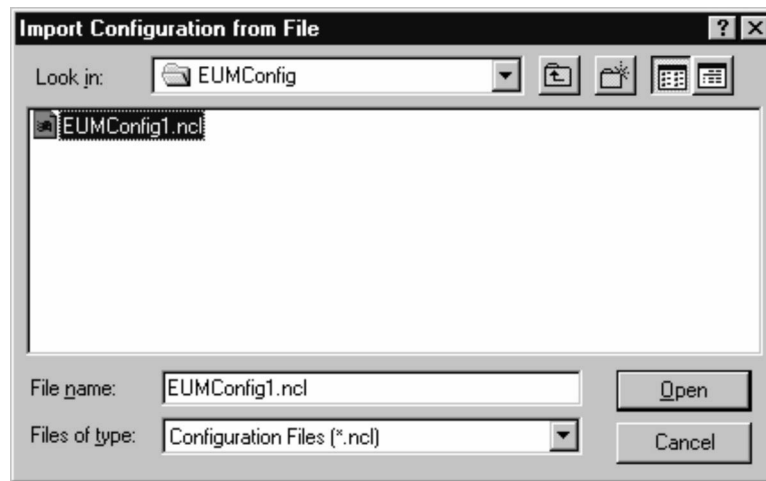
If you already have a saved EUM configuration file, you can use it to create a new EUM record more quickly. If you do not have a saved EUM configuration file, skip ahead to [Naming an EUM](#), on page 89.

To Import a Saved EUM Configuration

1. Create a blank EUM record.
2. Click .

The **Import Configuration from File** dialog box opens.

Figure 72 Import Configuration From File



3. Navigate to the directory containing the relevant .ncl configuration file.
4. Select the configuration file to import into the current EUM record.
5. Click **Open**.

7.2.3 Naming an EUM

Every EUM in your LMS2000 network must have a unique name, which is defined in the **EUM Name** field of the **General** tab. If your company has designated naming conventions for the devices, name the EUM according to those conventions. Otherwise, you can give it any name you choose as long as it uniquely identifies the device.

7.2.4 Assigning a Password

The EUM is factory configured with no name and no password. To properly secure your network, use a different password for each EUM in your network. Record the password in a secure location for future reference. The NMS database stores the password in a hidden field in the database. When you connect to the EUM from the NMS, it uses the password from this hidden field. Remember to download the password change to the EUM before you close the **Properties** dialog box.

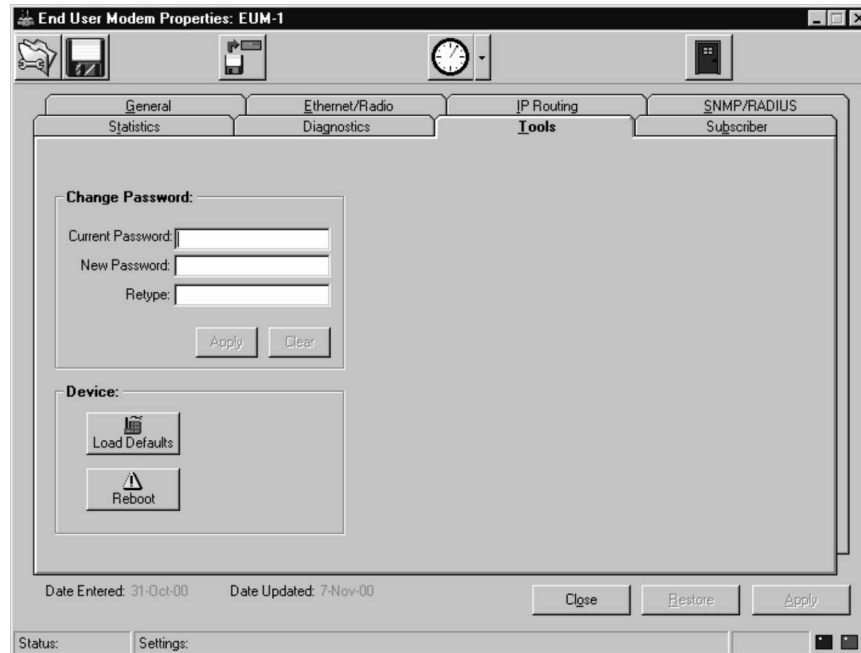



CAUTION: For security, WaveRider recommends that you change the password in the EUM before you enable the radio transmission.

To Set the EUM Password

1. In the **End User Modem Properties** dialog box, click the **Tools** tab.

Figure 73 End User Modem Properties—Tools Tab



2. Click  to connect to the EUM.




CAUTION: You must connect to the EUM before changing the password. Otherwise, the NMS will no longer be authorized to access the device.

3. Type the current password in the **Current Password** box.
4. Type your new password in the **New Password** box.



TIP: Use a maximum of sixteen (16) alphanumeric, ASCII characters. Passwords are case-sensitive. For example, “abc” is not the same as “aBc”.

5. Type the password again in the **Retype** box.
6. Record the password in a secure location.
7. Click **Apply** in the **Change Password** group to accept the new password.
8. Click  to upload the changes to the EUM.

7.3 Configuring the Ethernet and Radio Properties

The Ethernet/Radio tab contains properties for enabling communications between the EUM, the CCU, and the subscriber's PC or network.

Figure 74 End User Modem Properties—Ethernet/Radio Tab

End User Modem Properties: eum-1

Statistics | Diagnostics | Tools | Subscriber
General | **Ethernet/Radio** | IP Routing | SNMP/RADIUS

Network Addressing:
 * IP Address: 192 . 168 . 210 . 2
 * Netmask: 24 255.255.255.0

Radio Addressing:
 IP Address: 192 . 168 . 110 . 2

Radio Parameters:
 Regulatory Domain: IEEE
 Local EUM ID: * Local ID: 1

Radio Channel Parameters:
 Radio Enabled: ☒
 Radio Channel: 1 2412 MHz

CCU IDs:

Unit ID	Destination Radio IP
1010	192.168.110.1

Add Edit Delete

Date Entered: 20-Sep-00 Date Updated: 21-Sep-00
 Close Restore Apply

Status: Settings:

The following paragraphs describe the properties on the Ethernet/Radio tab, and the subsequent procedures explain the steps in configuring them.

Network Addressing

The EUM has a default Ethernet IP address, which enables it to communicate with the NMS. After you have uploaded the configuration to the device, you will have to reconfigure the EUM to use an Ethernet IP address that is compatible with the subscriber's PC or network. If you are configuring an EUM in inventory, you will not be able to assign an Ethernet IP address because the EUM is not yet associated with a subscriber.

Radio Addressing

The EUM has a default Radio IP address. Verify that the address belongs to the same network as the connected CCU. If not, you must assign the EUM a radio IP that belongs to the same network as the CCU to which it connects.

Radio Channel Parameters

The EUM must use the same radio channel as the CCU. Refer to the CCU record to determine which radio channel to assign to the EUM.

You **MUST** enable radio transmission on both the CCU and a connected EUM so the devices can communicate with each other.

Local EUM ID

Every EUM and CCU in your network must have a Local ID number. You can choose any Local ID number you want, as long as it is between 1 and 16384 and is unique within the network.

CCU ID

The CCU ID list must contain the Unit ID and Radio IP address for the CCU to which the EUM connects. Each EUM may have only one CCU defined in this list.

Whether you must update the CCU ID list depends on how you created the EUM record:

- If you created a new EUM record by adding a device to the CCU, then the CCU ID list already contains the information about that CCU.
- If you created the new EUM record in inventory, then you will have to complete the following procedure to add the CCU.
- If you imported a saved EUM configuration, you may need to change the CCU information by clicking the **Edit** button.

To Configure Ethernet and Radio Properties for the EUM

1. In the **End User Modem Properties** dialog box, click the **Ethernet/Radio** tab.
2. In the **Radio Channel** box, select the channel for the EUM.

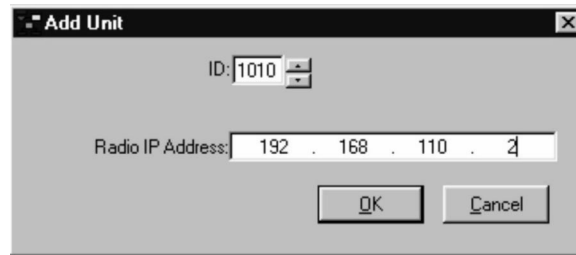
NOTE: This channel must be the same channel as the CCU to which the EUM connects.

3. In the **Radio Channel Parameters** group, select **Radio Enabled**.
4. In the **Local ID** box, type the ID number for the EUM.
5. Click **Apply** to save the changes to the database.

To Add a CCU to the CCU ID List

1. On the **Ethernet/Radio** tab of the EUM record, click **Add** in the **CCU ID** list group.

Figure 75 Add Unit



2. In the **ID** box, type the CCU ID.
3. In the **Radio IP Address** box, type the Radio IP of the CCU.
4. Click **OK**.
5. Click **Apply** to save the changes to the database.

7.4 Configuring the IP Routing Properties

Use the IP Routing tab to set up the routing tables for the EUM. Routing tables define the gateways available from the EUM. The LMS2000 currently supports static routing and RIP.

The EUM routing table should include the IP address of the CCU through which the EUM connects to the network. Before the EUM will route traffic to the Internet, you must also define the routing tables on the CCU and NAP router.

NOTE: RIP may not be configured in some LMS2000 releases. Contact your **WaveRider Sales Representative** for details on availability.

7.4.1 Configuring Static Routing

The buttons in the Static Routing table have the following functions:

- The **Flush Table** button removes all dynamic entries from the Routing Table.
- The **Erase Table** button removes all static and dynamic entries from the Routing Table. This command cannot be undone.
- The **Delete** button removes a selected entry from the Routing Table.
- The **Add** button appends a static route to the Routing Table.
- The **Edit** button displays the current IP address, netmask, and Gateway IP address, and lets you modify the information for that static route entry.

To Add a Default Static Route

1. Click the **IP Routing** tab.

Figure 76 End User Modem Properties—IP Routing Tab

End User Modem Properties: eum-1

Statistics | Diagnostics | Tools | Subscriber

General | Ethernet/Radio | **IP Routing** | SNMP/RADIUS

Routing Mode:
☒ Static ☐ RIP ☐ OSPF

Routing Table:

Destination Network	Destination Netmask	Gateway (Next Hop)
0.0.0.0	0	192.168.110.1

Flush Table | Erase Table | Delete | Add | Edit

DHCP:
☐ Enabled

Servers

IP Address

Add | Edit | Delete

RIP Options:
 Activity: ☐ Quiet ☒ Active
 RIP Version: ☒ Version 1 ☐ Version 2
 Interval of: [30] | Expire in: [180]
 Default Router: ☒ No ☐ Yes
 Multicast: ☐ Broadcast ☒ Multicast
 Static Routes Updating: ☐ No Updating ☒ Updating

Date Entered: 12-Jan-01 | Date Updated:

Close | Restore | Apply

Status: | Settings:

2. Select **Static** in the **Routing Mode** group.
3. Click **Add** in the **Routing Table** group.

Figure 77 Add Network Routes

Add Network Routes

Destination Network: 0 . 0 . 0 . 0

Netmask: 0 [0.0.0.0]

Gateway: 192 . 168 . 110 . 1

OK | Cancel

4. In the **Add Network Routes** dialog box, type an IP address in the **Destination Network** box to define a static route.
5. Select the **Netmask** for the destination from the drop-down list.
6. Type the IP address for the gateway in the **Gateway** box.



TIP: To add a default static route to route all traffic to the CCU, set the **Destination Network** to 0.0.0.0, the **Netmask** to 0, and the **Gateway** to the radio IP address of the CCU.

7. Click **OK**.

The static route is added to the **Routing Table**.

8. Click **Apply** to save the changes to the database.

7.4.2 Configuring RIP

RIP is the routing information protocol, which is an alternate method of configuring routing for the EUMs. It dynamically updates the routing tables for the device.

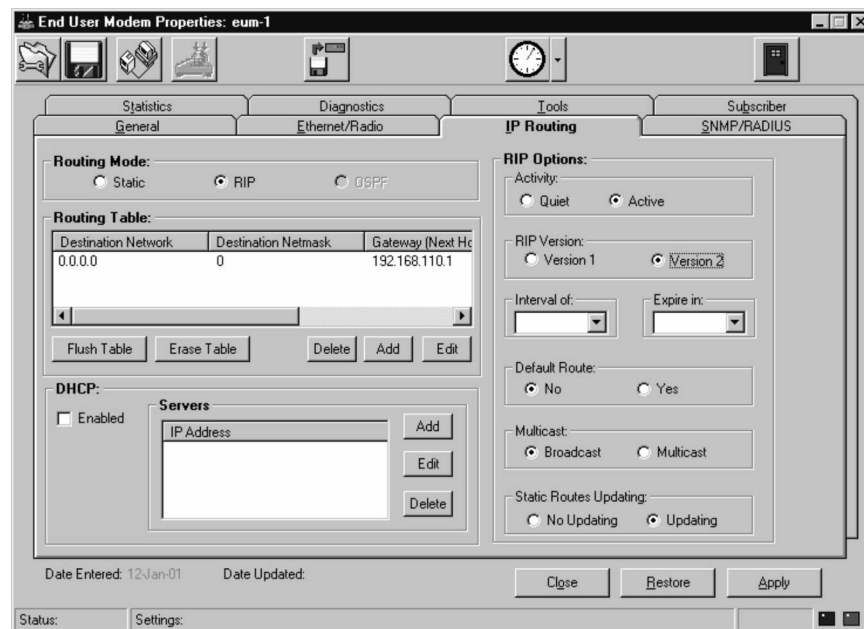
The EUM supports RIP version 1 only. You can set RIP Version 2 to Multicast or Broadcast.

To Configure the EUM for RIP

1. In the **End User Modem Properties** dialog box, click the **IP Routing** tab.
2. In the **Routing Mode** group, select **RIP**.

The **RIP Options** group becomes active.

Figure 78 End User Modem Properties—IP Routing—RIP



3. In the **Activity** group, select **Active** to enable RIP to transmit packets to other interfaces. Select **Quiet** to receive and process RIP packets but not transmit them.
4. In the **RIP Version** group, select the version of **RIP** your network is using.

NOTE: LMS2000 R6 does not support RIP version 1.

5. In the **Default Route** group, select **Yes** or **No** to indicate whether a default route exists for the subnetwork.

6. In the **Multicast** group, select **Broadcast** if you want the CCU to send routing information packets to everyone on the subnetwork or **Multicast** to send packets to select devices on the subnetwork.

NOTE: The **Multicast** option is only available if you are using RIP Version 2.

7. In the **Static Routes Updating** group, select one of the following options:
 - **No Updating** if you do not want the static routes to update dynamically
 - **Updating** to dynamically update the all routes

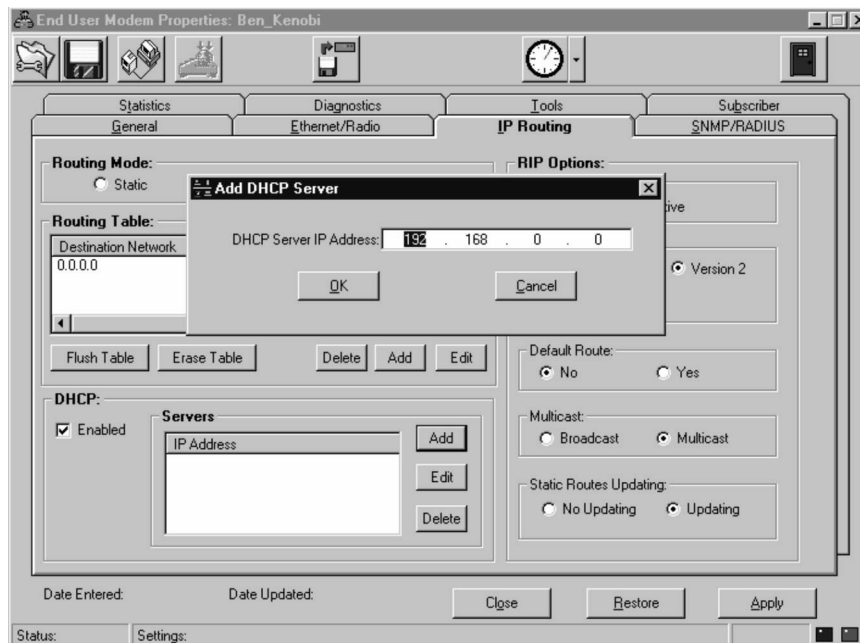
7.4.3 Configuring DHCP Relay

DHCP is an acronym for Dynamic Host Configuration Protocol. A DHCP Server dynamically assigns IP addresses to devices each time they log on to the network. You may assign a DHCP server in the EUM record, which client networks may use to obtain their network IPs by DHCP. The DHCP Server resides upstream from the NAP on the ISP's network. DHCP Servers are optional in the LMS2000 network, but if your network includes one, you must specify its IP address on each EUM record. An EUM record can support a maximum of five DHCP servers, although it will typically only use one.

To Configure a DHCP Relay Server in an EUM Record

1. In the EUM record, click the **IP Routing** tab.
2. In the **DHCP** group, click **Add**.

Figure 79 Add DHCP Server Dialog Box



3. Type the IP address for the DHCP Server.
4. Click **OK**.

5. Click the **Enabled** check box.
6. Click **Apply** to save the changes to the database.

7.5 Configuring SNMP and DNS Server Properties

SNMP Server enables you to define SNMP community strings and DNS Server options for the EUM.

Figure 80 End User Modem Properties—SNMP/RADIUS Tab

The screenshot shows the 'End User Modem Properties: CCU1-EUM1' dialog box with the 'SNMP/RADIUS' tab selected. The dialog has a title bar with standard window controls and a toolbar with icons for Statistics, Diagnostics, Tools, and Subscriber. Below the toolbar are tabs for General, Ethernet/Radio, IP Routing, and SNMP/RADIUS. The main content area is divided into four sections:

- General SNMP Information:** Contains text boxes for 'System Name' (EUM2000), 'System Contact' (www.waverider.com), and 'System Location' (Toronto, Ontario, Canada).
- DNS Servers:** Contains a 'DNS Domain Name' text box (jwaverider.com) and a list box with the IP address '192.168.111.11'. To the right of the list box are 'Add', 'Edit', and 'Delete' buttons.
- SNMP Communities:** Contains a table with two columns: 'Community String' and 'Properties'. The table has two rows: 'public' with 'read' and 'private' with 'write'. To the right of the table are 'Add', 'Edit', and 'Delete' buttons.
- Trap Servers:** Contains a table with two columns: 'Trap Server IP Address' and 'Trap Community String'. The table has one row: '192.168.10.7' and 'New Trap Server'. To the right of the table are 'Add', 'Edit', and 'Delete' buttons.

At the bottom of the dialog, there are fields for 'Date Entered:' and 'Date Updated:', and buttons for 'Close', 'Restore', and 'Apply'. At the very bottom, there are 'Status:' and 'Settings:' labels.

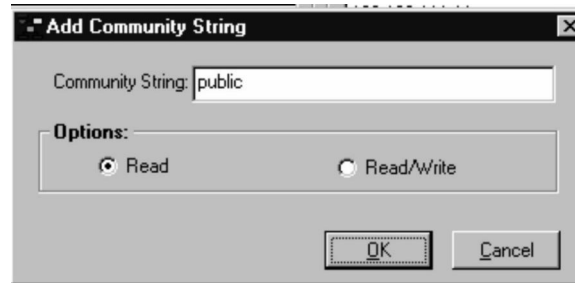
7.5.1 Configuring SNMP Properties

The following procedures describe how to configure standard SNMP security for read/write access to the EUM SNMP agent.

To Add an SNMP Community

1. Click **Add** in the **SNMP Communities** group.

Figure 81 Add Community String



2. In the **Add Community String** dialog box, type a new community in the **Community String** box.
3. Select **Read** or **Read/Write** to define the type of community you want to add.
4. Click **OK**.

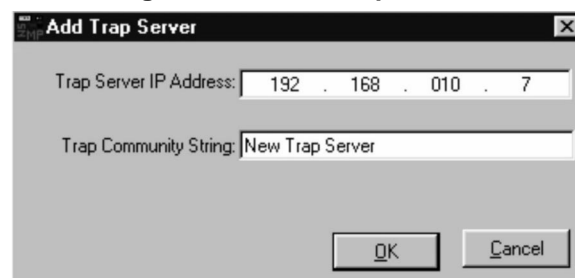
The community is added to the **SNMP Communities** list.

5. Click **Apply** to save the changes to the database.

To Add an SNMP Trap Server

1. Click **Add** in the **Trap Servers** group.

Figure 82 Add Trap Server



2. In the **Add Trap Server** dialog box, type a new IP Address in the **Trap Server IP Address** box.
3. Type a new name in the **Trap Community String** box to define the name of the community on the Trap Server.
4. Click **OK**.

The Trap Server is added to the **Trap Servers** list.

- Click **Apply** to save the changes to the database.

7.5.2 Configuring DNS Server Options

Configuring DNS Server for your LMS2000 network is optional, depending on whether you have a DNS Server on your network. A DNS Server resolves host names to IP addresses, so you can use host names when using Telnet or sending ping messages to a device.

When you configure DNS Server options for an EUM, provide the IP address of the DNS server and host name for the EUM. Each DNS Server defined in the list will then recognize the EUM by both its IP address and its host name.

To Assign a Host Name to an EUM

- In the **EUM Properties** dialog box, click the **SNMP/RADIUS** tab.

Figure 83 End User Modem Properties—SNMP/RADIUS Tab

The screenshot shows the 'End User Modem Properties: CCU1-EUM1' dialog box with the 'SNMP/RADIUS' tab selected. The dialog is divided into several sections:

- General SNMP Information:**
 - System Name: EUM2000
 - System Contact: www.waverider.com
 - System Location: Toronto, Ontario, Canada
- SNMP Communities:**

Community String	Properties
public	read
private	write
- Trap Servers:**

Trap Server IP Address	Trap Community String
192.168.10.7	New Trap Server
- DNS Servers:**
 - DNS Domain Name: jwaverider.com
 - 192.168.111.11

At the bottom, there are fields for 'Date Entered:' and 'Date Updated:', and buttons for 'Close', 'Restore', and 'Apply'. A 'Status:' field and a 'Settings:' button are also present at the very bottom.

- In the **DNS Servers** group, type a unique host name for the EUM in the **DNS Domain Server** field.

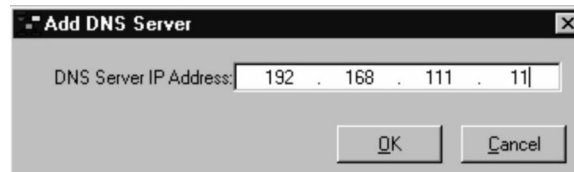
NOTE: A host name can be a maximum of 256 ASCII characters.

- Click **Apply** to save the changes to the database.

To Add a DNS Server

1. Click **Add** in the **DNS Servers** group.

Figure 84 Add DNS Server



2. In the **DNS Server IP Address** field, type the IP address of the DNS server.
3. Click **OK**.

The IP address is added to the **DNS Servers** list.

4. Repeat steps 1-3 for every DNS Server in your network.

NOTE: You may define up to 5 DNS Servers in your network.

5. Click **Apply** to save the changes to the database.

7.6 Saving the EUM Configuration to a File

At this point, you have finished configuring the EUM record in the NMS software. You can optionally save the EUM configuration to a file for use as a basic configuration that you can use to configure other EUMs.

When you want to retrieve this configuration, click the **Load Configuration File** icon on the task bar and locate the file in the **Open** dialog box. The settings will load into the NMS software and can be modified and downloaded from the file to another EUM.

To Save the Configuration

1. When you have finished configuring the properties for the EUM, click **Save**.
2. In the **Save Configuration to File** dialog box, type the filename for the EUM configuration settings.


The .ncl extension will be added to the file name automatically.

3. Save the file to a directory on the NMS Workstation or to a floppy disk.

7.7 Uploading the Configuration to the EUM

Once you configure the EUM record in the NMS software, upload that configuration to the physical device using the following procedure.

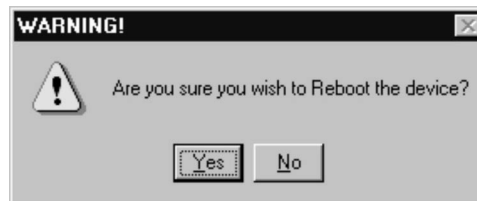
To Upload an EUM Configuration to the Device

1. In the NMS software, open the Properties screen for the EUM.
2. Change the device configuration as necessary.
3. Click **Apply** to save changes to the database.
4. Click  to upload the changes.

As FTP uploads the configuration, status messages appear in the status bar on the Properties screen.

After the upload is complete, the Device Reboot Confirmation dialog box opens.

Figure 85 Device Reboot Confirmation Dialog Box



5. Click **Yes** to reboot the device.

The configuration is successfully updated.

7.8 Assigning a Subscriber and Service Level to an EUM

An account record defines the contact information for the individual or organization that is using the LMS2000 service. All subscribers must belong to accounts.

Subscriber records identify the individual or group that uses a specific EUM. Every active EUM must be assigned to one subscriber only.

Service Levels define the data rate available for a subscriber/EUM to connect to the network.

Account, Subscriber, and Service Level records are integral to deploying an EUM. The following list outlines the minimum requirements for an EUM to be deployed and functioning:

- EUM must be associated with an enabled Subscriber record.
- Account record to which the Subscriber record is associated must be enabled.
- EUM must be associated with a Service Level.
- EUM must be assigned to a CCU.

The following points describe the relationships between the various records associated with an EUM:

- An Account record may have many Subscriber records associated with it.
- A Subscriber record must have one (and only one) EUM record associated with it.
- An EUM record is associated with one Service Level record.
- A CCU record has many EUM records associated with it.

To Add an Account

1. In the NMS, right-click **Account** in the Network tree structure.
2. On the shortcut menu, click **Add New Account**.

Figure 86 Account Properties

The screenshot shows the 'Account Properties : AccountABC(1)' dialog box. It contains the following fields and controls:

- Account ID:** 1
- Enabled?:** ☒
- * Account Name:** AccountABC
- * Contact Name:** J. Smith
- Address 1:** 404, 111 Main Street
- Address 2:** 901 111 Main Street
- City:** City
- Province/State:** Ontario
- Country:** Canada
- Postal/Zip Code:** T2T 1T1
- Phone 1:** 01-1-403-999-9999
- Phone 2:** 01-1-403-999-9998
- Fax:** 01-1-403-999-8888
- Email:** JSmith@accountabc.com
- Comments:** (Empty text area)
- Date Entered:** 15-Apr-00
- Date Updated:** 30-May-00
- Buttons:** Close, Restore, Apply

3. Fill out the fields with the account contact information.

NOTE: The **Account Name** and **Contact Name** fields must be completed before you can save the record.

4. Select the **Enabled?** check box.
5. Click **Apply** to save the changes to the database.

To Add a Subscriber Record

1. In the **Accounts** tree structure, right-click the Account to which you want to add a subscriber.
2. Select **Add New Subscriber** from the shortcut menu.

Figure 87 Subscriber Properties

Subscriber Properties: J.Smith (3)

Account Name: CompanyABC

Subscriber ID: 3 ☒ Enabled?

EUM

eum101

* Contact Name: J.Smith

Address 1: 14 Rose Street

Address 2: 18 4th Ave

City: RoseTown Province/State: North Carolina

Country: USA Postal/Zip Code: 20018

Phone 1: 555-555-5555 Phone 2: 555-555-5556

Fax: 555-555-5557 Email: jsmith@companyabc.com

Comments:

Date Entered: 11-Jun-00 Date Updated: 11-Jun-00

3. Fill out the fields with the subscriber information.

NOTE: The **Contact Name** field must be completed before you can save the record.

4. From the **EUM** drop-down list, select an EUM for the subscriber.
5. Select the **Enabled?** check box.

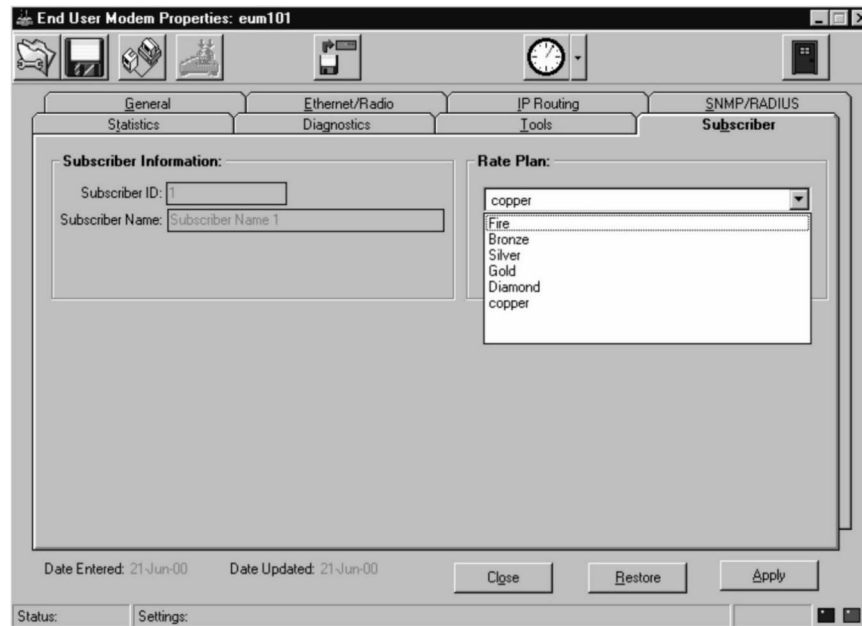
NOTE: You cannot select this check box if the Account to which the Subscriber is assigned has been disabled.


6. Click **Apply** to save the changes to the database.

To Assign a Service Level

1. Click the **Subscriber** tab in the **End User Modem Properties** dialog box.

Figure 88 End User Modem Properties—Subscriber Tab



2. From the drop-down list, select a **Rate Plan** to apply to the EUM.
3. Click **Apply** to save the changes to the database.
4. Click **Close**.
5. Open the **NAP Router Properties** screen.
6. Click  to upload the changes to the NAP Router.

7.9 Adding an EUM to a CCU Record

An EUM and a CCU communicate through a radio connection. After the EUM has been configured, update the CCU configuration with the new EUM information.

NOTE: A CCU can communicate with a maximum of 30 EUMs.

To Add an EUM to a CCU Record

1. Right-click the CCU in the NMS tree structure and select **Properties**.
2. Click the **Ethernet/Radio** tab.

Figure 89 Channel Unit Properties—Ethernet/Radio Tab

The screenshot shows the 'Channel Unit Properties: CCU-1' dialog box with the 'Ethernet/Radio' tab selected. The dialog is divided into several sections:

- Network Addressing:** IP Address: 192 . 168 . 10 . 13, Netmask: 24 (dropdown), 255.255.255.0.
- Radio Addressing:** IP Address: 192 . 168 . 110 . 1.
- Radio Parameters:**
 - Regulatory Domain: FCC (dropdown).
 - Radio Channel Parameters: Radio Enabled (checkbox), Radio Channel: 3 (dropdown), 2422 MHz.
 - Local CCU ID: * Local ID: 1010 (dropdown).
- EUM IDs:** A table with columns 'Unit ID' and 'Destination Radio IP'. It contains one entry: Unit ID 101, Destination Radio IP 192.168.110.2. There are 'Add', 'Edit', and 'Delete' buttons to the right of the table.

At the bottom, there are fields for 'Date Entered: 25-Jul-00' and 'Date Updated: 26-Jul-00', and buttons for 'Close', 'Restore', and 'Apply'. A 'Status:' and 'Settings:' section is at the very bottom.

3. Click **Add** in the **EUM IDs** group.

Figure 90 Add Unit Dialog Box

The screenshot shows the 'Add Unit' dialog box. It has two main input fields:

- ID:** A text box with the value '1' and a dropdown arrow.
- Radio IP Address:** A text box with the value '0 . 0 . 0 . 0'.

At the bottom, there are 'OK' and 'Cancel' buttons.

4. In the **ID** box, type the **Local ID** for the EUM.
5. In the **Radio IP Address** box, type the Radio IP Address for the EUM.

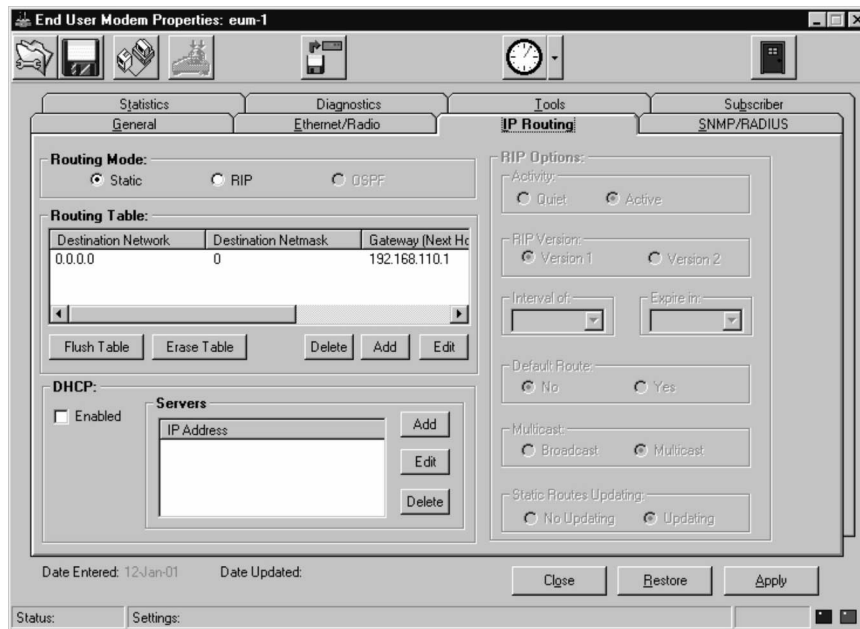
6. Click **OK**.
7. Click **Apply** to save the changes to the database.

To Add an EUM to the CCU Routing Table

NOTE: If you already added the EUM to the routing table for the CCU in [Configuring the IP Routing Properties](#), on page 76, then you do not need to complete this procedure.

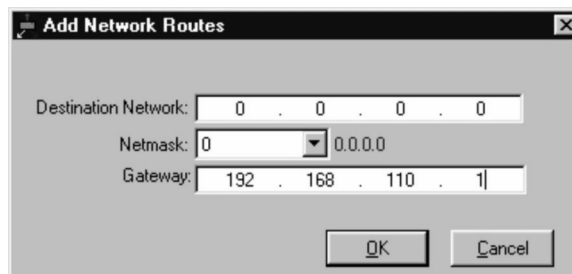
1. Click the **IP Routing** tab.

Figure 91 End User Modem Properties—IP Routing Tab



2. Click **Add** in the Routing Table group.

Figure 92 Add Network Routes Dialog Box



3. In the **Destination Network** box, type the network IP address of the subscriber's PC or network.



TIP: Use 0.0.0.0 as a **Destination Network** for any device that communicates with the CCU through the NAP router.


4. Select the appropriate **Netmask** for the destination from the drop-down list.
5. Type an IP address for the Gateway in the **Gateway** box.



TIP: Use the radio IP address of the EUM as a gateway from the CCU to the subscriber's PC or network.

6. Click **OK**.


You have successfully added the route to the routing table.

7. Repeat steps 3 through 6 until you have added every EUM on the CCU network, as a gateway in the routing table.
8. Click **Apply** to save the changes to the database.
9. Click  to upload the changes to the CCU.

7.10 Changing the Ethernet IP Address

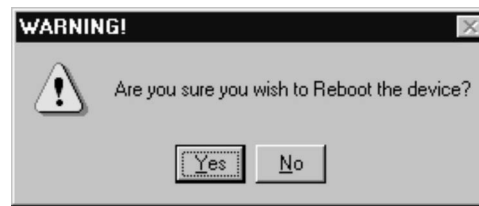
At this point, the EUM is configured with the Ethernet address to communicate with the NMS workstation, which will not enable the EUM to communicate with the subscriber's network or PC once it has been deployed. Change the Ethernet address of the EUM as a last stage before deployment.

To Change the Ethernet IP Address

1. Open the **End User Modem Properties** dialog box for the EUM, and click the **Ethernet/Radio** tab.
2. In the **Network Addressing** group, change the **IP Address** and **Netmask** to an IP address on the subscriber's network.
3. Click **Apply** to save the changes to the database.
4. Click  to upload the changes.

As FTP uploads the configuration, status messages appear in the status bar on the Properties screen.

After the upload is complete, the Device Reboot Confirmation dialog box opens.

Figure 93 Device Reboot Confirmation Dialog Box

5. Click **Yes** to reboot the device.

The configuration is successfully updated.

7.11 Deploying an EUM

Once you have configured an EUM and uploaded the configuration to the device, it is ready to deploy in the field. At the site, complete the following procedure to set up the EUM connections.

To Deploy an EUM

1. Connect one end of an RJ-45 straight-through cable to the Ethernet port on the EUM.
2. Connect the other end into an Ethernet connection on the subscriber's PC or network.
3. Terminate the EUM by attaching an antenna to the unit's antenna lead.

NOTE: The EUM radio transmission capabilities are disabled prior to shipment to prevent equipment damage. However, as a general precaution, WaveRider recommends that you always connect the antenna or load before connecting to a power source.

WARNING!



Antennas and associated transmission cable must be installed by qualified personnel. Failure to terminate the antenna port correctly can permanently damage the EUM. WaveRider assumes no liability for failure to adhere to this recommendation or to recognized general safety precautions.

4. Plug the EUM into an AC power source.
5. Confirm the following conditions on the EUM.
 - Red power LED is on.
 - Green network link LED is on.
 - Cooling fan is operating.

8

Configuring RFSM

RFSM is the radio frequency switching matrix—a device that resides within the CAP. CCUs and their associated antennas connect through the RFSM. The RFSM facilitates redundancy of CCUs. It uses polling engines to monitor CCU health. If a CCU fails, the RFSM automatically configures the backup CCU to operate as the failed CCU until the unit can be replaced.

The following diagrams illustrate how the RFSM switches over to the backup CCU whenever an operating CCU fails. [Figure 94](#) shows each of the CCUs connected to antennas through the RFSM under normal conditions. [Figure 95](#) shows that CCU 3 has failed and its antenna has been re-routed to the backup CCU, which is operating as CCU 3.

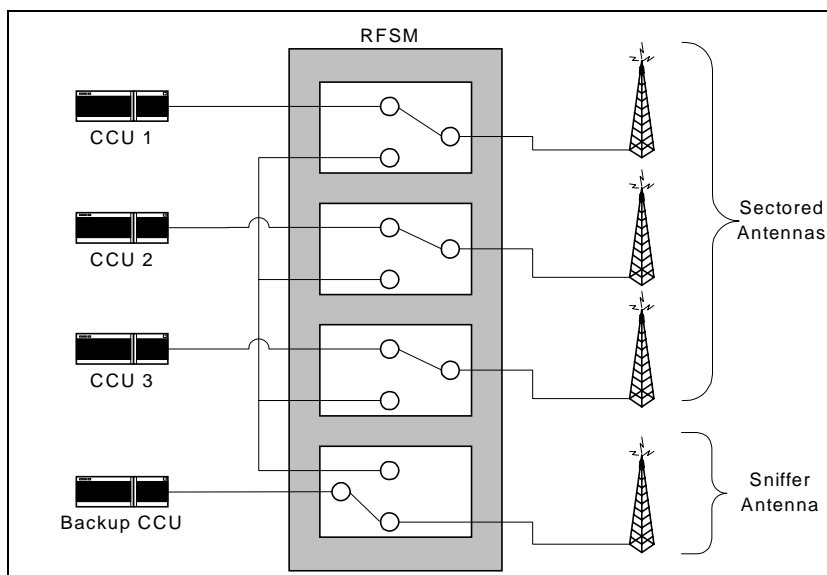
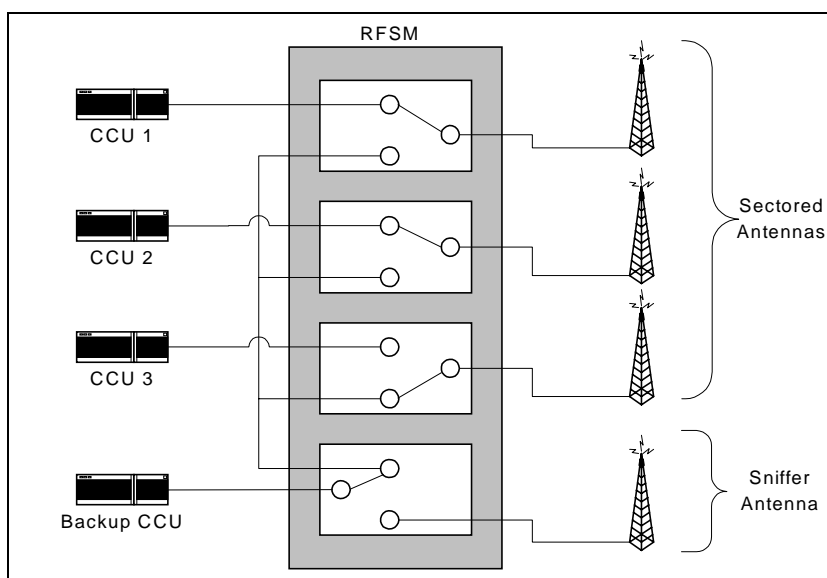
Figure 94 RFSM Connections Under Normal Conditions**Figure 95 RFSM Connections Under Switch Conditions**

Table 5 describes each of the symbols on the RFSM device and in the RFSM Properties screen within the NMS.

Table 5 RFSM Symbols—Front Plane













Symbol	What it represents
	A light-emitting diode (LED) on the RFSM.
	An antenna port on the RFSM. The number in the square indicates whether it is the antenna port for CCU 1, 2, or 3.
	The antenna port for the backup CCU.
	Status of the RFSM CPU. This light is green whenever the RFSM CPU is running.
	Power supply of the RFSM. This light is green whenever the RFSM is connected to a power source.
	RFSM output. (Reserved for future LMS2000 functionality.)
	RFSM input. (Reserved for future LMS2000 functionality.)

Table 6 RFSM Symbols—Back Plane

Symbol	What it represents
	RF Port for CCU 1. (Those marked 2 and 3 are for CCUs 2 and 3 respectively.)
	Antenna port for CCU 1. (Those marked 2 and 3 are for CCUs 2 and 3 respectively.)
	RF Port for backup CCU.
	Port for sniffer antenna.
	Unused port.

8.1 Installing an RFSM into a CAP

If you purchased a CAP with an RFSM pre-installed, you do not need to use the procedures described in this section. Proceed directly to the next section, [Configuring the RFSM](#), on page 115.

If you are installing an RFSM into an existing CAP, follow the procedures in this section. Install an RFSM in each CAP. Once you have installed the RFSM units, change the IP addresses using the command line interface, and then configure them through the NMS. Instructions for these procedures are included on the following pages.

WARNING!



When adding an RFSM to an existing CAP, the existing EUMs and CCUs must be fully configured before you configure the RFSM in the NMS. Once you have the RFSM installed and configured, you can safely add new CCUs and EUMs.

[Figure 96](#) and [Figure 97](#) describe the components of the RFSM front and back planes.

Figure 96 RFSM Front Plane

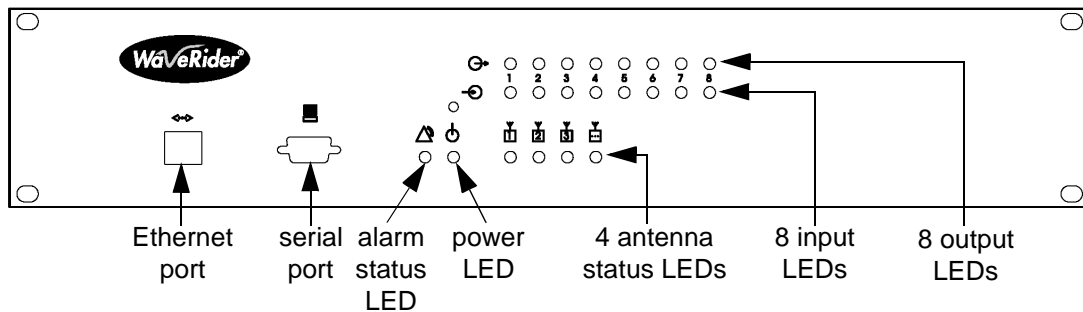
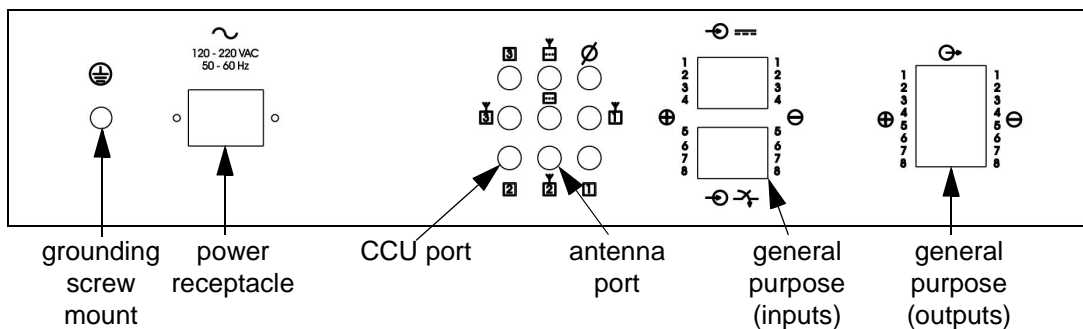


Figure 97 RFSM Back Plane



To Install the RFSM into the CAP

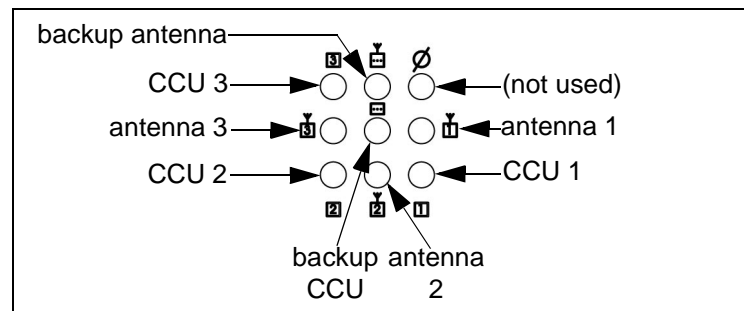
1. Power down all radios.
2. Remove the CCU RF cables from the copper plate and the CCU.
3. Place two rail clips on each rail at the front of the cabinet for the screws.
 - Fourth hole from top on both sides.
 - Ninth hole from top on both sides.
4. Position the RFSM in the rack.
5. Screw the RFSM into the rail clips.
6. Install surge protectors into the copper plate.
7. Connect RF cables from the surge protectors to the RFSM antenna ports as shown in [Figure 98](#).
8. Connect RF cables from the CCU into each of the RFSM CCU ports as shown in [Figure 98](#).

NOTE: Ensure the reverse SMA end goes to the CCU.

9. Connect a terminator to the blank RF port as shown in [Figure 98](#).

NOTE: For neatness, loop the RF cables once and fasten them with a cable tie.

Figure 98 RF Cable Ports on RFSM Backplane



10. Attach an Ethernet cable from the CAP Ethernet switch into the Ethernet port on the RFSM, running the cable along the inside of the CAP rail.

NOTE: It is assumed that the CCUs are already connected to the CAP Ethernet switch with Ethernet cables.

11. Plug the RFSM power cord into the CAP power bar.
12. Ensure the light for the RFSM port on the Ethernet switch is green.

NOTE: If the light is orange, plug the RFSM Ethernet cable into a different port on the switch.

8.1.1 Changing the IP Address of the RFSM

The Network IP address is the IP address for the RFSM device itself. The first and last octets of the Network IP address must not contain 255 or 0. The following list shows four Network IP addresses that would not be allowed:

- 255.xxx.xxx.xxx
- 0.xxx.xxx.xxx
- xxx.xxx.xxx.0
- xxx.xxx.xxx.255

For a list of configuration defaults for RFSM units, please refer to [Device Configuration Defaults](#), on page 291.

NOTE: For information about RFSM command line syntax, please refer to [Entering RFSM Commands](#), on page 312.

To Change the IP Address of the RFSM

1. Use a serial cable or null modem cable to connect a terminal to the DB9 console port on the RFSM.
2. Start a computer terminal-emulation program, such as HyperTerminal.

NOTE: When completing the following steps, you may not see your keystrokes displayed on the screen.

3. Select the communications port that you are using to connect to the device.
4. Configure the communications parameters as follows:
 - Bits per second = 9600
 - Data bits = 8
 - Parity = None
 - Stop bits = 1
 - Flow control = None
5. At the : prompt, type the password for the device.

The default password is PASSWORD, all uppercase.

NOTE: When typing your password, the screen will not display your keystrokes.

6. At the ? prompt, type **S10=<ip address>** and press **Enter** to set the Ethernet IP address of the RFSM. (For example, **S10=192.168.010.012.**)

For the RFSM, all octets must be three digits.

NOTE: To determine which Ethernet IP, Netmask, and Gateway to assign to the RFSM, refer to [Device Configuration Defaults](#), on page 291.

7. At the ? prompt, type **S11=<netmask>** and press **Enter** to set the netmask.
8. At the ? prompt, type **S12=<gateway>** and press **Enter** to set the default gateway IP address.
9. At the ? prompt, type **X** and press **Enter** to save the changes to the RFSM.
10. At the ? prompt, type **R** and press **Enter** to reboot the RFSM.
11. Disconnect the serial cable from the RFSM.

8.2 Configuring the RFSM

Each CAP contains a single RFSM. If you purchased a CAP with an RFSM unit included, the RFSM record in the NMS will contain pre-configured defaults. If you are adding a new RFSM unit to an existing CAP, it will not contain default values. The procedure in this section describes configuring an RFSM record under both circumstances.

The following fields are required on the RFSM record:

- Switch Matrix Name
- Network IP
- Netmask
- Gateway

NOTE: The first and last octets of the Network IP address must not contain 255 or 0.

The Network IP address is the IP address for the RFSM device itself. The following list shows four Network IP addresses that would not be allowed:

- 255.xxx.xxx.xxx
- 0.xxx.xxx.xxx
- xxx.xxx.xxx.0
- xxx.xxx.xxx.255

For a list of configuration defaults for RFSM units, please refer to [Device Configuration Defaults](#), on page 291.

To Configure an RFSM

1. In the **LMS2000** branch of the NMS software, right-click the CAP and select **Add New Device**.
2. From the shortcut menu, select **RF Switch Matrix**.

A new RFSM screen opens.

Figure 99 RFSM Properties—General Tab

RFSM Maintenance

CAP: LMS2000 CAP

General | RFSM Control | Switch Control

General Information

Switch Matrix ID: 1 Active Status: ☒

* Switch Matrix Name: HOSTNAME Description:

Comments:

Password

Current Password: New Password: Retype:

Apply Clear

Address

* Network IP: 192 . 168 . 10 . 12

Netmask: 24 255.255.255.0

Gateway: 192 . 168 . 10 . 1

Switched IP: 192 . 168 . 10 . 16

FirmWare

Version: 1.02 Date: 21-Aug-00

Close Restore Apply

Disconnected Ready

3. In the **Switch Matrix Name** field, type a name that uniquely identifies the device.

NOTE: The name must be eight alphanumeric characters, all uppercase.
The default is HOSTNAME.

4. Verify that the following fields have been defined correctly.
- Network IP
 - Netmask
 - Gateway


They should match the settings indicated in [Device Configuration Defaults](#), on page 291.

If these fields are already defined correctly, proceed to step 7.

5. If the Network IP, Netmask, and Gateway fields are blank, define them to match the settings in [Device Configuration Defaults](#), on page 291.
6. Click **Apply** to save the changes to the database.

7. Click  to connect to the RFSM.

8. Click **Apply** again.

9. Click  to upload the changes to the RFSM.

The new RFSM record has now been saved in the database.

8.2.1 Changing the RFSM Password

By default, the RFSM password is PASSWORD, all uppercase. Change the password when you create a new RFSM record.



CAUTION: The password must be exactly eight alphanumeric characters. It may be upper or lowercase, but it is case sensitive.

To Change the RFSM Password

1. Open the **RFSM** screen.

Figure 100 RFSM Properties—General Tab

The screenshot shows the 'RFSM Maintenance' window with the 'General' tab selected. The 'CAP' field is set to 'LMS2000 CAP'. The 'General Information' section includes 'Switch Matrix ID' (1), 'Switch Matrix Name' (HOSTNAME), 'Description' (empty), and 'Comments' (empty). The 'Active Status' checkbox is checked. The 'Password' section has 'Current Password' (masked), 'New Password' (empty), and 'Retype' (empty). The 'Address' section has 'Network IP' (192.168.10.12), 'Netmask' (24, 255.255.255.0), 'Gateway' (192.168.10.1), and 'Switched IP' (192.168.10.16). The 'Firmware' section has 'Version' (1.02) and 'Date' (21-Aug-00). Buttons for 'Apply', 'Clear', 'Close', 'Restore', and 'Apply' are at the bottom right. The status bar at the bottom shows 'Disconnected' and 'Ready'.

2. Click  to connect to the RFSM.



CAUTION: You must be connected to the RFSM before you change the password. If you change the password while disconnected, you will be unable to re-establish a connection.


3. Type the new password in both the **New Password** and **Retype** fields.
4. Click **Apply** to save the changes to the database.

The Password Change dialog box opens.

Figure 101 Password Change Dialog Box



5. Click **OK** to accept the password change.

6. Click  to upload the changes to the RFSM.

The password has now been changed.

8.3 Configuring CCU Connections to the RFSM

Each CCU in the CAP, including the backup CCU, must be assigned to an RFSM antenna port. The CCU connects to EUMs through this port. In the NMS record, the connections between the CCUs and the antenna ports must reflect the physical connections.

Connecting a CCU to the RFSM is a two-step process:

- Assign a CCU to an antenna port.
- Activate RFSM polling of the CCU.

Once you have completed these procedures, the CCU and its connected EUMs can begin passing traffic.



CAUTION: When assigning CCUs to RFSM antenna ports in the NMS, ensure that the antenna assignments reflect the physical connections.

For more information about RFSM, please refer to [Operating RFSM](#), on page 211.

To Assign a CCU to an Antenna Port


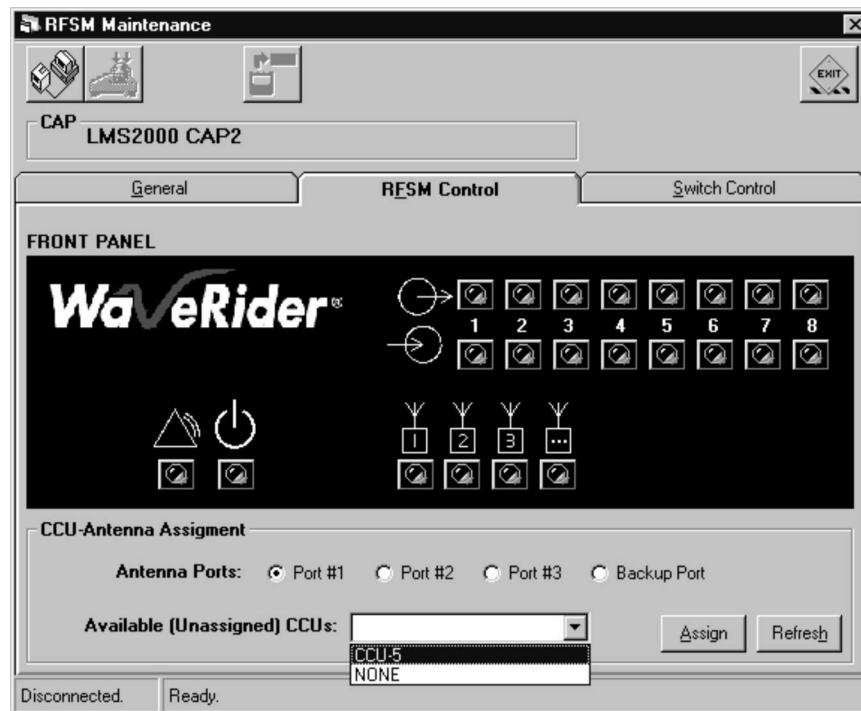
1. Open the **RFSM** screen, and click the **RFSM Control** tab.
2. If you are not already connected to the RFSM, click  to connect.
3. In the **CCU-Antenna Assignment** group, select the **Port #1** option.

Figure 102 RFSM CCU-Antenna Assignment



NOTE: Functionality for the 16 input/output LEDs will be incorporated into future revisions of the NMS.

- From the **Available (Unassigned) CCUs** drop-down list, select the CCU that is connected to port 1 on the RFSM.


NOTE: Only unassigned CCUs residing within that CAP appear in the list.

- Click the **Assign** button.

NOTE: If you click a port to which a CCU has already been assigned, you will see an error message.

The CCU is now assigned to the antenna port.

- Repeat this procedure for every CCU in the CAP, assigning CCUs to antenna ports that reflect the physical configuration.

- Click  to upload the changes to the RFSM.

To Activate RFSM Polling of a CCU



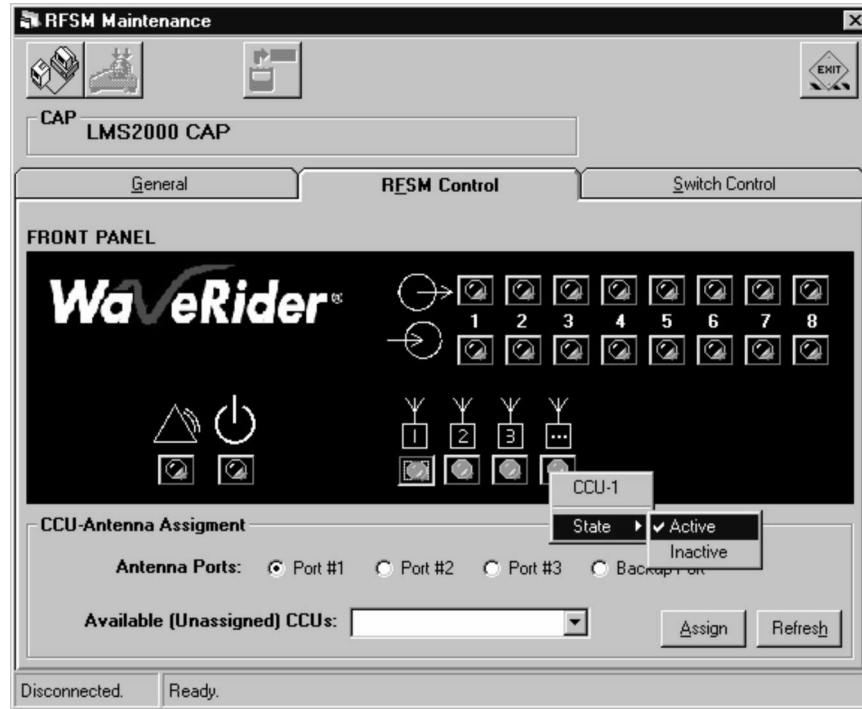
1. If you are not already connected to the RFSM, click  to connect.
2. On the **RFSM Control** tab of the RFSM screen, right-click  for the CCU you want to activate.

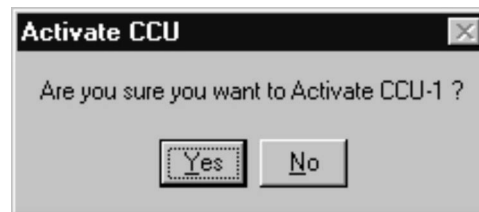
Figure 103 Activate CCU Shortcut Menu



3. On the shortcut menu, select **State > Active**.

The **Activate CCU** dialog box opens.

Figure 104 Activate CCU Dialog Box



4. Click **Yes** to activate CCU polling.

NOTE: When CCU redundancy is activated, a check mark appears beside the word “Active” in the shortcut menu.


5. Repeat this procedure for every antenna port.

When you activate polling for the Backup CCU, the following dialog box opens.

Figure 105 RFSM Backup Antenna Reminder



This is just a reminder that your RFSM should have an RF cable for an antenna connected to the backup port.

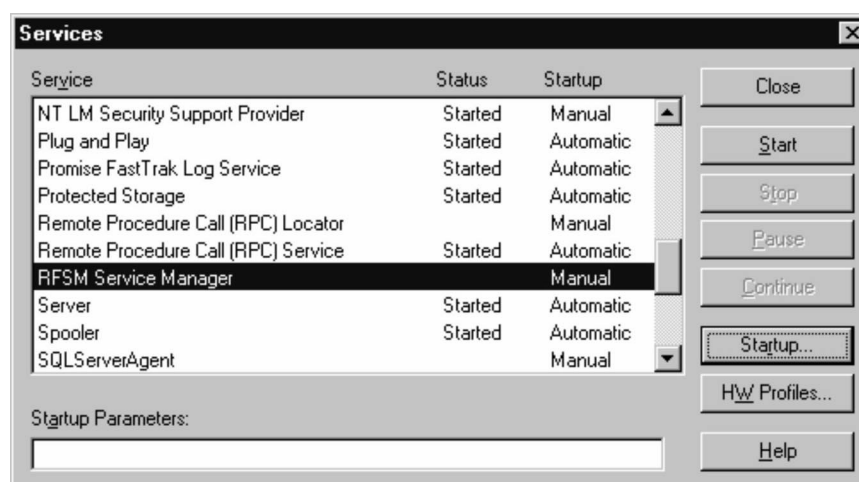
6. Click **OK** to close the dialog box.
7. Click  to upload the changes to the RFSM.

8.4 Starting the RFSM Service

Once you have installed and configured the RFSM, you must start the RFSM service in Windows NT. You must also configure the RFSM service to start automatically every time you log on to Windows NT.

To Start the RFSM Service

1. Click the **Start** button.
2. Select **Settings > Control Panel**.
The Control Panel window opens.
3. In the Control Panel window, double-click the **Services** icon.

Figure 106 RFSM Service Manager in Services Window

4. Scroll down to RFSM Service Manager and select it.

Note that the service is currently set to Manual startup.

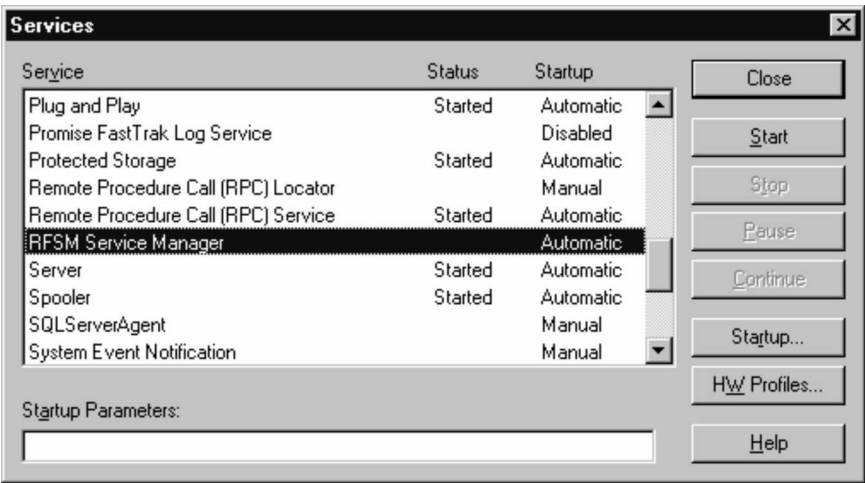
5. Click the **Startup** button.

Figure 107 Service Startup Dialog Box

6. In the **Service Startup** dialog box, select **Automatic** from the Startup Type group.

7. Click **OK**.

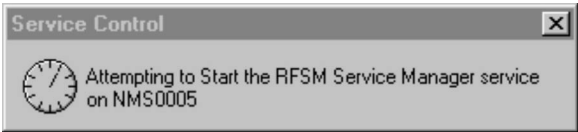
Figure 108 RFSM Service Manager in Services Window




- 8. Ensure the **RFSM Service Manager** is still selected.
- 9. Click **Start**.

While the Service Control is starting the RFSM Service Manager, you will see the following window.

Figure 109 Service Control



When the service is started, the status changes to Started and the  icon appears in the Windows task bar.


- 10. Click **Close** in the **Services** window.
- 11. Close the **Control Panel** window.

8.5 Verifying the Polling Engine is Running

Each RFSM uses a polling engine, which runs in the background and monitors CCU status. There is one polling engine for each CAP. These polling engines start automatically when you start the NMS, but you should verify that they are running.

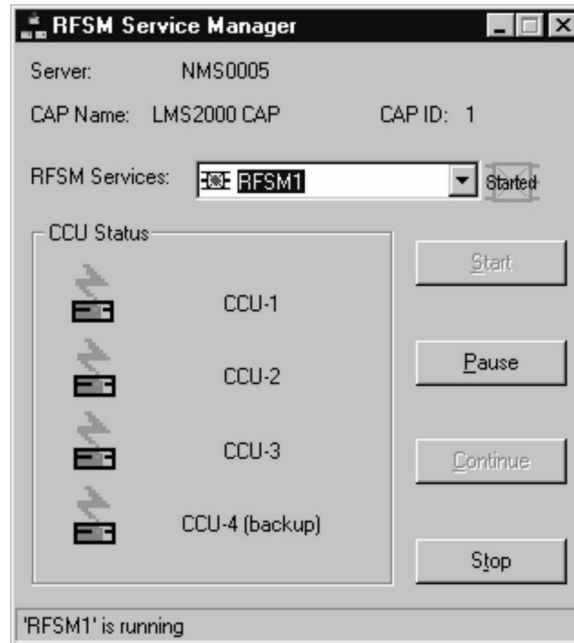
If a polling engine is not running, you will have to restart it from the RFSM Service Manager. The following procedures explain how to verify a polling engine is running and restart an RFSM polling engine.

To Verify the Polling Engine is Running

1. In the Windows system tray, in the bottom right corner, double-click the  icon to open the RFSM Service Manager window.

NOTE: If the icon does not appear in your system tray, you must restart the RFSM Service Manager as described in [To Start the RFSM Service](#), on page 121.


Figure 110 RFSM Service Manager



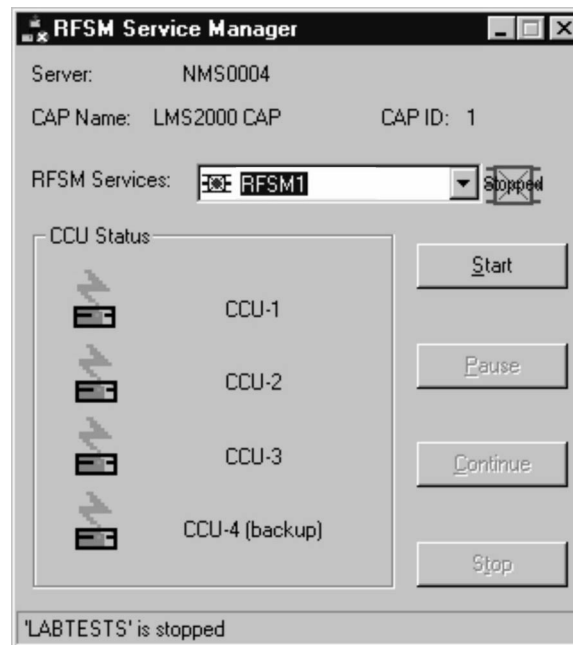
2. From the **RFSM Services** drop-down list, select the RFSM unit for which to verify polling engine status.
3. Verify that the **Started** icon appears beside the drop-down list.

If the **Stopped** icon appears, you will have to restart the polling engine for that RFSM unit, as described in the following procedure.

To Restart the RFSM Polling Engine

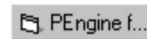
1. In the Windows system tray, double-click the  icon to open the RFSM Service Manager window.

NOTE: If the icon does not appear in your system tray, you must restart the RFSM Service Manager, as described in [To Start the RFSM Service](#), on page 121.

Figure 111 RFSM Service Manager

2. From the **RFSM Services** drop-down list, select the RFSM unit to start.
3. Click the **Start** button.

The status icon beside the RFSM Services drop-down list changes to **Started** and the **PEngine** icon appears in the Windows task bar.

Figure 112 PEngine Icon

8.6 Testing the Backup Antenna

The backup antenna is a necessary component of the RFSM polling engine functionality. In the event that the RFSM polling engine is able to poll a CCU, but unable to poll any of the EUMs connected to the CCU, the backup CCU will simulate an EUM to verify the CCU is functioning properly. The backup antenna is necessary for this verification process to occur, as it is an RF process. If the CCU is functional, there is no reason to switch the CCU configuration over to the backup.

The backup antenna—preferably a dipole antenna—can be placed inside the CAP cabinet. When the RFSM polling engine can poll a CCU, but not the EUMs attached to it, the backup antenna will provide an RF link between the backup CCU and the CCU.



CAUTION: Ideally, you should only conduct this test during initial system installation. Testing the backup antenna in this manner requires that there are no operational links between any CCUs and EUMs.

To Test the Backup Antenna

1. Ensure that the following conditions exist:
 - All CCUs are installed and properly configured.
 - RFSM is installed and properly configured.
 - EUMs have been configured in the NMS database, but no CCU-EUM radio links are operating.
 - Backup antenna, ideally a dipole antenna, is connected to the RFSM backup antenna port located in the CAP cabinet.
2. Ensure the RFSM polling engine is running. If it is not, start it. (For instructions on starting the RFSM polling engine, please refer to [To Restart the RFSM Polling Engine](#), on page 124.)
3. Allow the RFSM polling engine to run for at least one hour.
4. Monitor the system to verify that no CCUs switch their configuration over to the backup CCU.

9

Configuring the Advanced Bandwidth Manager

The LMS2000 system uses service policies to manage EUM bandwidth. The Advanced Bandwidth Manager (ABWM) is an option that provides additional control of data throughput to EUMs. It is server software that integrates bandwidth allocation, prioritization, metering, and usage charting. Throughout this document, the ABWM hardware is referred to as the controller.

Advanced Bandwidth Manager provides the following features:

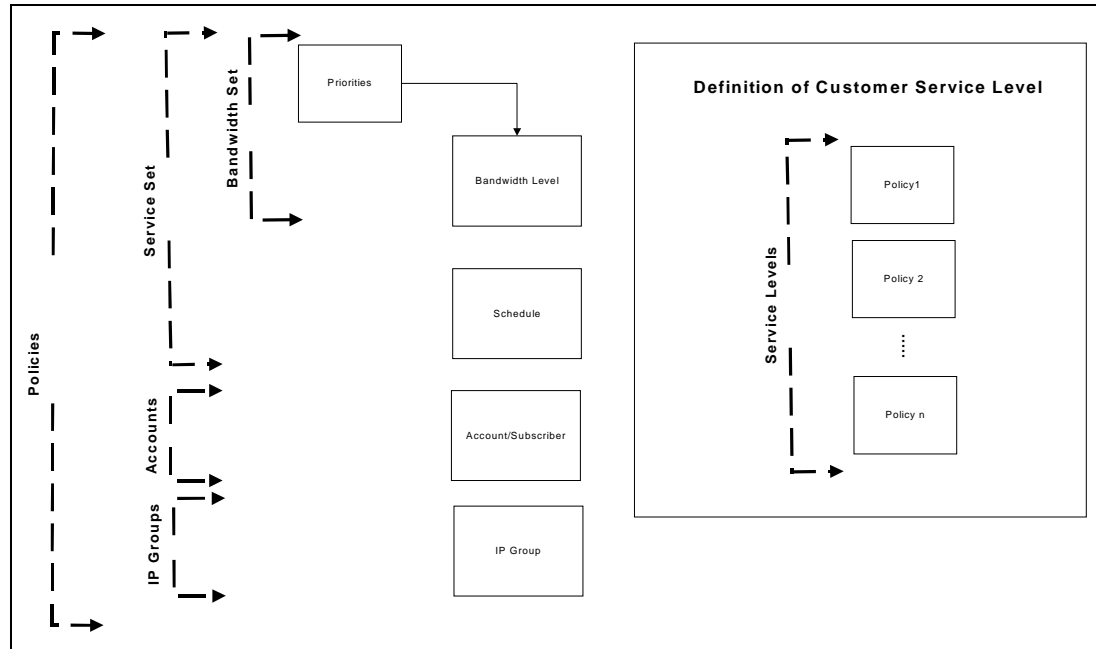
- Enables you to dynamically allocate, manage, prioritize, and control your bandwidth for up to 20,000 IP groups based on IP addresses
- Alerts you to unusual or sudden surges of bandwidth consumption to prevent usage abuse
- Provides an easy-to-use administration interface
- Enables you to use data collected by the controller for real-time charting
- Supports SNMP management functions
- Centralizes management of multiple distributed controllers through server-based software
- Supports password-protected access at several points
- Provides redundant configurations that maintain uninterrupted traffic flow, even if a controller fails.
- Manages bandwidth usage between IP ports, non-IP ports, and TCP ports
- Streamlines the importing and exporting of large amounts of subscriber information and usage data
- Provides a quick and easy method of creating classes of service and traffic policies

Setting up advanced bandwidth management in the NMS involves the following procedures:

1. *Installing iSurfRanger Hardware into the NAP*, on page 130
 - *Installing the iSurfRanger Controller*, on page 130
 - *Initializing the iSurfRanger Controller*, on page 132
 - *Connecting the Controller to the Network*, on page 134
 - *Installing a Dual Controller*, on page 135
 - *Installing Non-redundant Controllers*, on page 135
 - *Cabling a Serial Redundant Controller*, on page 136
 - *Cabling a Parallel Redundant Controller*, on page 137
2. *Adding a Bandwidth Manager Record to the NMS*, on page 138
3. *Defining Controller Properties*, on page 143
 - *Configuring Redundancy*, on page 143
 - *Configuring Bandwidth Controls*, on page 148
4. *Defining System Security Parameters*, on page 151
5. *Configuring Bandwidth Sets*, on page 153
 - *Setting Priorities*, on page 153
 - *Configuring a Bandwidth Set*, on page 155
6. *Establishing Schedules*, on page 160
7. *Setting a Traffic Policy*, on page 161

To aid your understanding of configuring the ABWM, [Figure 113](#) contains a flowchart of the relationship between the various ABWM elements.

Figure 113 Relationship Between ABWM Elements



Configuring advanced bandwidth manager policies requires you to define the following elements:

- **Priorities** are part of a bandwidth set, and they determine how quickly a user reaches its maximum burst rate (MBR).
- **Bandwidth levels** are also part of a bandwidth set and determines the bandwidth available to a user.
- **Schedules** establish a pattern of time(s) during which a traffic policy applies.
- In the context of ABWM, **subscribers**, or **accounts**, are billable entities that identify who to charge for specific portions of the bandwidth managed by the controller.
- An **IP group** is a collection of IP addresses associated with a subscriber.

These elements have the following associations:

- A bandwidth set is comprised of a priority and a bandwidth level.
- A service set is comprised of a bandwidth set and a schedule.
- A policy is comprised of a bandwidth set, a service, and account, and an IP group.
- Policies comprise a service level.

9.1 Installing iSurfRanger Hardware into the NAP

If your NAP includes a pre-installed ABWM controller, proceed directly to [Configuring Bandwidth Sets](#), on page 153.

Installing an iSurfRanger controller consists of the following general steps:

1. Connecting the controller.
2. Initializing the controller.
3. Connecting the controller to the network.

You can install an iSurfRanger controller in a network with no redundancy, with serial redundancy, or with parallel redundancy. Both serial and parallel redundancy provide fail-safe, non-stop operation.

9.1.1 Installing the iSurfRanger Controller

The following steps describe how to install an iSurfRanger controller containing a single module. If you are installing a dual controller or a redundant controller, see also the applicable directions later in this section.

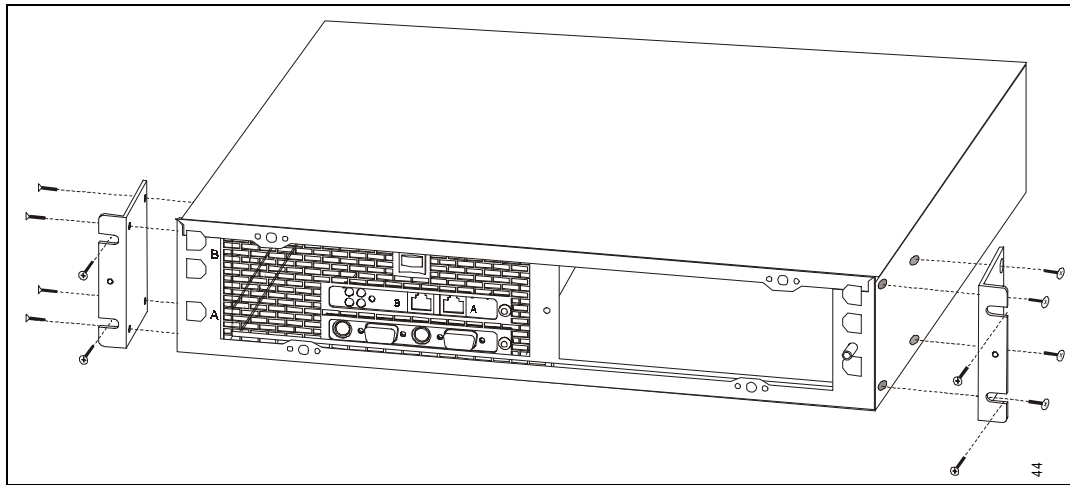
WARNING!



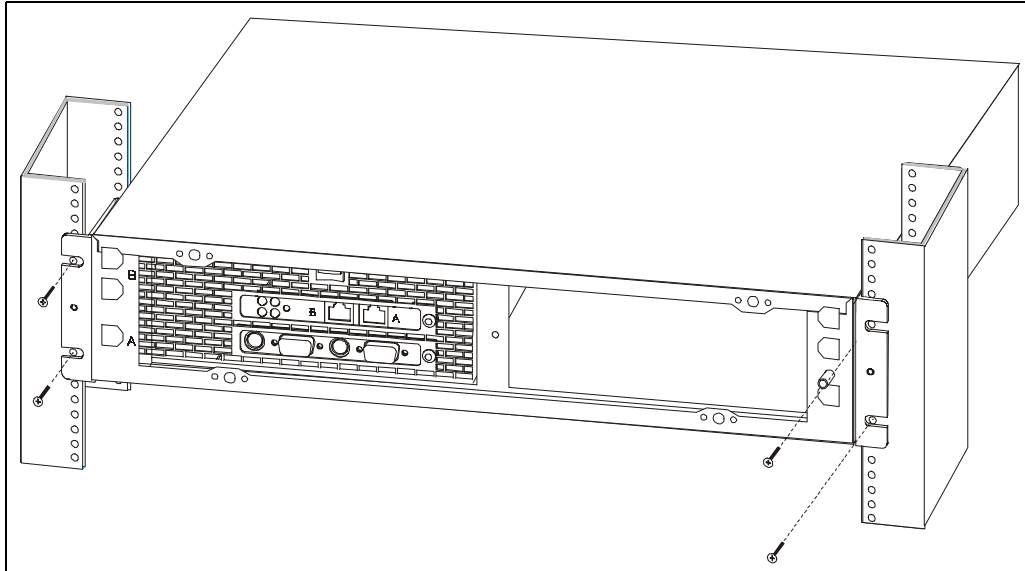
Failure to follow equipment installation instructions could damage the assembly and render the unit unusable. Read the entire procedure before installing.

To Install the iSurfRanger Controller into the NAP

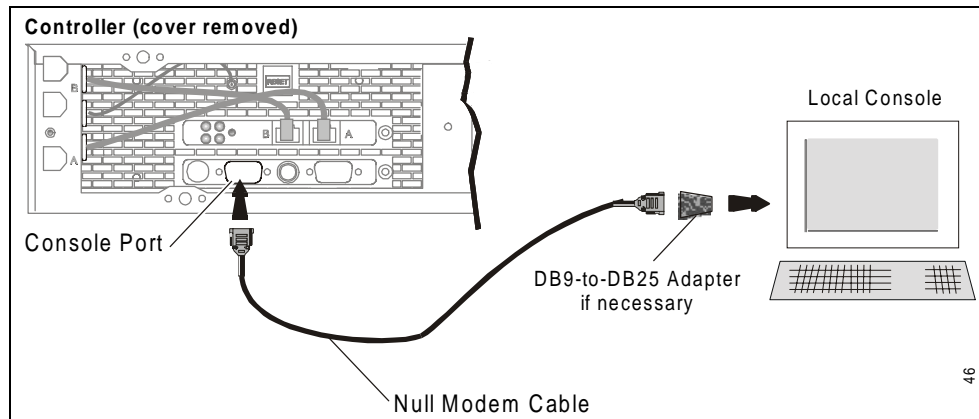
1. Place the iSurfRanger controller in the NAP rack.
2. Ensure the controller has adequate space around it for ventilation.
3. Attach the mounting brackets to the controller.

Figure 114 Attaching the Mounting Brackets

4. Mount the controller in the rack.

Figure 115 Mounting the Controller

5. Ensure the module in the controller and the NMS server are turned off.
6. Remove the cover from the front of the controller by grasping the cover on the top and bottom edges and firmly pulling it straight out.
7. Connect the null modem cable, and the DB-to-DB25 adapter if necessary, to the left console port on the module and to the NMS server.

Figure 116 Cabling the iSurfRanger Controller to the NMS

9.1.2 Initializing the iSurfRanger Controller

To Initialize the iSurfRanger Controller

1. Run terminal emulation software on the NMS.
2. Ensure the terminal's communication settings are as follows:
 - 38400 bps
 - 8 bit
 - no parity
 - 1 stop bit
3. Ensure the module in the controller is not connected to the network.
4. Turn on the module.
5. Wait a few seconds while the controller firmware starts processing.

NOTE: During the following procedure, respond to prompts and enter commands quickly. Slow responses cause the firmware to continue processing without allowing you to initialize the controller.

6. At the login prompt, type **isr**, which is a factory-set login name (case sensitive).
7. At the password prompt, type **amplify**, which is a factory-set password (case sensitive).
8. Press **Enter** to display the C:\> command line prompt.

An "init failure..." message appears, ending with the message "Switching to command line prompt." This is normal.

9. At the C:\> prompt, type **password** in lowercase.
10. At the present-login-name prompt, type **isr**.
11. At the preset-password prompt, type **amplify**.

12. At the new-login and new-password prompts, enter the new login name and new password of your choice.

NOTE: The new login name and new password can each be from 3-14 case-sensitive alphanumeric characters. You must enter this new login name and new password in the NMS to enable internal communication between the ABWM controller and the NMS. Once the ABWM has been added to the NMS, add the login name and password to the System/Security tab of the ABWM properties, as described in [To Specify a User Name and Password for Controllers](#), on page 152.

13. When prompted to update the name and password, type **y**.

The controller displays a message that the update (login name and password change) is complete.

14. Assign an IP address to the module by typing **chgip <address>** at the C:\> prompt.

NOTE: The IP address must be in the format a.b.c d. Ensure you type a space but no period between the c and d segments. This address is also required information for configuring the controller from the NMS. For this IP address and all other IP addresses required for configuring the iSurfRanger controller, the range for each of the four segments is from 1-254.

The controller displays miscellaneous initialization messages.

15. Ensure the IP address just entered is correct by typing **type conf** at the C:\> prompt:

The controller displays the IP address you just entered.

16. Turn off the module.

17. If the controller has two modules, repeat the preceding steps to initialize the second module.

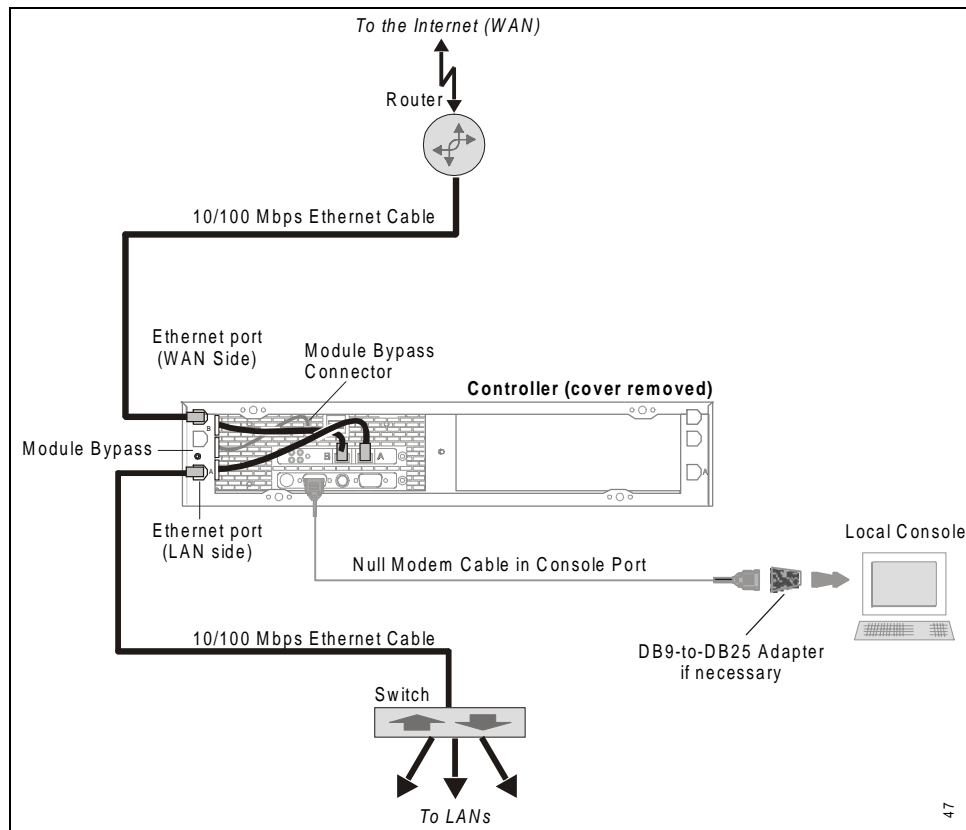
18. You can now connect the controller to the network at the current location or send it to another location for connecting.

9.1.3 Connecting the Controller to the Network

To Connect the Controller to the Network

1. Connect the module in the controller to the network at the “edge” that separates the WAN from the LAN.

Figure 117 ABWM Controller Cabling

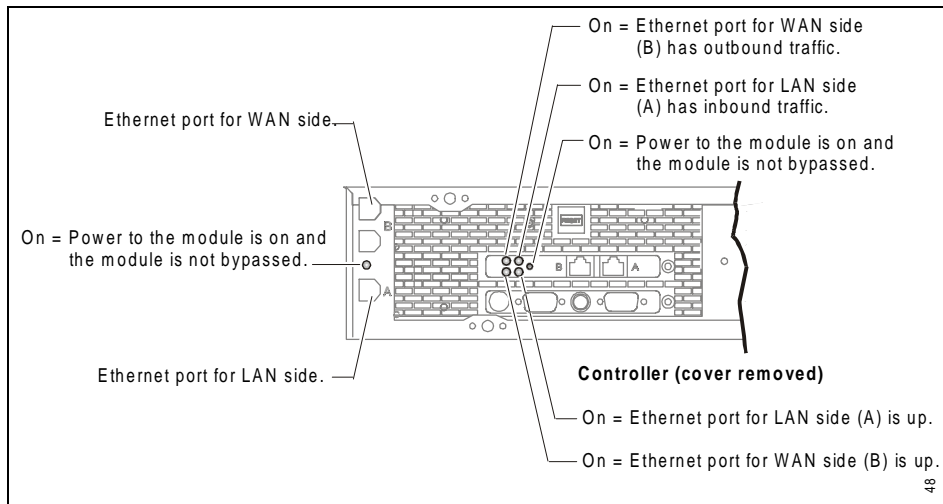


2. Turn on the module.

iSurfRanger controller cycles through the login prompt and other initialization messages at the NMS server, ending with the message Initialization Complete.

3. Check the lamps on the module front panel.

When the controller is operating correctly, lamp activity is as shown in [Figure 118](#).

Figure 118 ABWM Controller Lamp Activity

4. If lamps are on as shown in the following figure, install iSurfRanger controller software.

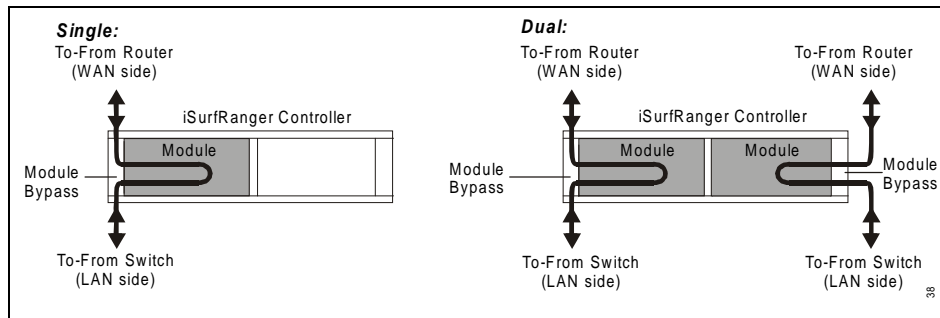
9.1.4 Installing a Dual Controller

A dual controller contains two modules that operate independently of each other. Neither of the modules in a dual controller is aware of the other. If this is how you want iSurfRanger controller to operate, simply repeat the preceding steps for the second module.

9.1.5 Installing Non-redundant Controllers

In non-redundant configurations you can have a single iSurfRanger controller (containing one module) or a dual iSurfRanger controller (containing two modules). When there is no redundancy, modules in a dual iSurfRanger controller operate independently of each other even though they are in the same controller.

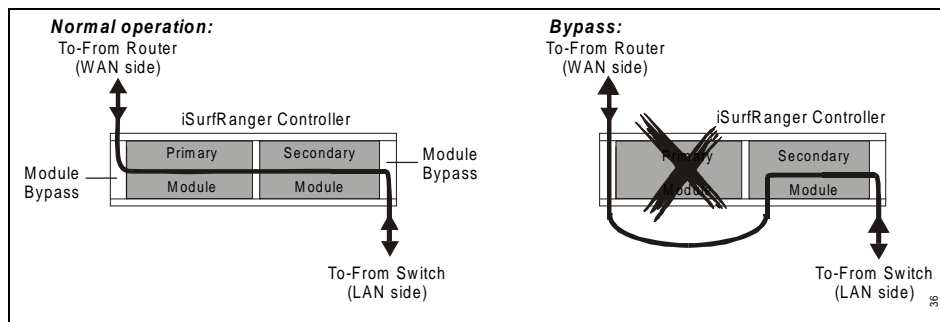
Traffic flows through a single or dual iSurfRanger controller as shown in [Figure 119](#).

Figure 119 iSurfRanger Controller Configured for No Redundancy

9.1.6 Cabling a Serial Redundant Controller

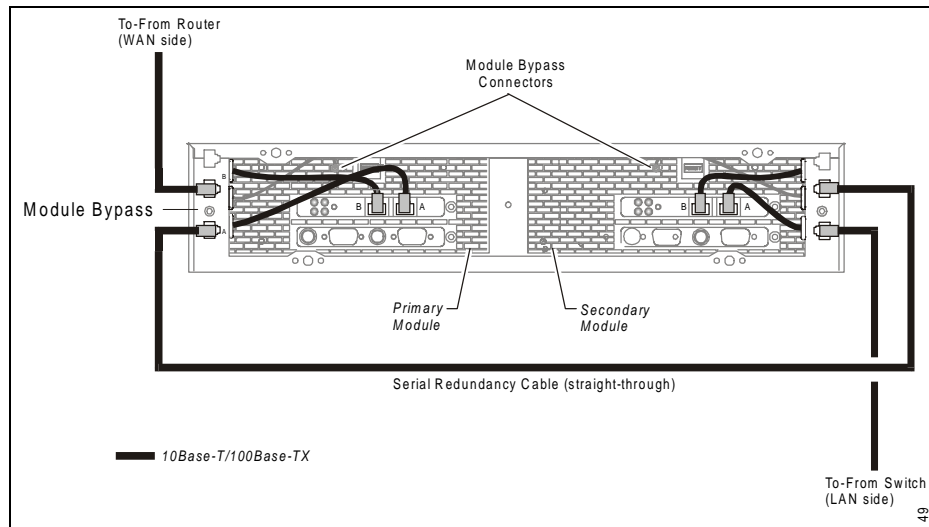
A serial redundant controller contains two modules wired to provide non-stop fail-safe operation. Configuring for serial redundancy requires the modules to be connected to their respective module bypasses the same as when there is no redundancy. In addition, the module bypasses must be connected to each other. The modules are then initialized as a primary and a secondary module. In normal operation, both modules are online, processing traffic, and transmitting traffic. If the primary module fails, it goes into bypass mode and the secondary module takes over with no disruption to traffic.

Traffic flows through a serial redundant ABWM controller as shown in [Figure 120](#).

Figure 120 iSurfRanger Controller Configured for Serial Redundancy

To Cable for Serial Redundancy

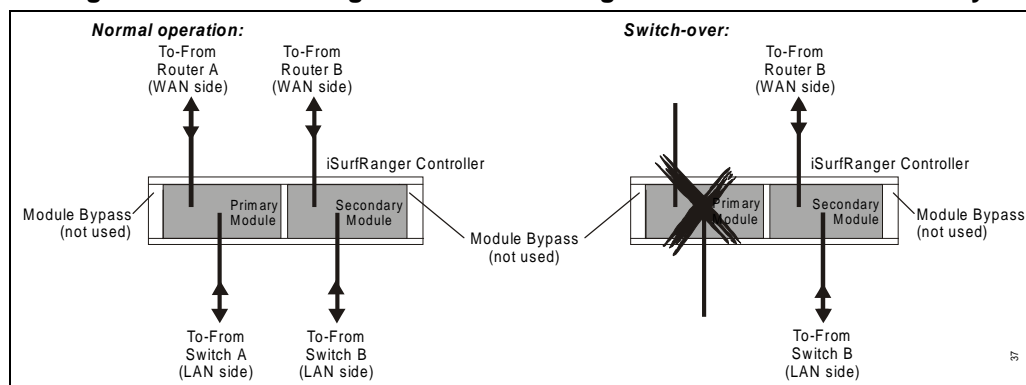
1. If the front cover has not been removed, remove it by grasping the cover on the top and bottom edges and firmly pulling it straight out.
2. Ensure cables are connected between the module bypass and the modules as shown in [Figure 121](#).

Figure 121 Cabling for Serial Redundancy

9.1.7 Cabling a Parallel Redundant Controller

A parallel redundant controller contains two modules wired independently of each other. A parallel redundant iSurfRanger controller contains two modules wired independently of each other. The modules are connected directly to the network. Module bypasses are not used. The modules are then initialized as a primary and a secondary module. In normal operation, both modules are online and processing traffic, but only the primary module transmits traffic. The modules exchange “keep-alive” messages with each other over the network. If the primary module fails, a switch-over occurs. That is, the secondary module takes over, and there is no bypass mode.

Traffic flows through a parallel redundant iSurfRanger controller in a network as shown in [Figure 122](#).

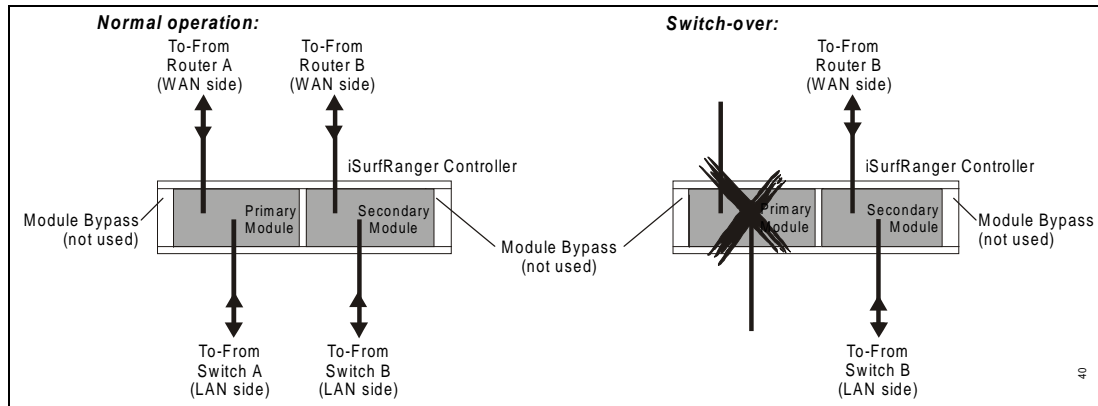
Figure 122 iSurfRanger Controller Configured for Parallel Redundancy

CAUTION: Observe precautions for handling electrostatic sensitive devices.

To Cable for Parallel Redundancy

1. If the front cover has not been removed, remove it by grasping the cover on the top and bottom edges and firmly pulling it straight out.
2. Ensure cables are connected to the network as shown in [Figure 123](#).

Figure 123 Cabling for Parallel Redundancy



3. Add the second module

9.2 Adding a Bandwidth Manager Record to the NMS

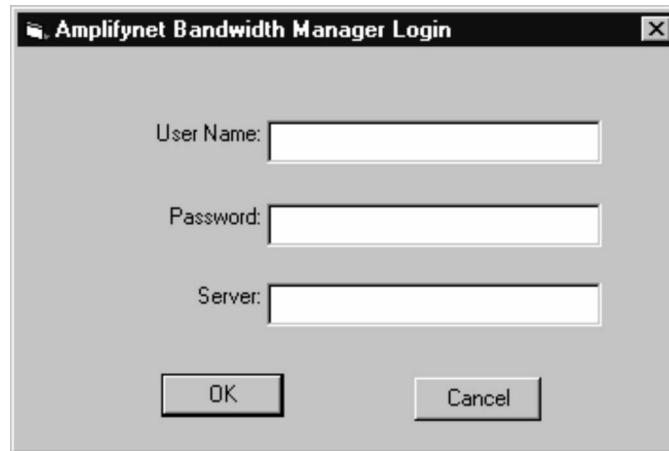
Once you have installed the controller into the NAP, create an ABWM record in the NMS and configure the controller. If you have an existing router-based bandwidth manager, you can convert it to ABWM. Procedures for converting a BWM to ABWM or creating a new ABWM follow.

NOTE: Throughout the NMS, required fields are indicated by a red asterisk (*).

To Create a New Bandwidth Manager Record

1. In the NMS software, right-click the **LMS2000 NAP** branch.
2. From the shortcut menu, select **Add New Device > Bandwidth Manager**.

The ABWM Login dialog box opens.

Figure 124 Amplifynet Bandwidth Manager Login Dialog Box


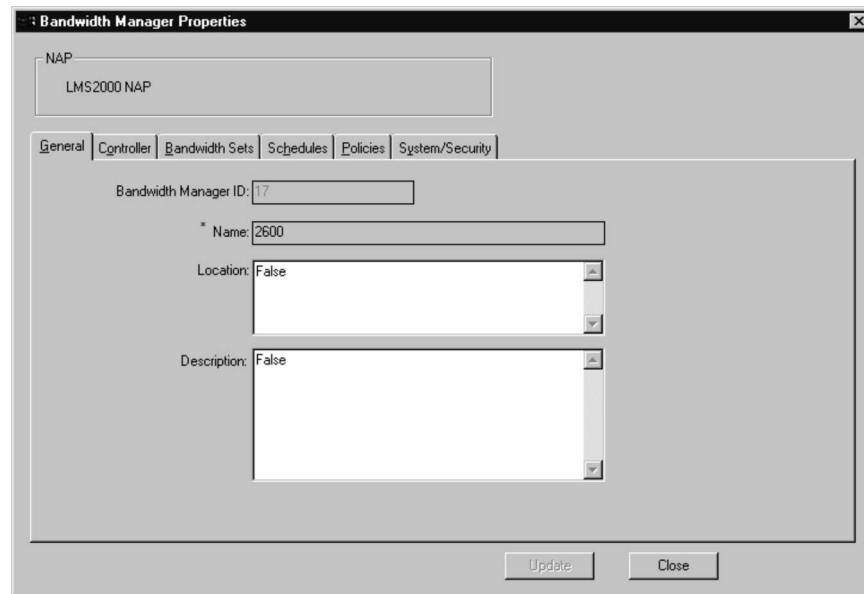
The dialog box is titled "Amplifynet Bandwidth Manager Login". It contains three text input fields: "User Name:", "Password:", and "Server:". Below these fields are two buttons: "OK" and "Cancel".

3. Fill in the **User Name**, **Password**, and **Server** fields, and click **OK**.

NOTE: By default the User Name and Password are both **admin**. The Server is the identification of the NMS Server PC.

The new ABWM record opens.

4. On the **General** tab of the **Bandwidth Manager Properties** screen, type a unique name to identify the Bandwidth Manager.

Figure 125 Bandwidth Manager Properties—General Tab


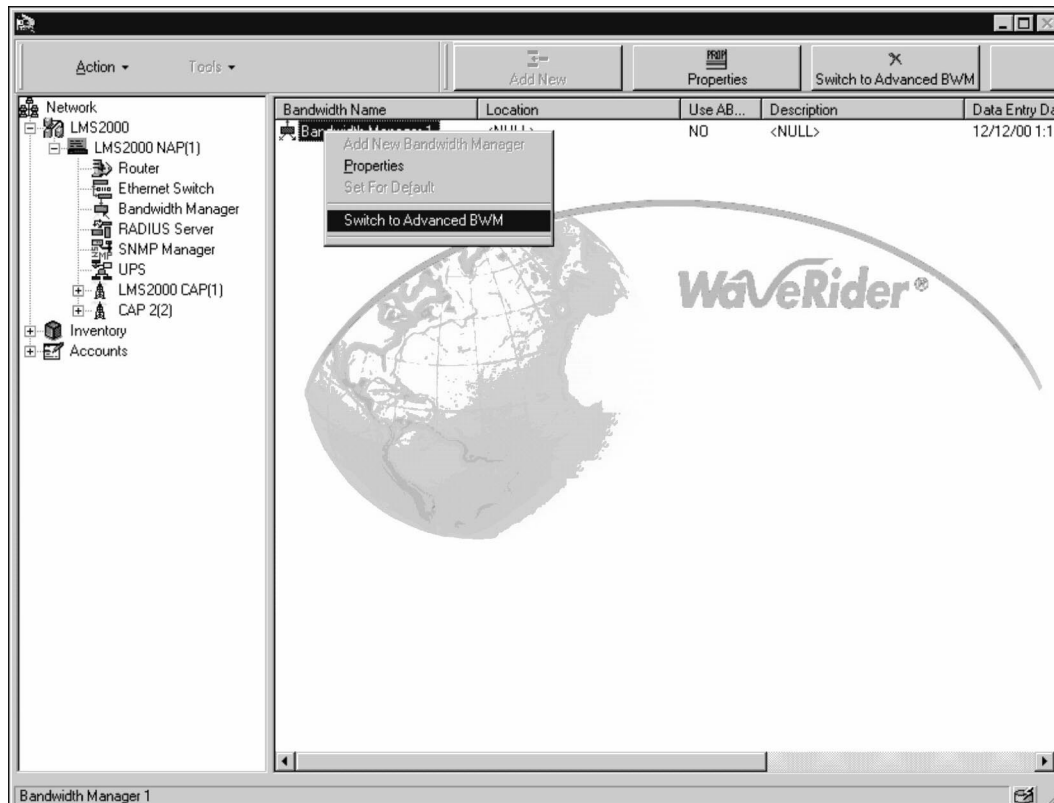
The "Bandwidth Manager Properties" dialog box has a title bar and a close button. Below the title bar is a text field labeled "NAP" containing "LMS2000 NAP". Below this is a tabbed interface with tabs: "General", "Controller", "Bandwidth Sets", "Schedules", "Policies", and "System/Security". The "General" tab is selected. It contains the following fields: "Bandwidth Manager ID:" with a value of "17"; "* Name:" with a value of "2600"; "Location:" with a value of "False" and a dropdown arrow; and "Description:" with a value of "False" and a large text area below it. At the bottom right are "Update" and "Close" buttons.

5. Ensure all fields marked by a red asterisk, on all tabs of the Bandwidth Manager Properties screen, are filled out as described in the remainder of this chapter, beginning with [Defining Controller Properties](#), on page 143.

To Convert Router-based Bandwidth Management to ABWM

1. In LMS2000 tree of the NMS, click **Bandwidth Manager**.
2. In the right pane, right-click the Bandwidth Manager record.

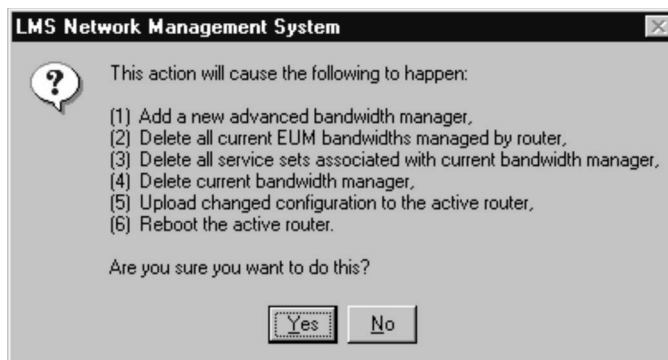
Figure 126 Bandwidth Manager Shortcut Menu



3. Click **Switch to Advanced BWM**.

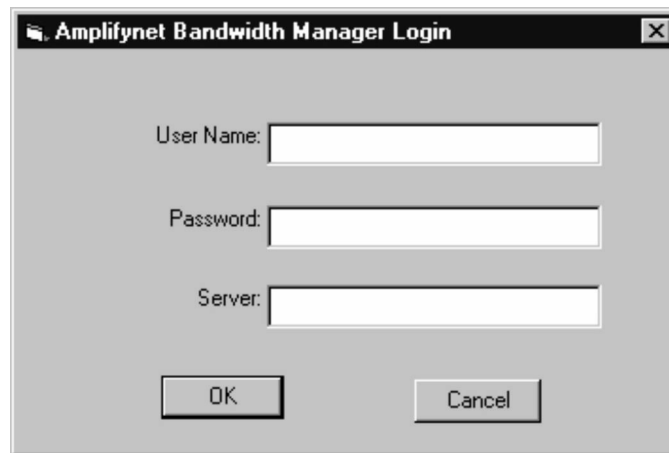
The Switch to ABWM dialog box opens.

Figure 127 Switch to ABWM Dialog Box



4. Click **Yes**.

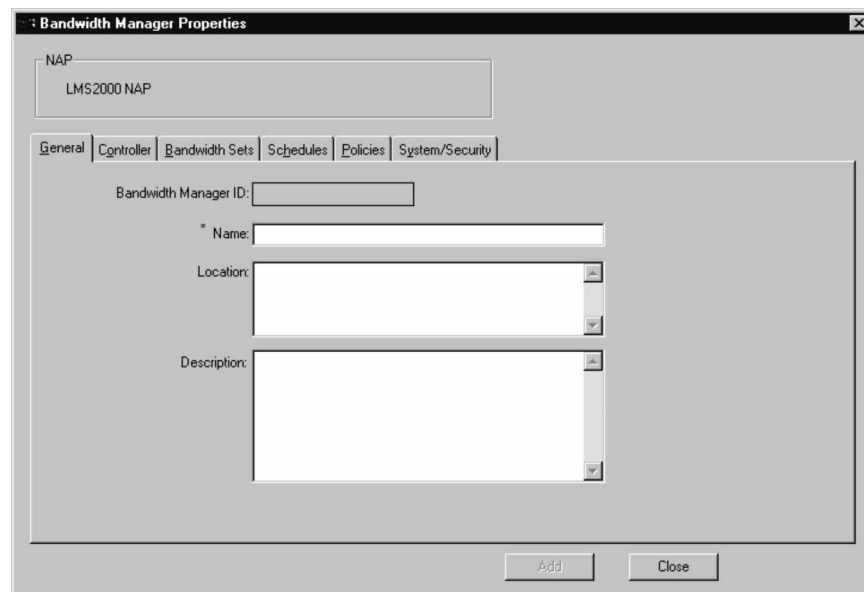
The ABWM Login dialog box opens.

Figure 128 Amplifynet Bandwidth Manager Login Dialog BoxA login dialog box titled "Amplifynet Bandwidth Manager Login". It contains three text input fields labeled "User Name:", "Password:", and "Server:". Below the fields are two buttons: "OK" and "Cancel".

5. Fill in the **User Name**, **Password**, and **Server** fields, and click **OK**.

NOTE: By default the User Name and Password are both **admin**. The Server is the identification of the NMS Server PC.

The new ABWM record opens.

Figure 129 Bandwidth Manager PropertiesA dialog box titled "Bandwidth Manager Properties". At the top, there is a text field labeled "NAP" containing "LMS2000 NAP". Below this is a tabbed interface with tabs for "General", "Controller", "Bandwidth Sets", "Schedules", "Policies", and "System/Security". The "General" tab is selected. It contains fields for "Bandwidth Manager ID:", "* Name:", "Location:", and "Description:". At the bottom right are "Add" and "Close" buttons.

The following dialog box opens.

Figure 130 BWM to ABWM Switch Success Dialog Box



6. Click **OK**.
7. The Router Restart dialog box opens.

Figure 131 Router Restart Dialog Box



8. Click **OK**.
The router restarts and the conversion is complete.
9. Ensure all fields marked by a red asterisk, on all tabs of the Bandwidth Manager Properties screen, are filled out as described in the remainder of this chapter, beginning with [Defining Controller Properties](#), on page 143.

To Open the Bandwidth Manager Record

1. In the NMS, click **Bandwidth Manager**.
2. Double-click the **Bandwidth Manager** icon.

The Amplifynet Bandwidth Manager Login window opens.

Figure 132 Bandwidth Manager Login



3. Fill in the **User Name**, **Password**, and **Server** fields to connect to the database.

NOTE: The defaults for each of these fields are User Name: **admin**, Password: **admin**; Server: **<identification of NMS PC>**.

4. Click **OK**.

The Bandwidth Manager Properties screen opens.

5. Define the Advanced Bandwidth Manager properties as described in the remainder of this chapter.

NOTE: Fields with a red asterisk are required.

9.3 Defining Controller Properties

The first step in setting up ABWM in the NMS is to configure the controller. Controller settings enforce the real time distribution of bandwidth according to policy.

Figure 133 Bandwidth Manager Properties—Controller Tab

The screenshot shows the 'Bandwidth Manager Properties' dialog box with the 'Controller' tab selected. The 'NAP' field is set to 'LMS2000 NAP'. The 'Redundancy Mode' section has three radio buttons: 'None' (selected), 'Serial', and 'Parallel'. The 'IP Addressing' section has two fields: 'Primary' (192.168.10.2) and 'Secondary' (N/A). The 'Physical Connection Capacity' section has two fields: 'Pipe In Size (Kbps)' (100000) and 'Pipe Out Size (Kbps)' (100000). The 'CIR Thresholds' section has four fields: 'Activity Reset Timer(sec)' (10), 'Max Burst Rate In (Kbps)' (15000), 'Max Burst Rate Out (Kbps)' (15000), 'Reserved Margin In (Kbps)' (15000), and 'Reserved Margin Out (Kbps)' (15000). The 'Alert Thresholds' section has two fields: 'Soft' (1) and 'Hard' (5). The 'Parallel Redundancy' section is disabled. The 'Keep Alive Port' section has three radio buttons: 'A', 'B', and 'Both' (selected). The 'Keep Alive Interval (sec)' field is set to 1. The 'Number of Packets before Switch-Over' field is set to 1. The 'Update' and 'Close' buttons are at the bottom right.

9.3.1 Configuring Redundancy

A controller connected for serial or parallel redundancy must be configured accordingly. By default, the **Redundancy Mode** is None. Configure redundancy on the Controller tab of the Bandwidth Manager Properties screen. The Secondary IP Address field is only enabled if redundancy mode is Serial or Parallel, and the Parallel Redundancy group is only enabled if the redundancy mode is Parallel.

The **Primary IP Address** of the controller is the address given to the primary module during hardware setup. If only one module is in the controller, it is considered the primary module and you must enter its IP address here. If the controller has two modules, configured for

redundancy, you must identify one module as primary and the other as secondary. The primary module processes and logs the traffic flow; the secondary module also processes traffic flow, but does not log data, remaining in “hot” standby mode.

Secondary IP Address applies only to serial or parallel redundancy. It is the address that was given to the secondary module during hardware setup. When two modules are installed and properly cabled for redundancy, the secondary module takes over immediately if the primary module fails.

Default Router IP applies to parallel redundancy only. It applies only if the primary module is linked to the secondary module through a router. If so, enter the IP address of that router. For this IP address, as well as all other IP addresses required for configuring ABWM, the range for each of the four segments is 1–254.

The **Keep Alive Port** applies to parallel redundancy only. It specifies whether both modules in a parallel redundant configuration use only port A, port B, or both for exchanging keep-alive messages.

The **Keep Alive Interval** field only applies to parallel redundancy. It is the number of seconds during which the secondary module must receive a keep alive message for their primary module. If a time-out occurs, traffic transmission switches to the secondary module.

The **Number of Packets before Switchover** field applies to parallel redundancy only. It identifies the number of packets that can be dropped before a switch-over actually occurs. This parameter prevents an unjustified switch-over that results when a keep-alive message is among the packets dropped, even though the modules are in communication.

To change from a redundant configuration to two modules operating independently (dual controllers), delete the redundant controller, and then reconfigure each module as a new controller.

To Configure for No Redundancy

1. In the Bandwidth Manager Properties screen, click the **Controller** tab.

Figure 134 Bandwidth Manager Properties—Controller Tab

The screenshot shows the 'Bandwidth Manager Properties' dialog box with the 'Controller' tab selected. The 'NAP' field is set to 'LMS2000 NAP'. The 'Redundancy Mode' section has 'None' selected. The 'IP Addressing' section has 'Primary' set to '192.168.10.2' and 'Secondary' set to 'N/A'. The 'Physical Connection Capacity' section has 'Pipe In Size (Kbps)' and 'Pipe Out Size (Kbps)' both set to '100000'. The 'CIR Thresholds' section has 'Activity Reset Timer(sec)' set to '10', 'Max Burst Rate In (Kbps)' and 'Max Burst Rate Out (Kbps)' both set to '15000', and 'Reserved Margin In (Kbps)' and 'Reserved Margin Out (Kbps)' both set to '15000'. The 'Alert Thresholds' section has 'Soft' set to '1' and 'Hard' set to '5'. The 'Update' and 'Close' buttons are at the bottom right.

2. In the Redundancy Mode group, select **None**.
3. In the **Primary** field, type the IP address of the controller.

NOTE: Default IP address is 192.168.10.2.

4. Click **Update** to save the changes in the database and upload the configuration to the controller.
5. Configure the physical connection capacity, CIR thresholds, and alert thresholds, as described on [To Configure Physical Connection Capacity](#), on page 149.

To Configure Serial Redundancy

1. In the Bandwidth Manager Properties screen, click the **Controller** tab.

Figure 135 Bandwidth Manager Properties—Controller Tab

The screenshot shows the 'Bandwidth Manager Properties' dialog box with the 'Controller' tab selected. The 'NAP' field contains 'LMS2000 NAP'. The 'Redundancy Mode' section has three radio buttons: 'None', 'Serial' (selected), and 'Parallel'. The 'IP Addressing' section has two fields: 'Primary' with the value '192.168.10.2' and 'Secondary' with the value '192.168.10.3'. The 'Parallel Redundancy' section has a 'Default Router IP' field with the value '192.168.10.1' and a 'Keep Alive Port' section with three radio buttons: 'A', 'B', and 'Both' (selected). The 'Physical Connection Capacity' section has two fields: 'Pipe In Size (Kbps)' and 'Pipe Out Size (Kbps)', both with the value '100000'. The 'CIR Thresholds' section has four fields: 'Activity Reset Timer(sec)' with '10', 'Max Burst Rate In (Kbps)' with '50000', 'Max Burst Rate Out (Kbps)' with '50000', 'Reserved Margin In (Kbps)' with '25000', and 'Reserved Margin Out (Kbps)' with '25000'. The 'Alert Thresholds' section has two fields: 'Soft' with '3' and 'Hard' with '1'. At the bottom are 'Update' and 'Close' buttons.

2. In the Redundancy Mode group, select **Serial**.
3. In the **Primary** field, type the IP address of the primary controller.

NOTE: The default IP address is 192.168.10.2.

4. In the **Secondary** field, type the IP address of the second controller.

NOTE: The default IP address is 192.168.10.3.

5. Click **Update** to save the changes in the database and upload the configuration to the controller.
6. Configure the physical connection capacity, CIR thresholds, and alert thresholds, as described on [To Configure Physical Connection Capacity](#), on page 149.

To Configure Parallel Redundancy

1. In the Bandwidth Manager Properties screen, click the **Controller** tab.

Figure 136 Bandwidth Manager Properties—Controller Tab

The screenshot shows the 'Bandwidth Manager Properties' dialog box with the 'Controller' tab selected. The 'NAP' field at the top contains 'LMS2000 NAP'. The 'General' tab is active in the top navigation bar. The 'Redundancy Mode' group has three radio buttons: 'None', 'Serial', and 'Parallel', with 'Parallel' selected. The 'IP Addressing' group has two text fields: 'Primary' with '192.168.10.2' and 'Secondary' with '192.168.10.3'. The 'Parallel Redundancy' group has a 'Default Router IP' field with '192.168.10.1', a 'Keep Alive Port' group with radio buttons 'A', 'B', and 'Both' (selected), a 'Keep-Alive Interval (sec)' field with '2', and a 'Number of Packets before Switch-Over' field with '2'. The 'Physical Connection Capacity' group has two text fields: 'Pipe In Size (Kbps)' and 'Pipe Out Size (Kbps)', both with '100000'. The 'CIR Thresholds' group has five text fields: 'Activity Reset Timer(sec)' with '10', 'Max Burst Rate In (Kbps)' with '50000', 'Max Burst Rate Out (Kbps)' with '50000', 'Reserved Margin In (Kbps)' with '25000', and 'Reserved Margin Out (Kbps)' with '25000'. The 'Alert Thresholds' group has two spinners: 'Soft' with '3' and 'Hard' with '1'. At the bottom right are 'Update' and 'Close' buttons.

2. In the Redundancy Mode group, select **Parallel**.

The Parallel Redundancy group becomes active.

3. In the **Default Router IP** field, type the IP address of the NAP Router.

NOTE: The default IP address of the NAP router is 192.168.10.1.

4. In the Keep Alive Port field, select **A**, **B**, or **Both**, to specify which port the modules use for exchanging keep-alive messages.
5. In the Keep Alive Interval field, type the number of seconds during which the secondary module must receive a keep-alive message from the primary module.
6. In the **Number of Packets Before Switch-Over** field, type the number of packets that can be dropped before switch-over actually occurs.
7. Click **Update** to save the changes in the database and upload the configuration to the controller.
8. Configure the physical connection capacity, CIR thresholds, and alert thresholds, as described on [To Configure Physical Connection Capacity](#), on page 149.

9.3.2 Configuring Bandwidth Controls

Configure bandwidth controls to identify the maximum bandwidth available and the committed information rate (CIR) thresholds.

The **Pipe In Size** and **Pipe Out Size** fields identify the maximum bandwidth available (in Kbps) for all the traffic through the controller from the WAN side (Pipe In) and LAN side (Pipe Out). The bandwidth should be the same for Pipe In and Pipe Out.

The **Activity Reset Timer** field identifies the total number of seconds, without controller traffic, that can elapse before bandwidth is reset to the committed information rate (CIR). For example, an activity-reset timer set to 120 would cause the bandwidth to be reset every 2 minutes, if there were no traffic during that 2 minute period. The minimum is 60 seconds.

The **Max Burst Rate In** and **Out** fields identify the maximum bandwidth (in Kbps) that each user is allowed to burst, regardless of the policy setting. The maximum bandwidth is 100Mbps.

The **Reserved Margin In** field defines a reserved in traffic bandwidth with which to satisfy the demand of new users to meet their CIR.

Reserved Margin Out is very similar to Margin In, except that Margin Out defines a reserved out traffic bandwidth with which to satisfy the demand of new users to meet their CIR. Margin In and Out both define a level of total traffic, below which every user is allowed to burst towards its maximum burst rate (MBR). Exceeding either level, every user is brought back towards its CIR.

The alerts are the percentage of the CIR that, when exceeded, cause an SNMP trap message to be sent. There are two alert thresholds:

- **Soft alert threshold** — This threshold is usually lower than the hard alert threshold and indicates an undesirable situation, rather than severe abuse. A typical value for a soft alert threshold is 10%.
- **Hard alert threshold** — This threshold is usually higher than the soft alert threshold and indicates severe abuse. A typical value for hard alert threshold is 20%.

Configure the soft and hard alert thresholds on the controller tab of the Bandwidth Manager Properties screen.

To Configure Physical Connection Capacity

1. Open the **Controller** tab on the Bandwidth Manager Properties screen.

Figure 137 Bandwidth Manager Properties—Controller Tab

The screenshot shows the 'Bandwidth Manager Properties' dialog box with the 'Controller' tab selected. The 'NAP' field is set to 'LMS2000 NAP'. The 'General' tab is also visible. The 'Controller' tab contains the following sections:

- Redundancy Mode:** Radio buttons for 'None' (selected), 'Serial', and 'Parallel'.
- IP Addressing:**
 - * Primary: 192.168.10.2
 - * Secondary: N/A
- Parallel Redundancy:**
 - * Default Router IP: [Empty field]
 - Keep Alive Port: Radio buttons for 'A', 'B', and 'Both' (selected).
 - * Keep Alive Interval (sec): 0
 - * Number of Packets before Switch-Over: 0
- Physical Connection Capacity:**
 - * Pipe In Size (Kbps): 100000
 - * Pipe Out Size (Kbps): 100000
- CIR Thresholds:**
 - * Activity Reset Timer(sec): 10
 - * Max Burst Rate In (Kbps): 15000
 - * Max Burst Rate Out (Kbps): 15000
 - * Reserved Margin In (Kbps): 15000
 - * Reserved Margin Out (Kbps): 15000
- Alert Thresholds:**
 - * Soft: 1
 - * Hard: 5

At the bottom of the dialog are 'Update' and 'Close' buttons.

2. In the **Pipe In Size** field, type the maximum number of kilobits per second (Kbps) available for all traffic through the controller from the WAN side.
3. In the **Pipe Out Size** field, type the maximum number of Kbps available for all traffic through the controller from the LAN side.
4. Click **Update** to save the changes in the database and upload the configuration to the controller.

To Configure Committed Information Rate Thresholds

1. Open the **Controller** tab on the Bandwidth Manager Properties screen.

Figure 138 Bandwidth Manager Properties—Controller Tab

The screenshot shows the 'Bandwidth Manager Properties' dialog box with the 'Controller' tab selected. The 'NAP' field is set to 'LMS2000 NAP'. The 'General' tab is also visible. The 'Controller' tab contains the following fields:

- Redundancy Mode:** Radio buttons for None (selected), Serial, and Parallel.
- IP Addressing:**
 - * Primary: 192.168.10.2
 - * Secondary: N/A
- Parallel Redundancy:**
 - * Default Router IP: (empty)
 - Keep Alive Port: Radio buttons for A, B, and Both (selected).
 - * Keep Alive Interval (sec): 0
 - * Number of Packets before Switch-Over: 0
- Physical Connection Capacity:**
 - * Pipe In Size (Kbps): 100000
 - * Pipe Out Size (Kbps): 100000
- CIR Thresholds:**
 - * Activity Reset Timer(sec): 10
 - * Max Burst Rate In (Kbps): 15000
 - * Max Burst Rate Out (Kbps): 15000
 - * Reserved Margin In (Kbps): 15000
 - * Reserved Margin Out (Kbps): 15000
- Alert Thresholds:**
 - * Soft: 1
 - * Hard: 5

Buttons at the bottom: Update, Close.

2. In the **Activity Reset Timer** field, type the number of seconds, without controller traffic, that can elapse before bandwidth is reset to the CIR.

NOTE: The minimum for the Activity Reset Timer is 60 seconds.

3. In the **Maximum Burst Rate In** field, type the maximum Kbps that each user is allowed to burst their incoming data rate, regardless of policy setting.

NOTE: The maximum bandwidth for **Maximum Burst Rate In** and **Out** is 10 000Kbps.

4. In the **Maximum Burst Rate Out** field, type the maximum Kbps that each user is allowed to burst their outgoing data rate, regardless of policy setting.
5. In the **Reserved Margin In** field, type the number of Kbps of reserved in-traffic bandwidth for satisfying the demand of new users to meet their CIR.

NOTE: The **Reserved Margin In** and **Out** also define a level of total traffic, below which every user is allowed to burst towards its MBR. Exceeding this level, every user is brought back towards its CIR.

6. In the **Reserved Margin Out** field, type the number of Kbps of reserved out traffic bandwidth for satisfying the demand of new users to meet their CIR.
7. Click **Update** to save the changes in the database and upload the configuration to the controller.

To Configure Alert Thresholds

1. On the **Bandwidth Manager Properties** screen, click the **Controller** tab.

Figure 139 Bandwidth Manager Properties—Controller Tab

The screenshot shows the 'Bandwidth Manager Properties' dialog box with the 'Controller' tab selected. The 'NAP' field is set to 'LMS2000 NAP'. The 'Redundancy Mode' has radio buttons for 'None' (selected), 'Serial', and 'Parallel'. The 'IP Addressing' section has 'Primary' set to '192.168.10.2' and 'Secondary' set to 'N/A'. The 'Physical Connection Capacity' section has 'Pipe In Size (Kbps)' and 'Pipe Out Size (Kbps)' both set to '100000'. The 'CIR Thresholds' section has 'Activity Reset Timer(sec)' set to '10', and 'Max Burst Rate In (Kbps)', 'Max Burst Rate Out (Kbps)', 'Reserved Margin In (Kbps)', and 'Reserved Margin Out (Kbps)' all set to '15000'. The 'Alert Thresholds' section has 'Soft' set to '1' and 'Hard' set to '5'. At the bottom are 'Update' and 'Close' buttons.

2. In the **Soft** field, type the percentage for the soft alert threshold, or select the percentage using the scroll buttons.
3. In the **Hard** field, type the percentage for the hard alert threshold, or select the percentage using the scroll buttons.
4. Click **Update** to save the changes in the database and upload the configuration to the controller.

9.4 Defining System Security Parameters

The System/Security tab of the Bandwidth Manager Properties screen enables you to set a user name, password, and time zone for the controller. The user name and password must match the ABWM login name and password defined during the ABWM command line interface setup, as described in [Initializing the iSurfRanger Controller](#), on page 132.

Defining the user name and password on the System/Security tab does not change the ABWM login name and password. However, to enable communication between the NMS and the ABWM, the user name and password on the System/Security tab must match the login name and password on the ABWM device, as configured through the command line interface. The only way you can change the login name and password on the ABWM is through the command line interface. Once you change them through the CLI, you must change the fields on the System/Security tab to match.

To Specify a User Name and Password for Controllers

1. On the Bandwidth Manager Properties screen, click the **System/Security** tab.
2. In the **User Name** field, type the user name for the software or hardware controller personnel.
3. Click the **Change Password** button.

Figure 140 Password Change Dialog Box

The dialog box is titled "Change Password". It contains three text input fields, each preceded by an asterisk: "Current Password:", "New Password:", and "Retype:". At the bottom of the dialog are two buttons: "Apply" and "Cancel".

4. In the **Change Password** dialog box, fill out each of the fields and click **Apply**.

To Set the Time Zone

1. On the **Bandwidth Manager Properties** screen, click the **System/Security** tab.

Figure 141 Bandwidth Manager Properties—System/Security Tab

The screenshot shows the "Bandwidth Manager Properties" window. At the top, it says "NAP" and "LMS2000 NAP". Below that are several tabs: "General", "Controller", "Bandwidth Sets", "Schedules", "Policies", and "System/Security" (which is selected). The "System/Security" tab contains a "Time Zone Setting" section with a dropdown menu for "Difference of Time Zone from GMT" currently set to "-7". Below this is a "BWM Hardware Controller" section with "Username:" and "Password:" labels and corresponding text boxes. A "Change Password" button is located below the password field. At the bottom of the window are "Update" and "Close" buttons.

2. In the **Difference of Time Zone from GMT** drop-down box, select the appropriate time zone.

NOTE: Time zones which have half-hour differences from the GMT are not included in the drop-down list. Instead, use the closest available time zone.



TIP: To determine your time zone's difference from GMT, click **Start > Settings > Control Panel**, double-click the **Date/Time** icon, and click the **Time Zone** tab. Look up your time zone in the drop-down list.

3. Click the **Update** button before configuring Bandwidth Sets, Schedules, Priorities, and Policies.

9.5 Configuring Bandwidth Sets

Use bandwidth sets to control application bandwidth and to streamline traffic policy configuration. A bandwidth set saves you from entering each traffic policy parameter when you create a new traffic policy. A bandwidth set also gives you a quick way of changing an existing traffic policy for large groups of subscribers by simply changing the bandwidth set.

A bandwidth set is a named collection of parameters that specify bandwidth rate and capacity information. You would typically configure several bandwidth sets, any of which you can then include in a traffic policy. Once you configure a bandwidth set, access the set by selecting its name.

A bandwidth set includes the following parameters:

- CIR In and Out
- Maximum Burst Rate (MBR) In and Out
- Priority

To understand the role of the CIR, MBR, and priority, think of the total bandwidth available to a subscriber as a virtual pipe through which Internet traffic flows. The controller treats the WAN link as a conduit, which it divides into multiple virtual pipes. The CIR, MBR, and priority allocate levels of bandwidth utilization within the virtual pipe. The priority specified for a bandwidth set determines how quickly a virtual pipe can ramp up to its Maximum Burst Rate:

- A high priority allows a rapid ramp-up.
- A low priority allows a slow ramp-up.

You can offer a greater percentage of excess bandwidth to subscribers who pay a higher tariff by allowing a quick ramp-up to the maximum burst rate.

9.5.1 Setting Priorities

Setting priorities is a prerequisite to configuring a bandwidth set. Setting a priority for a bandwidth set lets you define how quickly a user reaches its MBR. This priority only effects those bandwidth sets that have MBRs associated with them.

A priority consists of an Attack Rate and a Retreat Rate. An **Attack Rate** identifies the number of Kbps that bandwidth will increase every 10 seconds to accommodate the initially high bandwidth (also known as bursting) needed when a subscriber accesses a web site. The attack rate controls how quickly traffic ramps up from the CIR to the MBR. The higher the rate, the quicker bandwidth ramps up from the CIR.

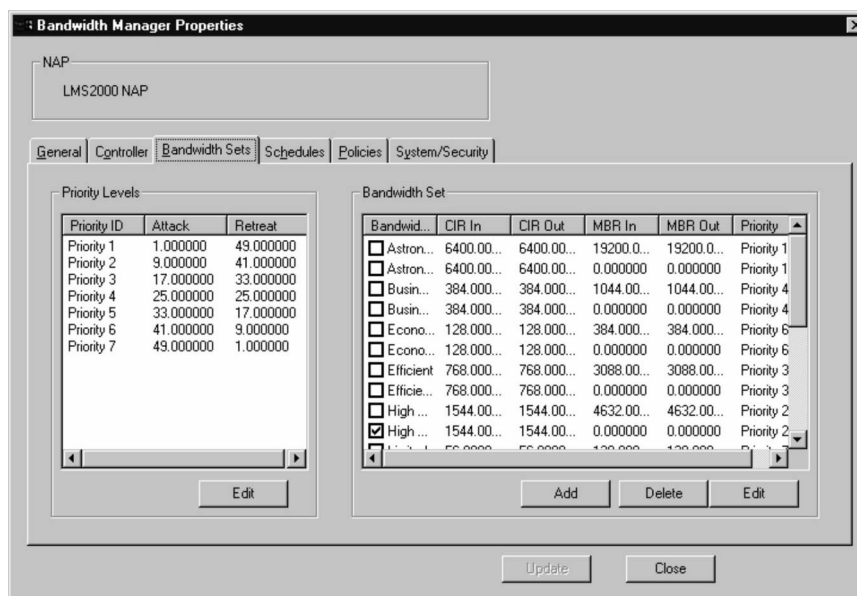
A **Retreat Rate** identifies the number of Kbps that bandwidth will decrease every 10 seconds to the CIR after bursting. The retreat rate controls how quickly traffic ramps down from the MBR to the CIR. This value must be no greater than the MBR minus the CIR. In most cases, this value should be much smaller than the attack rate. The lower the rate, the slower bandwidth ramps down to the CIR. The Attack-and-Retreat function works best when the attack rate is high and the retreat rate is 0.

To streamline configuring a bandwidth set, ABWM supplies you with seven Attack-Rate-Retreat-Rate pairs, each assigned to a priority. You can specify any of the seven priorities supplied, or you can change them. You can then assign the priority representing the desired Attack-Rate-Retreat-Rate pair to the bandwidth set.

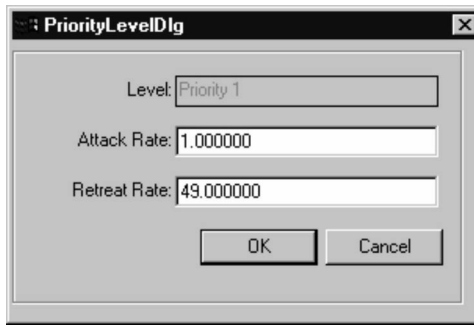
To Set Priorities

1. Open the Bandwidth Manager Properties screen, and click the **Bandwidth Sets** tab.

Figure 142 Bandwidth Manager Properties—Bandwidth Sets Tab



2. In the **Priority Levels** group, select a priority level to edit.
3. Click **Edit**.

Figure 143 Priority Edit Dialog Box

4. In the **Attack Rate** field, type the number of Kbps that bandwidth will increase every 10 seconds.
5. In the **Retreat Rate** field, type the number of Kbps that bandwidth will decrease every 10 seconds.

NOTE: The Retreat Rate must be no greater than the MBR minus the CIR.

6. Click **OK**.
7. Click **Update** to save the changes in the database and upload the configuration to the controller.

9.5.2 Configuring a Bandwidth Set

Before configuring a bandwidth set, you need to set priorities. For your convenience, Advanced Bandwidth Manager comes with 21 supplied pre-configured bandwidth sets. You can edit or delete any of the supplied bandwidth sets as well as create additional bandwidth sets.

The **CIR In** and **CIR Out** fields identify the amount of bandwidth for traffic from the WAN side (CIR In) or the LAN side (CIR Out), in Kbps, that you guarantee as a minimum for each account associated with this bandwidth set. The range is 0–100Mbps. If you did not specify an MBR In, the CIR In will be the maximum bandwidth available.

The **MBR In** and **Out** fields identify the bandwidth utilization limit (in Kbps) that you set for each message received from the WAN side (In) and the LAN side (Out). The range for MBR In is 0Mbps; the range for MBR Out is 0–100Mbps. MBR Out operates in the same way as MBR In, except that it applies to outgoing traffic. If the CIR Out equals the maximum bandwidth available, you cannot specify an MBR Out.

WARNING!



The MBR Out value must be equal to or greater than the CIR Out.

The **Priority Level** field identifies the priority to assign to this bandwidth set. The selected priority will apply to traffic flowing to and from each IP group governed by this bandwidth set.

Once you have configured the bandwidth sets, you must select one as the default fallback rate. Any IP addresses that are not specified in any policy on this controller will use the default fallback rate. Set a bandwidth set the default by selecting its corresponding check box. Only one bandwidth set may be the default.

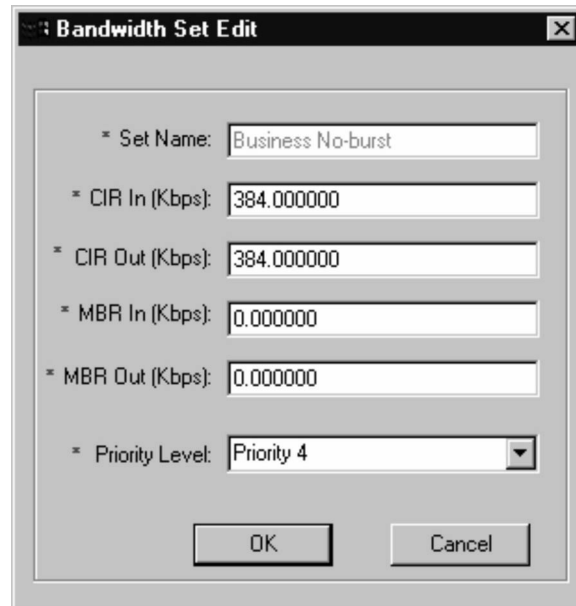


CAUTION: Only one bandwidth set may be the default. This default bandwidth set must have a CIR In of at least 1 meg; otherwise, the bandwidth set will not limit bandwidth.

To Edit a Bandwidth Set

1. Open the Bandwidth Manager Properties screen, and click the **Bandwidth Sets** tab.
2. In the Bandwidth Set group, select the Bandwidth Set to edit.
3. Click the **Edit** button.

Figure 144 Bandwidth Set Edit Dialog Box



The dialog box titled "Bandwidth Set Edit" contains the following fields and controls:

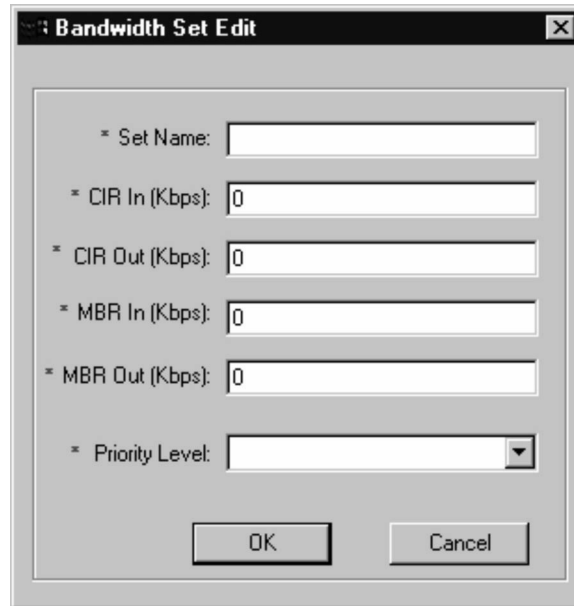
- * Set Name:** Text field with the value "Business No-burst".
- * CIR In (Kbps):** Text field with the value "384.000000".
- * CIR Out (Kbps):** Text field with the value "384.000000".
- * MBR In (Kbps):** Text field with the value "0.000000".
- * MBR Out (Kbps):** Text field with the value "0.000000".
- * Priority Level:** Dropdown menu with "Priority 4" selected.
- Buttons:** "OK" and "Cancel" buttons at the bottom.

4. In the **CIR In** field, type the amount of bandwidth (in Kbps) allowed for traffic from the WAN side.
5. In the **CIR Out** field, type the amount of bandwidth (in Kbps) allowed for traffic from the LAN side.
6. In the **MBR In** field, type the bandwidth utilization limit (in Kbps) that you set for each message received for the WAN side and destined for an account.
7. In the **MBR Out** field, type the bandwidth utilization limit (in Kbps) that each user is allowed to burst, regardless of the policy setting (maximum 100Mbps).
8. In the **Priority Level** field, type the priority level number to associate with this bandwidth set.
9. Click **OK**.
10. Click **Update** to save the changes in the database and upload the configuration to the controller.

To Create a Bandwidth Set

1. Open the **Bandwidth Manager Properties** screen, and click the **Bandwidth Sets** tab.
2. Click **Add**.

Figure 145 Bandwidth Set Edit Dialog Box



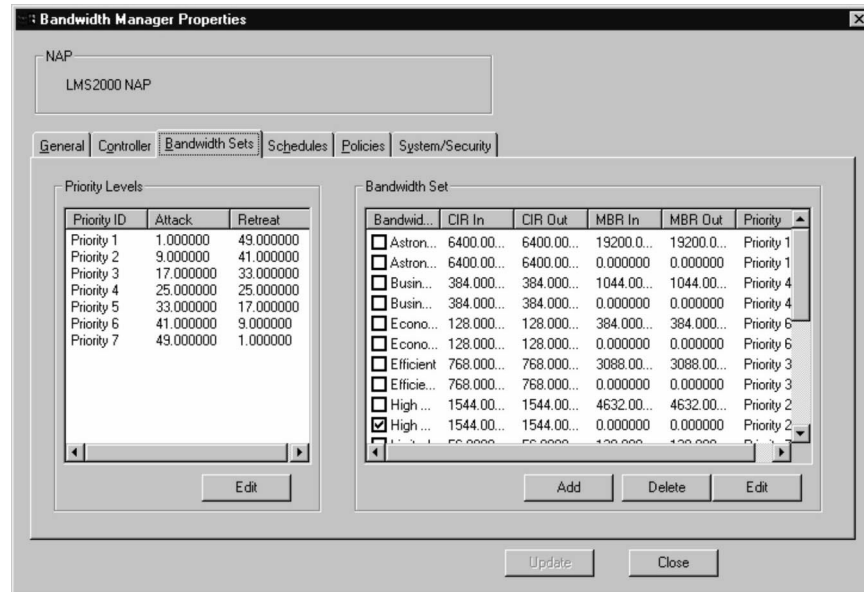
The image shows a dialog box titled "Bandwidth Set Edit". It contains several input fields and a dropdown menu, each preceded by an asterisk (*). The fields are: "Set Name" (a text box), "CIR In (Kbps)" (a text box with "0"), "CIR Out (Kbps)" (a text box with "0"), "MBR In (Kbps)" (a text box with "0"), "MBR Out (Kbps)" (a text box with "0"), and "Priority Level" (a dropdown menu). At the bottom of the dialog box are two buttons: "OK" and "Cancel".

3. In the **Set Name** field, type a name of your choice, up to 30 alphanumeric characters, that uniquely identifies this bandwidth set.
4. In the **CIR In** field, type the amount of bandwidth (in Kbps) for traffic from the WAN side.
5. In the **CIR Out** field, type the amount of bandwidth (in Kbps) for traffic from the LAN side.
6. In the **MBR In** field, type the bandwidth utilization limit (in Kbps) that you set for each message received for the WAN side and destined for an account.
7. In the **MBR Out** field, type the bandwidth utilization limit (in Kbps) that each user is allowed to burst, regardless of the policy setting. (Maximum 100 000Kbps.)
8. In the **Priority Level** field, type the priority level number to associate with this bandwidth set.
9. Click **OK**.
10. Click **Update** to save the changes in the database and upload the configuration to the controller.

To Select a Default Bandwidth Set

1. Open the **Bandwidth Manager Properties** screen, and click the **Bandwidth Sets** tab.

Figure 146 Bandwidth Manager Properties—Bandwidth Sets Tab



2. In the **Bandwidth Sets** group, click the check box for the bandwidth set to define as default.



CAUTION: Only one bandwidth set may be the default. This default bandwidth set must have a CIR In of at least 1 meg; otherwise, the bandwidth set will not limit bandwidth.

9.6 Establishing Schedules

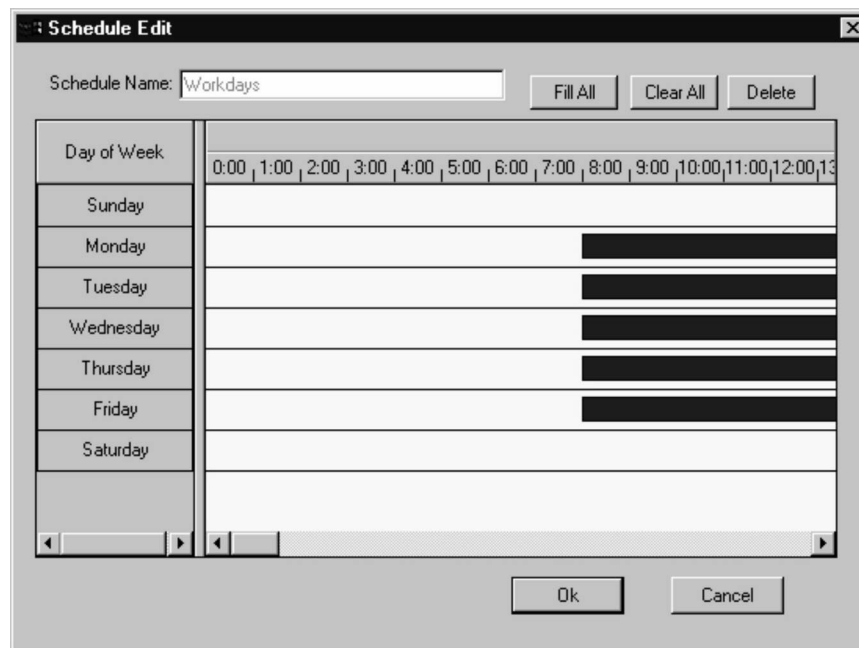
A schedule is a part of a traffic policy. You use the Schedule function to create the pattern of times when a traffic policy is applied. Establishing a range of schedules by high–low volume use patterns also enables you to refine bandwidth management. You can employ scheduling to provide suitable bandwidth to the correct IP groups during the appropriate times.

For your convenience, Advanced Bandwidth Manager includes two supplied schedules: 24x7 and Workdays. You can edit or delete the supplied schedules and add your own.

To Edit a Schedule

1. Open the **Bandwidth Manager Properties** screen, and click the **Schedules** tab.
2. In the **Schedules** group, select the schedule to change and click **Edit**.

Figure 147 Schedule Edit Dialog Box—Edit Mode

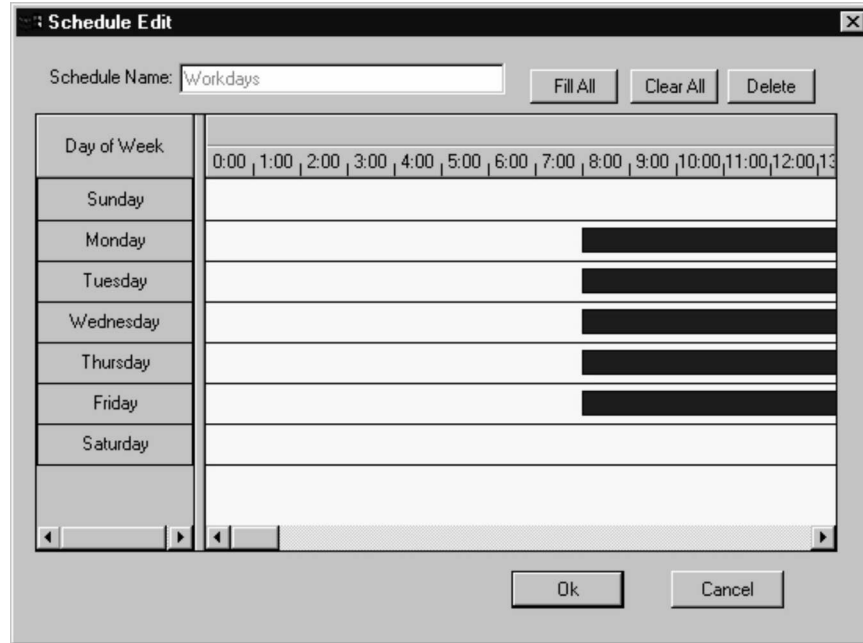


3. Modify the schedule as necessary.
 - Click **Fill All** to set the schedule to 24x7.
 - Click **Clear All** to remove all current schedule settings.
 - Click and drag on the schedule to set schedule days and times.
 - Drag and drop to move a schedule bar to another time slot.
4. Click **OK**.
5. Click **Update** to save the changes in the database and upload the configuration to the controller.

To Add a Schedule

1. Open the Bandwidth Manager Properties screen, and click the **Schedules** tab.
2. Click **Add**.

Figure 148 Schedule Edit Dialog Box—Add Mode



3. In the **Schedule Name** field, type a unique name for the schedule.
4. Set the schedule in the Date/Time graph.
 - Click **Fill All** to set the schedule to 24x7.
 - Click **Clear All** to remove all current schedule settings.
 - Click and drag on the schedule to set schedule days and times.
 - Drag and drop to move a schedule bar to another time slot.
5. Click **OK**.
6. Click Update to save the changes in the database and upload the configuration to the controller.

9.7 Setting a Traffic Policy

A traffic policy governs the bandwidth used by subscribers. The following procedures are prerequisites to setting a traffic policy:

- Configuring subscribers, as described in [Assigning a Subscriber and Service Level to an EUM](#), on page 101
- Configuring the controller
- Configuring a bandwidth set
- Establishing a schedule

Traffic policies implement a bandwidth management Service Level Agreement (SLA). A comprehensive and complete set of policies will cover the full spectrum of your needs. Each policy is an association of an account, an IP group, a schedule, and a bandwidth set. Each policy accommodates one specific scenario. To accommodate multiple scenarios for a single IP group, create multiple policies for that group.

A subscriber is a billable, or charge-back, entity that identifies who to charge for specific portions of the bandwidth managed by the controller. Through a policy, a subscriber is linked to an IP group, schedule, priority, and bandwidth set. The subscriber identifies who to bill for the bandwidth usage of the associated IP Group. (One IP group may include a large collection of individual IP addresses.)

NOTE: An SLA includes all policies associating the same subscriber and IP group. Within the policies for one SLA, the schedule, priorities and bandwidth set vary. Through creating multiple policies, you can schedule all the bandwidth access variations that you may require.

An IP group is a collection of IP addresses and is associated with a subscriber. A traffic policy governs each IP group. An IP group may contain one or more single IP addresses. An address cannot appear in more than one IP group.

NOTE: All additional policies for the same subscriber and IP group must use a different, as well as non-overlapping, schedule. The bandwidth set data may have the same or different settings.

When different traffic policies govern two communicating IP groups, the traffic policy with the lower bandwidth setting governs the connection. Suppose one IP address has a traffic policy specifying a 10Mbps bandwidth limit and communicates with an IP address that has a traffic policy specifying a 5Mbps bandwidth limit. The connection between these IP addresses would automatically be limited to 5Mbps of bandwidth.

To effectively limit the bandwidth of an EUM and its associated network, it is advised that the entire IP range for the EUM network be assigned to one policy definition. This will force the network attached to that EUM to share the bandwidth for the entire policy. By defining multiple policies for a network attached to an EUM, you are allowing multiple virtual bandwidth pipes to be created and governed separately for each definition. This situation is elaborated in the following diagram.

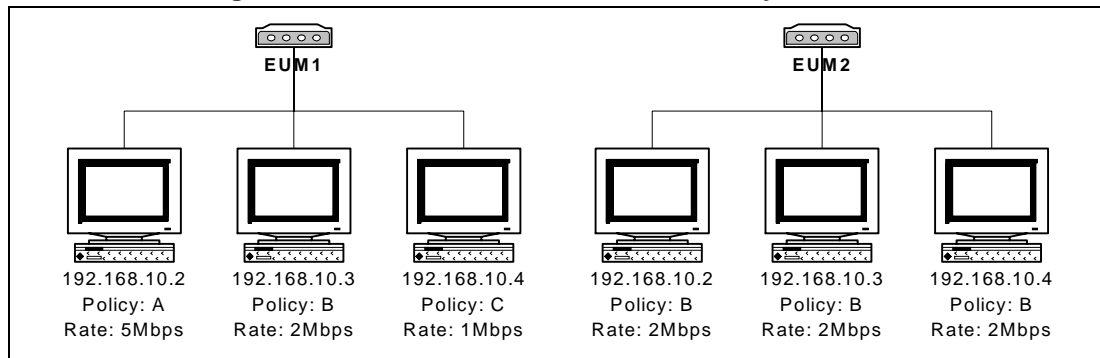
Figure 149 Two Different Bandwidth Policy Scenarios

Figure 149 shows two different IP groups—an IP group associated with EUM1, and an IP group associated with EUM2. The IPs associated with EUM1 are each using a different policy and therefore have different data rates. The IPs associated with EUM2 are each using the same policy and the same data rate.

When the IPs associated with an EUM use different data rates, as exemplified with EUM1 in Figure 149, you can determine the effective data rate by adding the data rates for each of the different policies. Therefore, the effective data rate for EUM1 would be 8Mbps.

When the IPs associated with an EUM use the same policy, and consequently the same data rate, as exemplified with EUM2 in Figure 149, the effective data rate is the data rate for that policy. Therefore, the effective data rate for EUM2 would be 2Mbps.

9.7.1 Adding a Policy

Adding a policy involves the following procedures:

- Creating an IP group
- Defining policy control options for the IP group

On the New Policy Definition screen, **EUM/Subscriber Name** identifies an existing EUM and the subscriber associated with that EUM.

IP Group Name is a descriptive name of up to 30 alphanumeric characters that uniquely identifies the IP group within the account.

IP/IP Range is a list of IP addresses that comprise the IP group. This field may contain up to 256 alphanumeric characters. An IP address cannot appear in more than one IP group.

Bandwidth Set identifies the bandwidth set available to the IP addresses in this policy. This drop-down list contains all of the bandwidth sets identified on the Bandwidth Sets tab.

Schedule includes a drop-down list of all schedules defined in the Bandwidth Manager record. The bandwidth identified in the Bandwidth Set field is available to the IP addresses in the IP group during the time periods identified in the selected schedule.

Traffic Policy Direction specifies blocking or non-blocking of traffic flowing to and from the designated IP group. There are three traffic policy directions: None, Inbound, and Outbound. **None** allows traffic through both port A (LAN side) and port B (WAN side). **Inbound** blocks

traffic originated from the WAN side (i.e., blocks traffic received on B, which has a source address outside the defined IP group). **Outbound** blocks traffic originating from the LAN side to keep it from going out (i.e., blocks traffic received on A, which has a source address in the defined IP group).

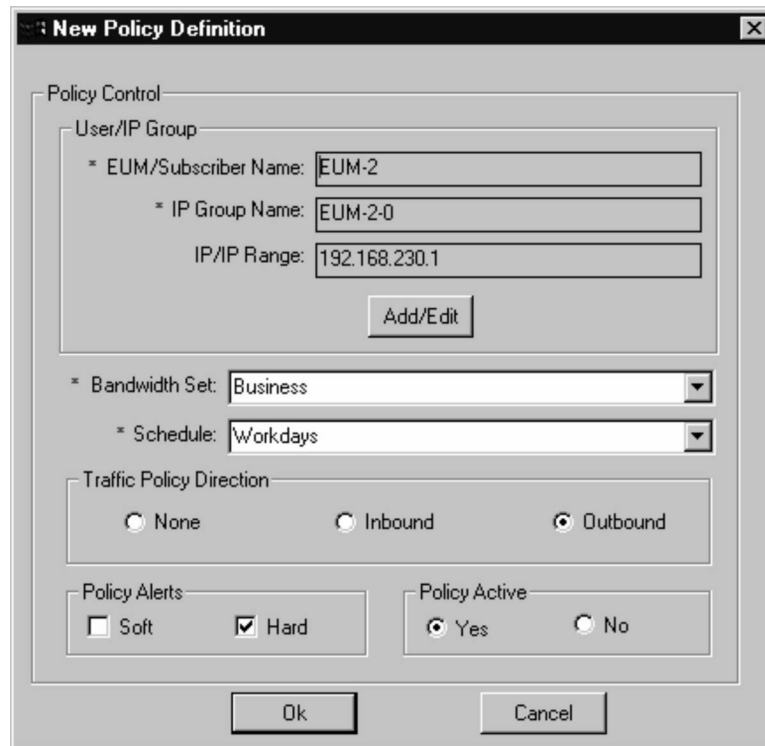
Policy Alerts enable you to select an alert type in the traffic policy to arm and activate the alert, but only if that alert was originally configured for the current controller. You may select both, either, or no alerts.

Policy Active identifies whether a policy is in the NMS database and whether this policy should govern the specified IP group whenever the controller is operating.

To Add an IP Group for an EUM

1. Open the **Policies** tab of the Bandwidth Manager Properties screen.
2. Click **Add**.

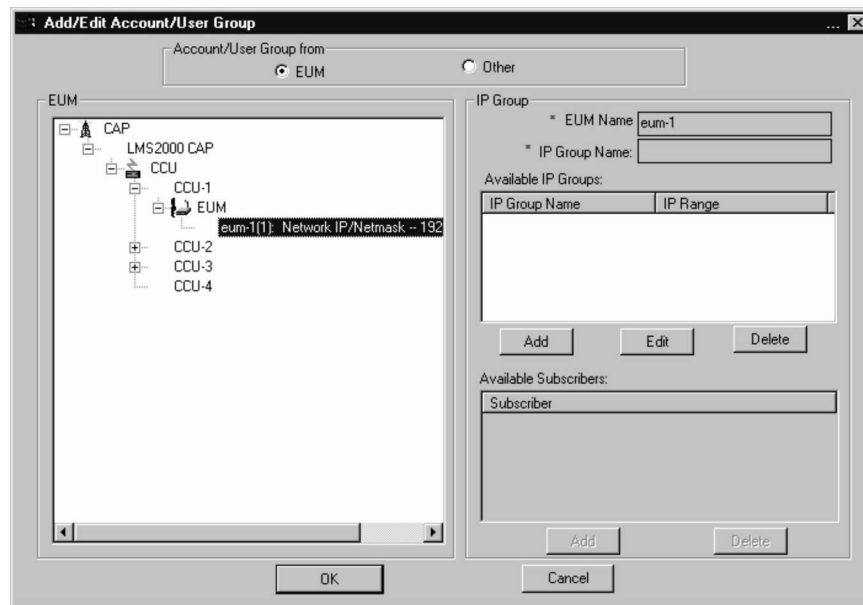
Figure 150 New Policy Definition Dialog Box



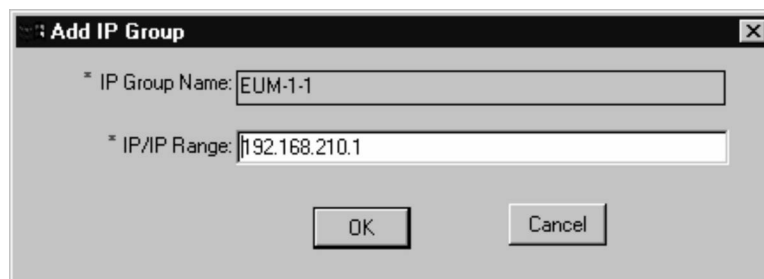
The dialog box is titled "New Policy Definition". It contains the following sections and controls:

- Policy Control**
 - User/IP Group**
 - * EUM/Subscriber Name:
 - * IP Group Name:
 - IP/IP Range:
 -
 - * Bandwidth Set:
 - * Schedule:
 - Traffic Policy Direction**
 - ☐ None
 - ☐ Inbound
 - ☒ Outbound
 - Policy Alerts**
 - ☐ Soft
 - ☒ Hard
 - Policy Active**
 - ☒ Yes
 - ☐ No
- At the bottom are and .

3. Click **Add/Edit**.

Figure 151 Add/Edit Account/User Group

4. Ensure the **EUM** option is selected.
5. In the EUM group, expand the tree and select the EUM for which to create an IP group.
6. Under Available IP Groups, click **Add**.

Figure 152 Add IP Group

7. In the **IP/IP Range** field, type the IP address of the computer to add to the group.

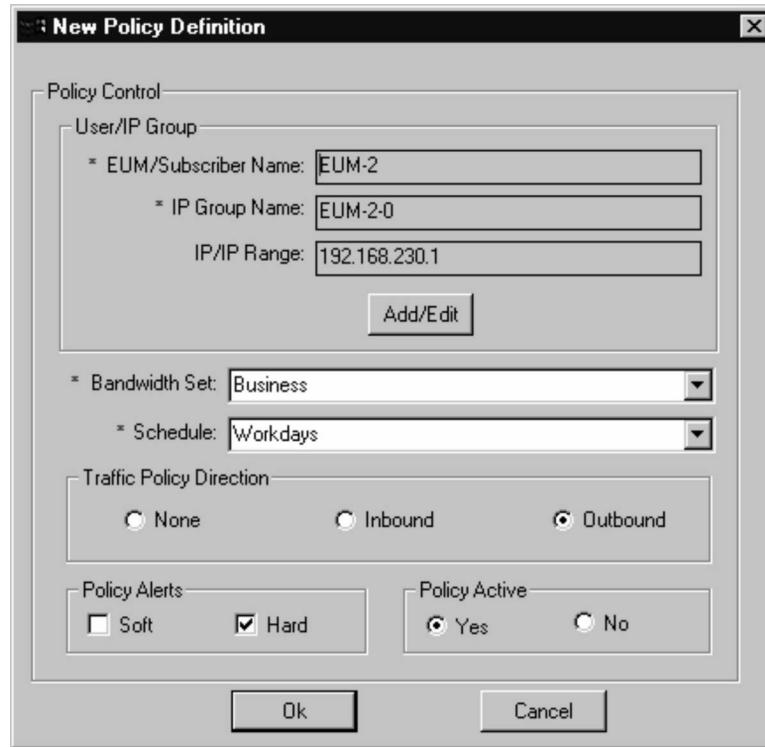
NOTE: To add a range of IP addresses, type the first IP address followed by a dash and the last IP address in the range. If the initial octets in the IP range match, you need only include the changed portion of the IP address in the second portion of the range. For example, typing **192.168.10.1-254** would add all IP addresses in that range to the IP group. DO NOT include spaces when typing the IP address range.

8. Click **OK** to close the Add IP Group dialog box.
9. Click **OK** to close the Add/Edit Account/User Group dialog box.

To Define Policy Control Options for the IP Group

1. Complete the steps in [To Add an IP Group for an EUM](#), on page 164.

Figure 153 New Policy Definition Dialog Box



The dialog box is titled "New Policy Definition". It contains several sections for configuring policy control:

- Policy Control** (Group Box):
 - User/IP Group** (Group Box):
 - * EUM/Subscriber Name:
 - * IP Group Name:
 - IP/IP Range:
 -
 - * Bandwidth Set:
 - * Schedule:
 - Traffic Policy Direction** (Group Box):
 - ☐ None
 - ☐ Inbound
 - ☒ Outbound
 - Policy Alerts** (Group Box):
 - ☐ Soft
 - ☒ Hard
 - Policy Active** (Group Box):
 - ☒ Yes
 - ☐ No
- At the bottom are and .

2. From the **Bandwidth Set** drop-down list, assign a bandwidth set to the members of this IP group.
3. From the **Schedule** drop-down list, select the schedule to which the bandwidth set applies.
4. Select one of the following traffic policy options:
 - **None** allows traffic through both port A (LAN side) and port B (WAN side).
 - **Inbound** blocks traffic originating from the WAN side.
 - **Outbound** blocks traffic originating from the LAN side to keep it from going out.
5. Select the desired policy alerts.

NOTE: You may select one, both, or no policy alerts.

6. Select **Yes** to activate the policy.
7. Click **OK** to close the New Policy Definition screen.
8. Click **Update** to save changes in the database and upload them to the controller.

10

Testing Communications

Once you have configured the devices on the LMS2000 network, you should test the communications. This chapter includes instructions for running communications tests for new and existing devices on the network. They are useful for performance monitoring and troubleshooting.

There are four tests available:

- Continuous Transmit (Tx)
- Continuous Receive (Rx)
- Transmit/Receive Loopback
- Ping

NOTE: You should not run more than one test at a time on a device.

For information about monitoring the performance of network devices, refer to [Monitoring Performance](#), on page 239.

The first three tests in this chapter report on the radio packet error rate (PER) ratio. [Table 7](#) identifies the transmission quality indicated by each of the radio PER ratios.

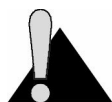
Table 7 Radio Packet Error Rate Definitions

Radio PER Ratio	Transmission Quality
less than 1%	excellent
less than 2%	good
less than 5%	marginal
greater than 5%	poor

10.1 Running the Continuous Transmit (Tx) Test

This test should only be used when setting up a new CCU. The purpose of this test is to send a continuous stream of messages broadcasted from a CCU to EUMs, which receive and discard the messages, or to a spectrum analyzer for signal monitoring. The Radio Packet Error Rate (PER) is displayed at an EUM receiving the Continuous Transmit messages and, using that information, an installer aligns the antenna accordingly. Refer to [Radio Packet Error Rate](#), on page 245 for more information.

You will need one CCU. At the other end of the link, you must have at least one EUM or a spectrum analyzer. The following procedure describes the test for a CCU and EUM configuration. If you are using a spectrum analyzer, adjust the antenna for a maximum received signal.



CAUTION: Do NOT run this test in a working CCU configuration. Doing so will cause the CCU and all associated EUMs to slow down.

To Run the Continuous Transmit (Tx) Test

1. Ensure that the CCU is operating.
2. Deploy the EUM, connecting the antenna as required.

WARNING!



Antennas and associated transmission cable must be installed by qualified personnel. Failure to terminate the antenna port correctly can permanently damage the CCU or EUM. WaveRider assumes no liability for failure to adhere to this recommendation or to recognized general safety precautions.

3. Connect a terminal and log into the EUM using a serial cable.
4. From the NMS Workstation, open a Telnet session to the CCU and log into the device.
5. Type `<radio txTest start>` to begin the Continuous Transmit Test. "Radio Tx Test On" is displayed above the device prompt when the test is running.
6. At the EUM console terminal, type `<radio per continuous>` to begin displaying the Radio PER. Refer to [Radio Packet Error Rate](#), on page 245 for more information.
7. Using the information from Radio PER, align the antenna at the EUM so that the number of packets missed is at a minimum rate.
8. When done with the antenna alignment, stop the test at the CCU. Type `<radio txTest stop>`.

9. At the EUM, press any key to end the Radio PER output.

NOTE: By default, a CCU keeps track of the Radio PER of each EUM. An EUM does not track the Radio PER of another visible EUM unless it is running the Continuous Receive test. Refer to [Running the Continuous Receive \(Rx\) Test](#), on page 170. An EUM does track the Radio PER of both direct and broadcast communication with the CCU.

The information received from Radio PER during the Continuous Transmit test will be similar to the following output. The following output is from an EUM (ID 2) communicating with the CCU (ID 1) that is running the Continuous Transmit test.

EUM> radio per continuous

Unit Id	Link Status	Total # Received	Total # Missed	PER (%)
1	UP	2	0	0
broadcast		5	0	0

Unit Id	Link Status	Total # Received	Total # Missed	PER (%)
1	UP	2	0	0
broadcast		820	56	6

Unit Id	Link Status	Total # Received	Total # Missed	PER (%)
1	UP	2	0	0
broadcast		1679	91	5

Unit Id	Link Status	Total # Received	Total # Missed	PER (%)
1	UP	2	0	0
broadcast		2545	126	4

Unit Id	Link Status	Total # Received	Total # Missed	PER (%)
1	UP	2	0	0
broadcast		3411	149	4

EUM>

10.2 Running the Continuous Receive (Rx) Test

The purpose of this test is to help you deploy an additional EUM in an existing network without interrupting traffic to the currently active EUMs in the network. The test is run from the new EUM to “sniff” packets destined to every other EUM (originated by the CCU) in the system. The test is run simultaneously with Radio PER which displays the number of packets received and missed for each EUM that is sniffed.

To Run a Continuous Receive Test

1. Ensure that the new EUM has been configured and tested.
2. Deploy the EUM, and connect the antenna.

WARNING!



Antennas and associated transmission cable must be installed by qualified personnel. Failure to terminate the antenna port correctly can permanently damage the EUM. WaveRider assumes no liability for failure to adhere to this recommendation or to recognized general safety precautions.

3. Connect a terminal at the EUM using a serial cable and log into the device.
4. At the EUM, type `<radio rxTest start>` to begin “sniffing” the transmissions and automatically start the Radio PER display. “Continuous Rx test started” is displayed when the test is started.

NOTE: If you stop the Radio PER display (press any key), you can restart the display by typing `<radio per continuous>`.

5. Using the information from Radio PER, align the antenna at the EUM so that the number of packets missed is at a minimum rate.
6. When done with the antenna alignment, press any key to stop the Radio PER display, then type `<radio rxTest stop>` to stop the test.

NOTE: When the Continuous Receive test is stopped, the CCU statistics, both direct and broadcast, remain in the Radio PER list and continue to be updated. If the Continuous Receive test is restarted, the statistics for the CCU and broadcast will continue from where they left off. The EUMs will start from zero again.

The information received from Radio PER during the Continuous Receive test will be similar to the following output. The following output is from an EUM (ID 2) communicating with the CCU (ID 1) that is also transmitting to another EUM (ID 3).

```
EUM> radio rxtest start
```

```
Continuous Rx test started
```

Unit Id	Link Status	Total # Received	Total # Missed	PER (%)
1	UP	1	0	0
broadcast		509	0	0
3	UP	1	0	0

Unit Id	Link Status	Total # Received	Total # Missed	PER (%)
1	UP	1	0	0
broadcast		510	0	0
3	UP	1	0	0

Unit Id	Link Status	Total # Received	Total # Missed	PER (%)
1	UP	1	0	0
broadcast		512	0	0
3	UP	1	0	0

Unit Id	Link Status	Total # Received	Total # Missed	PER (%)
1	UP	1	0	0
broadcast		515	0	0
3	UP	1	0	0

Unit Id	Link Status	Total # Received	Total # Missed	PER (%)
1	UP	1	0	0
broadcast		518	0	0
3	UP	1	0	0

```
[Radio Rx Test On]
```

```
EUM> radio rxtest stop
```

```
EUM>
```

10.3 Running the Transmit/Receive Loopback Test

This test should only be used when setting up a new network. The purpose of this test is to ensure that the CCU can “see” the EUM. It also determines the quality of the links between CCU and EUM. The test originates at the CCU, repeatedly sending test packets to the EUMs. An EUM recognizes these as test packets from the CCU and echoes them back to the CCU. When the CCU receives the replies from the EUM, it updates its Radio PER for that EUM. One CCU can have up to 30 EUMs simultaneously echoing test packets back to it.

You will need one CCU and at least one EUM.



CAUTION: Do NOT run this test in a working CCU configuration. Doing so will cause the CCU and all associated EUMs to slow down.

To Run the Transmit/Receive Loopback Test

1. Ensure that the CCU and EUMs have been configured and tested.
2. Deploy the CCU and at least one EUM, connecting the antennas for each device as required.

WARNING!



Antennas and associated transmission cable must be installed by qualified personnel. Failure to terminate the antenna port correctly can permanently damage the EUM. WaveRider assumes no liability for failure to adhere to this recommendation or to recognized general safety precautions.

3. Open a Telnet session to the CCU and log into the device.
4. Type `<radio txrx start>` to begin the Transmit/Receive Loopback test and automatically start the Radio PER display. “Tx/Rx test started” is displayed when the test is started.
5. Using the information from Radio PER, determine the quality of the link between the CCU and EUMs.
6. When done, press any key to stop Radio PER, then stop the Transmit/Receive Loopback Test by typing `<radio txrx stop>`.

The information received from Radio PER during the Transmit/Receive Loopback test will be similar to the following output. The following output is from a CCU (ID 1) communicating with two EUMs (IDs 2 and 3).

```
CCU> radio txrx start
```

```
Tx/Rx test started
```

Unit Id	Link Status	Total # Received	Total # Missed	PER (%)
2	UP	9	0	0
3	UP	5	0	0

Unit Id	Link Status	Total # Received	Total # Missed	PER (%)
2	UP	827	53	6
3	UP	820	56	6

Unit Id	Link Status	Total # Received	Total # Missed	PER (%)
2	UP	1689	85	4
3	UP	1679	91	5

Unit Id	Link Status	Total # Received	Total # Missed	PER (%)
2	UP	2566	109	4
3	UP	2545	126	4

Unit Id	Link Status	Total # Received	Total # Missed	PER (%)
2	UP	3423	141	3
3	UP	3411	149	4

```
[Radio TxRx Test On]
CCU> radio txrx stop
CCU>
```

10.4 Performing a Ping Test

The ping test is used to verify that a radio link exists between two devices. You can perform the ping test from an EUM or CCU or from the NMS Workstation.

To Perform a Ping Test from an EUM or CCU

1. At the terminal console keyboard, log into the EUM or CCU.
2. At the prompt, type `<ip ping ip_address>` where *ip_address* is the IP address LMS2000 network.
3. Let the `ip ping` command run for approximately 10 seconds. Press any key to end the `ip ping` command. If your configuration is correct, you should get a response similar to the following:

```
EUM>
EUM> ip ping 10.0.2.52
Press any key to stop.
PING 10.0.2.52: 56 data bytes
64 bytes from 10.0.2.52: icmp_seq=0. time=0. ms
64 bytes from 10.0.2.52: icmp_seq=1. time=30. ms
64 bytes from 10.0.2.52: icmp_seq=2. time=0. ms
64 bytes from 10.0.2.52: icmp_seq=3. time=0. ms
64 bytes from 10.0.2.52: icmp_seq=4. time=0. ms
64 bytes from 10.0.2.52: icmp_seq=5. time=0. ms
64 bytes from 10.0.2.52: icmp_seq=6. time=0. ms
----10.0.2.52 PING Statistics----
7 packets transmitted, 7 packets received, 0% packet loss
round-trip (ms) min/avg/max = 0/4/30
```

If the connection does not work, you will receive the following message:

```
EUM>
EUM> ip ping 10.0.2.52
Press any key to stop.
PING 10.0.2.52: 56 data bytes
no answer from 10.0.2.52
```

You receive replies only if the link is operational.

To Perform a Ping Test from the NMS Workstation

1. At the NMS Workstation, select **Start**, then **Command Prompt** to open an MS DOS window.
2. Type `<ping ip_address>` where *ip_address* is the IP address of a device in the LMS2000 network.
3. Let the ping command run to completion. If your configuration is correct, you should get a response similar to the following:

```
D:\>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.10.1: bytes=32 time<10ms TTL=255
Reply from 192.168.10.1: bytes=32 time<10ms TTL=255
Reply from 192.168.10.1: bytes=32 time<10ms TTL=255
Reply from 192.168.10.1: bytes=32 time<10ms TTL=255
```

If the connection does not work, you will receive the following message:

```
D:\>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

When the ping test has finished returning messages, close the DOS window.

— This page is intentionally left blank —

11

Backing up the System

This chapter describes how to back up your LMS2000 system using Backup Exec.

WaveRider recommends that you back up the NMS Workstation daily using the tape drive and Backup Exec on the NMS Workstation. A daily backup secures your system and subscriber information.

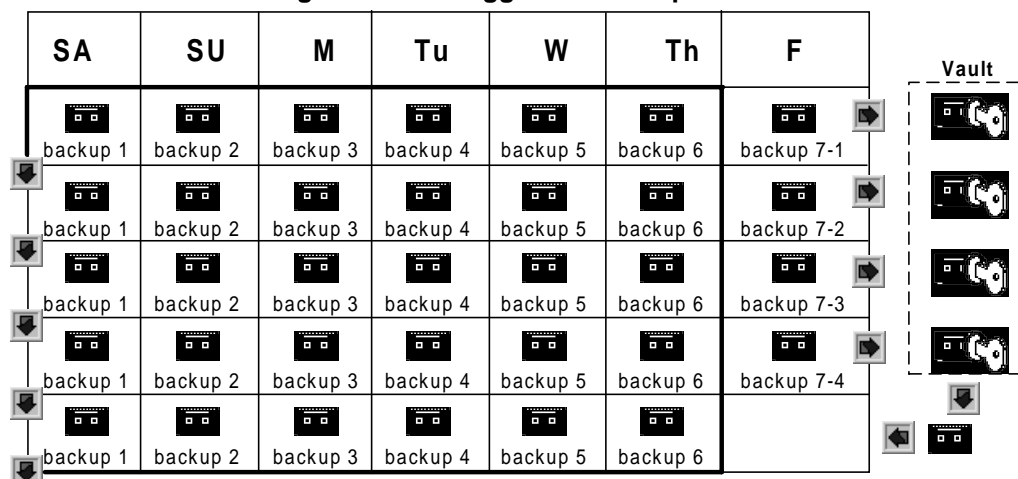
For detailed instructions about Backup Exec, refer to the *Backup Exec Administrator's Guide* included with your NAP equipment.

The SQL Server Agent plug-in to Backup Exec allows you to do hot backups of the SQL database. After installation, an SQL tab opens on the **Backup**, **Restore**, and **Tools > Options** screens.

11.1 Recommended Backup Schedule

The Backup Exec program transfers system information to a pre-formatted, labeled tape. A tape drive for backups is included as part of the NMS Workstation.

WaveRider recommends that you back up your system every day, and store each week's seventh backup off-site. [Figure 154](#) shows a schedule for sites that require a 30-day retention schedule.

Figure 154 Suggested Backup Process

11.2 Setting Backup Properties

Before you can back up your system, you must configure your backup settings through the VERITAS Backup Exec. Configuring backup settings involves three procedures:

1. **Set backup application defaults.** These application defaults apply to every backup job.
2. **Backup SNMP.**
3. **Define backup job properties.** These job properties are job specific, and you must re-define them for each backup.
4. **Schedule the backup.**

The following pages describe the steps in each of these procedures. Once you have completed them, you are ready to back up your system.



TIP: Remember to create a reminder in your daily process tasks to change the tape each day before the next backup. The once-a-week archived tape should be stored off-site in a secure location.

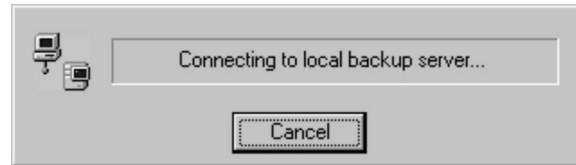
The following procedures include settings recommended by WaveRider. However, choose the settings that best meet your backup requirements.

To Set Application Defaults

1. From the **Start** menu select **Programs**, and then click **VERITAS Backup Exec** to open Backup Exec.

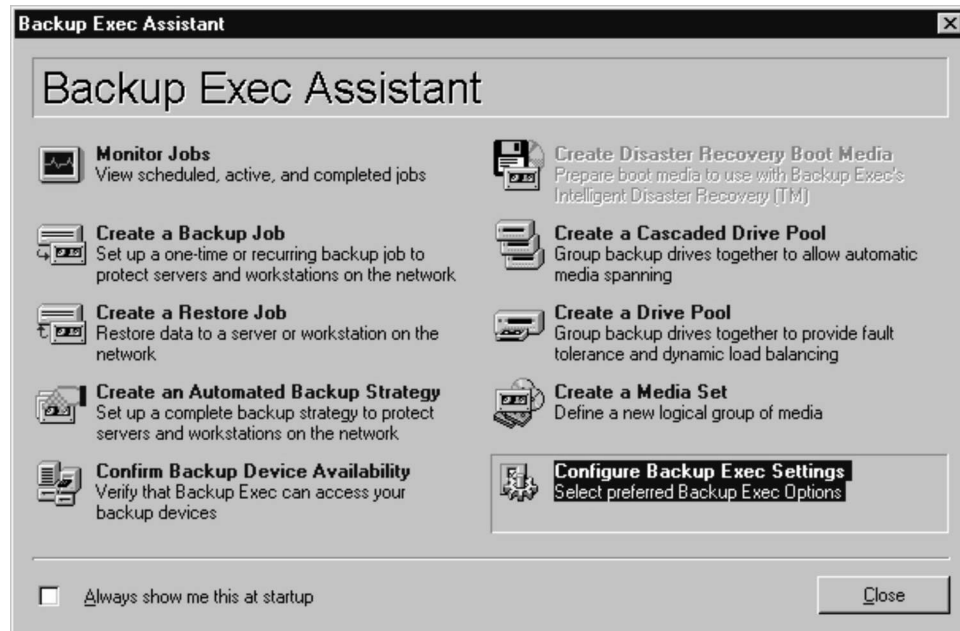
A progress indicator appears while the program is connecting to the server.

Figure 155 Progress Indicator



When the connection is established, the Backup Exec Assistant window opens.

Figure 156 Backup Exec Assistant



NOTE: If the Backup Exec Assistant doesn't open automatically, click the **Tools** menu and select **Backup Exec Assistant**.

2. In the Backup Exec Assistant, click **Configure Backup Exec Settings**.

The Options - Set Application Defaults screen opens.

3. Set the application defaults as shown in the following figures.

You need modify properties on the following tabs only:

- Media Overwrite
- Backup
- SQL
- Job History

NOTE: These figures show the WaveRider recommended settings. You may configure your backup properties to suit your backup needs.

Figure 157 Options - Set Application Defaults—Media Overwrite

Options - Set Application Defaults

NetWare SMS | Network | AppleTalk | Job History | Catalog
General | **Media Overwrite** | Backup | Restore | SQL

Media overwrite protection level

- ☐ Full - protect allocated and imported media
- ☐ Partial - protect only allocated media
 - ☐ Prompt before overwriting imported media
- ☒ None
 - ☐ Prompt before overwriting allocated or imported media

Media overwrite options

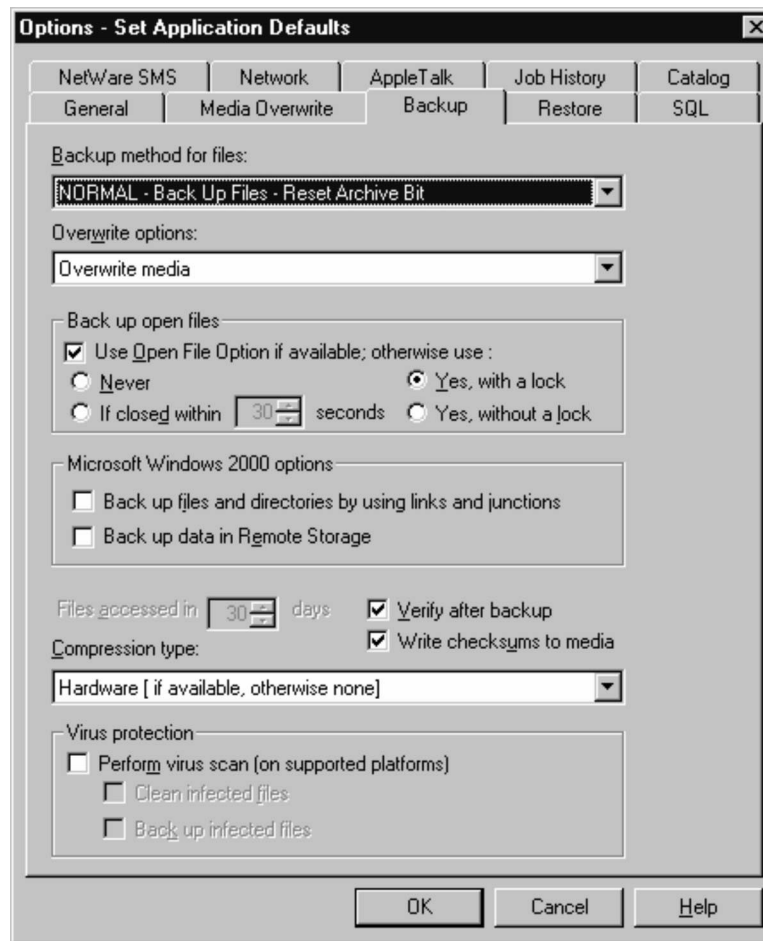
- ☒ Overwrite scratch media before overwriting recyclable media contained in the targeted media set
- ☐ Overwrite recyclable media contained in the targeted media set before overwriting scratch media

Media overwrite default label

Cartridge type:
4mm

Prefix: 4MM Next value: 1 Digits: 6

OK Cancel Help

Figure 158 Options - Set Application Defaults—Backup Tab

NOTE: In the Microsoft Windows 2000 options group, uncheck the **Back up files and directories by using links and junctions** option, which is checked by default.

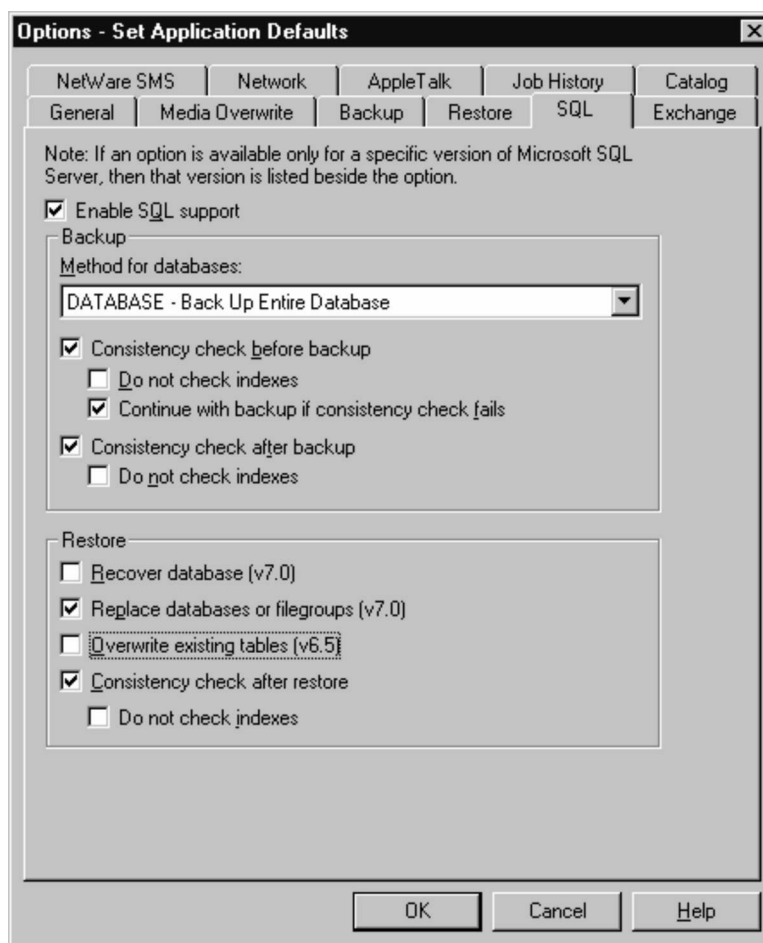
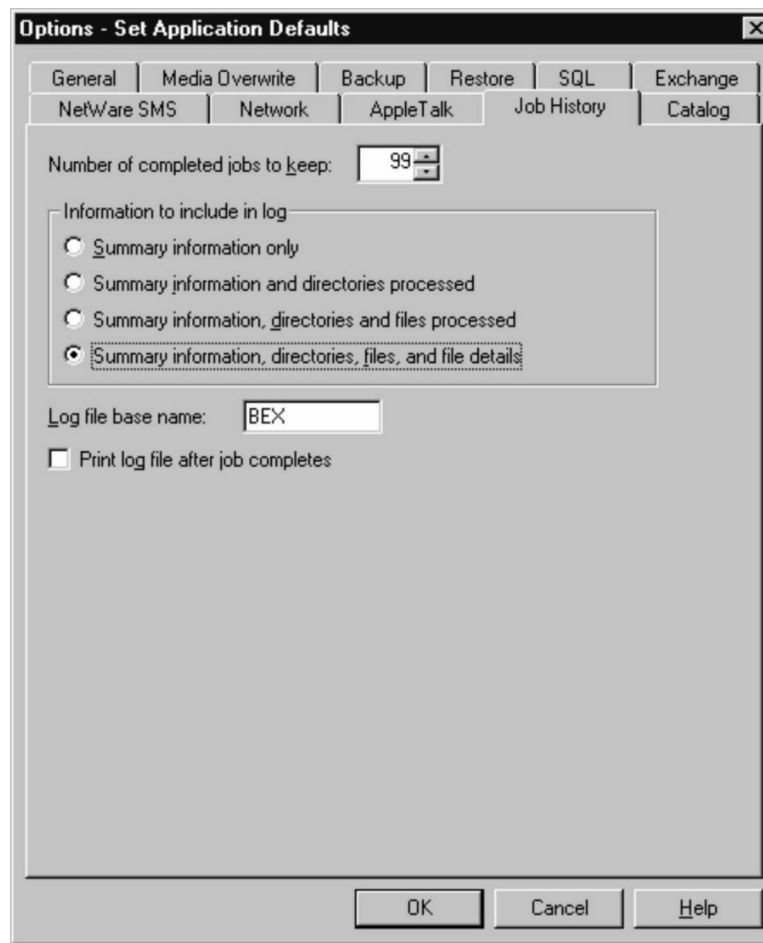
Figure 159 Options - Set Application Defaults—SQL Tab

Figure 160 Options - Set Application Defaults—Job History

NOTE: By default, the **Information to include in log** option is set to **Summary information only**. Change this option to **Summary information, directories, files, and file directories**.

4. Click **OK** to close the Options - Set Application Defaults dialog box.
5. Close the Backup Exec Assistant window.
6. Define your backup properties, as described in the following procedure.

To Backup SNMP

1. Open SNMPc Server.
2. Click **File > Backup**.

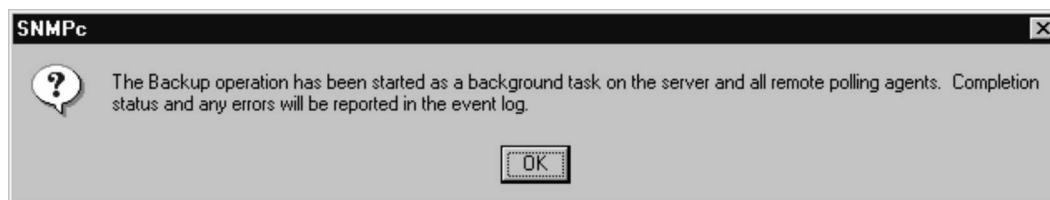
The Backup SNMPc Files dialog box opens.

Figure 161 Backup SNMPc Files



3. In the Backup SNMPc Files dialog box, type a name for the backup file in the **Backup To** field.
4. Click **Backup**.
5. The SNMP dialog box opens.

Figure 162 SNMPc Backup Confirmation Dialog Box



6. Click **OK**.
7. Click **Done**.

To Define Backup Job Properties

1. Click the **Backup** button on the Backup Exec button bar.

The **Backup Job Properties** screen opens with the **Selections** tab showing.

2. In the left pane, expand the tree for the C: drive to select the following directory:

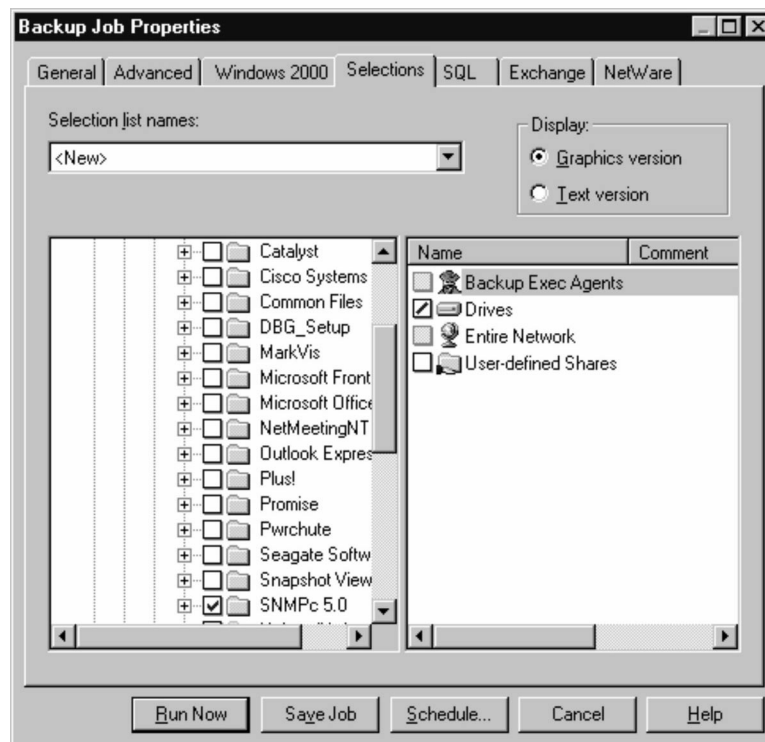
C:\Program Files\SNMPc 5.0.

NOTE: This is the default path for the file, but it may be located elsewhere if it has been moved.

3. Ensure the following directory is not selected: **C:\MSSQL7\Data.**

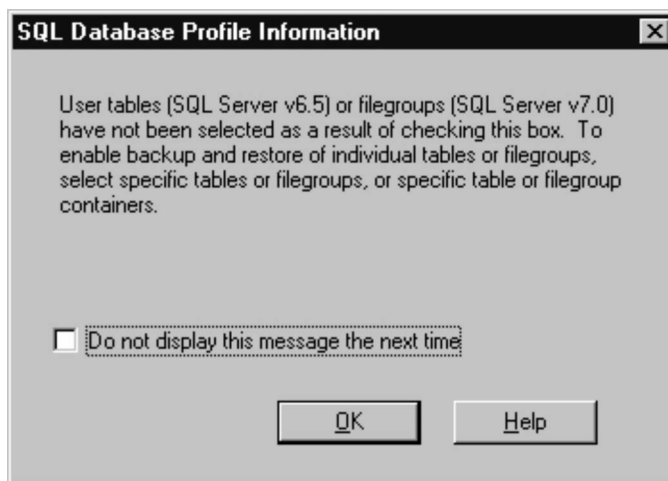
NOTE: Typically, SNMPc 5.0 is the only directory you will back up on the C: drive.

Figure 163 Backup Job Properties—Selections Tab—C Drive Backup

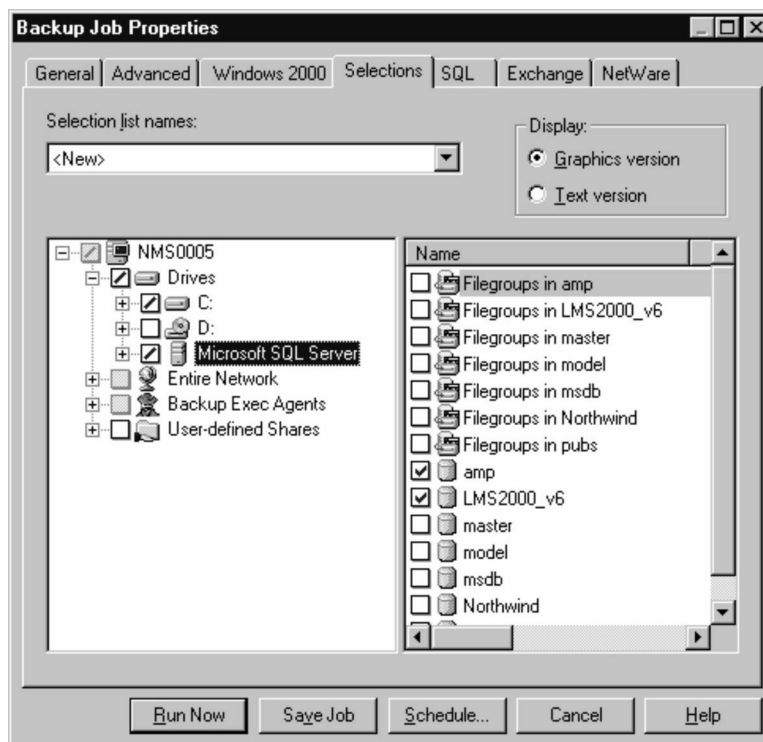


4. Select the **Microsoft SQL Server** check box.

The SQL Database Profile Information dialog box opens.

Figure 164 SQL Database Profile Information Dialog Box

5. Click **OK** to close the dialog box.

Figure 165 Backup Job Properties—Microsoft SQL Server Backup

6. In the right pane, select the **LMS2000_v6** and **amp** databases and leave the other databases and file groups unchecked.
7. Click the **General** tab.

Figure 166 Backup Job Properties—General Tab

Backup Job Properties

General | Advanced | Windows 2000 | Selections | SQL | Exchange | NetWare

Job name: Backup 0001

When this job begins:

- ☒ Overwrite media
- ☐ Append to media, overwrite if no appendable media is available
- ☐ Append to media, terminate job if no appendable media is available

Media name: Media created 10/24/00 06:36:50 PM

Backup set description: Backup 0001

Backup method for files: NORMAL - Back Up Files - Reset Archive Bit

Files accessed in: 30 days

Destination:

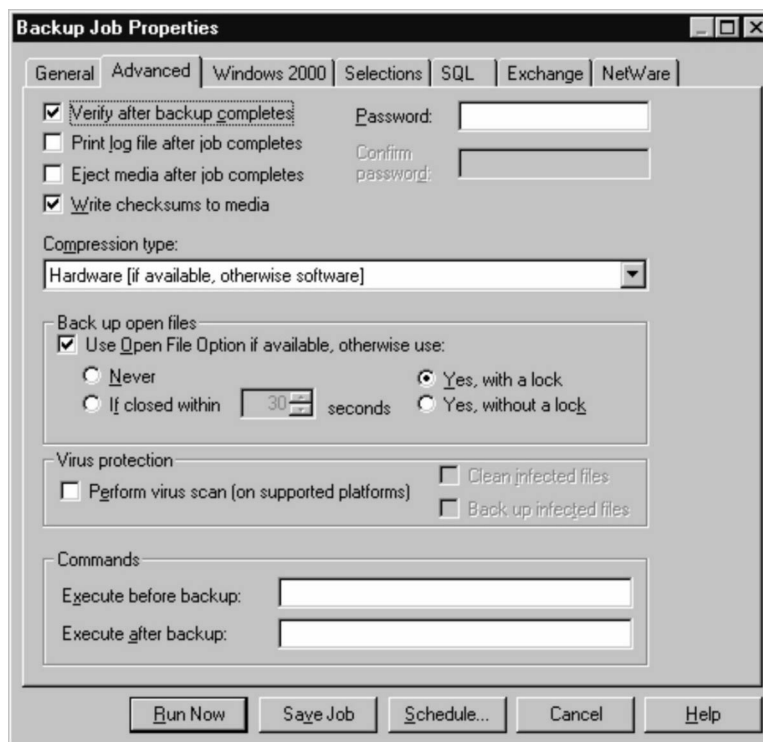
Device: All Drives (NMS0005)

Media set: Media Set 1

Run Now | Save Job | Schedule... | Cancel | Help

8. Enter a **Job Name** to identify this schedule.
9. Configure the other properties as shown in [Figure 166](#) or to suit your backup needs.
10. Click the **Advanced** tab.

Figure 167 Backup Job Properties—Advanced Tab



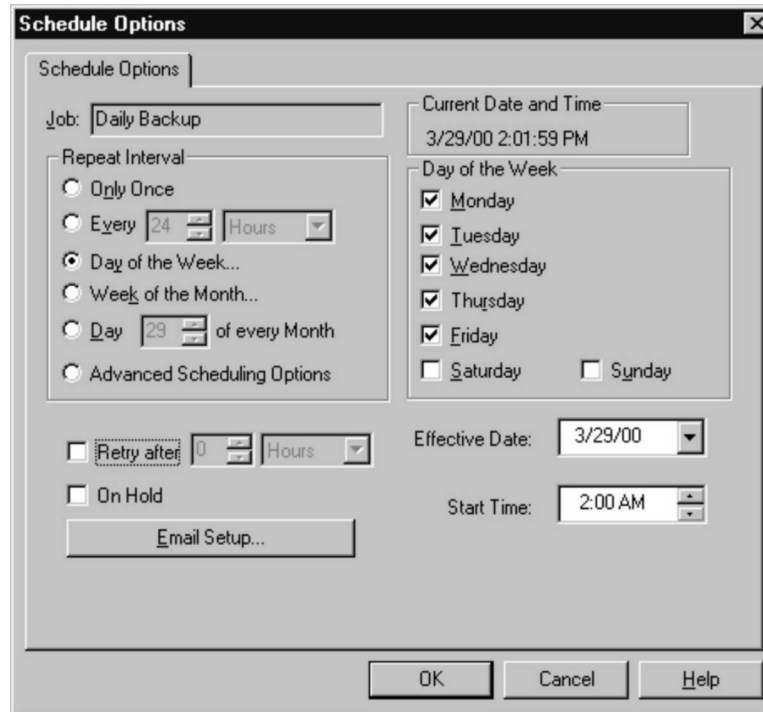
11. Leave the other settings as default.
12. Schedule the backup, as described in the following procedure.

To Schedule the Backup

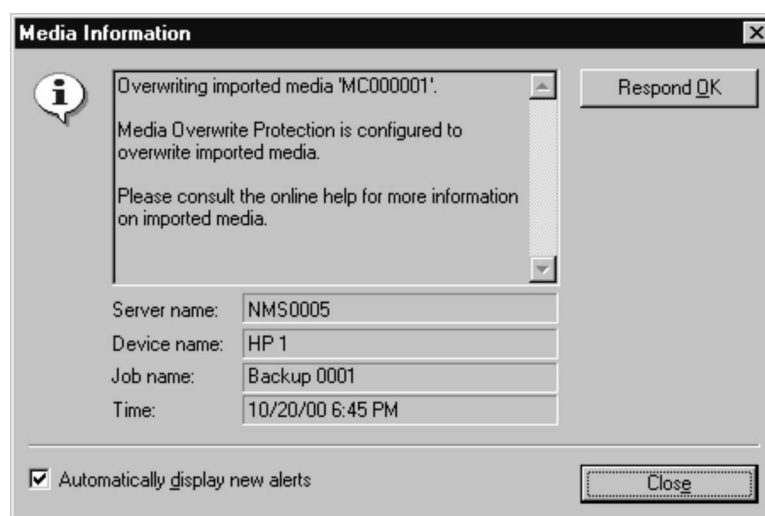
1. In the **Backup Job Options** window, click the **Schedule** button.

The Schedule Options window opens.

Figure 168 Schedule Options



2. Choose the options on the screen to define your backup schedule.
i.e. day, time, repeat interval, etc.
3. Click **OK** to save the schedule.
4. Place a formatted and labeled tape in the tape drive.
The program executes automatically at the time indicated.
5. If the backup tape already contains data, the following Media Request dialog box opens.

Figure 169 Media Request Dialog Box

6. Click **Respond OK** to overwrite the tape.

11.3 Backing Up Manually

If you want to back up only some of the files, or if your backup schedule is not consistent enough to schedule, you can perform a manual backup.



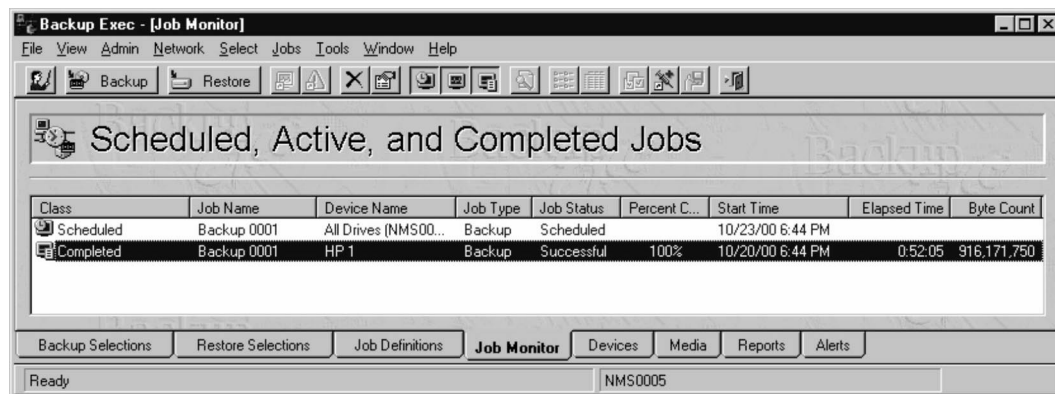
CAUTION: This procedure will cause system delays. Perform this procedure during off hours or low traffic times, so there is minimal impact to users.

To Back up Manually

1. Follow the steps in [To Define Backup Job Properties](#), on page 185.
2. Ensure that you have a formatted and labeled tape in the tape drive.
3. Click **Run Now**.

The backup starts immediately. When the backup is complete, the completed job appears in the Job Monitor of Backup Exec.

Figure 170 Backup Exec Job Monitor with Completed Job



11.4 Checking the Backed-up Files



CAUTION: As part of your daily schedule, WaveRider recommends that you check that the last backup occurred without error.

The **Scheduled, Active, and Completed Jobs** screen shows a list of jobs that have been processed as well as jobs that are waiting or which had errors. This includes both backup and restored jobs.

To Check a Backup File

1. Start VERITAS Backup Exec.
2. If the Backup Exec Assistant window is open, close it.
3. Ensure you are on the Job Monitor tab.

The **Job Monitor** screen opens and shows scheduled, active, and completed jobs.

Figure 171 Job Monitor

Class	Job Name	Device Name	Job Type	Job Status	Percent Complete	Start Time	Elapsed Time	Byte Count
Sche...	Backup 0001	HP 1	Backup	Scheduled		3/30/00 2:00 AM		
Active	Daily Backup	HP 1	Backup	Running		3/29/00 2:02 PM	0:01:29	3,746,222
Compl...	Restore 0057	HP 1	Restore	Successful	100%	3/29/00 12:00 PM	0:00:40	3,031,652
Compl...	Restore 0055	HP 1	Restore	Successful	100%	3/29/00 11:53 AM	0:00:42	3,031,652
Compl...	Backup 0045	HP 1	Backup	Failed	Unknown	3/29/00 10:51 AM	0:55:28	2,204,575...

You can perform a number of operations on the entries, including accessing the log file which identifies the specifics of what the job did when it executed.

For detailed information about the specific activities you might want to perform, refer to the OEM *VERITAS Backup Exec Administrator's Manual* included with your NAP equipment.

12

Restoring Backups

To restore backed-up files, complete the following procedures in order:

1. Close all files and programs, including the RFSM Service Manager, SNMPC, and NMS.
2. Restore SNMP.
3. Stop MSSQLServer and SQLServerAgent.
4. Switch the LMS2000_v6 database to single-user mode.
5. Switch the AMP database to single-user mode.
6. Stop and Restart MSSQLServer.
7. Restore files.
8. Verify that the LMS2000_v6 database has returned to multi-user mode.
9. Verify that the AMP database has returned to multi-user mode.
10. Restart MSSQLServer.
11. Reboot the computer.

Each of these procedures are outlined in detail on the following pages.

WARNING!



During this restore procedure, you must stop MSSQLServer, which will cause your LMS2000 system to stop operating. Whenever possible, run this restore procedure during low traffic periods.

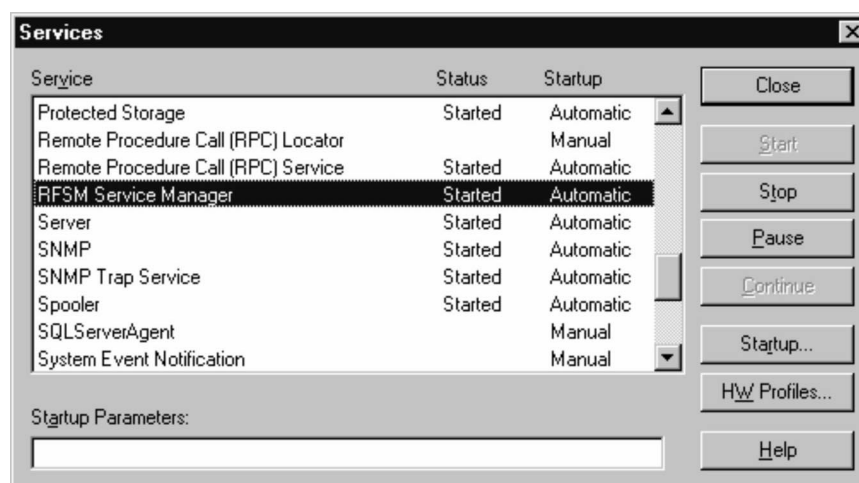
To Stop the RFSM Service Manager

1. Click the **Start** button.
2. Select **Settings > Control Panel**.

The Control Panel window opens.

3. In the Control Panel window, double-click the **Services** icon.


Figure 172 RFSM Service Manager in Services Window



4. Scroll down to RFSM Service Manager and select it.
5. Click the **Stop** button.

Figure 173 Service Control




When the service is stopped, the  icon disappears from the Windows task bar.

6. Click **Close** in the **Services** window.
7. Close the **Control Panel** window.

To Close SNMPc

1. Open the SNMPc Server.
2. On the **File** menu, click **Exit**.

To Close the NMS

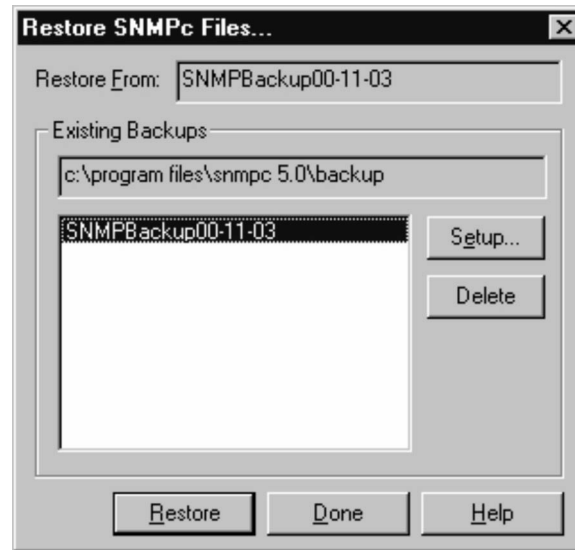
On the NMS main screen, click the  button.

To Restore SNMP

1. Open SNMPc Server.
2. Click **File > Restore**.

The Restore SNMP Files dialog box opens.

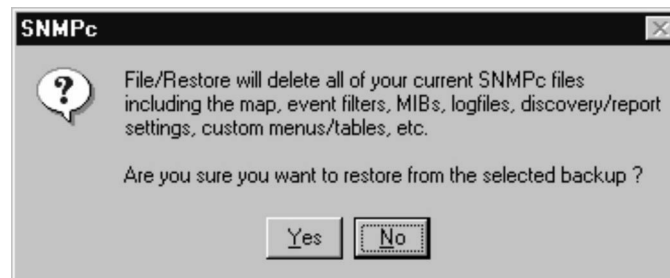
Figure 174 Restore SNMP Files Dialog Box



3. In the Restore SNMPc Files dialog box, select the backup file to restore.
4. Click **Restore**.

The SNMPc dialog box opens.

Figure 175 SNMPc File Restoration Dialog Box



5. Click **Yes**.
6. Click **Done** in the Restore SNMP Files dialog box.

The restoration of SNMP is complete.

To Stop MSSQLServer and SQLServerAgent

1. In the Windows System Tray, in the bottom right corner of your screen double-click the MSSQLServer icon.

Figure 176 MSSQLServer Icon in Windows System Tray



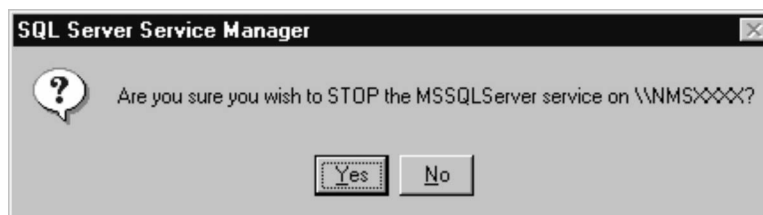
The SQL Server Service Manager opens.

Figure 177 SQL Server Service Manager



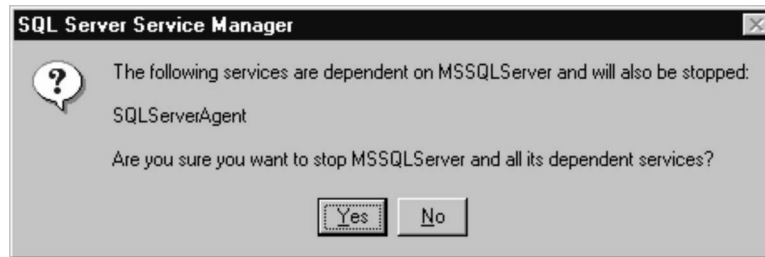
2. From the **Server** drop-down list, select the NMS Server on which to pause a database.
3. From the **Services** drop-down list, select **MSSQLServer**.
4. Click the **Stop** button.

Figure 178 Stop Database Confirmation Dialog Box



5. Click **Yes** to stop the MSSQLServer service.

The following dialog box opens to confirm that SQLServerAgent will stop.

Figure 179 Stopping SQLServerAgent Confirmation Dialog Box

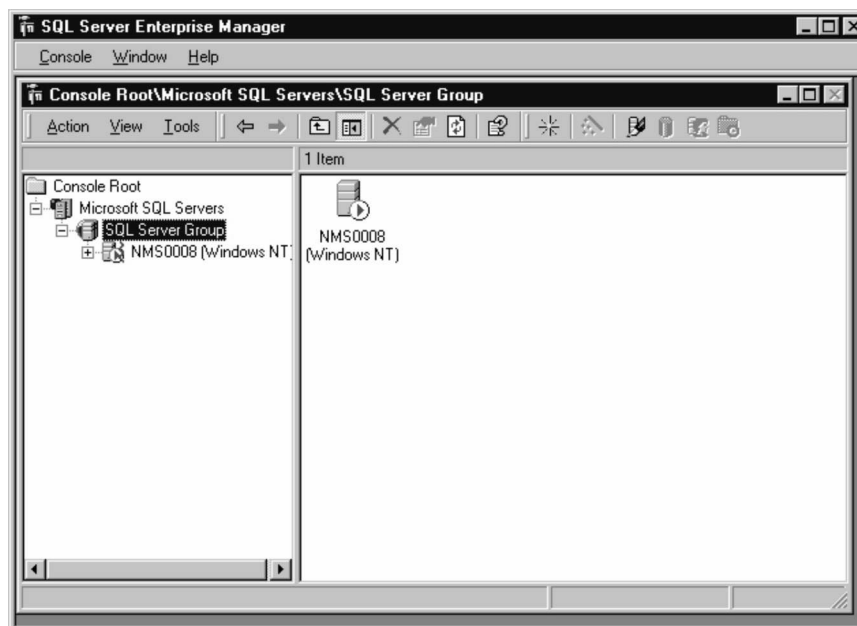
6. Click **Yes** to stop SQLServerAgent and close the dialog box.
7. From the **Services** drop-down list, select **SQLServerAgent**.
8. Verify that the SQLServerAgent has stopped, as shown in [Figure 180, SQL Server Service Manager—SQLServerAgent Stopped](#), on page 197.

Figure 180 SQL Server Service Manager—SQLServerAgent Stopped

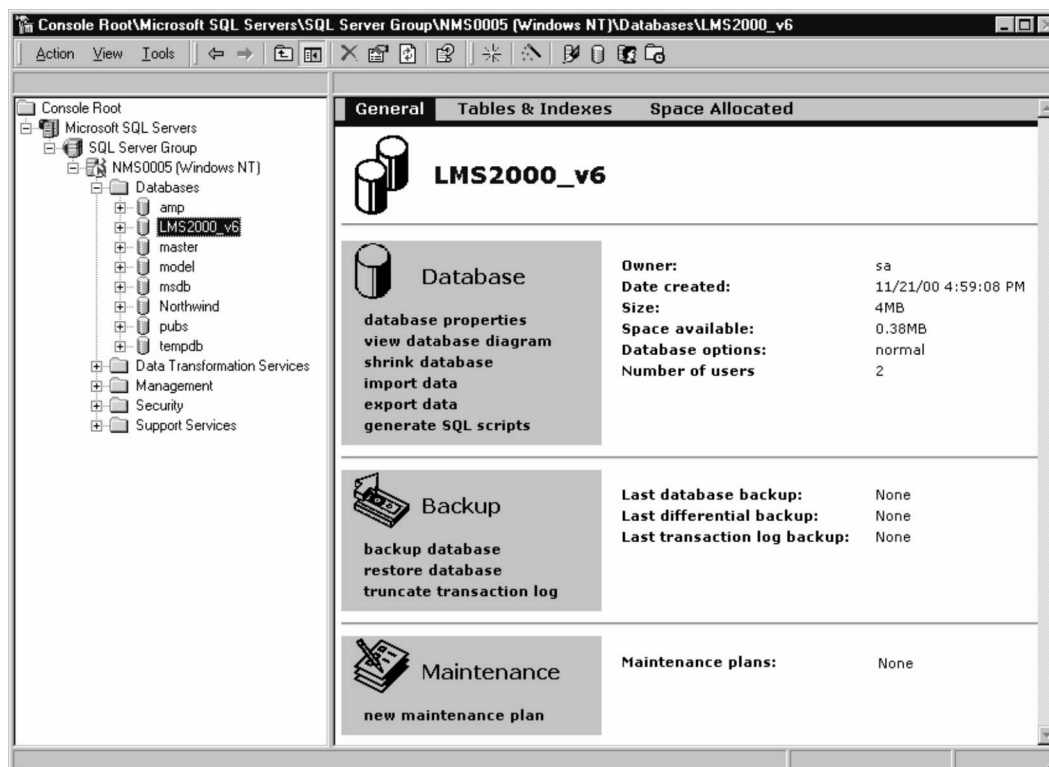
9. If the SQLServerAgent is not stopped, click the **Stop** button.
10. From the **Services** drop-down list, select **MSSQLServer**.
11. Click the **Start** button.
12. When MSSQLServer has restarted, close the SQL Server Service Manager.

To Switch the LMS2000_v6 Database to Single-user Mode

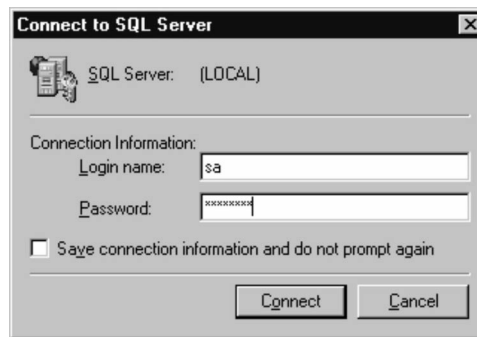
1. Click the Windows **Start** button and select **Programs > Microsoft SQL Server 7.0 > Enterprise Manager**.
2. Select the SQL Server Group.
3. Wait until the green arrow appears on the server icon, as shown in [Figure 181, SQL Server Group Started](#), on page 198.

Figure 181 SQL Server Group Started

4. In the left pane, navigate to the **LMS2000_v6** database and select it.

Figure 182 Microsoft SQL Server Enterprise Manager

The following dialog box opens.

Figure 183 Connect to SQL Server Dialog Box

5. In the dialog box, type your **Login name** and **Password**.

The Login name is **sa**; the password is **wave2000** (all lowercase).

6. Click **Connect**.

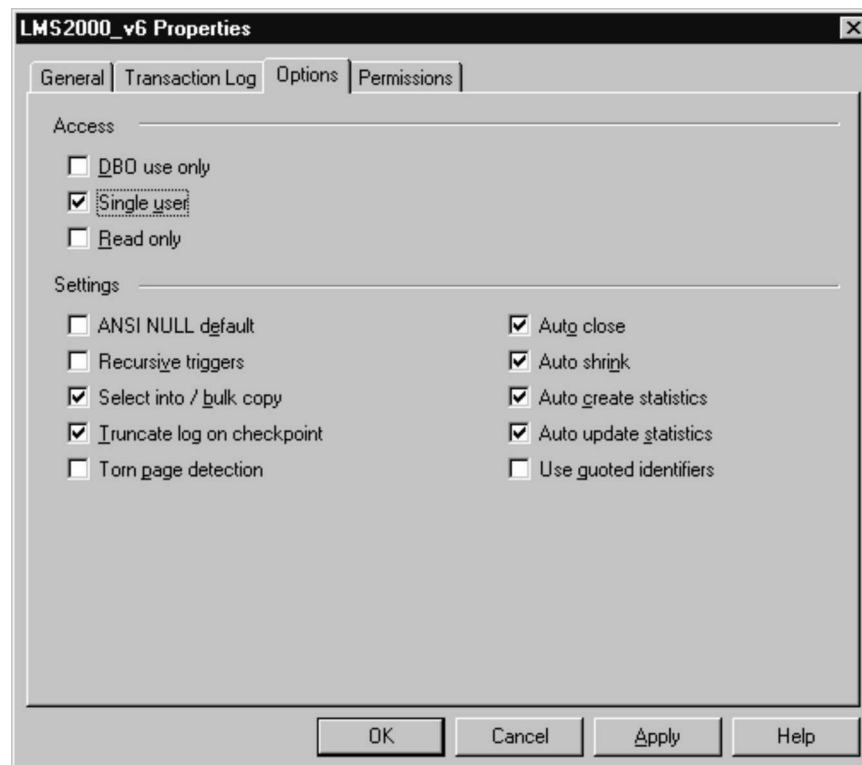
7. Right-click **LMS2000_v6** to open the shortcut menu.

8. Select **Properties** from the shortcut menu.

The LMS2000_v6 Properties dialog box opens.

9. Click the **Options** tab.

10. Select the **Single User** option.

Figure 184 LMS2000_v6 Properties Dialog Box

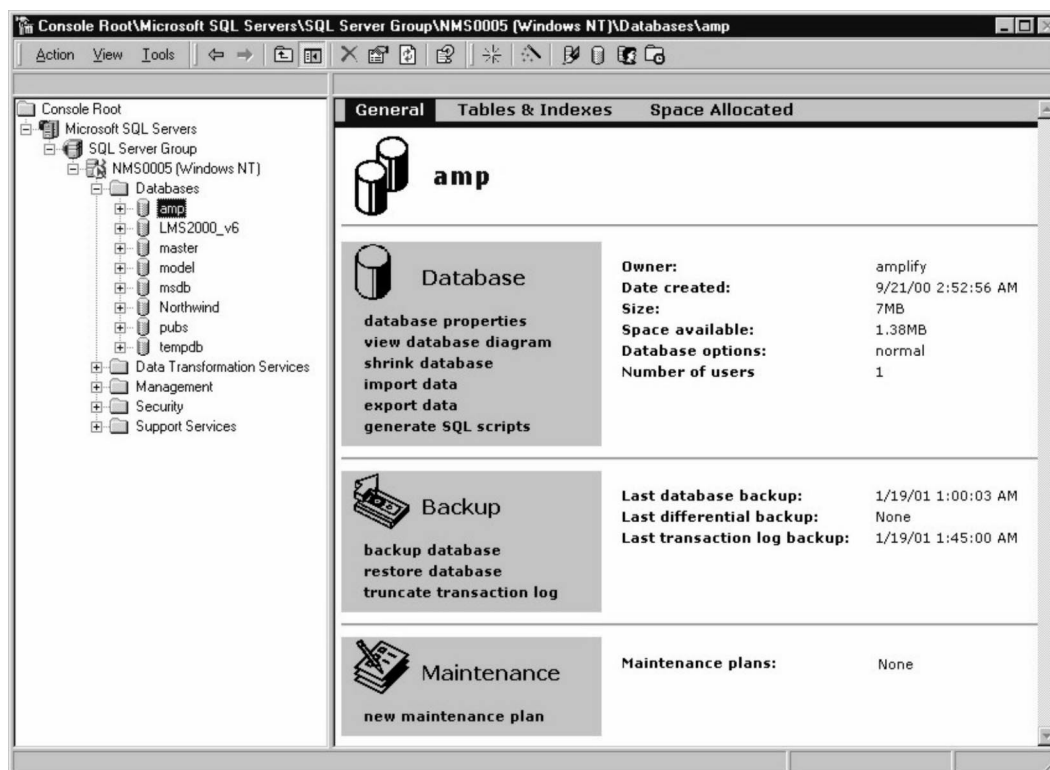
11. Click **Apply**.

12. Click **OK**.

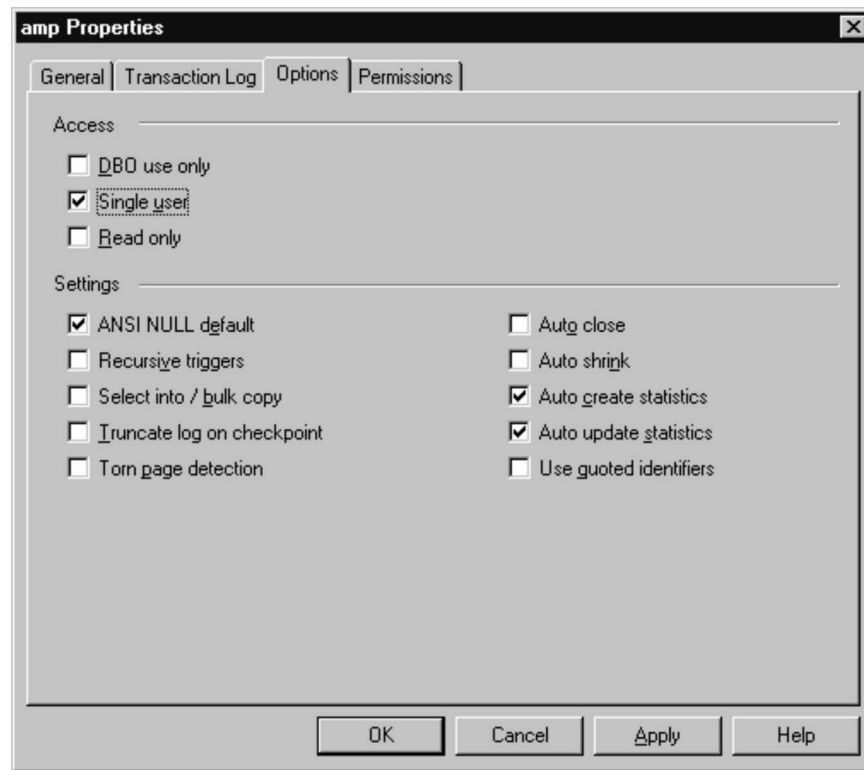
To Switch the AMP Database to Single-user Mode

1. In the left pane of SQL Server Enterprise Manager, navigate to the **amp** database and select it.

Figure 185 Microsoft SQL Server Enterprise Manager



2. Right-click **amp** to open the shortcut menu.
3. Select **Properties** from the shortcut menu.
The amp Properties dialog box opens.
4. Click the **Options** tab.
5. Select the **Single User** option.

Figure 186 AMP Properties Dialog Box

6. Click **Apply**.
7. Click **OK**.
8. Close Microsoft SQL Server Enterprise Manager.

To Stop and Restart MSSQLServer in Single-User Mode

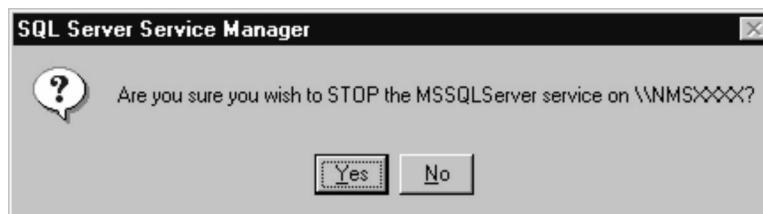
1. In the Windows System Tray, in the bottom right corner of your screen, double-click the MSSQL Server icon.

Figure 187 MSSQL Server Icon in Windows System Tray

The SQL Server Service Manager opens.

Figure 188 SQL Server Service Manager

2. From the **Server** drop-down list, select the NMS Server on which to pause a database.
3. From the **Services** drop-down list, select **MSSQLServer**.
4. Click the **Stop** button.

Figure 189 Stop Database Confirmation Dialog Box

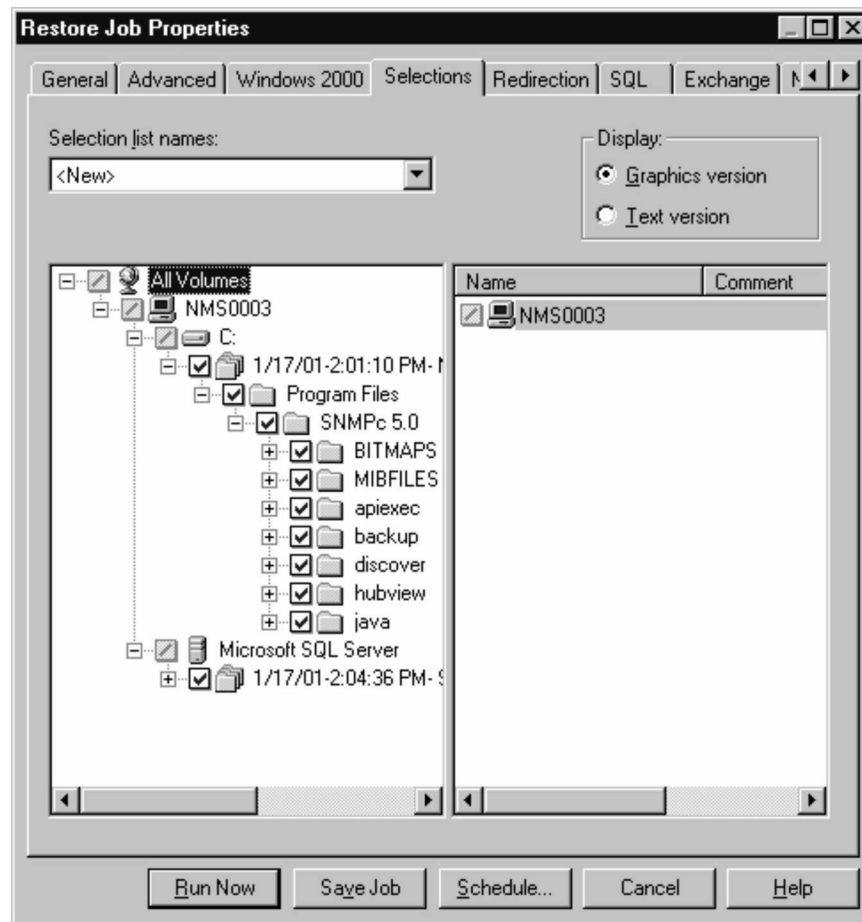
5. Click **Yes** to stop the MSSQLServer service.
6. Click the **Start** button.

To Restore Files

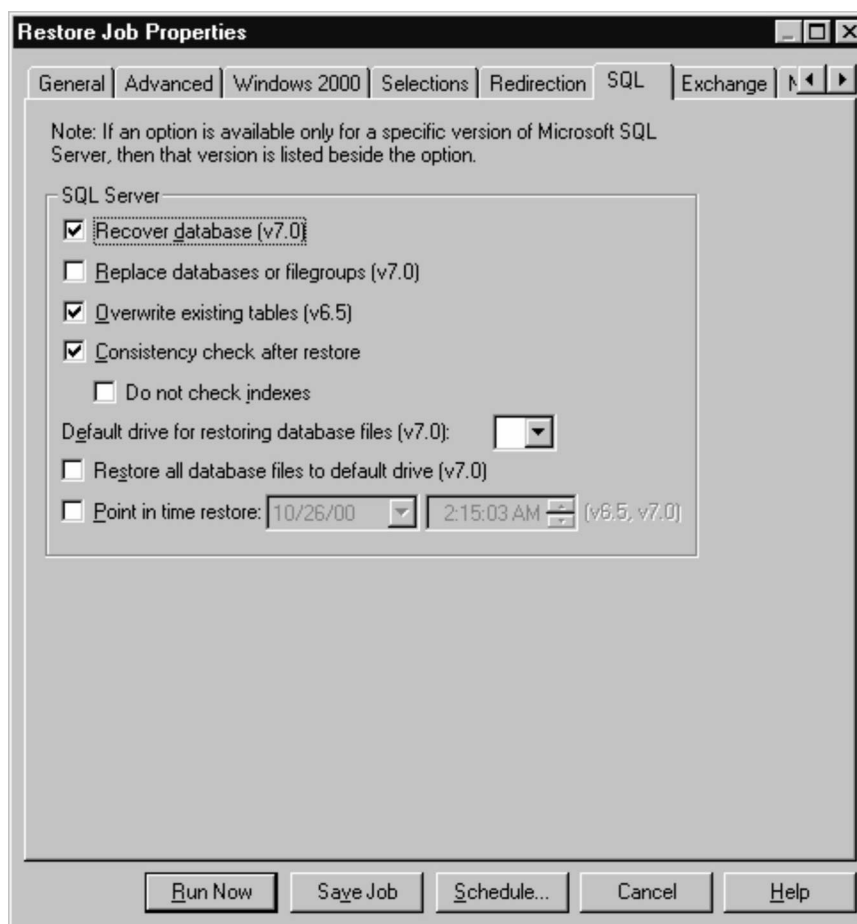
1. Start VERITAS Backup Exec.
2. Click the **Restore** button on the Backup Exec menu bar.

The **Restore Job Properties** screen opens with the **Selections** tab displayed.

NOTE: By default, the Backup Exec is set to do a full restore.

Figure 190 Restore Job Properties—Selections Tab

3. Ensure the folders are selected as shown in [Figure 190, Restore Job Properties—Selections Tab](#), on page 203.
4. Click the **SQL** tab.

Figure 191 Restore Job Properties—SQL Tab

5. Before you restore the final or only backup tape, select the **Recover database (v7.0)** check box.

If you have a multi-tape restore, leave this check box cleared until just before you restore the final tape.



CAUTION: You must select the Recover database (v7.0) check box before you restore the final or only tape. Otherwise, your restore will fail.

6. Ensure the **Replace databases or filegroups (v7.0)** check box is not selected.
7. Ensure the **Overwrite existing tables (v6.5)** check box is selected.



CAUTION: Ensure that Enterprise Manager is closed before proceeding. Otherwise, your restore will fail.

8. To restore immediately, click the **Run Now** button.

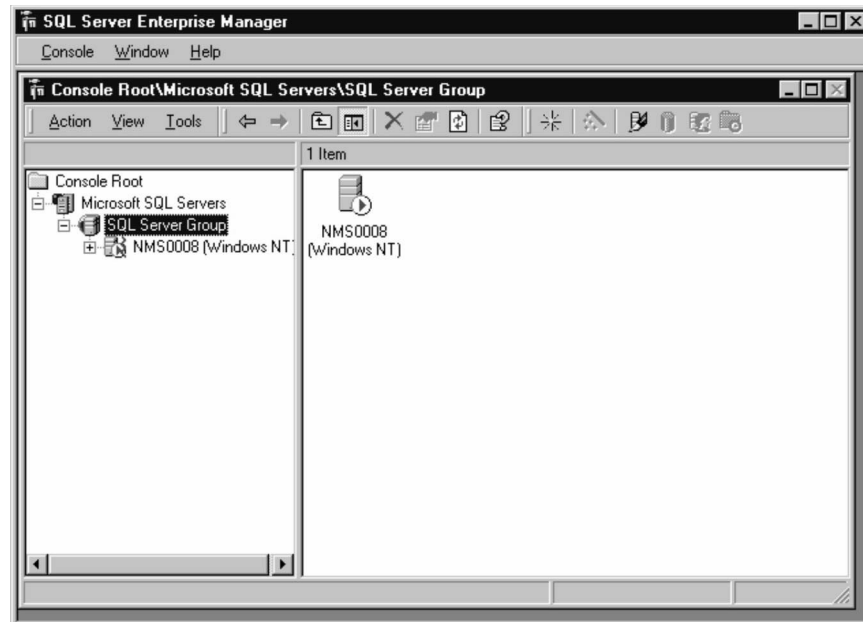
OR

To schedule the restore for later, click the **Schedule** button, and set the Schedule properties accordingly.

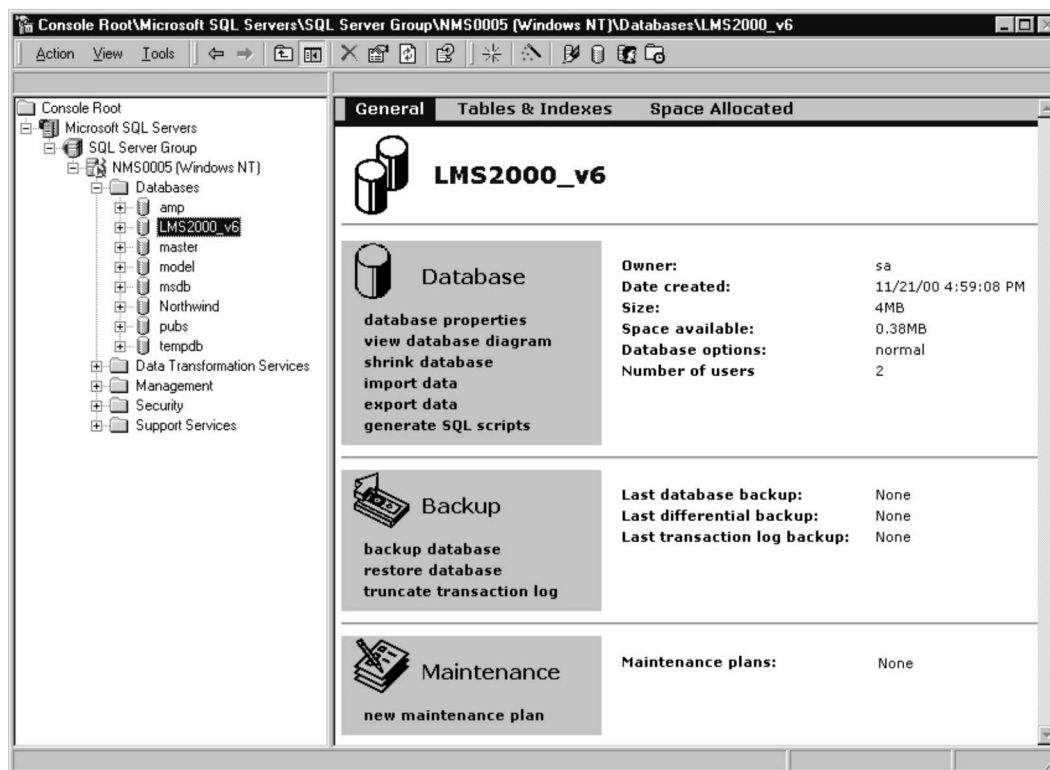
To Verify that the LMS2000_v6 Database Has Returned to Multi-user Mode

1. Click the Windows **Start** button and select **Programs > Microsoft SQL Server 7.0 > Enterprise Manager**.
2. Select the SQL Server Group.
3. Wait until the green arrow appears on the server icon, as shown in [Figure 192, SQL Server Group Started](#), on page 205.

Figure 192 SQL Server Group Started

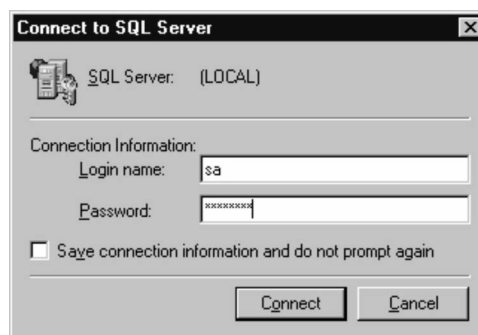


4. In the left pane, navigate to the **LMS2000_v6** database and select it.

Figure 193 Microsoft SQL Server Enterprise Manager

NOTE: The LMS2000_v6 database icon appears gray instead of yellow if you did not complete step 5 in [To Restore Files](#), on page 202. Run the restore procedure again.

The following dialog box opens.

Figure 194 Connect to SQL Server Dialog Box

5. In the dialog box, type your **Login name** and **Password**.

The Login name is **sa**; the password is **wave2000** (all lowercase).

6. Click **Connect**.

7. Right-click **LMS2000_v6** to open the shortcut menu.

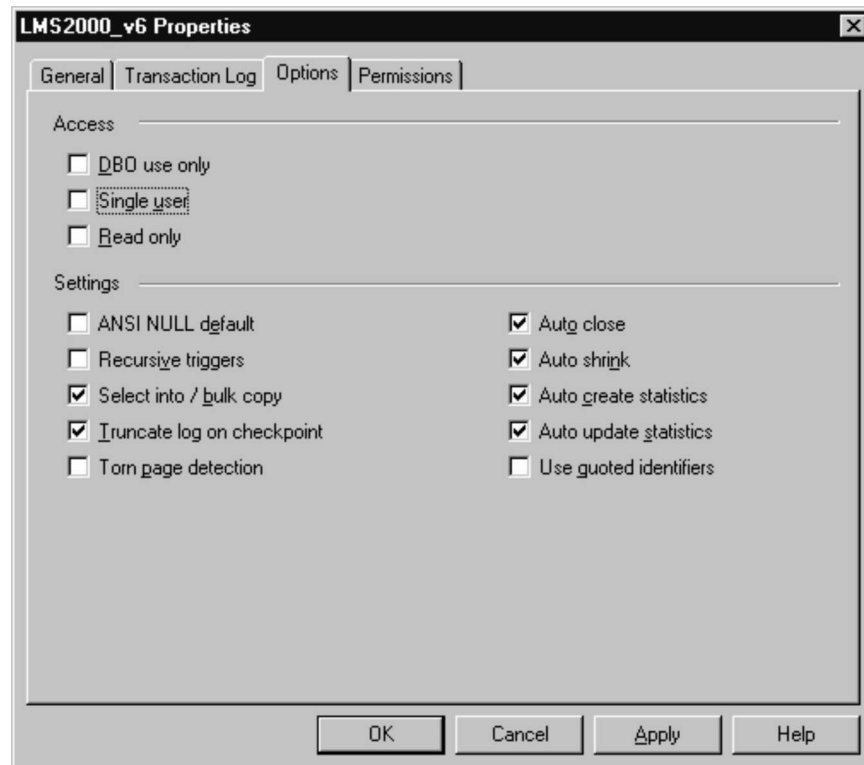
8. Select **Properties** from the shortcut menu.

The LMS2000_v6 Properties dialog box opens.

9. Click the **Options** tab.

10. Ensure that the **Single User** option is unchecked.

Figure 195 LMS2000_v6 Properties Dialog Box



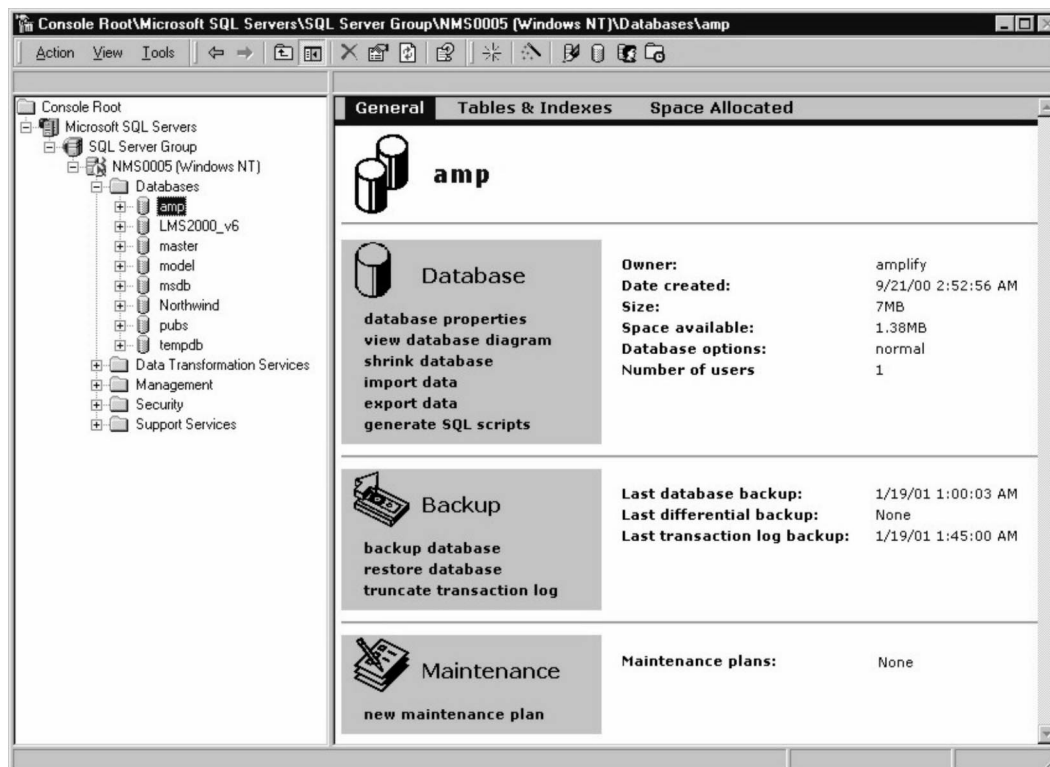
11. Click **Apply**.

12. Click **OK**.

To Verify that the AMP Database Has Returned to Multi-user Mode

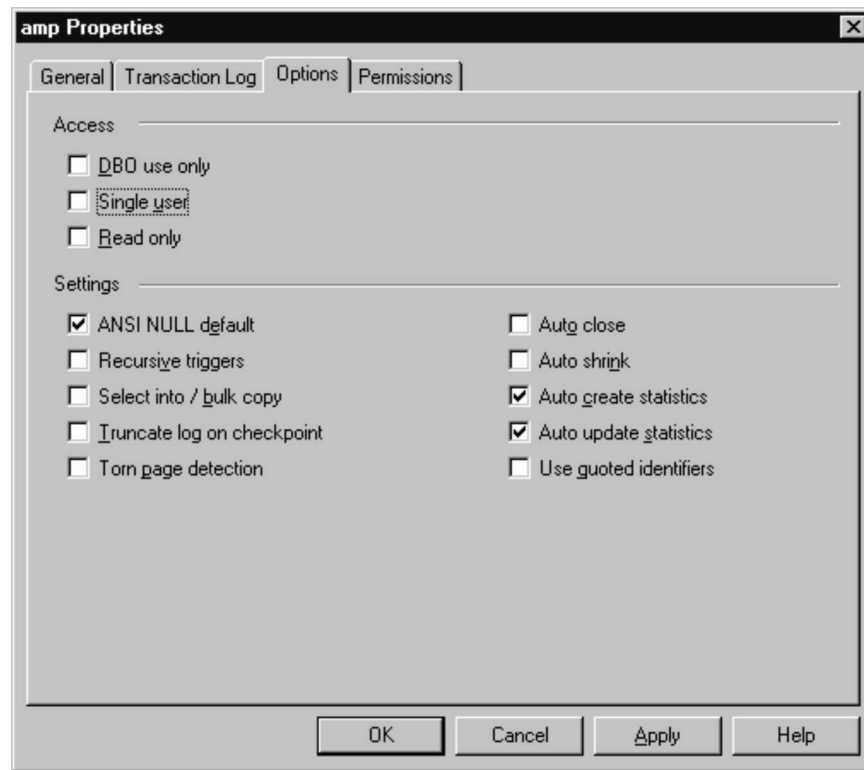
1. In the left pane of SQL Server Enterprise Manager, navigate to the **amp** database and select it.

Figure 196 Microsoft SQL Server Enterprise Manager



NOTE: The amp database icon appears gray instead of yellow if you did not complete step 5 in [To Restore Files](#), on page 202. Run the restore procedure again.

2. Right-click **amp** to open the shortcut menu.
3. Select **Properties** from the shortcut menu.
The amp Properties dialog box opens.
4. Click the **Options** tab.
5. Ensure that the **Single User** option is unchecked.

Figure 197 AMP Properties Dialog Box

6. Click **Apply**.
7. Click **OK**.
8. Close SQL Server Enterprise Manager.

To Verify that MSSQLServer has Restarted

1. In the Windows System Tray, in the bottom right corner of your screen double-click the MSSQL Server icon.

Figure 198 MSSQL Server Icon in Windows System Tray

The SQL Server Service Manager opens.

Figure 199 SQL Server Service Manager

2. From the **Server** drop-down list, select the NMS Server on which to pause a database.
3. From the **Services** drop-down list, select **MSSQLServer**.
4. Verify that the MSSQLServer is running, as it is in [Figure 199, SQL Server Service Manager](#), on page 210.
If not, click the **Start** button.
5. From the **Services** drop-down list, select **SQLServerAgent**.
6. Verify that the SQLServerAgent is running.
If not, click the **Start** button.
7. Verify that the Auto-start service when OS starts check box is selected.
If not, select the check box.
8. Reboot the computer.

13

Operating RFSM

The radio frequency switching matrix (RFSM) monitors CCUs. When a CCU fails, the RFSM automatically reconfigures the backup CCU to replace the failed CCU, preventing service disruption. This chapter explains RFSM functionality and how to replace failed CCUs.

13.1 Monitoring CCU Status Using RFSM

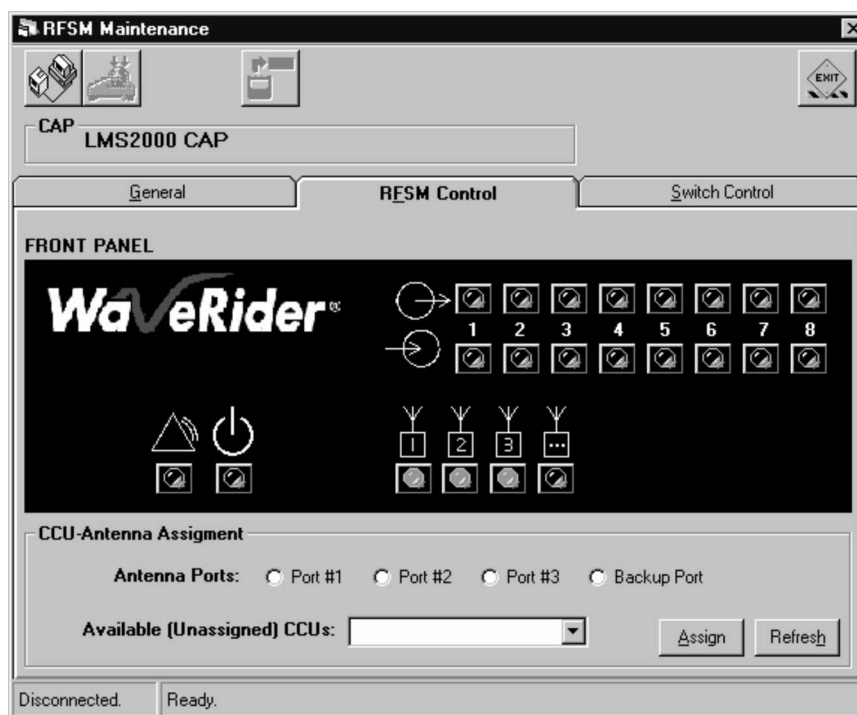
The RFSM uses color codes to indicate the status of CCUs and antenna ports. The color codes for CCU status are reflected in three places:

- On the front panel of the RFSM
- On the RFSM control tab of the RFSM Properties screen
- In the tree view of the NMS (These icons will be red or green to reflect CCU status, but they will not flash.)

The color codes for each CCU state are outlined in [Table 8, on page 212](#).

[Table 9, on page 213](#) outlines the color codes on the Switch Control tab of the RFSM Properties screen, which reflect switched configurations or antennas.

Figure 200 RFSM Control

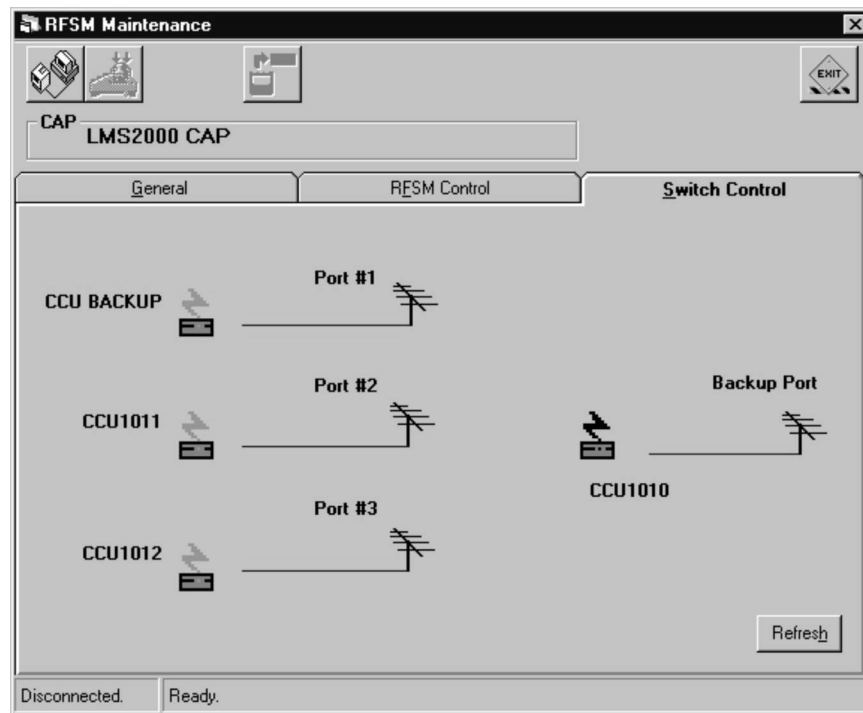


The following table outlines the CCU LED colors on the **RFSM Control** tab and the states they reflect. These colors are also reflected on the front panel of the RFSM and in the tree view of the NMS. The icons in the NMS tree view will be red or green, but they will not flash.

NOTE: To refresh the CCU icons in the NMS tree view, collapse and then re-expand the branch for the CAP containing those CCUs.

Table 8 CCU LED Colors

State	CCU Color	Backup Color
The RFSM, CCUs, and Backup CCU are in normal operational mode. All systems are performing within accepted limits, and the RFSM is polling the CCUs for possible failure.	Solid Green	Slow Flash Green
A backup CCU has been manually switched to direct its radio frequency (RF) traffic through the designated antenna.	Fast Flash Green	Solid Green
The operator has manually switched the backup CCU into operational mode. The original CCU is now offline.	Solid Red	Solid Green
The RFSM has detected a failure in an operational CCU and has switched the backup CCU into operational mode, taking over the communication and administrative duties of the failed CCU. The failed CCU will be indicated by the flashing red icon.	Slow Flash Red	Solid Green

Figure 201 Switch Control

The following table outlines the colors on the **Switch Control** tab and the states they reflect.

Table 9 Switch Control Icon Colors

CCU	Assigned	Active in RFSM	Lightning Bolt Color	Color of Line from CCU to Antenna
CCU	no	no	n/a	no line
CCU	yes	no	black	blue line
CCU	yes	yes	black	blue line
CCU (failed)	yes	yes	red	red line
Backup CCU	no	no	n/a	no line
Backup CCU	yes	no	black	no line
Backup CCU	yes	yes	slow flash green	blue line
Backup CCU In Use	yes	yes	green	red line to antenna being replaced
Backup CCU In Use (failed)	yes	yes	flashing red	red line

13.1.1 Refreshing the Display

Refresh the RFSM display periodically to reflect any changes made by the RFSM polling engine.

To Refresh the Display

- Click the **Refresh** button.

13.2 Monitoring CCUs with the RFSM Polling Engine

The polling engine for the RFSM monitors CCU status. If a CCU fails, the RFSM will switch the configuration from the failed CCU to the backup CCU. The backup CCU will act in place of the failed CCU until the failed unit is repaired or replaced.

There are three possible conditions under which the RFSM will switch the configuration to the backup CCU:

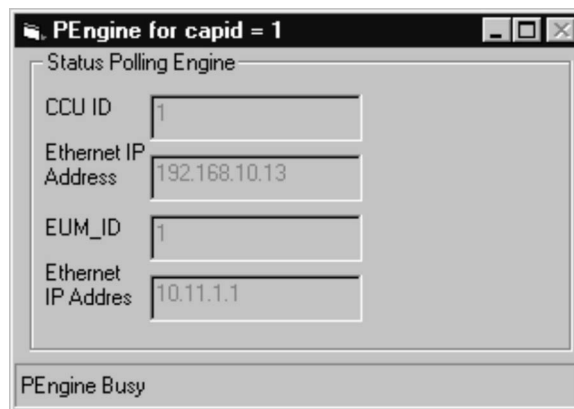
- Ethernet link to the CCU is disconnected or broken.
- CCU loses power.
- CCU radio fails.

The RFSM will not switch the configuration to the backup CCU under the following condition:

- Radio link failure between an EUM and CCU.

The RFSM polling engine monitors CCU status by polling the EUMs attached to the CCU. [Figure 202](#) shows a RFSM polling engine window with device information.

Figure 202 RFSM Polling Engine Window



13.3 Replacing a CCU After Configuration has Switched to Backup

When a CCU fails, you must replace the unit. To replace a CCU, complete the following procedures:

1. Stop the RFSM Polling Engine.
2. Power down the failed CCU.
3. Disconnect the Ethernet and RF cables from the CCU.
4. Change the IP address of the new CCU to the original IP address of the backup CCU before it was activated.

NOTE: Before you restore the configuration, the backup CCU is using the configuration of the failed CCU. When you restore the configuration, the backup CCU will be restored to its original configuration and the new CCU will receive the configuration of the failed CCU.




TIP: To check the IP, use the NMS to view the properties of the CCU you are about to replace. The IP shown on the screen is the IP to assign to the replacement CCU.

5. Replace the failed CCU with the new CCU in the CAP.
6. Connect the Ethernet and RF cables to the new CCU.
7. Restore configuration from backup CCU to new CCU.
8. Restart the RFSM polling engine.

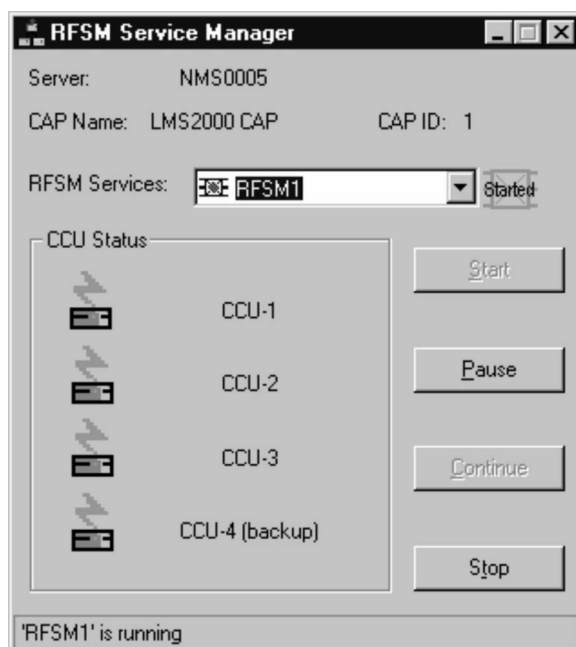
Each of these procedures is described below.

NOTE: This procedure only applies to replacing CCUs when the CCU has failed and the backup CCU is using the configuration of the failed CCU. This procedure is not applicable to replacing CCUs under any other circumstances.

To Stop the RFSM Polling Engine

1. In the Windows system tray, double-click the  icon to open the RFSM Service Manager window.

NOTE: If the icon does not appear in your system tray, you must restart the RFSM Service Manager, as described in [To Start the RFSM Service](#), on page 121.

Figure 203 RFSM Service Manager

2. From the **RFSM Services** drop-down list, select the RFSM unit to stop.
3. Click the **Stop** button.

The status icon beside the RFSM Services drop-down list changes to Stopped.

To Power Down a CCU

- Disconnect the power supply from the back of the failed CCU.

To Disconnect the Cables from the CCU

1. Disconnect the Ethernet cable from the back of the failed CCU.
2. Disconnect the RF antenna cable from the back of the failed CCU.

To Change the IP Address of the New CCU

1. Attach a 50-ohm load to the antenna connection on the back of the replacement CCU.



CAUTION: Do NOT plug the device into the power outlet until you have the 50-ohm load connected.

2. Use a serial cable to connect a terminal to the DB9 console port on the CCU.
3. Start a computer terminal-emulation application, such as HyperTerminal.

4. Select the communications port that you are using to connect to the device.
5. Configure the application using the following settings:
 - 9600 bps
 - 8 data bits
 - No parity
 - 1 stop bit
 - No flow control
6. Plug the CCU into a 110 or 220 V AC power source using the power cord provided with the unit.

An initialization sequence displays progress messages to the terminal screen.

7. Type the password for the device at the prompt.
8. Type **ip address ethernet <network IP> <netmask>**, where <network IP> and <netmask> are that of the original backup CCU configuration.

NOTE: Remember that, at this point, the backup CCU is using the configuration of the failed CCU.

9. Press **Enter**.
 10. Type **save** and press **Enter**.
 11. Disconnect the serial cable.
- The replacement CCU is now ready for installation into the CAP.


To Replace the Failed CCU in the CAP

1. Remove the failed CCU from the CAP.
2. Place the new CCU in the CAP.

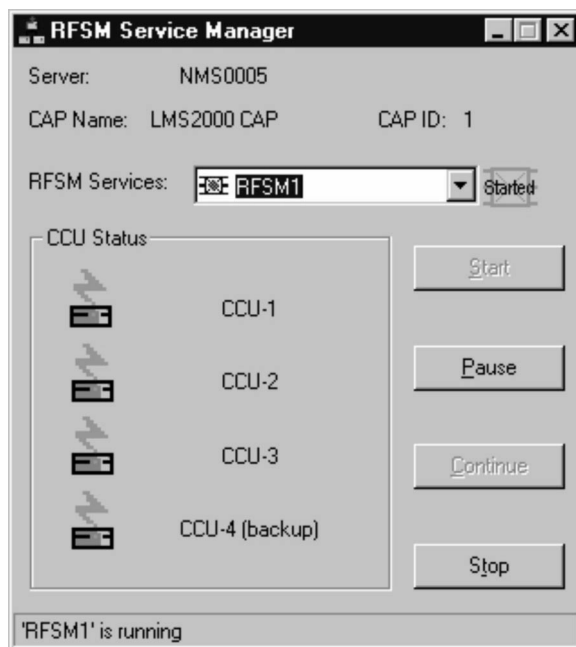
To Connect the Ethernet and RF Cables to the New CCU

1. Connect the Ethernet cable to the back of the replacement CCU.
2. Connect the RF antenna cable to the back of the replacement CCU.

To Restore the Configuration from the Backup CCU to the New CCU

1. In the Windows system tray, double-click the  icon to open the RFSM Service Manager window.

NOTE: If the icon does not appear in your system tray, you must restart the RFSM Service Manager as described in [To Restart the RFSM Service Manager](#), on page 220.

Figure 204 RFSM Service Manager

2. From the **RFSM Services** drop-down list, select the RFSM unit to stop.
3. Click the **Stop** button.

The status icon beside the RFSM Services drop-down list changes to Stopped and the PEngine icon disappears from the Windows task bar.


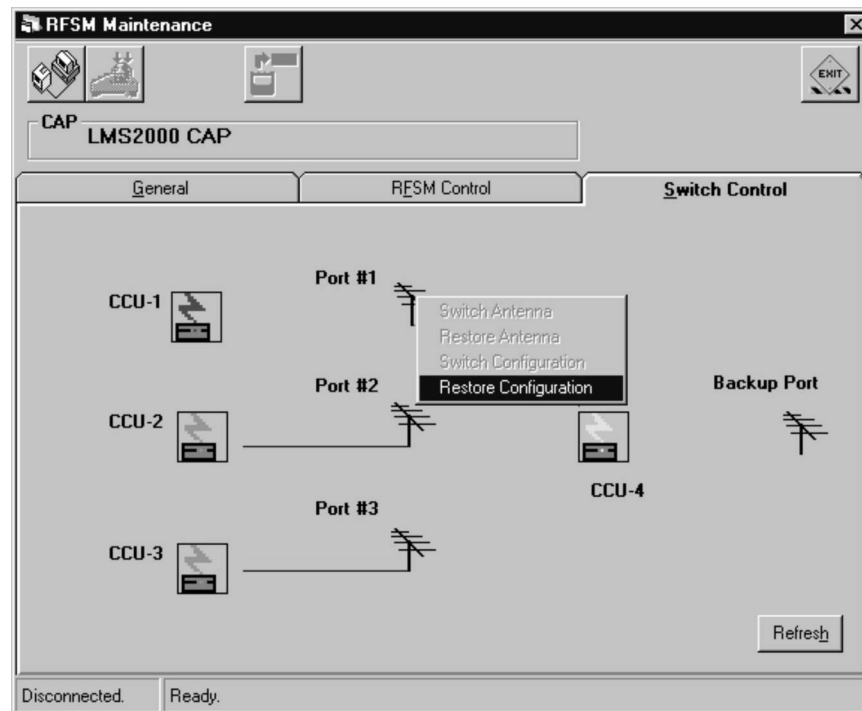

4. Open the RFSM record, and click the **Switch Control** tab.
5. If you are not already connected to the RFSM, click  to connect.
6. Right-click the antenna port to open the shortcut menu.


Figure 205 RFSM Switch Control Shortcut Menu—Restore Configuration

7. On the shortcut menu, select **Restore Configuration**.

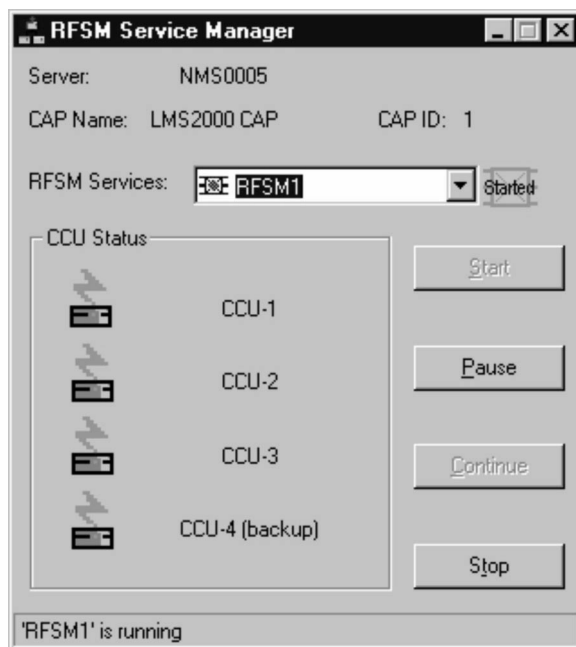
The CCUs now return to their original configuration.

8. Click  to upload the changes to the RFSM.

To Restart the RFSM Polling Engine

1. In the Windows system tray, double-click the  icon to open the RFSM Service Manager window.

NOTE: If the icon does not appear in your system tray, you must restart the RFSM Service Manager. The procedure for restarting the RFSM Service Manager follows this procedure.

Figure 206 RFSM Service Manager

2. From the **RFSM Services** drop-down list, select the RFSM unit to start.
3. Click the **Start** button.

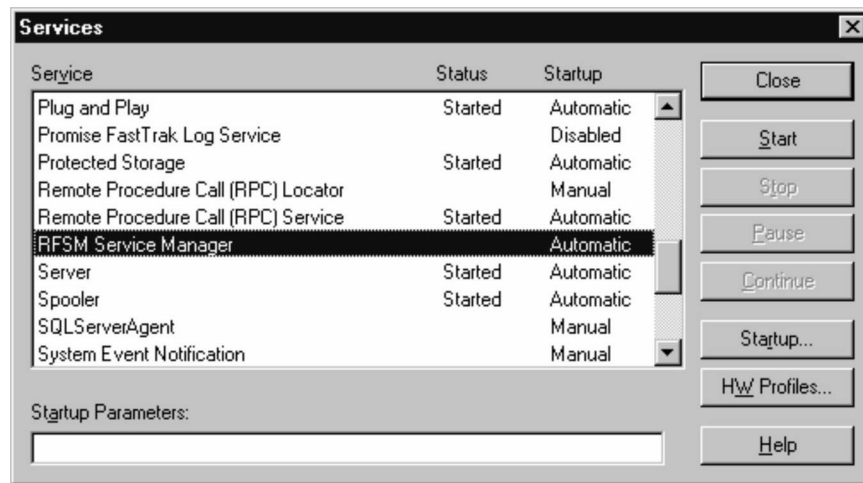
The status icon beside the RFSM Services drop-down list changes to Started and the PEngine icon appears in the Windows task bar.

To Restart the RFSM Service Manager

1. Click the **Start** button.
2. Select **Settings > Control Panel**.

The Control Panel window opens.


3. In the Control Panel window, double-click the **Services** icon.

Figure 207 RFSM Service Manager in Services Window

4. Scroll down to RFSM Service Manager and select it.
5. Click **Start**.

While the Service Control is starting the RFSM Service Manager, you will see the following window.

Figure 208 Service Control

When the service is started, the status changes to Started and the  icon appears in the Windows task bar.

6. Click **Close** in the **Services** window.
7. Close the **Control Panel** window.

13.4 Switching CCU Antennas and Configurations Using RFSM

Once you have assigned and activated the connections between CCUs and antenna ports, the RFSM polling engine will begin monitoring the CCU status. One instance of the polling engine runs for each RFSM. If any CCUs fail, RFSM takes the following actions:

- Switches the backup CCU to the configuration of the failed CCU
- Takes the failed CCU out of service
- Switches the backup CCU to the antenna of the failed CCU

The **Refresh** button updates the RFSM display to reflect any changes that the RFSM made dynamically.

13.4.1 Switching CCU Configurations

Typically, the RFSM polling engine will automatically switch the CCU configurations. You have the option of switching manually for testing purposes.



CAUTION: Ensure redundancy has been activated for all CCUs before switching configurations. For instructions, please refer to [To Activate RFSM Polling of a CCU](#), on page 120.

To Switch CCU Configuration Manually


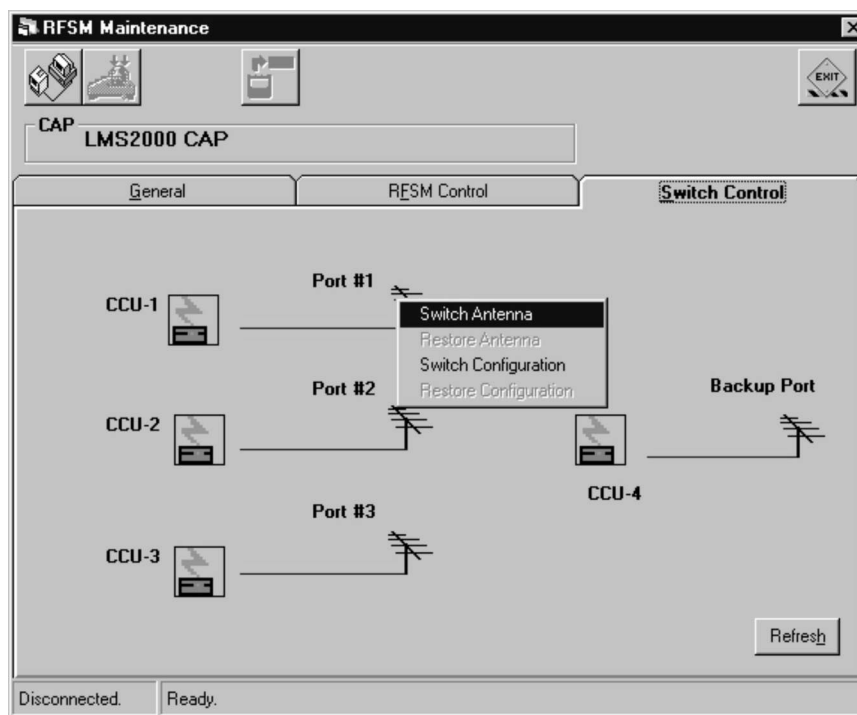

1. Open the RFSM screen, and click the **Switch Control** tab.
2. If you are not already connected to the RFSM, click  to connect.
3. Right-click the antenna port of the CCU with the configuration you want to transfer to the backup CCU.

Figure 209 RFSM Switch Control Shortcut Menu—Switch Configuration



4. On the shortcut menu, select **Switch Configuration**.

The configuration of the CCU has now been switched to the backup CCU.

5. Click  to upload the changes to the RFSM.

13.4.2 Switching Antennas

RFSM enables you to switch an antenna to the backup CCU. When you switch the antenna, it disables the radio on the affected CCU. When you restore the antenna, it will re-enable the radio on that CCU.

To Switch Antennas


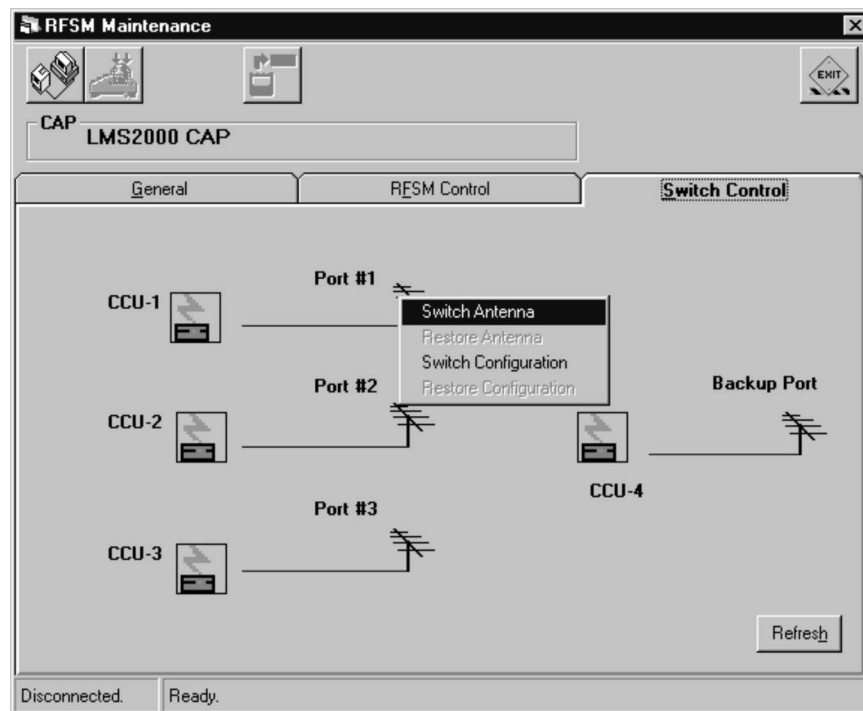

1. Open the RFSM screen, and click the **Switch Control** tab.
2. If you are not already connected to the RFSM, click  to connect.
3. Right-click the antenna port to open the shortcut menu.

Figure 210 RFSM Switch Control Shortcut Menu—Switch Antenna



4. On the shortcut menu, select **Switch Antenna**.
The antenna is now switched to the backup CCU.
5. Click  to upload the changes to the RFSM.

To Restore an Antenna


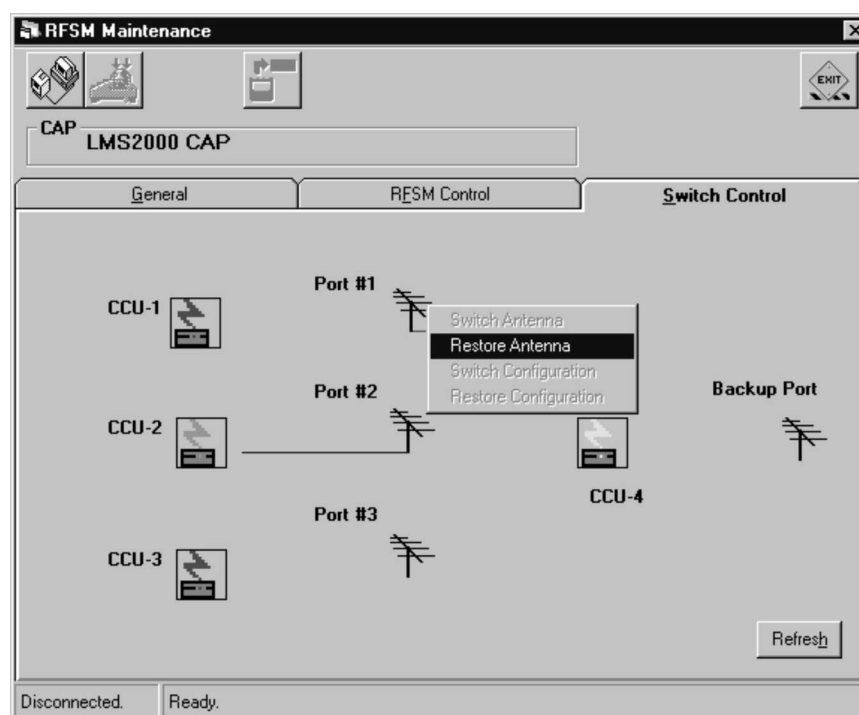
1. Open the RFSM record in the NMS software, and click the **Switch Control** tab.
2. If you are not already connected to the RFSM, click  to connect.
3. Right-click the disabled antenna port to open the shortcut menu.

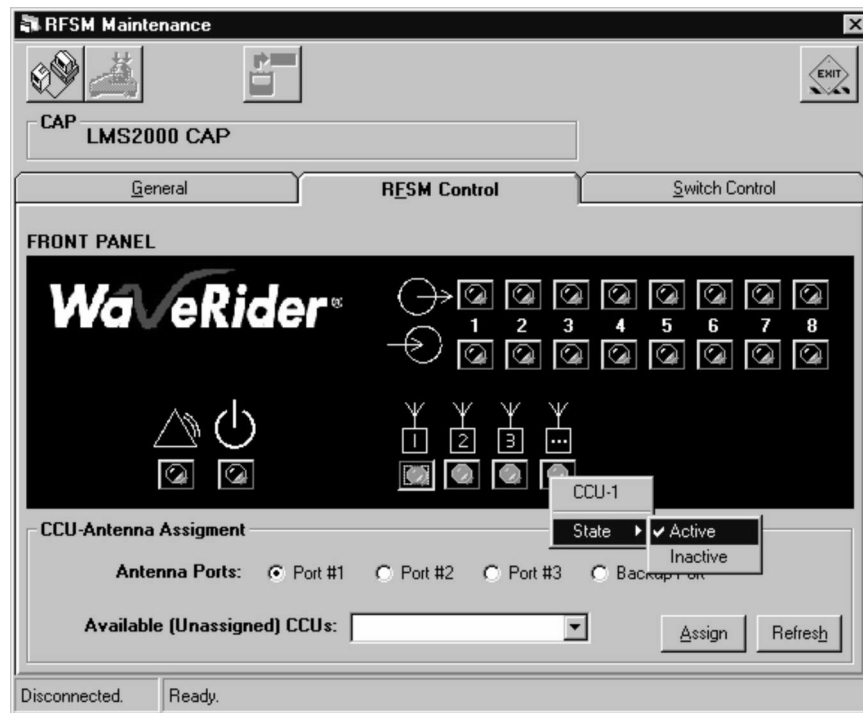
Figure 211 RFSM Switch Control Shortcut Menu—Restore Antenna

4. On the shortcut menu, select **Restore Antenna**.


The antenna is now restored to the CCU.

5. Click the **RFSM Control** tab.
6. Right-click the port for the CCU with the restored antenna.

Figure 212 RFSM Control Shortcut Menu



7. From the shortcut menu, select **State > Active**.

8. Click  to upload the changes to the RFSM.

13.5 Re-establishing RFSM Polling

In the event that the CAP loses power, or the NMS loses its Ethernet connection, the RFSM becomes unable to poll the CCUs within the CAP. Consequently, the RFSM considers the CCUs to be permanently out of service.

There are three indicators that this situation has occurred:

- CCU icons on the RFSM Switch tab of the RFSM Properties screen appear red.
- Buttons on the polling engine window are grayed-out.
- CCUs on the NMS tree appear yellow. (You may have to collapse and expand the tree before the color change appears.)

To re-establish RFSM polling of the CCUs, complete the following procedures:

1. Power up the CAP.
2. Re-activate RFSM CCU states (procedure described later in this section).
3. Upload the configuration to the RFSM.

NOTE: This procedure only applies when the backup CCU is not operating in place of a failed CCU.

To Activate RFSM CCU States



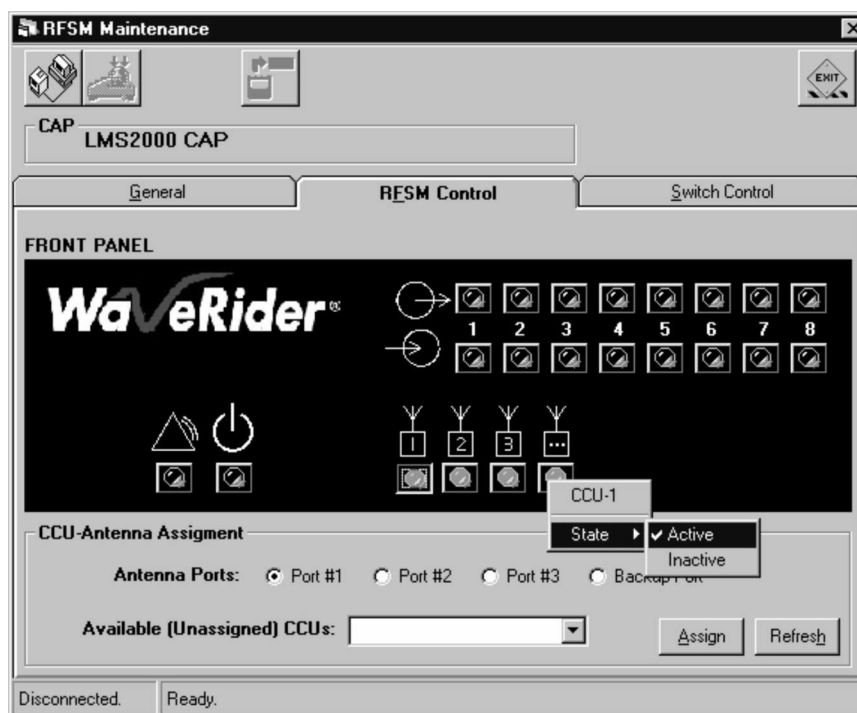
1. If you are not already connected to the RFSM, click  to connect.
2. On the **RFSM Control** tab of the RFSM screen, right-click  of the CCU to activate.

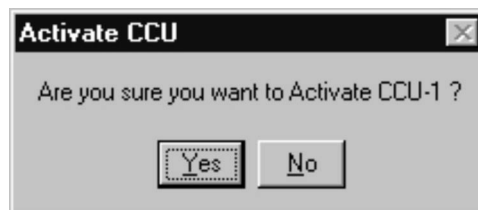
Figure 213 Activate CCU Shortcut Menu



3. On the shortcut menu, select **State > Active**.

The **Activate CCU** dialog box opens.

Figure 214 Activate CCU Dialog Box



4. Click **Yes** to activate CCU polling.

NOTE: When CCU redundancy is activated, a check mark appears beside the word "Active" in the shortcut menu.


5. Repeat this procedure for every antenna port.

When you activate polling for the Backup CCU, the following dialog box opens.

Figure 215 RFSM Backup Antenna Reminder



This is just a reminder that your RFSM should have an RF cable for an antenna connected to the backup port.

6. Click **OK** to close the dialog box.
7. Click  to upload the changes to the RFSM.

— This page is intentionally left blank —

14

Running Reports

The NMS software includes the following reports:

- Accounts Report
- CCU/EUM Firmware Report
- Network IP Report
- Service Level Report
- SNMPc Trend Reports

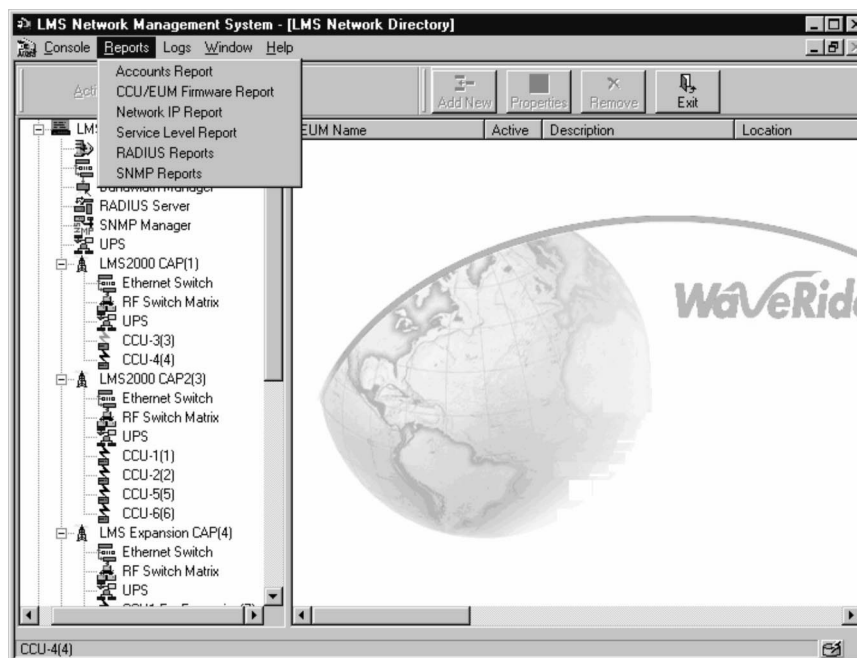
14.1 Running a Report

The procedure for running reports in the NMS software is the same for all reports except the SNMPc reports. Instructions for running a report are below. The subsequent sections simply describe the information you will find in each of the reports.

To Run a Report

1. On the menu bar at the top of the main screen, click **Reports**.

Figure 216 NMS Reports Menu



2. On the **Reports** menu, click the name of the report to run.

14.1.1 Adding Your Logo to Reports

Most of the NMS reports include a logo graphic. The sample reports in this chapter show the default graphic. To change the logo graphic to your company's logo, create a graphic file with the following parameters:

- Graphic must be in bitmap (.bmp) format.
- Graphic file must be named **logo.bmp**.
- File must reside in the **...reports\images** sub-directory of the application directory.

14.2 Accounts Report

The Accounts report contains information about EUMs, the subscribers they are associated with, their service level, and their activity state (enabled or disabled). This report generates a separate report page for each account. [Figure 217](#) shows a sample report for an individual account.

Specifically, it reports on the following fields:

- Account Name
- Account ID
- Account Information
 - Contact Name
 - Entry Date
 - Country
 - Address1
 - City
 - Phone
 - Address2
 - State or Province
 - Zip or Postal Code
 - E-mail Name
 - Fax
 - Service Level
- Subscriber Information
 - EUM Name
 - EUM ID
 - Active
 - Contact Name
 - E-Mail Name
 - Phone

Figure 217 Sample Accounts Report

Your Company, Inc.

Insert a 1"x3" logo here for report distribution

(See LogoHelp.txt in the Reports/Images directory for help)

my Account
WaveRider Communications
Calgary, Alberta, Canada
T2H 0G3

Accounts Report
September 18, 2000 16:55
Page 1 of 1

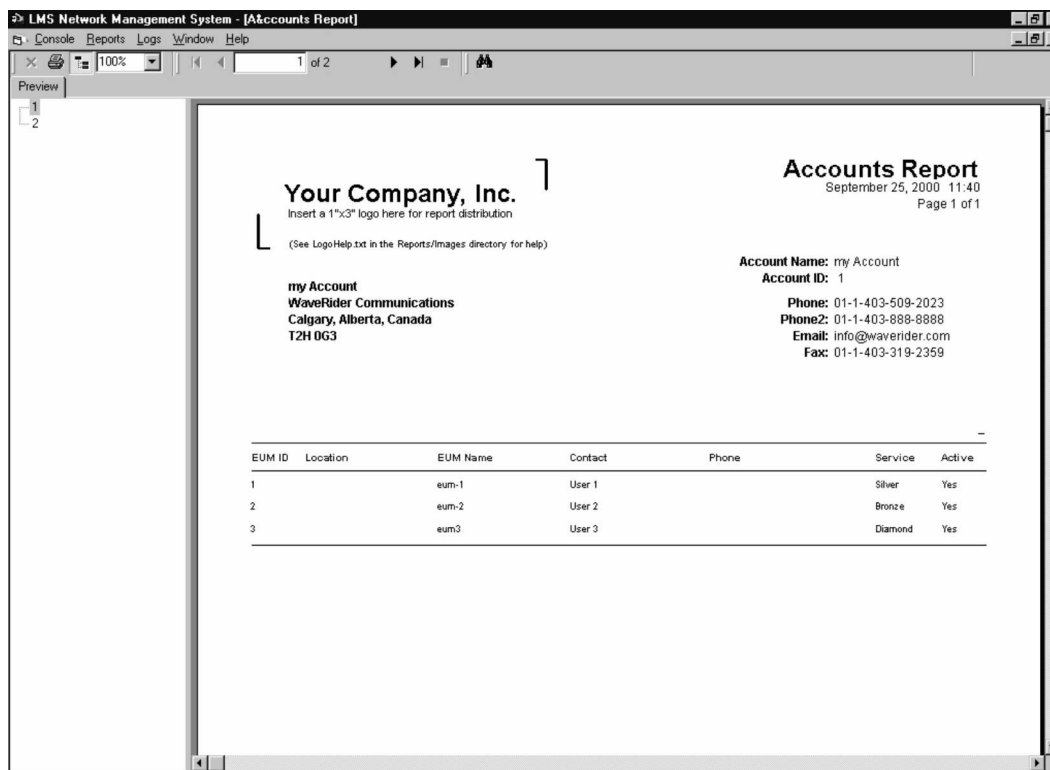
Account Name: my Account
Account ID: 1

Phone: 01-1-403-509-2023
Phone2: 01-1-403-888-8888
Email: info@waverider.com
Fax: 01-1-403-319-2359

EUM ID	Location	EUM Name	Contact	Phone	Service	Active
1		EUM1	Subscriber Name 1	01-1-403-509-2023	Diamond	Yes
2		EUM2	User2		Bronze	Yes
3		EUM3	User3		Bronze	Yes

To Open the Report for the Next Account

1. Run the **Accounts** report.

Figure 218 Sample Accounts Report with Report Window

The left pane lists numbers for each of the accounts. By default, the report opens with the first account.

2. In the left pane, click the number for the account report to view.

In the sample report, there are only two accounts: 1 and 2. Account 1 opens by default. To view a report for the second account, click **2**.

14.3 CCU/EUM Firmware Report

The CCU/EUM Firmware report contains the following information:

- CCU information, including firmware version and enabled state of the radio
- EUM information, including firmware version and serial number

Specifically, it reports on the following fields:

- CCU Name
- CCU ID
- CCU Active (Yes/No)
- Description
- Model/Firmware Version
- Location
- EUM Name
- EUM ID
- Model/Firmware Version
- Serial Number

Figure 219 Sample Firmware Report

Your Company, Inc. Insert a 1"x3" logo here for report distribution (See LogoHelp.txt in the Reports/Images directory for help)		Firmware Report September 18, 2000 16:58 Page 1 of 1			
Device	Device ID	Firmware Version	ESN	Location	Active
CCU1 For Expansion	4	Firmware		Calgary	Yes
CCU2 For Expansion	4	Firmware		Calgary	Yes
CCU3 For Expansion	4	Firmware		Calgary	Yes
CCU4 For Expansion	4	Firmware		Calgary	Yes
CCU1 For Expansion	5	Firmware		Calgary	Yes
CCU2 For Expansion	5	Firmware		Calgary	Yes
CCU3 For Expansion	5	Firmware		Calgary	Yes
CCU4 For Expansion	5	Firmware		Calgary	Yes
CCU-3	1	1.7	CCU2000_V0_00013	Calgary	Yes
CCU-4	1	1.7	CCU2000_V0_00014	Calgary	Yes
CCU-1	3	1.7	CCU2000_V0_00011	Calgary	Yes
CCU-2	3	1.7		Calgary	Yes
CCU-5	3				No
CCU-6	3				No
*** End of Report ***					

14.4 Service Level Report

The Service Level report contains the following information:

- EUMs sorted by service level and account
- Account contact information
- Active/inactive EUMs

Specifically, it reports on the following fields:

- Service Level
- Service Level ID
- Account Information
- Account ID
- Contact Name
- Entry Date
- Country
- Address1
- City
- Phone
- Address2
- State/Province
- Zip/Postal code
- E-Mail
- Fax
- EUM Name
- EUM ID
- Subscriber Enabled (Yes/No)

Figure 220 Sample Service Level Report

Your Company, Inc. <small>Insert a 1"x3" logo here for report distribution</small> <small>(See LogoHelp.txt in the Reports/Images directory for help)</small>				Service Level Report September 18, 2000 16:56 Page 1 of 1		
				Service Level Legend Gold= 1 Silver= 2 Bronze= 3 Wood= 4		
CCU Name	CCU ID	EUM ID	EUM Name	Location	Service	Active
CCU-1	1	1	EUM1		Service level 6	Yes
CCU-1	1	7	bob		Service level 3	Yes
CCU-2	2	2	EUM2		Service level 3	Yes
CCU-3	3	3	EUM3		Service level 3	Yes
CCU2 For Expansion	8	6	testing123		Service level 4	No
*** End of Report ***						

14.5 Network IP Address Report

The Network IP report lists IP addresses for all equipment, sorted in hierarchical order from NAP to CAP to EUM.

Specifically, it reports on the following fields:

- NAP Name/ID/Description
- Router Name/ID/Description
 - Router IP/Subnet/Router Internet IP/Subnet
- UPS Name/ID/Description
 - UPS IP/Subnet
- Ethernet Switch Name/ID/Description
 - Ethernet Switch IP/Subnet
- RADIUS Server Name/ID/Description
 - RADIUS Server IP/Subnet
- SNMP Server Name/ID/Description
 - Trap Server IP/Subnet
- CAP Name/ID/Description
- CCU Name/ID/Description
 - CCU IP/Subnet/CCU Radio IP/Subnet/Device Active/Local ID
- EUM Name/ID/Description
 - EUM IP/Subnet/EUM Radio IP/Subnet/Subscriber Enabled/Local ID

Figure 221 Sample Network IP Address Report

Your Company, Inc.

Insert a 1"x3" logo here for report distribution

(See LogoHelp.txt in the Reports/Images directory for help)

Network IP Address Report

September 20, 2000 13:23

Page 1 of 2

LMS2000 NAP (ID: 1)

Component ID	Device ID	Internet (WAN) Port	Subnet	LMS (LAN) Port
2600	1	10.2.23.1	24	192.168.10.1
CISCO Switch -- NAP	1	n/a	24	192.168.10.5
NAP UPS	1	n/a	24	192.168.10.6
Radius Server 1	1	n/a	24	192.168.10.7
SNMP Server 1	1	n/a	24	192.168.10.7

LMS2000 CAP (ID: 1)

Component ID	Device ID	Ethernet IP Address	Subnet
CISCO Switch -- CAP	2	192.168.10.10	24
CAP 1 UPS	2	192.168.10.11	24

LMS2000 CAP CCU/EUM Information

CCU Name	CCU ID	EUM Name	EUM ID	Active	Radio Channel	Ethernet IP Address	Subnet	Radio IP Address
CCU-1	1			Yes	1	192.168.10.13	24	192.168.110.1
		EUM1	1	Yes	1	192.168.210.2	24	192.168.110.2
CCU-2	2			Yes	6	192.168.10.14	24	192.168.111.1
		EUM2	2	Yes	6	192.168.220.2	24	192.168.111.2
CCU-3	3			Yes	11	192.168.10.15	24	192.168.112.1
		EUM3	3	Yes	11	192.168.230.2	24	192.168.112.2
CCU-4	4			Yes	3	192.168.10.16	24	192.168.113.1

LMS Expansion CAP (ID: 6)

Component ID	Device ID	Ethernet IP Address	Subnet
CISCO Switch -- CAP	6	192.168.10.80	24
CAP Expansion UPS	5	192.168.10.81	24

LMS Expansion CAP CCU/EUM Information

CCU Name	CCU ID	EUM Name	EUM ID	Active	Radio Channel	Ethernet IP Address	Subnet	Radio IP Address

14.6 SNMPc Trend Report

The SNMPc Trend Reports are available in hourly, daily, weekly, and monthly increments, and you can select time intervals on which to report. These reports consume system resources, and it is recommended that you record hourly and daily reports only for troubleshooting. SNMPc Trend Reports assigned to each new device allow the system to recover individual device statistics and display them in graphical format through a Web-based report. Use this report to help you forecast trends and monitor system activity.

To add a Trend Report to new devices, refer to [Adding a Trend Report](#), on page 40.

To Open an SNMP Report

1. In the NMS software, click the Reports menu.
2. From the Reports menu, select SNMP Reports.
The SNMPc Trend Reports window opens in your Web browser.
3. From the links across the top of the screen, select the type of Trend report:
 - Hourly Reports
 - Daily Reports
 - Weekly Reports
 - Monthly Reports

A list of reports available for that time period appears in the left pane of your browser.

4. From the left pane, select the report to view.
The report opens in your browser.

Figure 222 Sample SNMPc Trend Report—Daily

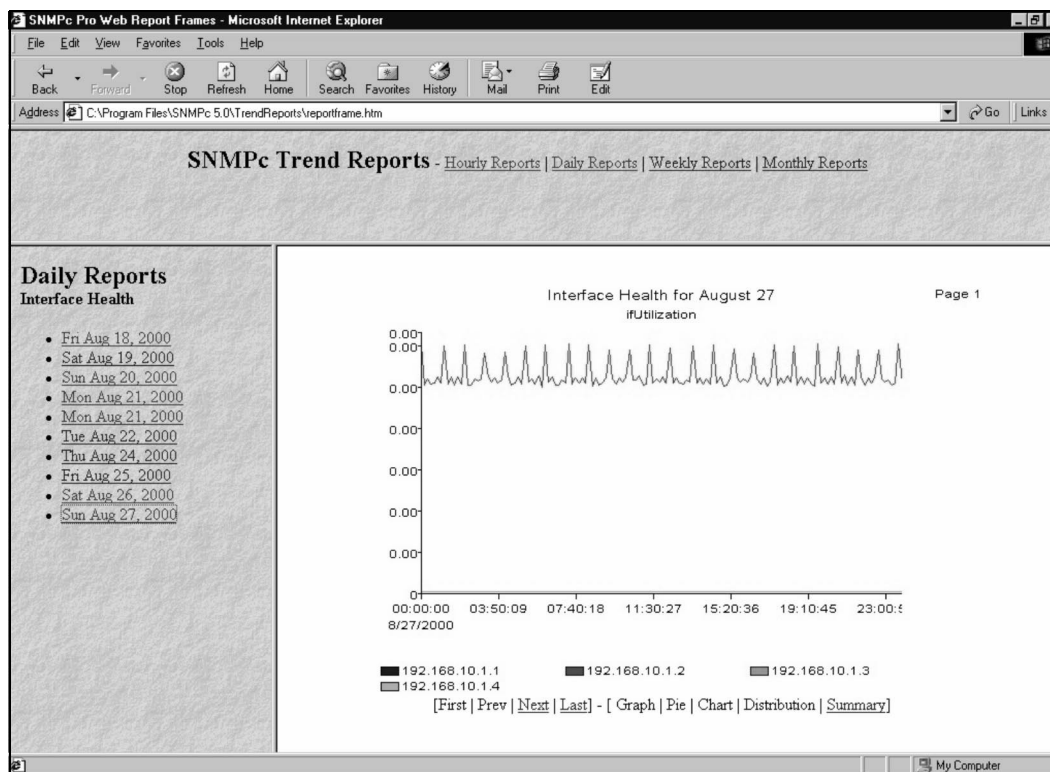
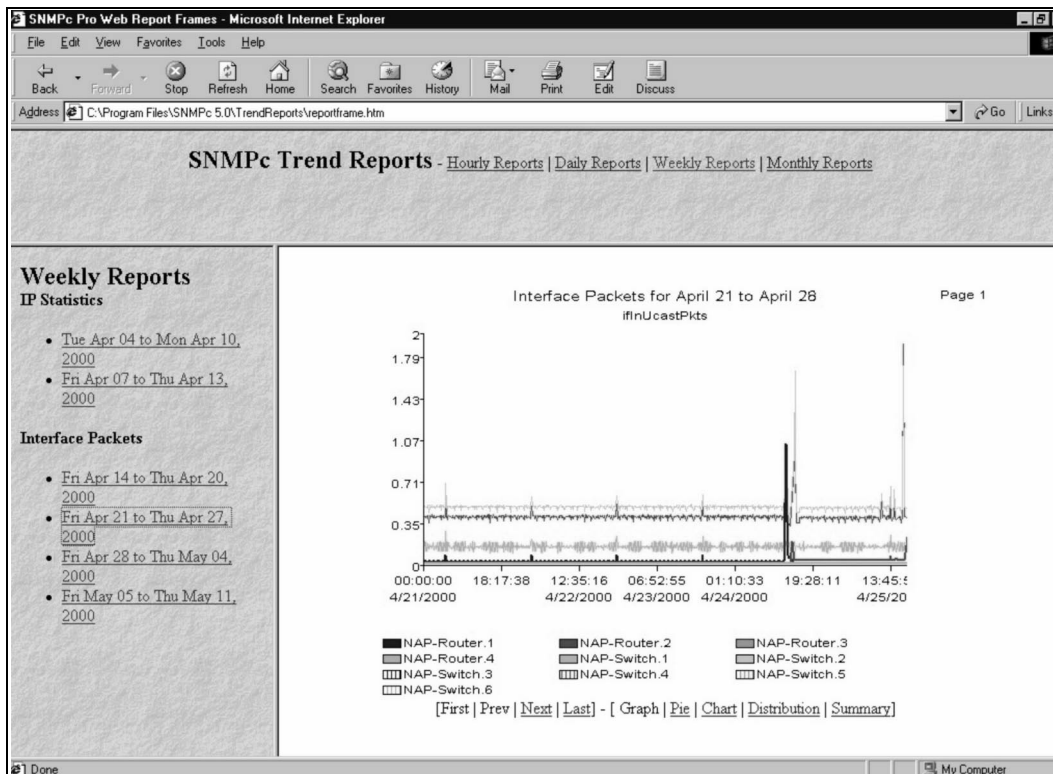


Figure 223 Sample SNMPc Trend Report—Weekly



15

Monitoring Performance

Your system operations activities should include monitoring the performance of the network devices to determine whether they are operating efficiently. The NMS workstation includes the following tools that you can use to monitor device performance:

- [Network Interface Statistics](#), on page 239
- [IP Statistics](#), on page 242
- [Radio Packet Error Rate](#), on page 245
- [NMS Application Logs](#), on page 246
- [NMS Transaction Logs](#), on page 248
- [RADIUS Server Error Log](#), on page 251
- [RADIUS Server User Log](#), on page 252
- [RADIUS Server Statistics](#), on page 253
- [SNMPc Server Device Management Details](#), on page 254

[SNMPc Server Event Logs](#), on page 258 When you need to verify a wireless connection between two devices, or verify the re-establishment of the wireless connection between two devices, test the connection using the ping test described in [Performing a Ping Test](#), on page 174.

15.1 Network Interface Statistics

The Statistics tab of the CCU and EUM records displays network interface statistics, which are statistics on the data flowing in and out of the CCU or EUM through its network interface. [Table 10](#) describes each of the fields in the Network Interface Statistics table. Following the table, you will find an explanation of how to access the Network Interface Statistics.

Table 10 Network Interface Statistics

Label	Description
Flags	Specify the operational state and properties of the interface. Possible flags are: <ul style="list-style-type: none"> • BROADCAST: interface is for a broadcast network • MULTICAST: interface supports multicasting • POINT-TO-POINT: interface is for a point-to-point network • LOOPBACK: interface is for a loopback network • RUNNING: resources are allocated for this interface • SIMPLEX: interface cannot receive its own transmissions • ALLMULTI: interface is receiving all multicast packets • DEBUG: debugging is enabled for the interface • NOARP: do not use ARP on this interface • NOTRAILERS: avoid using trailer encapsulation • PROMISCUOUS: interface receives all network packets • TX: a transmission is in progress • UP: interface is operating
MTU	Maximum transmission unit or the size of the largest packet the interface can handle.
Hardware Address	MAC or Ethernet address of the interface.
Administrative Status	Desired state of the interface. The CCU supports UP and DOWN states.
Operational Status	Current operational state of the interface.
Input Octets	Number of bytes that arrived on this interface since the last interface reset or device reboot.
Input Unicast Packets	Number of unicast packets that arrived on this interface since the last interface reset or device reboot.
Input Non-Unicast Packets	Number of non-unicast packets that arrived on this interface since the last interface reset or device reboot.
Input Discards	Number of packets that arrived on this interface and were discarded since the last interface reset or device reboot.
Input Errors	Number of packets that arrived on this interface with errors since the last interface reset or device reboot.
Output Octets	Number of bytes that were sent from this interface since the last interface reset or device reboot.
Output Unicast Packets	Number of unicast packets that were sent from this interface since the last interface reset or device reboot.
Output Non-Unicast Packets	Number of non-unicast packets that were sent from this interface since the last interface reset or device reboot.

Label	Description
Output Discards	Number of outbound packets that were dropped because of implementation limits since the last interface reset or device reboot.
Output Errors	Number of outbound packets dropped because of errors since the last interface reset or device reboot.

To View Network Interface Statistics


1. In the NMS software, open the record for the EUM or CCU you want to monitor.
2. Click  to connect to the device.
3. Click the **Statistics** tab.
4. Click the **Network Interface Statistics** option.

Figure 224 Channel Unit Properties—Network Interface Statistics

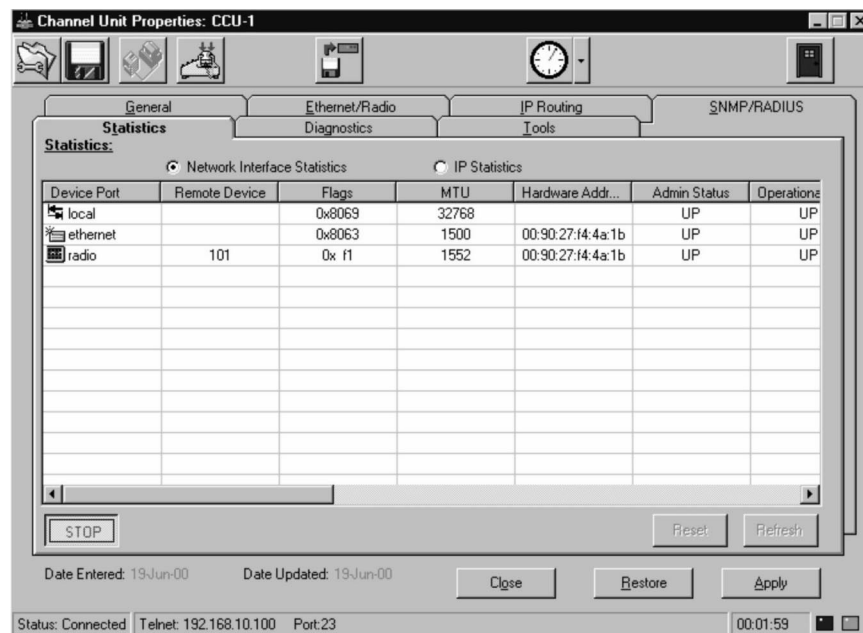
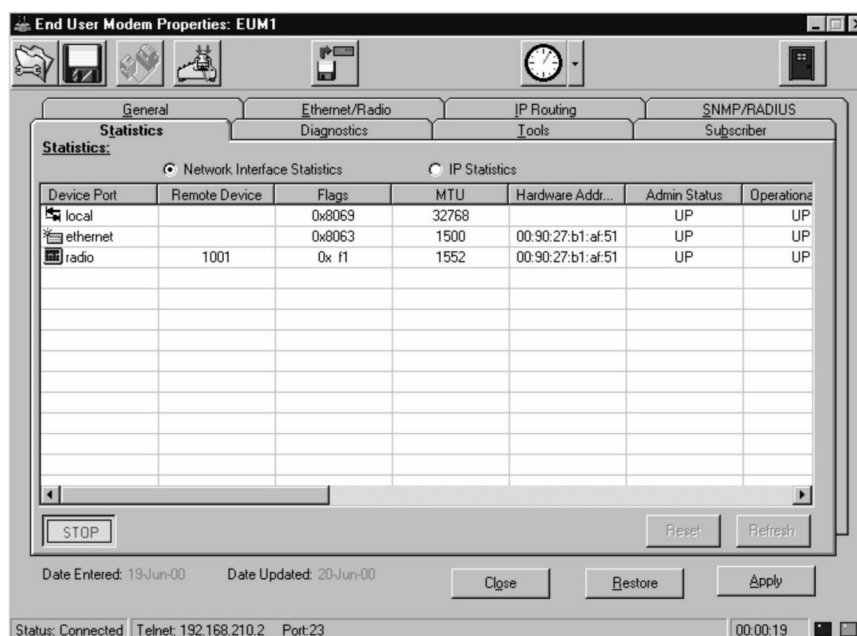




Figure 225 End User Modem Properties—Network Interface Statistics

5. To change the monitoring rate, click the arrow beside  and select a time interval of **5**, **30**, or **60 seconds**.
6. Click **Monitor**.
7. Click **STOP** when you are finished.
8. Click  to disconnect from the device.



15.2 IP Statistics

The Statistics tab of the CCU and EUM records displays IP statistics, which are statistics on the quantity and quality of packets transmitted to and from the CCU or EUM. [Table 11](#) describes each of the fields in the IP Statistics table. Following the table, you will find an explanation of how to access the IP Statistics.

Table 11 IP Statistics

Label	Descriptions
Total packets received	Number of packets sent to the IP layer.
Bad checksum discards	Number of packets discarded due to a bad checksum.
Packet too short discards	Number of packets dropped due to an invalid data length.
Not enough data discards	Number of packets dropped because they did not contain enough data to be an IP packet.

Label	Descriptions
Bad header length discards	Number of packets discarded because of inconsistent IP header and IP data lengths.
Fragment received	Number of packet fragments received.
Fragments dropped	Number of fragments dropped due to lack of space or duplicates.
Fragments timed out	Number of fragments that were timed-out.
Packets forwarded	Number of packets forwarded at the IP layer.
Couldn't forward discards	Number of packets received for unreachable destinations.
Redirected forwards	Number of redirect messages that were sent.
Unknown protocol discards	Number of packets of unknown or unsupported protocol received and discarded.
No space discards	Number of packets dropped because of resource shortages.
Packets reassembled	Number of packets that needed to be reassembled.
Fragments sent	Number of fragments successfully sent.
No route discards	Number of packets discarded because there was no route to the destination given.

5. To change the monitoring rate, click the arrow beside , and select a time interval of **5**, **30**, or **60 seconds**.
 6. Click **Monitor**.
- [Table 11](#) describes the information shown on the screen.
7. Click **STOP** when you finish.
 8. Click  to disconnect from the device.
 9. Click **Close** to exit the screen or choose another device to monitor.

15.3 Radio Packet Error Rate

Radio Packet Error Rate (PER) information helps you analyze your device capacity. If the packet error rate suddenly increases, or occurs only at specific times of the day, your CCU may be overloaded. [Table 12](#) identifies the quality of transmission for each Radio PER.

Table 12 Radio Packet Error Rate Definitions

Radio PER Ratio	Transmission Quality
less than 1%	excellent
less than 2%	good
less than 5%	marginal
greater than 5%	poor

To Display the Packet Error Rate for a CCU


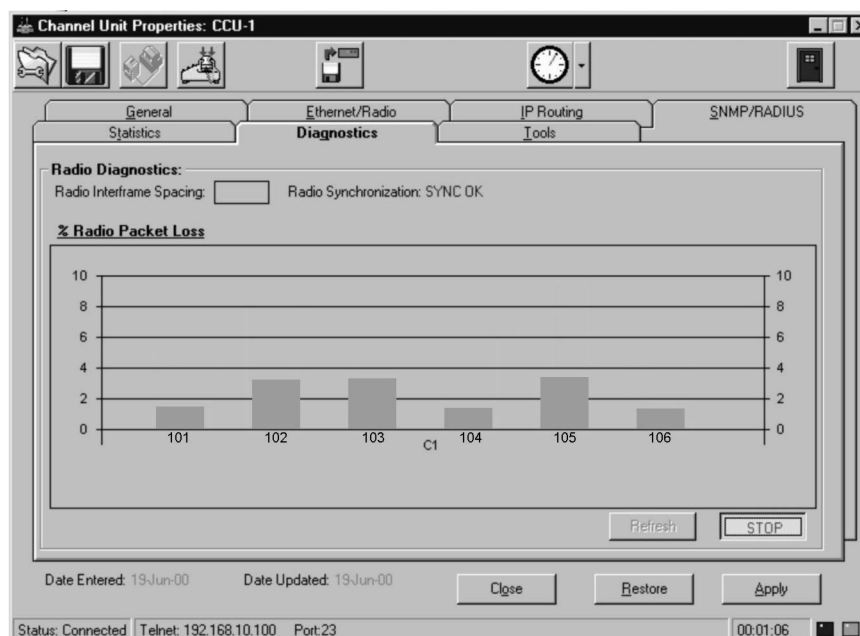


1. Open the CCU record that you want to monitor.
2. Click  to connect to the device.
3. Click the **Diagnostics** tab.

Figure 228 Channel Unit Properties—Diagnostics

4. Click **Refresh** to reset the statistics.
5. Click the arrow beside  and select an interval of **5**, **30**, or **60 Seconds**.
6. Click **Monitor**.
7. Click **STOP** when you finish.
8. Click  to disconnect from the CCU.
9. Click **Close** to exit the screen.

15.4 NMS Application Logs

The **NMS Log** displays all the events that occur during NMS operation. Use this report to help analyze the source of events occurring in the NMS application.

Table 13 Fields in the NMS Application Log File

Field	Description
Date	Date the event occurred.
Time	Time the event occurred.
Source	Program that triggered the event.

Field	Description
Category	Type of event.
User	Name of user logged in.
Computer	Name of computer where the event occurred.

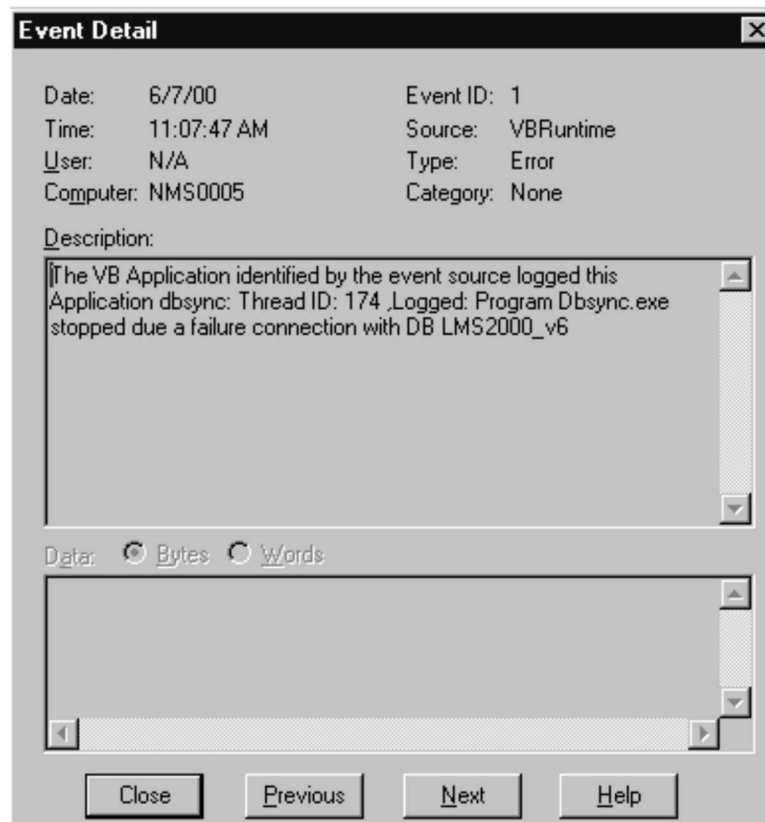
To Access the NMS Logs File

1. On the menu bar at the top of the NMS software, click **Logs > NMS Application Log**.

Figure 229 Application Log File

Date	Time	Source	Category	Event	User	Computer
9/22/00	2:50:33 PM	VBRuntime	None	1	N/A	NMS0005
9/22/00	2:50:23 PM	VBRuntime	None	1	N/A	NMS0005
9/22/00	2:50:03 PM	VBRuntime	None	1	N/A	NMS0005
9/22/00	2:49:48 PM	VBRuntime	None	1	N/A	NMS0005
9/22/00	2:49:33 PM	VBRuntime	None	1	N/A	NMS0005
9/22/00	2:49:28 PM	VBRuntime	None	1	N/A	NMS0005
9/22/00	2:49:18 PM	VBRuntime	None	1	N/A	NMS0005
9/22/00	2:49:03 PM	VBRuntime	None	1	N/A	NMS0005
9/22/00	2:48:53 PM	VBRuntime	None	1	N/A	NMS0005
9/22/00	2:48:33 PM	VBRuntime	None	1	N/A	NMS0005
9/22/00	2:48:18 PM	VBRuntime	None	1	N/A	NMS0005
9/22/00	2:48:03 PM	VBRuntime	None	1	N/A	NMS0005
9/22/00	2:47:58 PM	VBRuntime	None	1	N/A	NMS0005
9/22/00	2:47:48 PM	VBRuntime	None	1	N/A	NMS0005
9/22/00	2:47:33 PM	VBRuntime	None	1	N/A	NMS0005
9/22/00	2:47:23 PM	VBRuntime	None	1	N/A	NMS0005
9/22/00	2:47:03 PM	VBRuntime	None	1	N/A	NMS0005
9/22/00	2:46:48 PM	VBRuntime	None	1	N/A	NMS0005
9/22/00	2:46:33 PM	VBRuntime	None	1	N/A	NMS0005
9/22/00	2:46:28 PM	VBRuntime	None	1	N/A	NMS0005
9/22/00	2:46:18 PM	VBRuntime	None	1	N/A	NMS0005
9/22/00	2:46:03 PM	VBRuntime	None	1	N/A	NMS0005
9/22/00	2:45:53 PM	VBRuntime	None	1	N/A	NMS0005
9/22/00	2:45:33 PM	VBRuntime	None	1	N/A	NMS0005
9/22/00	2:45:18 PM	VBRuntime	None	1	N/A	NMS0005
9/22/00	2:45:03 PM	VBRuntime	None	1	N/A	NMS0005
9/22/00	2:44:48 PM	VBRuntime	None	1	N/A	NMS0005
9/22/00	2:44:38 PM	VBRuntime	None	1	N/A	NMS0005
9/22/00	2:44:23 PM	VBRuntime	None	1	N/A	NMS0005

2. Double-click an entry to open a message box that displays the details of the event.

Figure 230 Event Detail

The Event Detail dialog box contains a detailed description of the specific event.

15.5 NMS Transaction Logs

NMS transaction logs record all changes made to database records in the NMS. [Table 14](#) describes the fields in the NMS Transaction Log file.

The log includes a logo graphic. To change the logo graphic to your company's logo, create a graphic file with the following parameters:

- Graphic must be in bitmap (.bmp) format.
- Graphic file must be named **logo.bmp**.
- File must reside in the **...reports\images** sub-directory of the application directory.

Table 14 Fields in the NMS Transaction Log File

Field	Description
Item	Type of record.
Item ID	Database identification number of the record in the database.
Item Name	Name of the record.
Action	Type of modification made to the record.
Description	Specifics of record modification.
Date	Date and time the record was changed.

To Open the NMS Transaction Log File

1. In the NMS software, click the **Logs** menu.
2. From the **Logs** menu, select **NMS Transaction Log**.

Figure 231 Sample NMS Transaction Log File

Your Company, Inc.					
Insert a 1"x3" logo here for report distribution (See LogoHelp.txt in the Reports/Images directory for help)					
NMS Transaction Log					
September 20, 2000 Page 1 of 1					
Item	Item_ID	Item_Name	Action	Description	Date
Accounts	1	Person Name	Added new Account	New Account: Person Name added.	9/20/00 1:55:10PM
Subscribers	1	Subscriber Name 1	Added new Subscribers	New Subscriber: Subscriber Name 1 inserted.	9/20/00 1:55:10PM
SNMP Server	1	SNMP Server 1	Default Change	Default flag is changed from 1 to 1.	9/20/00 1:55:11PM
SNMP Server	1	SNMP Server 1	Default Change	Default flag is changed from 1 to 1.	9/20/00 1:55:11PM
EUM	1	eum-1	Added new EUM	New EUM: eum-1 added.	9/20/00 2:44:46PM
Subscribers	2	User 1	Added new Subscribers	New Subscriber: User 1 inserted.	9/20/00 2:45:15PM
Subscribers	3	User 2	Added new Subscribers	New Subscriber: User 2 inserted.	9/20/00 2:45:27PM
Subscribers	4	User 3	Added new Subscribers	New Subscriber: User 3 inserted.	9/20/00 2:45:36PM
Subscribers	5	User 4	Added new Subscribers	New Subscriber: User 4 inserted.	9/20/00 2:45:50PM
Subscribers	2	User 1	Enable flag Change		9/20/00 2:46:08PM
EUM	1	eum-1	Subscriber ID changed		9/20/00 2:46:08PM
EUM	1	eum-1	CCU ID changed	CCU ID is changed from Null to 1.	9/20/00 2:46:14PM
EUM	1	eum-1	CCU ID changed	CCU ID is changed from 1 to 4.	9/20/00 3:50:02PM
EUM	1	eum-1	CCU ID changed	CCU ID is changed from 4 to 1.	9/20/00 3:51:52PM
EUM	2	eum-2	Added new EUM	New EUM: eum-2 added.	9/20/00 3:53:06PM
EUM	2	eum-2	Subscriber ID changed		9/20/00 3:53:18PM
Subscribers	3	User 2	Enable flag Change		9/20/00 3:58:24PM
EUM	3	eum-3	Added new EUM	New EUM: eum-3 added.	9/20/00 4:10:00PM
EUM	3	eum-3	Subscriber ID changed		9/20/00 4:10:06PM
Subscribers	4	User 3	Enable flag Change		9/20/00 4:10:12PM
*** End of Report ***					

15.6 Setting RADIUS Log Parameters

You can control the types of error messages being tracked in the RADIUS Server logs through the Windows Control Panel.

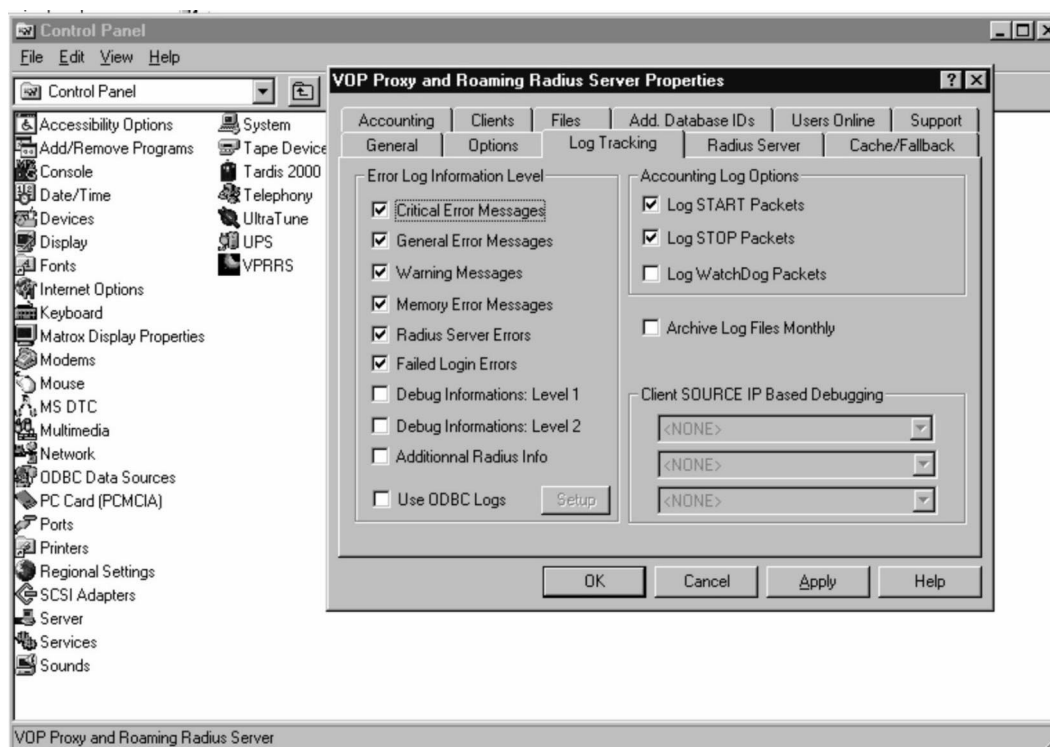
To Set RADIUS Log Parameters

1. Open **Control Panel**.
2. Double-click the **VPRRS** icon.

The **VOP Proxy and Roaming Radius Server Properties** screen opens.

3. Click the **Log Tracking** tab.

Figure 232 RADIUS Server Properties Screen



4. In the **Error Log Information Level** box, select the check boxes for the types of messages you want collected by RADIUS.
5. Leave other default settings as they are.
6. Click **Apply**.

A dialog box opens stating that the configuration options were successfully saved.

7. Click **Yes** to close the dialog box.
8. Click **OK** to exit the screen.

15.7 RADIUS Server Error Log

The RADIUS Error Log lists information about errors generated by RADIUS. The amount of information written to the file depends on the selections made through the RADIUS screen on the Control Panel.

The RADIUS Server Error Log contains the following types of information:

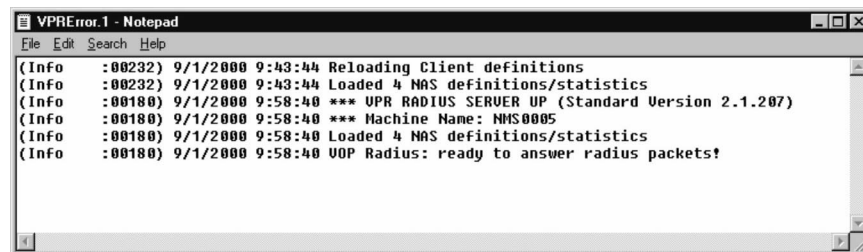
- Type of error
- Error number
- Date
- Time
- Error Description

To View the Current Error Log File

1. In the NMS software, click the **Logs** menu.
2. From the **Logs** menu, select **RADIUS Server Logs > Error Log**.

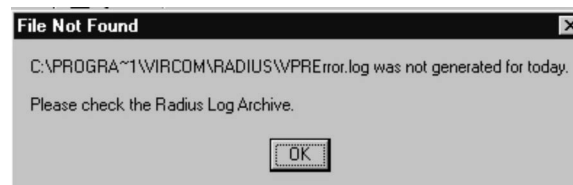
The Error Log file opens in Notepad.

Figure 233 Sample RADIUS Server Error Log File



If the error log needs to be generated, the File Not Found dialog box opens.

Figure 234 File Not Found Dialog Box



To Open an Archived Log

1. Open **Explorer**.
2. Navigate to the following directory:
 \Program Files\Vircom\RADIUS
3. Select the folder for the year you want to view.
4. Select the folder for the month you want to view.
5. Select the file you want to open.
6. Rename the extension to **.log**.
7. Double-click to open the file in **Notepad**.

15.8 RADIUS Server User Log

The RADIUS Server User Log is a record of RADIUS authentication of EUMs. Only enabled EUMs appear in the log. Check it periodically to verify that EUMs are connected to the CCUs and that they are functioning normally. Any fluctuation in the number of EUMs being authenticated indicates a problem.

Table 15 RADIUS Server User Log Fields

Field	Description
Port	Not used.
User ID	Contains the network IP address of the CCU to which the EUM is connected.
State	Indicates the current state of the authentication process for that EUM. Normally, this field is defined as "End".
Service	Indicates whether the EUM is Local or Roaming. For EUMs, this field will always be defined as "Local".
Time	Indicates the number of minutes since the RADIUS server last authenticated that EUM.
Limit	Not used.
IP Address	Not used.
Session ID	Not used.

To View the RADIUS Server Log File

1. In the NMS software, click the **Logs** menu.
2. From the **Logs** menu, select **RADIUS Server Logs > User Log**.

The file opens in Notepad.

Figure 235 Sample RADIUS Server User Log File

Port	UserID	State	Service	Time	Limit	IP Address	SessionID
Nas: 1	192.168.10.13 192.168.10.13 -1 1	End	Local	13	0	----	
Nas: 3	192.168.10.15 192.168.10.15 -1 3	End	Local	1	0	----	
Nas: 2	192.168.10.14 192.168.10.14 -1 2	End	Local	2	0	----	

15.9 RADIUS Server Statistics

This RADIUS Server Statistics log contains the following statistics generated by RADIUS. They are grouped by CCU, which is indicated by the NAS number and CCU network IP address. The bottom of the log contains totals for all CCUs for each time period.

Table 16 VPRStat.log File Fields

Field	Description
NAS	Network IP address of CCU.
0-1, 1-2, etc.	Hourly segments of operational detail, based on a 24-hour clock.
Maximum Usage	Total number of packets passed in the one-hour period.
Total Calls	Total number of authentication calls that occurred in the one-hour period.
Total AuthPkts	Total number of authenticated packets that were passed in the one-hour period.
Total AcctPkts	Not used.
Roaming Users	Not used.

To Access the RADIUS Server Statistics Log

1. In the NMS software, click the **Logs** menu.
2. From the **Logs** menu, select **RADIUS Server Logs > Statistics Log**.

The file opens in Notepad.

Figure 236 VPRStat.log File

NMS Servers-Statistics		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	10-11	11-12	12-13	13-14	14-15	15-16	16-17	17-18	18
NMS 1 : IP 192.168.10.13 (Livingston)																				
Maximum Usage																				
Total Calls																				
Total AuthPkts																				
Total AcctPkts																				
Roaming Users																				
NMS 2 : IP 192.168.10.14 (Livingston)																				
Maximum Usage																				
Total Calls																				
Total AuthPkts																				
Total AcctPkts																				
Roaming Users																				
NMS 3 : IP 192.168.10.15 (Livingston)																				
Maximum Usage																				
Total Calls																				
Total AuthPkts																				
Total AcctPkts																				
Roaming Users																				
NMS 4 : IP 192.168.10.16 (Livingston)																				
Maximum Usage																				
Total Calls																				
Total AuthPkts																				
Total AcctPkts																				
Roaming Users																				
*** TOTALS ***																				
Total AuthPkts																				
Total AcctPkts																				
Roaming Users																				

15.10 SNMPc Server Device Management Details

The SNMPc Server software enables you to monitor device operations and correlate events to specific conditions. You monitor these devices through the SNMPc Server software, where you can open a management detail view for each one. For most devices, you will open the management detail view from shortcut menus. However, you can open the view for a number of devices—particularly the Cisco devices and the NAP and CAP UPS—by double-clicking its icon. Use the information in the device management details to confirm that they are functioning properly.

The following tables describe the menus on the management detail view for each type of device.

Table 17 CCU and EUM Monitoring Reports

Menu Command	Description of Monitoring Device
Global Info	Displays information specific to an EUM or CCU, but not specific to the radio or Ethernet interface for the device—Serial Number, Software Version.
Radio Config	Displays configuration information for an EUM or CCU in the form of a system message.
Radio EUMs	Displays information about any units which communicate with the selected unit—EUM ID, State (up/down).
Radio Stats	Contains statistical information for the radio—Transmitted, TxDelayed, RxPackets, RxDataCRCError, RxHeaderCRCError, RxHeaderCRCFixed, RxInvalidLen, NICFailure, BroadCastDiscards.

Table 18 Ethernet Switch Monitoring Reports

Menu Command	Description of Monitoring Device
Traffic Input Packets/Sec	Displays the current input traffic in packets per second in graph format. You can choose from four styles of graph.
Traffic Output Packets/Sec	Displays the current output traffic in packets per second in graph format. You can choose from four styles of graph.
Processor Utilization	Displays the percentage of data traffic through the processor in graph format. You can choose from four styles of graph. This table helps you define system load.
Memory Allocation Failures	Displays current number of failures to allocate memory to data packets.
General Interface Info	General information about the switch interface.
Detailed Interface Info	Detailed information about the switch interface.

Table 19 Router Monitoring Reports

Menu Command	Description of Monitoring Device
Traffic Input Packets/Sec	Displays the current input traffic in packets per second in graph format. You can choose from four styles of graph.
Traffic Output Packets/Sec	Displays the current output traffic in packets per second in graph format. You can choose from four styles of graph.
Processor Utilization	Displays the percentage of data traffic through the processor in graph format. You can choose from four styles of graph. This table defines load.

Menu Command	Description of Monitoring Device
Memory Allocation Failures	Displays current number of failures to allocate memory to data packets.
General Interface Info	General information about the router interface.
Detailed Interface Info	Detailed information about the router interface.

Table 20 UPS Monitoring Reports

Menu Command	Description of Monitoring Device
UPS Identification	Identifies the static identification information from the device—Manufacturer, Model, Software Version.
Battery Info	Defines battery information—Time Remaining, Voltage, Current, Capacity, and Status.
Input Info	Displays the current device input frequency information—Frequency, LineBads, NumPhases.
Output Info	Displays the current device output frequency information—Frequency, LineBads, NumPhases.
Bypass Info	Indicates if a bypass is installed on the unit, and displays information about it—Frequency, NumPhases.
Environment Info	Displays state and temperature—Temp, Lower Limit, Upper Limit. If the state cannot be determined, the system returns “Unknown”.
Alarms	Displays the current valid alarm conditions—Alarms, AlarmNumEvents.
Self Test	Initiates a self-test and displays a current status message.
Control Info	Displays input/output timing controls—Off Delay, On Delay, Off Trap Delay, On Trap Delay, xups Control To Bypass Delay.
Config Info	Displays the configuration information for the device in a status message box.
Trap Control Info	Displays control features for trapping messages in a status message box.

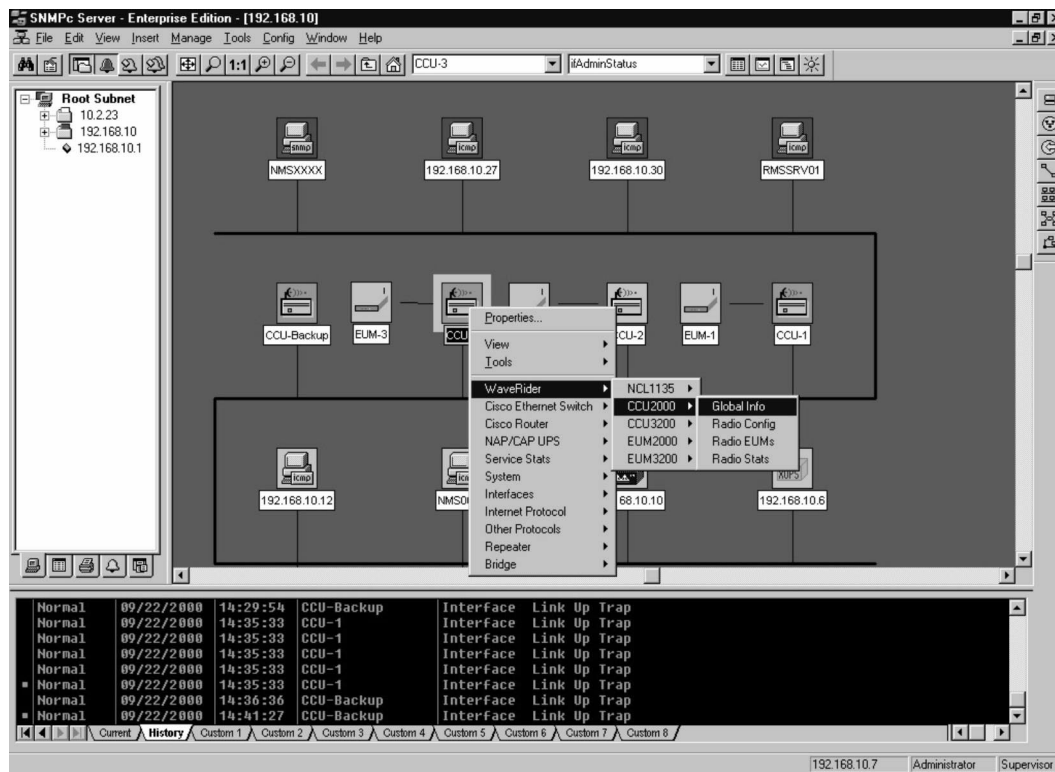
Menu Command	Description of Monitoring Device
Display Defined Traps	<p data-bbox="737 260 1271 289">Lists the Trap messages defined for the UPS:</p> <ul data-bbox="737 298 1073 1289" style="list-style-type: none"> <li data-bbox="737 298 902 327">• Control Off <li data-bbox="737 333 902 363">• Control On <li data-bbox="737 369 902 399">• On Battery <li data-bbox="737 405 915 434">• Low Battery <li data-bbox="737 441 1036 470">• Utility Power Restored <li data-bbox="737 476 1068 506">• Return From Low Battery <li data-bbox="737 512 971 541">• Output Overload <li data-bbox="737 548 951 577">• Internal Failure <li data-bbox="737 583 1000 613">• Battery Discharged <li data-bbox="737 619 951 648">• Inverter Failure <li data-bbox="737 655 902 684">• On Bypass <li data-bbox="737 690 1024 720">• Bypass Not Available <li data-bbox="737 726 894 756">• Output Off <li data-bbox="737 762 922 791">• Input Failure <li data-bbox="737 798 943 827">• Building Alarm <li data-bbox="737 833 1008 863">• Shutdown Imminent <li data-bbox="737 869 902 898">• On Inverter <li data-bbox="737 905 938 934">• Breaker Open <li data-bbox="737 940 997 970">• Alarm Entry Added <li data-bbox="737 976 1032 1005">• Alarm Entry Removed <li data-bbox="737 1012 987 1041">• Alarm Battery Bad <li data-bbox="737 1047 1068 1077">• Output Off As Requested <li data-bbox="737 1083 1032 1113">• Diagnostic Test Failed <li data-bbox="737 1119 1029 1148">• Communications Lost <li data-bbox="737 1155 1057 1184">• UPS Shutdown Pending <li data-bbox="737 1190 1040 1220">• Alarm Test in Progress <li data-bbox="737 1226 997 1255">• Ambient Temp Bad

To Monitor a Device

1. Open SNMPc Server.
2. Locate the icon of the device on the network map.
3. Right-click the icon to display the shortcut menu.
4. From the shortcut menu, select the type of device.

A shortcut menu of available reports opens.

Figure 237 SNMPc Main Screen



5. Click the report you want to view.

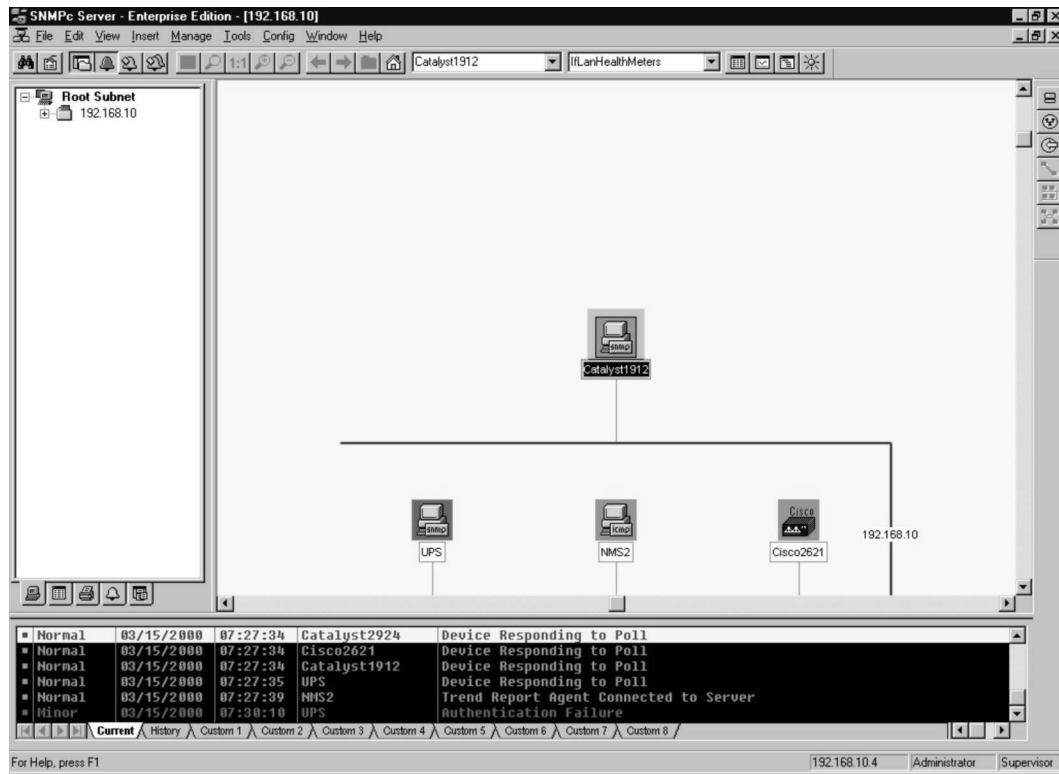
15.11 SNMPc Server Event Logs

The SNMPc Server displays the device event logs at the bottom of the main screen. By selecting one of the series of tabs along the bottom of the display, you can choose to view logs for various devices. Errors on this log usually indicate a problem at the device level.



Do not close SNMPc while the system is running. Closing SNMPc stops SNMP monitoring of the system. When you are finished with the screen, minimize it until you need it again.

Figure 238 SNMPc Server Main Screen



— This page is intentionally left blank —

16

Maintaining Hardware

This chapter describes how to maintain your LMS2000 system to help prevent problems. Specifically, it includes information about maintaining the operating environment and recovering from power outages.

16.1 Maintaining the LMS2000 Environment

The NAP and CAP components must be kept in a temperature-controlled and dust-free environment.

16.1.1 Maintaining Temperature and Humidity

Table 21 Recommended Temperature and Humidity for NAP and CAP

Equipment	Operating Temperature	Non-condensing Relative Humidity	Storage Temperature
NAP	+10° to +40°C	5% to 95%	-20° to +70°C
CAP	+10° to +40°C	5% to 95%	-20° to +70°C
EUM	0° to +55°C	5% to 95%	-20° to +70°C

16.1.2 Cleaning the Equipment

WARNING!



Ensure that you follow ESD precautions when you touch and clean components in the NAP or CAP cabinets.

You should be familiar with the following general guidelines for cleaning the NAP and CAP components:

- Use dry, static-free cloths to wipe dust from devices and cabinets.
- Use recommended screen cleaning products to wipe the NMS Workstation screen.
- Ensure that you do not disconnect any cables and wires when cleaning.

16.1.3 Checking the Cooling Fans

WARNING!



Exercise caution in close proximity to cooling fans. Disconnect AC power to fans prior to handling.

Verify the CAP cooling fans rotate at a high speed when connected to the power supply to ensure proper cooling for the CAP components.

16.2 Recovering From a Power Failure

The following procedures describe how to restore normal operations following a power failure.

16.2.1 Recovering from a Power Failure at the NMS Workstation

The Uninterruptible Power Supply (UPS) supporting the NMS Workstation provides a minimum of 10 minutes of power during a complete power outage. However, if the auxiliary power supply is exhausted, the NMS Workstation will power down. You will need to reboot the workstation when power is restored.

To Restart the NMS Workstation Software

1. Once power to the NMS Workstation is fully restored, power on the NMS Workstation.
The Windows NT logon process begins.
2. Press **Ctrl+Alt+Delete** at the **Begin Login** screen.
3. Type your Windows NT user name and password in the **Login Information** dialog box, and press **Enter**.
SNMPc Server and the LMS Network Management applications automatically launch.
4. In the **SNMPc Server Login** window, type your SNMPc Server user name and password.
5. Double-click the **SQL Server Service Manager** icon on the task bar to verify that it is running.
If it is not running, click the **Start/Continue** button to restart the **SQL Server Service Manager**.
The NMS Workstation automatically reconnects to the network and discovers all devices.
6. Open an **SNMPc Server** window to verify that all the connections are re-established.

NOTE: The SNMPc Server cannot monitor the network when the NMS Workstation is not operational. Any data generated during an NMS Workstation power failure will be lost.

16.2.2 Recovering From a Power Failure at the NAP

The uninterruptible power supply (UPS) in the NAP cabinet provides a minimum of 10 minutes of power during a complete power outage. Once power is fully restored, the NAP will power up and automatically reconnect to the network. Open an SNMPc Server window to verify that all the connections are re-established.

16.2.3 Recovering From a Power Failure at the CAP

The Uninterruptible Power Supply (UPS) in a remote CAP cabinet provides a minimum of 10 minutes power during a complete power outage. Once power is fully restored, the CAP will power up and automatically reconnect to the network.

Once power to the CAP is restored, open an SNMPc Server window to verify that all the connections are re-established.

16.2.4 Recovering From a Power Failure at an EUM

The EUM does not have a backup power source. If an EUM at a customer site experiences a power outage, the EUM will power up and automatically reconnect to the network once power is restored. Open the SNMPc Server window to verify that all the connections are re-established.

NOTE: WaveRider recommends the use of an Uninterruptible Power Supply (UPS) at the EUM site. For information on UPS equipment, contact your **WaveRider Sales Representative**.

16.3 Maintaining the ABWM Controller

16.3.1 Proper Use of a Module

A module can operate only when installed in the controller as described in this guide.

16.3.2 Replacement or Disposal of Batteries

When replacing a battery in an ABWM controller part, observe the caution stated below.



CAUTION: Danger of explosion if CPU battery is incorrectly replaced. Replace only with same or equivalent type recommended by the manufacturer. Dispose of used battery according to the manufacturer's instructions.

16.3.3 Removing and Replacing Modules



CAUTION: Observe precautions for handling electrostatic sensitive devices.

To Remove a Module from the Controller

1. Disconnect all cables from the front panel connectors.
2. Turn off the module.
3. Disconnect the power supply cable(s).
4. Loosen the set screw on the left side of the module's rear panel.
5. Grasp the fan guards on the rear panel of the module, then pull the module straight out a couple of inches.
6. Hold the side and rear panels of the module with one hand, support the module's bottom panel with the other hand, and pull the module straight out until it clears the controller chassis.

To Replace a Module in the Controller

1. Hold the side and rear panels of the module with one hand, support the module's bottom panel with the other hand, and push the module straight in along the guide rails until it touches the stop frame at the front of the controller.
2. Hand-tighten the set screw on the left side of the module's rear panel.

— This page is intentionally left blank —

17

Removing Components from your Network

17.1 Removing an EUM

If an account or subscriber discontinues service, you will need to remove the EUM(s) from the site.

When removing an EUM, complete the following procedures, each of which is explained in this chapter:

- Disable the subscriber (or disable the account if the entire account is discontinuing).
- Remove the EUM from the field.
- Delete the subscriber (or account if necessary) from the NMS software.

Each of these procedures is described in this chapter.

17.1.1 Disabling an Account or Subscriber

Disabling an account blocks all the associated subscribers from accessing the network. Disabling a subscriber blocks only the individual subscriber from the network. If you disable an account, you cannot re-enable any of the subscribers until the account is re-enabled.

NOTE: The menu tree icon for a disabled account or subscriber will have a red lock on it.

To Disable an Account

1. On the menu tree, right-click the Account record name.
2. Click **Disable Account**.

To Disable a Subscriber

1. On the menu tree, right-click the Subscriber record name.
2. Click **Disable Subscriber**.

17.1.2 Removing an EUM from the Field

Once you have disabled an account or subscriber, you are ready to remove the EUM from the field. After you have returned the EUM, you may delete the account or subscriber. You will not remove the EUM record from the NMS software. Rather, you will dissociate it from the subscriber, which returns the EUM record to unassigned inventory status.



CAUTION: Once you delete an account or subscriber record, you cannot restore it.

Once you have returned the EUM to inventory, you should reset it to the default configuration and upload that configuration to the device.

To Restore the EUM to Factory Default Configuration

1. In the NMS software, open the record for the EUM to reset.
2. Click the **Tools** tab.
3. Click the **Load Defaults** button.

To Connect to the EUM

1. Terminate the EUM antenna lead by attaching a 50-ohm RF load.
2. Attach an RS-232 crossover cable to the DB9 console port.
3. If not already, attach the other end of the RS-232 cable to the NAP.
4. Plug the EUM into an AC power source.
5. Confirm the following conditions:
 - EUM's red power LED is on.
 - Green network link LED is on.
 - Cooling fan is operating.

To Establish a HyperTerminal Session

1. In the NMS software, right-click the EUM record.
2. On the shortcut menu, click **Tools > Serial Interface**.

A HyperTerminal window opens.

3. In the **Connection Description** dialog box, type a name for the connection and click **OK**.

NOTE: You can give any name to the connection.

4. Configure the application using the following settings:
 - 9600 bps
 - 8 data bits
 - No parity
 - 1 stop bit
 - No flow control
5. At the **HyperTerminal** prompt, type **ip address ethernet <new ethernet address> <new netmask>**, and press **Enter**.

17.1.3 Deleting an Account or Subscriber

When you delete an account, you also delete the associated subscribers. Deleting a subscriber dissociates the EUM from the subscriber. When you delete a subscriber, the associated EUM returns to unassigned inventory status, and the EUM record disconnects from the CCU record.

To Delete an Account

1. On the menu tree, right-click the Account record name that you want to delete.
2. Click **Delete**.

If the account has subscribers with associated EUMs, you will be prompted to break the subscriber/EUM associations before you can delete the account.

3. Click **Yes** to unlink the subscribers and EUMs.

The subscribers and account records disappear from the database.



CAUTION: Deleted records cannot be recovered from the current database. If you accidentally delete an account, check your backup tapes. If you restore files, remember to check the links and to check for any recent updates. Refer to [12, Restoring Backups](#), on page 193.


17.2 Removing an RFSM

Removing an RFSM from your LMS2000 system involves the following procedures:

1. Stop the RFSM polling engine.
2. Stop the RFSM service.
3. Remove CCU assignments from RFSM.
4. Remove RFSM from service.

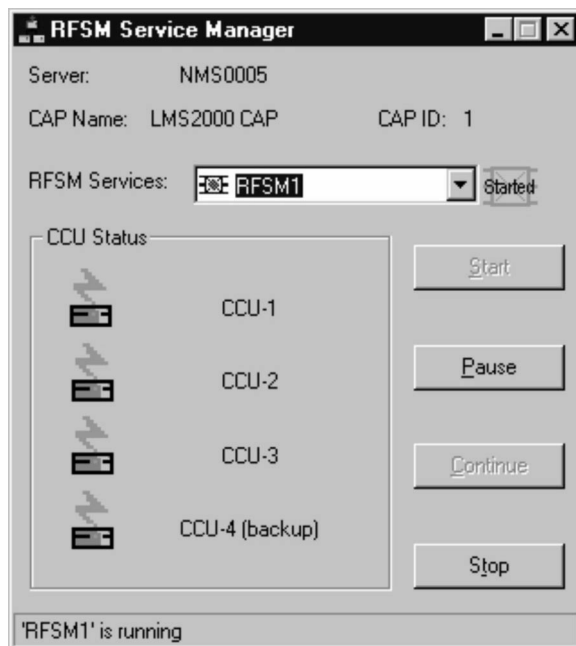
If your LMS2000 system includes multiple RFSMs, you will need to repeat these procedures for each RFSM that you are removing. Each procedure is described in detail below.

To Stop the RFSM Polling Engine

1. In the Windows system tray, double-click the  icon to open the RFSM Service Manager window.

NOTE: If the icon does not appear in your system tray, you must restart the RFSM Service Manager, as described in [To Start the RFSM Service](#), on page 121.

Figure 239 RFSM Service Manager



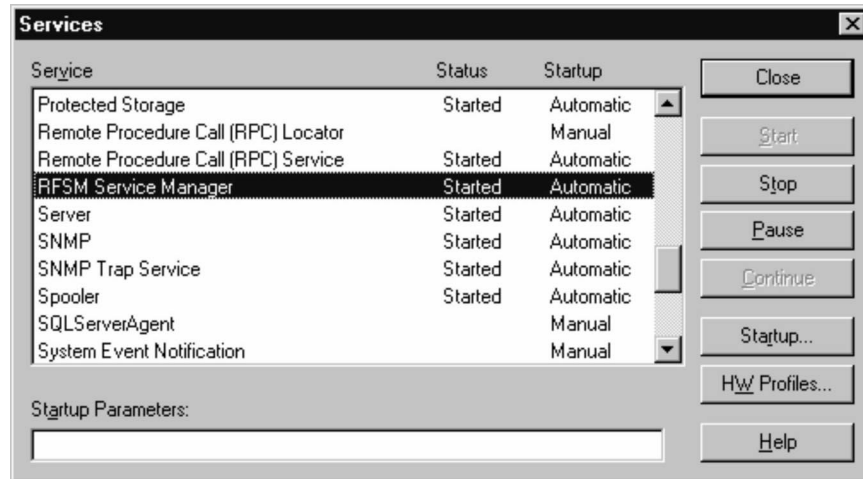
2. From the **RFSM Services** drop-down list, select the RFSM unit to stop.
3. Click the **Stop** button.

The status icon beside the RFSM Services drop-down list changes to Stopped.

To Stop the RFSM Service

1. Click the **Start** button.
2. Select **Settings > Control Panel**.
The Control Panel window opens.
3. In the Control Panel window, double-click the **Services** icon.


Figure 240 RFSM Service Manager in Services Window



4. Scroll down to RFSM Service Manager and select it.
5. Click the **Stop** button.

Figure 241 Service Control



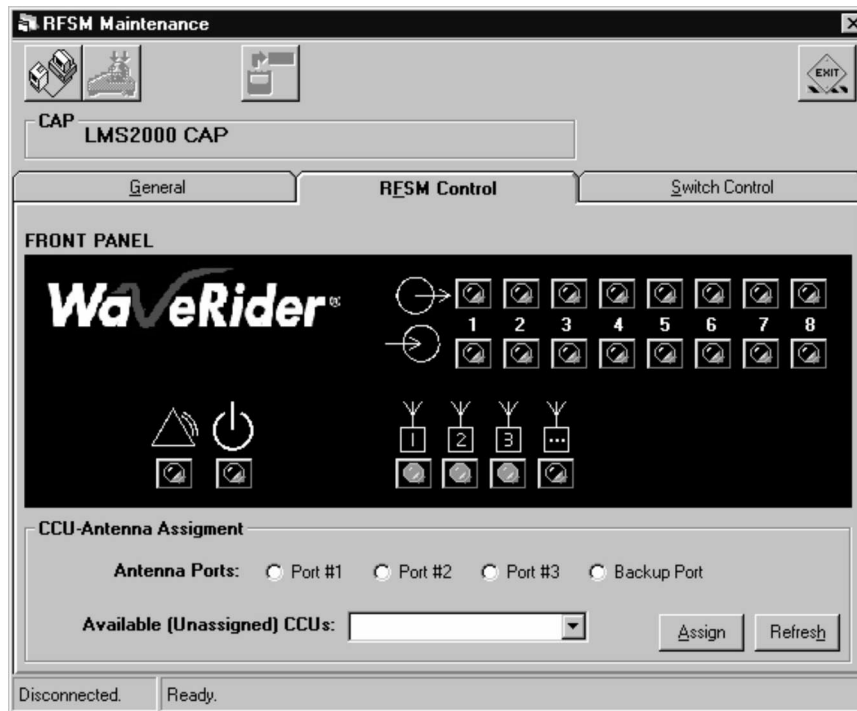
When the service is stopped, the  icon disappears from the Windows task bar.

6. Click **Close** in the **Services** window.
7. Close the **Control Panel** window.

To Remove CCU Assignments from RFSM

1. In the NMS, open the **RFSM Properties** screen.
2. Click the **RFSM Control** tab.

Figure 242 RFSM Maintenance—RFSM Control Tab



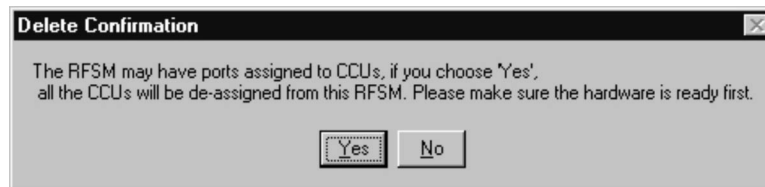
3. Click the **Port #1** option button.
4. From the **Available (Unassigned) CCUs** drop-down list, select **None**.
5. Click the **Assign** button.
6. Repeat steps 3 through 5 for **Port #2**, **Port #3**, and the **Backup Port**.
7. Click the **General** tab.
8. Click the **Apply** button to save the changes in the NMS database.

To Remove the RFSM from Service

1. In the NMS, click **RF Switch Matrix** under the LMS2000 CAP branch.
2. In the right pane, click the Switch Matrix Name for the RFSM.
3. On the NMS button bar, click the **Remove** button.

The Delete Confirmation dialog box opens.

Figure 243 RFSM Delete Confirmation Dialog Box



4. On the Delete Confirmation dialog box, click the **Yes** button.

— This page is intentionally left blank —

18

Upgrading the System

Periodically, WaveRider releases updates to NMS software, EUM firmware, and CCU firmware. You will receive these updates on CD with installation instructions in the accompanying release notes.

NOTE: All the programs on the NMS workstation are subject to update by the manufacturer. WaveRider does not guarantee compatibility of third-party software beyond the versions recommended with the initial install or with any subsequent NMS program updates.

This chapter explains how to update software and firmware, and how to replace hardware components in your LMS2000 system.


18.1 Synchronizing Database Information

The NMS includes a utility called Database Synchronization Manager, which automatically keeps an up to date record of the firmware versions installed in EUMs and CCUs. The database synchronization manager starts automatically when you run the NMS software. Leave it running at all times, except when you are updating EUM and CCU firmware.

WARNING!

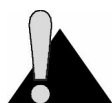


Synchronization of the firmware information and the database records must be maintained at all times.

To turn the Database Synchronization Manager on or off, click , which is located in the bottom right corner of the main screen of the NMS software. Select ON or OFF from the shortcut menu. If the button has an X through it, it is turned off.


18.2 Updating EUM and CCU Firmware

This section explains how to install new firmware on EUMs and CCUs. You can update the EUM and CCU firmware from the NMS or remotely. Use the first procedure when you have access to the NMS workstation. Otherwise, use the remote update procedure. Release notes will include additional information about the specific update.



CAUTION: When updating software that affects both CCUs and EUMs, update all the EUMs first, then update the CCUs. Otherwise, you will lose contact with your EUMs and a site visit will be required to re-establish contact with them.

To Update CCU and EUM Firmware through the NMS

1. In the bottom right corner of the NMS main screen, click  and click **OFF** to stop the Database Synchronization Manager.
2. In the NMS, click the **Tools** menu and select **Download**.


The **Firmware Download** screen opens.

Figure 244 Firmware Download—Connect

The screenshot shows a 'Firmware Download' dialog box. It has two main sections. The first section, 'Select Device', contains two radio buttons: 'EUM' (which is selected) and 'CCU'. Below each radio button is a dropdown menu; the 'EUM' dropdown shows 'EUM1(1)'. The second section, 'Firmware CCU/ EUM', contains several input fields: 'Path' with the value 'C:\wip\build\firmware\eum2000.exe', 'EUM ID' with the value '1', 'Version' with the value 'EUM20006', 'Address' with the value '192.168.210.1', and 'Status' with the value 'connecting to device...'. At the bottom of the dialog are 'Apply' and 'Cancel' buttons.

3. In the **Select Device** group, select either the **EUM** or **CCU** option to reflect which device type you are updating.

4. From the drop-down list, select the specific EUM or CCU to update.
5. Confirm that the path in the **Path** field shows the correct location of the update file.

If the path shown is incorrect, click  and navigate to the appropriate path.

WARNING!



Proceeding to the next step will disrupt service to EUMs until the system has been rebooted.

6. Click **Apply** to begin the update.

The **Status** field will display messages describing the background activities.

Figure 245 Firmware Download—Success

The screenshot shows a 'Firmware Download' dialog box. It has two main sections. The first section, 'Select Device', contains two radio buttons: 'EUM' (which is selected) and 'CCU'. Below the radio buttons are two dropdown menus; the first one shows 'eum101(1)'. The second section, 'Firmware CCU/ EUM', contains several input fields: 'Path' (with the value 'C:\wip\build\firmware\eum2000.exe' and a browse button), 'EUM ID' (with the value '1'), 'Version' (with the value '0.1'), and 'Address' (with the value '192.168.210.2'). At the bottom of this section is a 'Status' field displaying the text 'device being restarted'. At the very bottom of the dialog box are two buttons: 'Apply' and 'Cancel'.

When the download completes, the device restarts automatically.

7. Click **Cancel**.

OR

Repeat steps 3 through 6 to update another EUM or CCU.

8. Click  and click **ON** to start the Database Synchronization Manager.

18.2.1 Updating EUM or CCU Firmware Using Remote Connections

If you do not have access to the NMS workstation, you will have to update the firmware through a remote connection to the EUM or CCU. First, install the update through an FTP connection to the device, and then restart it using Telnet.

NOTE: If your network has a firewall, you will only be able to access the device from within the network. Before attempting to configure the EUM using a remote connection, you should be familiar with the configuration options available for the device.

To Update the EUM or CCU Firmware with FTP

1. Open a DOS window.
2. At the prompt, **FTP <ip address of EUM or CCU>**, and press **Enter**.
3. At the **Username** prompt, press **Enter** without typing a user name.
4. At the **Password** prompt, press **Enter** without typing a password.
5. At the prompt, type **binary**, and press **Enter**.
6. Type **hash**, and press **Enter**.

WARNING!



Proceeding to the next step will disrupt service to EUMs until the system has been rebooted.

7. Type **put <filename>**, and press **Enter**.
8. Type **bye** to exit FTP.
9. Restart the EUM or CCU using the following procedure.

To Restart an EUM or CCU using Telnet

1. In the DOS window, type **telnet <ip address of EUM or CCU>**, and press **Enter**.
2. If required, type the password for the EUM or CCU, and press **Enter**.
3. At the prompt, type **restart**.

This step automatically drops your Telnet connection, and the firmware is now installed.

18.3 Updating RFSM Firmware

You can update RFSM firmware using FTP. The following instructions explain this procedure and how to restart the RFSM unit using Telnet.

NOTE: If your network has a firewall, you will only be able to access the device from within the network.

To Update RFSM Firmware with FTP

1. Open a DOS window.
2. At the prompt, **FTP <ip address of RFSM>**, and press **Enter**.
3. At the **Password** prompt, type the password for the device.
4. At the prompt, type **binary**, and press **Enter**.
5. Type **hash**, and press **Enter**.
6. Type **put rom.bin**, and press **Enter**.

NOTE: If the file is not named "rom.bin", then you must rename it before you use the PUT command.

7. Type **bye** to exit FTP.
8. Restart the RFSM using the following procedure.

To Restart an RFSM Unit Using Telnet

1. In the DOS window, type **telnet <ip address of RFSM>** and press **Enter**.
2. If required, type the password for the RFSM and press **Enter**.
3. Type **V** and press **Enter** to ensure the version loaded successfully.
4. Type **W** and press **Enter** to write the firmware resident in the buffer to FLASH.
5. If the FLASH resident binary image did not correspond to the buffer resident image, a ! error results. Type **C** and press **Enter** to clear the error.
6. Type **R** and press **Enter** to restart the system.

This step automatically drops your Telnet connection, and the firmware is now installed.

18.4 Replacing Hardware Components

Occasionally, you may need to replace hardware components such as switches, routers, etc. After you replace the hardware, upload the database configuration for the device.

To Replace Hardware Components in a Cabinet

1. Ground yourself with an ESD strap to the cabinet frame or chassis.
2. Power down all the equipment attached to the component you are removing.
3. Power down the component you are removing.
4. Unplug the power cable from the power source.
5. Note the cable connections and mark the cables if necessary, so that you can reconnect the cables correctly to the new component.
6. Disconnect the cables from the component you are removing.
7. Support the component you are removing and loosen the screws holding it in the cabinet.

NOTE: Supporting the equipment may require more than one person.

8. Always place the new component in the same position from which the old component was removed.
9. When you are ready to install the new component in the cabinet, reconnect the cables in the reverse sequence that you disconnected them.
10. When the unit has been replaced, power up the NAP or CAP.

After the device is replaced in the cabinet, restore the previous configuration to the device, as described in the following procedure.

To Restore the Configuration to a Hardware Device

1. Connect a computer or terminal to the device via the serial port.
2. Log into the device using a terminal emulation program.
3. Change the IP address and netmask, if applicable, to the IP address assigned for that device.
4. Exit the terminal-emulation application, and disconnect the computer from the device.
5. Connect the device in your network, and from the NMS software, select the device.
6. Right-click the **Connect** button to connect to the device.
7. Click the **Update** button to upload the configuration settings to the device.

The device has now been restored with the settings from the NMS database.

18.5 Repairing the NMS Workstation

All repairs to the NMS Workstation should be completed by a reputable supplier and service technician in your area. If your NMS Workstation requires a new hard drive, you will have to reinstall the NMS Workstation software using the LMS Network Management Software CD, and restore your NMS database from your most recent backup.

To reinstall the NMS Workstation software, contact the **WaveRider Customer Support Centre** for detailed instructions.

To restore your NMS database from backup media, refer to [Restoring Backups](#), on page 193.

— This page is intentionally left blank —

19

Troubleshooting

19.1 Common Problems and Solutions

The following table describes problems that may occur with your LMS2000 system, the possible causes of those problems, and what you can do to resolve them.

Symptom	Possible Cause	Solution
Power LED on the back panel of CCU or EUM is not on (light is red when on).	Device is not receiving power.	<ul style="list-style-type: none">• Ensure that the device is plugged into a 110 - 220 V AC outlet and there is power at the outlet.• Check all cables for loose or faulty connections. Replace cables if necessary.

Symptom	Possible Cause	Solution
CCU is <u>not</u> responding at SNMP—all EUMs connected to the CCU do not respond and the Ethernet Link LED is off.	CCU is not receiving power.	<ul style="list-style-type: none"> • Ensure that the device is plugged into a 110 - 220 V AC outlet and that the power outlet is receiving power. • Check all cables for loose or faulty connections. Replace cables if necessary.
	Ethernet switch is configured incorrectly.	<ul style="list-style-type: none"> • From the NMS Workstation connect to the switch. • Verify that the port settings are enabled. • Verify that the Ethernet speed is correct.
	Ethernet cable is faulty.	<ul style="list-style-type: none"> • Verify that the Ethernet cable is securely plugged into the CCU and the Ethernet switch. • Verify that the Ethernet cable is not faulty. • Replace the Ethernet cable, if required.
	Ethernet switch is faulty.	<ul style="list-style-type: none"> • Replace the Ethernet switch, if required.
CCU is <u>not</u> responding at SNMP—all EUMs connected to the CCU do not respond and the Ethernet Link LED is on (light is green when on).	CCU configuration has changed.	<ul style="list-style-type: none"> • Connect a computer to the RS-232 port and log in to the CCU. • Verify that the configuration options are set correctly. • Verify that the CCU Routing Table is correct.

Symptom	Possible Cause	Solution
CCU is responding at SNMP—all EUMs connected to the CCU do not respond.	CCU is disabled.	<ul style="list-style-type: none"> From the NMS Workstation, connect to the CCU. Ensure that the radio transmission is enabled.
	CCU configuration has changed.	<ul style="list-style-type: none"> From the NMS Workstation, connect to the CCU. Verify that the radio channel is correct. Verify that the CCU ID is correct. Verify that all EUM IDs have been added to the EUM IDs list. Verify that the CCU Routing Table is correct.
	Problem with the antenna system at the CCU.	<ul style="list-style-type: none"> Verify that the antennas are aligned correctly. Verify the integrity of all RF connections. Verify that the RF cable has not been damaged.

Symptom	Possible Cause	Solution
CAP is not responding at SNMP—all CCUs, the UPS, and the Ethernet switch at the CAP are not responding at SNMP.	Device is not receiving power.	<ul style="list-style-type: none"> • Ensure that the UPS at the CAP is plugged into a 110 - 220 V AC outlet, and there is power at the outlet. • Ensure that the UPS is turned on. • Ensure that all the CCUs are securely plugged into the CAP cabinet power bar, and the power power bar is plugged securely into the UPS. • Check all cables for loose or faulty connections. Replace cables if necessary.
	The Ax uplink port is disabled or incorrect at the CAP switch.	<ul style="list-style-type: none"> • Connect a computer to the RS-232 port on the CAP switch. • Verify that the port is enabled. • Verify that the speed is correct (100BaseTx or 10BaseTx).
	The NAP switch port connected to the CAP is disabled or configured incorrectly.	<ul style="list-style-type: none"> • From the NMS Workstation, connect to the NAP switch. • Verify that the port for the CAP is enabled. • Verify that the speed is correct (100BaseTx or 10BaseTx).
	Ethernet switch is faulty.	<ul style="list-style-type: none"> • Replace Ethernet switch, if required.

Symptom	Possible Cause	Solution
EUM is not responding at SNMP.	Device is not receiving power.	<ul style="list-style-type: none"> Ensure that the device is plugged into a 110 - 220 V AC outlet and there is power at the outlet.
	Device has been physically damaged.	<ul style="list-style-type: none"> Check for visible signs of damage to the device or connections. For example, vandalism, lightning damage, etc. Check all cables for loose or faulty connections. Replace cables if necessary. Check antenna for damage. Replace EUM, if necessary.
	Antenna line-of-sight (LOS) to the CCU has been obstructed.	<ul style="list-style-type: none"> Ensure that a clear LOS still exists to the CCU antenna.
	EUM is not associated with the CCU.	<ul style="list-style-type: none"> From the NMS Workstation, connect to the same CCU as the EUM. Verify that the EUM is listed on the EUM IDs list for that CCU. Verify that the Routing Table has an entry for the EUM.
	SNMP settings for the EUM are incorrect.	<ul style="list-style-type: none"> At the NMS Workstation, open an SNMPc Server window. Verify that the EUM IP address is set correctly. Verify that the IP address for the Polling Agent (RADIUS server) is correct.
	EUM is disabled or the configuration has changed.	<ul style="list-style-type: none"> Connect a computer to the RS-232 port and log in to the EUM. Ensure that the radio transmission is enabled. Verify that the radio channel is correct. Verify that the EUM ID is correct. Verify that the CCU ID is correct. Verify that the EUM Routing Table is correct.
	EUM has failed.	<ul style="list-style-type: none"> Replace EUM, if necessary.

Symptom	Possible Cause	Solution
NAP is not responding at SNMP.	Device is not receiving power.	<ul style="list-style-type: none"> • Ensure that the UPS at the NAP is plugged into a 110 - 220 V AC outlet and there is power at the outlet. • Ensure that all devices are securely plugged into the NAP cabinet power bar and that it is plugged securely into the UPS. • Check all cables for loose or faulty connections. Replace cables if necessary.
	The port for the NAP is disabled or incorrect at the NAP switch.	<ul style="list-style-type: none"> • Connect a computer to the RS-232 port on the NAP switch. • Verify that the port is enabled. • Verify that the speed is correct (100BaseTx or 10BaseTx).
	The Ethernet cable is faulty.	<ul style="list-style-type: none"> • Verify that the Ethernet cables are securely plugged into the EUM. • Replace the Ethernet cables.
	The router is disabled or incorrect.	<ul style="list-style-type: none"> • Connect a computer to the RS-232 port on the NAP router. • Verify that the router is enabled. • Verify that the speed is correct (100BaseTx or 10BaseTx).
	Ethernet switch is faulty.	<ul style="list-style-type: none"> • Replace the Ethernet switch, if required.
CAP end of the back haul is not responding.	Devices are not receiving power, or the configuration is incorrect.	<ul style="list-style-type: none"> • Verify that the CAP back haul has power. • Verify the radio configurations at the CAP end. • Verify the routing configurations at the CAP end. • Verify the cable connections at both ends. • Verify that the radio link is operational.
NAP end and CAP end of back haul are not responding.	Devices are not receiving power or the configuration is incorrect.	<ul style="list-style-type: none"> • Verify power at the NAP end for back haul. • Verify the radio configuration at the NAP end. • Verify the routing configuration at the NAP end.

Symptom	Possible Cause	Solution
Internet connection is not working.	Devices are not receiving power or the configuration is incorrect.	<ul style="list-style-type: none">• Verify that the router is enabled.• Verify that the speed is correct.• Verify that the routing table is correct.• Verify that the Ethernet cable is not faulty. Replace if necessary.• Ensure that the other routers in the service area recognize the LMS2000 system.

— This page is intentionally left blank —

Appendix A Device Configuration Defaults

This appendix identifies the default configuration settings for devices within the NAP and the CAP.

Table 22 NAP Device Defaults

Device	Default Configuration
NAP Router	Internet Port: 10.2.23.1 LMS Port: 192.168.10.1
2924 Ethernet Switch	IP Address: 192.168.10.5 Netmask: 24 Gateway: 192.168.10.1
RADIUS Server	IP Address: 192.168.10.7 Netmask: 24 Gateway: 192.168.10.1
SNMP Server	IP Address: 192.168.10.7 Netmask: 24 Gateway: 192.168.10.1
Advanced Bandwidth Manager (Primary Controller)	IP Address: 192.168.10.2 Netmask: 24
Advanced Bandwidth Manager (Secondary Controller)	IP Address: 192.168.10.3 Netmask: 24
UPS	IP Address: 192.168.10.6 Netmask: 24 Gateway: 192.168.10.1
NMS Workstation	IP Address: 192.168.10.7 Netmask: 24 Gateway: 192.168.10.1

Table 23 CAP Device Defaults

Device	CAP	Default Configuration
1912 Ethernet Switch	CAP 1	192.168.10.10
	CAP 2	192.168.10.20
	CAP 3	192.168.10.30
	CAP 4	192.168.10.40
	CAP 5	192.168.10.50
	CAP 6	192.168.10.60
	CAP 7	192.168.10.70
	Expansion CAP	192.168.10.80
CAP UPS (switch port 1)	CAP 1	192.168.10.11
	CAP 2	192.168.10.21
	CAP 3	192.168.10.31
	CAP 4	192.168.10.41
	CAP 5	192.168.10.51
	CAP 6	192.168.10.61
	CAP 7	192.168.10.71
	Expansion CAP	192.168.10.81
RFSM	CAP 1	Ethernet IP: 192.168.10.12 Netmask: 24 Gateway: 192.168.10.1
	CAP 2	Ethernet IP: 192.168.10.22 Netmask: 24 Gateway: 192.168.10.1
	CAP 3	Ethernet IP: 192.168.10.32 Netmask: 24 Gateway: 192.168.10.1
	CAP 4	Ethernet IP: 192.168.10.42 Netmask: 24 Gateway: 192.168.10.1
	CAP 5	Ethernet IP: 192.168.10.52 Netmask: 24 Gateway: 192.168.10.1
	CAP 6	Ethernet IP: 192.168.10.62 Netmask: 24 Gateway: 192.168.10.1

Table 23 CAP Device Defaults (Continued)

Device	CAP	Default Configuration
	CAP 7	Ethernet IP: 192.168.10.72 Netmask: 24 Gateway: 192.168.10.1
	Expansion CAP	Ethernet IP: 192.168.10.82 Netmask: 24 Gateway: 192.168.10.1
CCU 1 (switch port 2)	CAP 1	Ethernet: 192.168.10.13 Radio: 192.168.110.1 Local ID: 1010 Radio Channel: 1
	CAP 2	Ethernet: 192.168.10.23 Radio: 192.168.120.1 Local ID: 1020 Radio Channel: 1
	CAP 3	Ethernet: 192.168.10.33 Radio: 192.168.130.1 Local ID: 1030 Radio Channel: 1
	CAP 4	Ethernet: 192.168.10.43 Radio: 192.168.140.1 Local ID: 1040 Radio Channel: 1
	CAP 5	Ethernet: 192.168.10.53 Radio: 192.168.150.1 Local ID: 1050 Radio Channel: 1
	CAP 6	Ethernet: 192.168.10.63 Radio: 192.168.160.1 Local ID: 1060 Radio Channel: 1
	CAP 7	Ethernet: 192.168.10.73 Radio: 192.168.170.1 Local ID: 1070 Radio Channel: 1
	Expansion CAP	Ethernet: 192.168.10.83 Radio: 192.168.180.1 Local ID: 1080 Radio Channel: 1

Table 23 CAP Device Defaults (Continued)

Device	CAP	Default Configuration
CCU 2 (switch port 3)	CAP 1	Ethernet: 192.168.10.14 Radio: 192.168.111.1 Local ID: 1011 Radio Channel: 6
	CAP 2	Ethernet: 192.168.10.24 Radio: 192.168.121.1 Local ID: 1021 Radio Channel: 6
	CAP 3	Ethernet: 192.168.10.34 Radio: 192.168.131.1 Local ID: 1031 Radio Channel: 6
	CAP 4	Ethernet: 192.168.10.44 Radio: 192.168.141.1 Local ID: 1041 Radio Channel: 6
	CAP 5	Ethernet: 192.168.10.54 Radio: 192.168.151.1 Local ID: 1051 Radio Channel: 6
	CAP 6	Ethernet: 192.168.10.64 Radio: 192.168.161.1 Local ID: 1061 Radio Channel: 6
	CAP 7	Ethernet: 192.168.10.74 Radio: 192.168.171.1 Local ID: 1071 Radio Channel: 6
	Expansion CAP	Ethernet: 192.168.10.84 Radio: 192.168.181.1 Local ID: 1081 Radio Channel: 6
Not all LMS installations have CCU 3 or CCU4 units. CCU4 is used as a backup unit. Contact your WaveRider Sales Representative for details on availability.		
Optional: CCU 3 (switch port 4)	CAP 1	Ethernet: 192.168.10.15 Radio: 192.168.112.1 Local ID: 1012 Radio Channel: 11

Table 23 CAP Device Defaults (Continued)

Device	CAP	Default Configuration
	CAP 2	Ethernet: 192.168.10.25 Radio: 192.168.122.1 Local ID: 1022 Radio Channel: 11
	CAP 3	Ethernet: 192.168.10.35 Radio: 192.168.132.1 Local ID: 1032 Radio Channel: 11
	CAP 4	Ethernet: 192.168.10.45 Radio: 192.168.142.1 Local ID: 1042 Radio Channel: 11
	CAP 5	Ethernet: 192.168.10.55 Radio: 192.168.152.1 Local ID: 1052 Radio Channel: 11
	CAP 6	Ethernet: 192.168.10.65 Radio: 192.168.162.1 Local ID: 1062 Radio Channel: 11
	CAP 7	Ethernet: 192.168.10.75 Radio: 192.168.172.1 Local ID: 1072 Radio Channel: 11
	Expansion CAP	Ethernet: 192.168.180.005 Radio: 192.168.182.1 Local ID: 1010 Radio Channel: 11
Optional: CCU 4 (backup) (switch port 5)	CAP 1	Ethernet: 192.168.10.16 Radio: 192.168.113.1 Local ID: 1013 Radio Channel: 4
	CAP 2	Ethernet: 192.168.10.26 Radio: 192.168.123.1 Local ID: 1023 Radio Channel: 4
	CAP 3	Ethernet: 192.168.10.36 Radio: 192.168.133.1 Local ID: 1033 Radio Channel: 4

Table 23 CAP Device Defaults (Continued)

Device	CAP	Default Configuration
	CAP 4	Ethernet: 192.168.10.46 Radio: 192.168.143.1 Local ID: 1043 Radio Channel: 4
	CAP 5	Ethernet: 192.168.10.56 Radio: 192.168.153.1 Local ID: 1053 Radio Channel: 4
	CAP 6	Ethernet: 192.168.10.66 Radio: 192.168.163.1 Local ID: 1063 Radio Channel: 4
	CAP 7	Ethernet: 192.168.10.76 Radio: 192.168.173.1 Local ID: 1073 Radio Channel: 4
	Expansion CAP	Ethernet: 192.168.10.866 Radio: 192.168.183.1 Local ID: 1081 Radio Channel: 4

Appendix B Operating Channel Frequencies

The following table defines the LMS2000 operating channel frequencies.

Channel ID	FCC/IC Channel Frequencies (USA/ Canada)	MKK Channel Frequencies (Japan)	ETSI Channel Frequencies (Europe)	French Channel Frequencies	Spanish Channel Frequencies
1	2412 MHz	not available	2412 MHz	not available	not available
2	2417 MHz	not available	2417 MHz	not available	not available
3	2422 MHz	not available	2422 MHz	not available	not available
4	2427 MHz	not available	2427 MHz	not available	not available
5	2432 MHz	not available	2432 MHz	not available	not available
6	2437 MHz	not available	2437 MHz	not available	not available
7	2442 MHz	not available	2442 MHz	not available	not available
8	2447 MHz	not available	2447 MHz	not available	not available
9	2452 MHz	not available	2452 MHz	not available	not available
10	2457 MHz	not available	2457 MHz	2457 MHz	2457 MHz
11	2462 MHz	not available	2462 MHz	2462 MHz	2462 MHz
12	not available	not available	2467 MHz	2467 MHz	not available
13	not available	not available	2472 MHz	2472 MHz	not available
14	not available	2484 MHz	not available	not available	not available

— This page is intentionally left blank —

Appendix C Command-Line Syntax

The EUM can be configured through a command-line interface using the commands listed in [EUM Command-Line Syntax](#) on page 300.

[Command-Line Syntax Conventions](#) on page 299 shows the typographical conventions used to represent command-line syntax. [Command-Line Shortcuts and Getting Help](#) on page 300 provides a list of shortcuts and methods to get help on commands. To execute a command, type the command and press **Enter**.

Table 24 Command-Line Syntax Conventions

Convention	Use	Examples
<monospaced font>	Indicates that you must type the text inside the angle brackets.	<ip route>
Enter	Indicates a keyboard key press. A plus sign (+) indicates key combinations. For example, for Ctrl+U , press and hold down the Ctrl key, then press the U key.	Enter Esc Ctrl+U
<i>italic</i>	Specifies a variable name or other information that you must replace with a real name or value.	ip address ethernet <i>ipaddress</i>
bold characters	Indicates the shortcut characters for a command.	< radio channel > can also be typed as <ra ch>
[]	Indicates optional items. Do not type the brackets as part of the command.	ip address [ethernet radio]
	Separates two mutually exclusive choices in a command. Type one choice and do not type the vertical bar.	interface if
()	Encloses a range of values from which you can choose a value.	radio channel (1-15)

Table 25 Command-Line Shortcuts and Getting Help

Type	To do this...
<code>?</code>	To display the names of the root commands.
<code>[command_name] ?</code>	To display the syntax for a command.
<code>help</code>	To display all the commands, their subcommands and the parameters and options for each command.
<code>help [command_name]</code>	To display the parameters and options for the command.
<code>!</code>	To repeat the last command that was executed.
<code>ESC</code>	To cancel the command you are typing.

Entering a Netmask

Where a command requires you to enter a netmask, you can do one of the following:

- Enter it as the number of bits (0-32 are valid) in the netmask.
- Do not enter it, and let the CCU or EUM decide what value to use. Note that the CCU or EUM does not necessarily pick the correct netmask.

Table 26 EUM Command-Line Syntax

Command Syntax	Description
<code>arp</code>	Displays the Address Resolution Protocol (ARP) configuration information.
<code>arp add aaa.bbb.ccc.ddd aa:bb:cc:dd:ee:ff</code>	Adds an entry to the ARP table. <i>aaa.bbb.ccc.ddd</i> is the IP address of the entry that you want to add. <i>aa:bb:cc:dd:ee:ff</i> is the MAC address associated with the IP address.
<code>arp del aaa.bbb.ccc.ddd</code>	Deletes a specified entry from the ARP table. <i>aaa.bbb.ccc.ddd</i> is the IP address of the entry that you want to delete.
<code>arp flush</code>	Removes the temporary ARP table entries from the ARP table.
<code>dhcp mode [none relay]</code>	Sets the EUM to use Dynamic Host Configuration Protocol (DHCP). <ul style="list-style-type: none"> • none—disables DHCP Relay. • relay—enables DHCP Relay.
<code>dhcp relay [add delete ip_address]</code>	Adds or removes the IP address of a Dynamic Host Configuration Protocol (DHCP) server. Available only if DHCP mode is set to Relay.
<code>exit quit bye</code>	Closes the console session.

Command Syntax	Description
help [<i>command</i>]	Displays a list of all commands. If you type a command name after help, the syntax for that command is displayed. For example, type help ip to display all IP commands and the syntax for each.
interface if reset	Resets the statistics for all interfaces.
interface if reset ethernet radio loopback	Resets the statistics for the specified interface.
interface if statistics	Displays configuration information and statistics for all interfaces.
interface if statistics ethernet radio loopback	Displays configuration information and statistics for each interface: Ethernet, radio, or loopback.
ip	Displays the IP configuration information.
ip address	Displays the IP addresses for the Ethernet and radio interface.
ip address ethernet <i>aaa.bbb.ccc.ddd [subnet mask]</i>	Changes the IP address for the Ethernet interface. <i>aaa.bbb.ccc.ddd</i> is the IP address for the Ethernet interface and <i>[subnet mask]</i> is specified in either dotted decimal format or number of bits.
ip address radio ccu_id <i>aaa.bbb.ccc.ddd eee.fff.ggg.hhh</i>	Changes the radio interface IP route, and binds the radio channel between the CCU and the EUM using the IP addresses. <i>ccu_id</i> is the CCU ID; <i>aaa.bbb.ccc.ddd</i> is the radio IP address for the EUM; and <i>eee.fff.ggg.hhh</i> is the radio IP address for the CCU.
ip dns	Displays the DNS configuration information.
ip dns domain	Displays the DNS domain name.
ip dns domain <i>DNS_domain_name</i>	Changes the DNS domain name. <i>DNS_domain_name</i> can be a maximum of 256 ASCII characters.
ip dns server	Displays the list of domain name servers.
ip dns server add del <i>aaa.bbb.ccc.ddd</i>	Adds a server to or deletes a server from the DNS table. <i>aaa.bbb.ccc.ddd</i> is the IP address for the DNS server that you want to add or delete.
ip ping destination	Sends ICMP echo requests to a remote host that is used to see if you can reach a remote IP address or for network debugging. <i>destination</i> is the radio IP address for the remote host that you want to reach.
ip rip	Displays the RIP configuration information. Available only if routing mode is set to RIP.

Command Syntax	Description
ip rip broadcast compatible multicast	<p>When RIP is set to version 2, specifies how RIP handles packets. Available only if routing mode is set to RIP and the RIP version is set to 2.</p> <ul style="list-style-type: none"> • broadcast—sends RIP version 2 advertisements as broadcast. • compatible—sends more compatible version 2 broadcasts to version 1 routers. • multicast—sends version 2 advertisements to RIP version 2 multicast addresses. Multicast is generally more efficient than broadcast.
ip rip nodefault default	<p>Disables or enables RIP to advertise the default route. Available only if routing mode is set to RIP.</p> <ul style="list-style-type: none"> • default—if a default route exists, it is sent in the advertisement. • nodefault—the default route is not sent, whether or not it exists.
ip rip noupdate update	<p>Disables or enables RIP to advertise static routes. Available only if routing mode is set to RIP.</p> <ul style="list-style-type: none"> • update—sends static route information in a RIP advertisement, as well as all other RIP information. • noupdate—sends everything except the static route information.
ip rip quiet active	<p>Disables or enables RIP to advertise routes.</p> <p>active - transmits route information, in packets, to the interfaces.</p> <ul style="list-style-type: none"> • quiet - disables RIP packets from being sent.
ip rip version	<p>Displays the RIP version. Available only if routing mode is set to RIP.</p> <ul style="list-style-type: none"> • ip rip version—displays the current version. <p>Note that only RIP version 2 is supported. It supports multicast, broadcast, or compatible (both).</p>
ip route	<p>Displays the routing table information. Local interface routes are always present as long as an address for the interface exists.</p>
ip route add del <i>Network</i> (<i>aaa.bbb.ccc.ddd</i>) <i>Gateway</i> (<i>eee.fff.ggg.hhh</i>) <i>Netmask</i> (<i>0-32</i>)	<ul style="list-style-type: none"> • Adds or deletes a static route. <i>Network</i> (<i>aaa.bbb.ccc.ddd</i>) is the IP address of the destination network • <i>Gateway</i> (<i>eee.fff.ggg.hhh</i>) is the IP address for the gateway; and <i>Mask</i> (<i>0-32</i>) is specified in either dotted decimal format or number of bits.

Command Syntax	Description
ip route erase	Removes all static and dynamic entries, except interface routes, from the routing table.
ip route flush	Removes all dynamic entries from the routing table. Dynamic entries are those routes that the system has learned.
ip routing	Displays the IP routing protocol.
ip routing static rip	Changes the IP routing protocol to either Static or RIP.
ip statistics	Displays the IP statistics information.
ip telnet host(aaa.bbb.ccc.ddd)	Establishes a Telnet session with a remote host to access and control a remote computer. <ul style="list-style-type: none"> • <i>host(aaa.bbb.ccc.ddd)</i> is the IP address of the remote host.
ip traceroute destination(aaa.bbb.ccc.ddd)	Displays the route that the packets take to a remote destination. <ul style="list-style-type: none"> • <i>destination(aaa.bbb.ccc.ddd)</i> is the IP address of the remote destination. The maximum is 30 hops. An asterisk (*) represents each unsuccessful try. For example, 1 * * *. Press any key to stop the <code>ip traceroute</code> output.
radio	Displays the radio configuration information.
radio ccuid	Displays the CCU ID to which the EUM belongs.
radio ccuid (1-16383)	Changes the CCU ID to which the EUM belongs.
radio channel	Displays the radio channel.
radio channel (1-14)	Changes the radio channel.
radio disable enable	Disables or enables the EUM radio transmission capabilities. The EUM is factory configured as disabled to prevent accidental damage should it be powered up without an antenna or load connected.
radio eumid	Displays the CCU IDEUM ID.
radio eumid(1-16383)	Changes the EUM ID. An EUM ID is a unique number between 1 and 16383.
radio per [single continuous reset]	Displays or resets the cumulative radio packet error rate statistics to the screen. This command is available during tests and normal operation. <ul style="list-style-type: none"> • single—displays the current statistics. • continuous—displays the statistics every one second. • reset—resets the calculations.
radio reset	Forces the CCU or EUM to reset. If you reset the CCU or EUM radio instead of shutting down, the statistics are not lost. If you use this command, the link service is disrupted for the duration of the test.

Command Syntax	Description
<code>radio rssi</code>	Displays the current RSSI in real time.
<code>radio rssi threshold</code>	Displays or changes the radio energy floor level, used to calculate the RSSI.
<code>radio rxtest start stop</code>	Starts and stops the Radio Continuous Receive Test. When you start this test, the Radio PER display is also automatically started. The test is available only at the EUM Use this test to deploy a new EUM in an existing network.
<code>radio setting</code>	Displays the IFS, slot time, backoff range, and backoff mode.
<code>radio statistics stats</code>	Displays the current radio statistics.
<code>radio stats reset</code>	Resets all radio stat counters to zero.
<code>radio txrx start stop</code>	Starts and stops the Radio Transmit/Receive Loopback Test. When you start this test, the Radio PER display is also automatically started. The test is available only at the CCU. Use this test for a new installation only.
<code>radio txtest start stop</code>	Starts and stops the Radio Continuous Transmit Test. The test is available only at the CCU. Use this test to set up a CCU and EUM for a new network.
<code>reboot restart reload reset</code>	Resets the EUM.
<code>snmp</code>	Displays the SNMP configuration information. SNMP is useful for monitoring network performance and debugging.
<code>snmp community</code>	Displays the SNMP community table. The default SNMP communities are: public read and private write.
<code>snmp community add del community read write</code>	<p>Adds a community name to, or deletes one from, the SNMP community table. A community name can be a maximum of 32 ASCII characters.</p> <ul style="list-style-type: none"> • read—enables the community to view the variables in SNMP. • write—enables the community to change and view the variables. <p>To change SNMP variables, you must have a write community. To view SNMP variables, you must have a write or read community.</p>
<code>snmp contact</code>	Displays the SNMP system contact (that is, the person or company).
<code>snmp contact contact</code>	Changes the SNMP system contact and telephone number. <i>contact</i> can be a maximum of 256 ASCII characters that you can use to define the contact person or address for the EUM.
<code>snmp location</code>	Displays the SNMP geographical location of the system.

Command Syntax	Description
snmp location <i>location</i>	Changes the SNMP geographical location of the system. <i>location</i> can be a maximum of 256 ASCII characters that you can use to define the physical location of the EUM.
snmp trap	Displays the list of SNMP trap servers defined for the EUM.
snmp trap add del <i>server(aaa.bbb.ccc.ddd)</i> <i>community</i>	Adds a trap to or deletes one from the SNMP trap server table. <i>server(aaa.bbb.ccc.ddd)</i> is the IP address for the trap server. <i>community</i> is the name of the community on the trap server and can be a maximum of 16 ASCII characters.
system	Displays the system configuration information.
system memory	Displays the memory statistics, such as memory allocation information.
system name	Displays the system name.
system name <i>name</i>	Changes the system name. <i>name</i> can be a maximum of 64 ASCII characters that you can use to name the EUM in your system. The system name is used for the command-line prompt for the EUM.
system network	Displays the network system statistics from the network buffer memory pools.
system network ethernet radio data system	Displays network buffer pool-allocation information for each parameter.
system password	Changes the password for the EUM.
system protocol	Displays information about the configuration of protocols bound to the interface.
system protocol <i>interface</i>	Displays the protocol configuration for the specific interface that you name. <i>interface</i> is either Ethernet or Radio.
system uptime	Displays how long the system has been running. If the uptime is more than 24 hours, the time appears as <i>n</i> days, <i>hh:mm:ss</i> where <i>n</i> is the number of days and <i>hh:mm:ss</i> is the hours:minutes:seconds.
system version	Displays the build date and time, and lists all software libraries and their version numbers.
test radio	Performs self tests and displays the results for the radio. If you use this command, the link service is disrupted for the duration of the test.
write default erase	Removes all configuration changes, even if you saved them, and resets the EUM to the factory default configuration.

Command Syntax	Description
<code>write save</code>	Saves the current configuration. If you want to save the new configuration, you must write (save) any configuration changes before you reboot the EUM; otherwise, the EUM reverts to the previously saved configuration.

Table 27 CCU Command-Line Syntax

Command Syntax	Description
<code>arp</code>	Displays the Address Resolution Protocol (ARP) configuration information.
<code>arp add <i>aaa.bbb.ccc.ddd</i> <i>aa:bb:cc:dd:ee:ff</i></code>	Adds an entry to the ARP table. <i>aaa.bbb.ccc.ddd</i> is the IP address of the entry that you want to add. <i>aa:bb:cc:dd:ee:ff</i> is the MAC address associated with the IP address.
<code>arp del <i>aaa.bbb.ccc.ddd</i></code>	Deletes a specified entry from the ARP table. <i>aaa.bbb.ccc.ddd</i> is the IP address of the entry that you want to delete.
<code>arp flush</code>	Removes the temporary ARP table entries from the ARP table.
<code>dhcp mode [none relay]</code>	Sets the CCU to use Dynamic Host Configuration Protocol (DHCP). <ul style="list-style-type: none"> none—disables DHCP Relay. relay—enables DHCP Relay.
<code>dhcp relay [add delete <i>ip_address</i>]</code>	Adds or removes the IP address of a Dynamic Host Configuration Protocol (DHCP) server. Available only if DHCP mode is set to Relay.
<code>exit quit bye</code>	Closes the console session.
<code>help [<i>command</i>]</code>	Displays a list of all commands. If you type a command name after help, the syntax for that command is displayed. For example, type <code>help ip</code> to display all IP commands and the syntax for each.
<code>interface if reset</code>	Resets the statistics for all interfaces.
<code>interface if reset ethernet radio loopback</code>	Resets the statistics for the specified interface.
<code>interface if statistics</code>	Displays configuration information and statistics for all interfaces.
<code>interface if statistics ethernet radio loopback</code>	Displays configuration information and statistics for each interface: Ethernet, radio, or loopback.
<code>ip</code>	Displays the IP configuration information.
<code>ip address</code>	Displays the IP addresses for the Ethernet and radio interface.

Command Syntax	Description
ip address ethernet <i>aaa.bbb.ccc.ddd [subnet mask]</i>	Changes the IP address for the Ethernet interface. <i>aaa.bbb.ccc.ddd</i> is the IP address for the Ethernet interface and <i>[subnet mask]</i> is specified in either dotted decimal format or number of bits.
ip address nap <i>aaa.bbb.ccc.ddd [netmask]</i>	Changes the IP address for the NAP Router. <i>aaa.bbb.ccc.ddd</i> is the IP address for the NAP Router and <i>[netmask]</i> is specified in either dotted decimal format or number of bits.
ip address radio <i>eum_id</i> <i>aaa.bbb.ccc.ddd eee.fff.ggg.hhh</i>	Changes the radio interface IP route and binds the radio channel between the CCU and the EUM using the IP addresses. <i>eum_id</i> is the EUM ID; <i>aaa.bbb.ccc.ddd</i> is the radio IP address for the CCU; and <i>eee.fff.ggg.hhh</i> is the radio IP address for the EUM. Repeat this command for each EUM that you have in the EUM List.
ip address radius <i>aaa.bbb.ccc.ddd [netmask]</i>	Changes the IP address for the RADIUS server controlling this CCU. <i>aaa.bbb.ccc.ddd</i> is the IP address for the RADIUS server and <i>[netmask]</i> is specified in either dotted decimal format or number of bits.
ip dns	Displays the DNS configuration information.
ip dns domain	Displays the DNS domain name.
ip dns domain <i>DNS_domain_name</i>	Changes the DNS domain name. <i>DNS_domain_name</i> can be a maximum of 256 ASCII characters.
ip dns server	Displays the list of domain name servers.
ip dns server add del <i>aaa.bbb.ccc.ddd</i>	Adds a server to or deletes a server from the DNS table. <i>aaa.bbb.ccc.ddd</i> is the IP address for the DNS server that you want to add or delete.
ip ping <i>destination</i>	Sends ICMP echo requests to a remote host that is used to see if you can reach a remote IP address or for network debugging. <i>destination</i> is the radio IP address for the remote host that you want to reach.
ip rip	Displays the RIP configuration information. Available only if routing mode is set to RIP.
ip rip broadcast compatible multicast	When RIP is set to version 2, specifies how RIP handles packets. Available only if routing mode is set to RIP and the RIP version is set to 2. <ul style="list-style-type: none"> • broadcast—sends RIP version 2 advertisements as broadcast. • compatible—sends more compatible version 2 broadcasts to version 1 routers. • multicast—sends version 2 advertisements to RIP version 2 multicast addresses. Multicast is generally more efficient than broadcast.

Command Syntax	Description
<code>ip rip nodefualt default</code>	<p>Disables or enables RIP to advertise the default route. Available only if routing mode is set to RIP.</p> <ul style="list-style-type: none"> • default—if a default route exists, it is sent in the advertisement. • nodefualt—the default route is not sent, whether or not it exists.
<code>ip rip nouupdate update</code>	<p>Disables or enables RIP to advertise static routes. Available only if routing mode is set to RIP.</p> <ul style="list-style-type: none"> • update—sends static route information in a RIP advertisement, as well as all other RIP information. • nouupdate—sends everything except the static route information.
<code>ip rip quiet active</code>	<p>Disables or enables RIP to advertise routes. active - transmits route information, in packets, to the interfaces.</p> <ul style="list-style-type: none"> • quiet - disables RIP packets from being sent.
<code>ip rip version</code>	<p>Displays the RIP version. Available only if routing mode is set to RIP.</p> <ul style="list-style-type: none"> • ip rip version—displays the current version. <p>Note that only RIP version 2 is supported. It supports multicast, broadcast, or compatible (both).</p>
<code>ip route</code>	<p>Displays the routing table information. Local interface routes are always present as long as an address for the interface exists.</p>
<code>ip route add del</code> <i>Network(aaa.bbb.ccc.ddd)</i> <i>Gateway(eee.fff.ggg.hhh)</i> <i>Netmask(0-32)</i>	<ul style="list-style-type: none"> • Adds or deletes a static route. <i>Network(aaa.bbb.ccc.ddd)</i> is the IP address of the destination network • <i>Gateway(eee.fff.ggg.hhh)</i> is the IP address for the gateway; and <i>Mask(0-32)</i> is specified in either dotted decimal format or number of bits.
<code>ip route erase</code>	<p>Removes all static and dynamic entries, except interface routes, from the routing table.</p>
<code>ip route flush</code>	<p>Removes all dynamic entries from the routing table. Dynamic entries are those routes that the system has learned.</p>
<code>ip routing</code>	<p>Displays the IP routing protocol.</p>
<code>ip routing static rip</code>	<p>Changes the IP routing protocol to either Static or RIP.</p>
<code>ip statistics</code>	<p>Displays the IP statistics information.</p>

Command Syntax	Description
ip telnet <i>host(aaa.bbb.ccc.ddd)</i>	Establishes a Telnet session with a remote host to access and control a remote computer. <ul style="list-style-type: none"> <i>host(aaa.bbb.ccc.ddd)</i> is the IP address of the remote host.
ip traceroute <i>destination(aaa.bbb.ccc.ddd)</i>	Displays the route that the packets take to a remote destination. <ul style="list-style-type: none"> <i>destination(aaa.bbb.ccc.ddd)</i> is the IP address of the remote destination. The maximum is 30 hops. An asterisk (*) represents each unsuccessful try. For example, 1 * *. Press any key to stop the ip traceroute output.
radio	Displays the radio configuration information.
radio ccuid	Displays the CCU ID.
radio ccuid (1-16383)	Changes the CCU ID. CCU ID is a unique number between 1 and 16383.
radio channel	Displays the radio channel.
radio channel (1-14)	Changes the radio channel.
radio disable enable	Disables or enables the CCU radio transmission capabilities. The CCU is factory configured as disabled to prevent accidental damage should it be powered up without an antenna or load connected.
radio eum	Displays the list of EUMs to which the CCU can talk.
radio eum add (1-16383)	Adds an EUM to the EUM List.
radio eum del (1-16383)	Removes an EUM from the EUM List.
radio eum disable enable <i>eumID</i>	Disables or enables the transmission capabilities of the EUM. <i>eumID</i> is the EUM ID for the unit that you want to enable or disable.
radio per [single continuous reset]	Displays or resets the cumulative radio packet error rate statistics to the screen. This command is available during tests and normal operation. <ul style="list-style-type: none"> single—displays the current statistics. continuous—displays the statistics every one second. reset—resets the calculations.
radio reset	Forces the CCU to reset. If you reset the CCU radio instead of shutting down, the statistics are not lost. If you use this command, the link service is disrupted for the duration of the test.
radio rssi	Displays the current RSSI in real time.
radio rssi threshold	Displays or changes the radio energy floor level, used to calculate the RSSI.

Command Syntax	Description
radio rxtest start stop	Starts and stops the Radio Continuous Receive Test. When you start this test, the Radio PER display is also automatically started. The test is available only at the EUM. Use this test to deploy a new EUM in an existing network.
radio setting	Displays the IFS, slot time, backoff range, and backoff mode.
radio statistics stats	Displays the current radio statistics.
radio stats reset	Resets all radio stat counters to zero.
radio txrx start stop	Starts and stops the Radio Transmit/Receive Loopback Test. When you start this test, the Radio PER display is also automatically started. The test is available only at the CCU. Use this test for a new installation only.
radio txtest start stop	Starts and stops the Radio Continuous Transmit Test. The test is available only at the CCU. Use this test to set up a CCU for a new network.
reboot restart reload reset	Resets the CCU.
snmp	Displays the SNMP configuration information. SNMP is useful for monitoring network performance and debugging.
snmp community	Displays the SNMP community table. The default SNMP communities are: public read and private write.
snmp community add del <i>community read write</i>	<p>Adds a community name to, or deletes one from, the SNMP community table. A community name can be a maximum of 32 ASCII characters.</p> <ul style="list-style-type: none"> • read—enables the community to view the variables in SNMP. • write—enables the community to change and view the variables. <p>To change SNMP variables, you must have a write community. To view SNMP variables, you must have a write or read community.</p>
snmp contact	Displays the SNMP system contact (that is, the person or company).
snmp contact contact	Changes the SNMP system contact and telephone number. <i>contact</i> can be a maximum of 256 ASCII characters that you can use to define the contact person or address for the CCU.
snmp location	Displays the SNMP geographical location of the system.
snmp location location	Changes the SNMP geographical location of the system. <i>location</i> can be a maximum of 256 ASCII characters that you can use to define the physical location of the CCU.
snmp trap	Displays the list of SNMP trap servers defined for the CCU.

Command Syntax	Description
snmp trap add del <i>server(aaa.bbb.ccc.ddd)</i> <i>community</i>	Adds a trap to or deletes one from the SNMP trap server table. <i>server(aaa.bbb.ccc.ddd)</i> is the IP address for the trap server. <i>community</i> is the name of the community on the trap server and can be a maximum of 16 ASCII characters.
system	Displays the system configuration information.
system memory	Displays the memory statistics, such as memory allocation information.
system name	Displays the system name.
system name <i>name</i>	Changes the system name. <i>name</i> can be a maximum of 64 ASCII characters that you can use to name the CCU in your system. The system name is used for the command-line prompt for the CCU.
system network	Displays the network system statistics from the network buffer memory pools.
system network ethernet radio data system	Displays network buffer pool-allocation information for each parameter.
system password	Changes the password for the CCU.
system protocol	Displays information about the configuration of protocols bound to the interface.
system protocol <i>interface</i>	Displays the protocol configuration for the specific interface that you name. <i>interface</i> is either Ethernet or Radio.
system uptime	Displays how long the system has been running. If the uptime is more than 24 hours, the time appears as <i>n</i> days, <i>hh:mm:ss</i> where <i>n</i> is the number of days and <i>hh:mm:ss</i> is the hours:minutes:seconds.
system version	Displays the build date and time, and lists all software libraries and their version numbers.
test radio	Performs self tests and displays the results for the radio. If you use this command, the link service is disrupted for the duration of the test.
write default erase	Removes all configuration changes, even if you saved them, and resets the CCU to the factory default configuration.
write save	Saves the current configuration. If you want to save the new configuration, you must write (save) any configuration changes before you reboot the CCU; otherwise, the CCU reverts to the previously saved configuration.

Entering RFSM Commands

The RFSM commands must be typed in uppercase. Press **Enter** after typing each command. The RFSM uses three different prompts, as described below:

- The logon prompt is a colon ":". Type the password for the RFSM at this prompt.
- The command prompt is a question mark "?".
- The error prompt is an exclamation mark "!". You will see this prompt when the previously entered command resulted in an error. To clear the error prompt, type **C** and **Enter**.

Table 28 RFSM Command Line Syntax

Command	Description
LOG OUT	Logs the user off the RFSM.
SET01= <i>hostname</i>	Saves the host name of the RFSM, which must be no more than 255 characters long and be alphanumeric.
SET02= <i>password;password</i>	Saves the system password. This must be eight characters long and alphanumeric.
SET10= <i>aaa.bbb.ccc.ddd</i>	Saves the network IP address.
SET11= <i>aaa.bbb.ccc.ddd</i>	Saves the netmask.
SET12= <i>aaa.bbb.ccc.ddd</i>	Saves the default gateway address.
SET41= <i>abababab</i>	Saves the enabled state of the eight system outputs. <ul style="list-style-type: none">• 0 = inactive• 1 = active
SET42= <i>abab</i>	Saves the state of the system's four RF relays. <ul style="list-style-type: none">• 0 = open• 1 = closed
GET01	Returns the host name of the RFSM, which must be no more than 255 characters long and be alphanumeric.
GET02	Returns the system password. This must be eight characters long and alphanumeric.
GET10	Returns the network IP address.
GET11	Returns the netmask.
GET12	Returns the default gateway address.
GET41	Returns the enabled state of the eight system outputs. <ul style="list-style-type: none">• 0 = inactive• 1 = active
GET42	Returns the state of the system's four RF relays. <ul style="list-style-type: none">• 0 = open• 1 = closed

Command	Description
WRITE FLASH	Writes data buffer to flash. Returns “success” on completion. Errors result in an error state.
VERIFY FIRMWARE	Verifies a file in the data buffer against the flash image. If a file had not been successfully verified, the error prompt displays.
UPLOAD FIRMWARE	Begins an X modem-based file transfer through the debug port. The file writes to the data buffer. If the file is not successfully transferred, the error prompt “!” displays.
QUERY	Queries the system. The system responds with a copyright notice and the firmware date and version.
CLEAR ERROR	Clears an error indication, returning the prompt to its normal state.
LAMP TEST	<p>Tests all LEDs by turning each one on red for 1/2 second and then green for 1/2 second. Starts with Input 1 and flows sequentially through each of the following LEDs:</p> <ul style="list-style-type: none"> • Input LED • Output LED • CPU LED • RF Switch LED

— This page is intentionally left blank —

Appendix D SNMP MIB Definitions

This appendix identifies the full WaveRider Enterprise MIB Definitions in an easy to use, tabulated format. It includes the WaveRider Enterprise MIBs and RFC MIB-II Traps for both the CCU and EUM.

CCU2000 MIB Definitions

Table 29 CCU2000 WaveRider Enterprise MIBs

MIB Name	OID	Access	Value Type	Accepted Values	Description
serialNumber	1.3.6.1.4.1.2979.4.1.1	read-only	String		Hardware serial number
softwareVersion	1.3.6.1.4.1.2979.4.1.2	read-only	String		WaveRider firmware version of device
radioConfigVersion	1.3.6.1.4.1.2979.4.2.1	read-only	String		Radio firmware
radioConfigChannel	1.3.6.1.4.1.2979.4.2.2	read-write	Integer	1 to 14	Radio channel in use
radioConfigSpeed	1.3.6.1.4.1.2979.4.2.3	read-write	Integer	1-one 2 -two 3-five 4-eleven	Radio speed being used in MBps
radioConfigDomain	1.3.6.1.4.1.2979.4.2.4	read-only	Integer	0 - IEEE 1 - FCC	Current regulatory domain of radio

MIB Name	OID	Access	Value Type	Accepted Values	Description
radioConfigIFS	1.3.6.1.4.1.2979.4.2.6	read-only	Integer	2,4,8,16,32,64,128	Interframe spacing of radio
radioCCUID	1.3.6.1.4.1.2979.4.2.7	read-write	Integer	1-16383	Unit ID of this CCU
reEums	1.3.6.1.4.1.2979.4.3.1	read-only	Integer		Number of EUMs with which this CCU is communicating
reTable	1.3.6.1.4.1.2979.4.3.2	not-accessible			List of EUMs to which the CCU is talking
reEntry	1.3.6.1.4.1.2979.4.3.2.1	not-accessible			Objects concerning communications with another EUM
reIndex	1.3.6.1.4.1.2979.4.3.2.1.1	read-only	Integer		Unique value for each EUM in communication
reEumID	1.3.6.1.4.1.2979.4.3.2.1.2	read-write	Integer	1-16383	EUM ID referred to by this entry
reState	1.3.6.1.4.1.2979.4.3.2.1.3	read-write	Integer	0-down 1-up	Indicates the current state of the radio interface 0-down 1-up
radioStatsTransmitted	1.3.6.1.4.1.2979.4.4.1	read-only	Counter		Number of transmitted frames
radioStatsTxDelayed	1.3.6.1.4.1.2979.4.4.2	read-only	Counter		Number transmitted blocks that have been delayed
radioStatsRxPackets	1.3.6.1.4.1.2979.4.4.3	read-only	Counter		Number of received packets
radioStatsRxDataCRC Error	1.3.6.1.4.1.2979.4.4.4	read-only	Counter		Number of received data CRC errors
radioStatsRxHeaderCRC Error	1.3.6.1.4.1.2979.4.4.5	read-only	Counter		Number received MAC header CRC errors

MIB Name	OID	Access	Value Type	Accepted Values	Description
radioStatsRxHeaderCRCFixed	1.3.6.1.4.1.2979.4.4.6	read-only	Counter		Number received MAC header CRC errors that have been fixed
radioStatsRxInvalidLen	1.3.6.1.4.1.2979.4.4.7	read-only	Counter		Number of invalid data lengths that have been received
radioStatsNICFailure	1.3.6.1.4.1.2979.4.4.8	read-only	Counter		Number of times the MAC has needed to be reloaded
radioStatsBroadCastDiscards	1.3.6.1.4.1.2979.4.4.9	read-only	Counter		Number of times a broadcast packet has been discarded

Table 30 CCU2000 RFC MIB-II Traps

MIB Name	OID	Access	Value Type	Accepted Values	Description
coldStart	1.3.6.1.2.1.11.0	read-only			Power cycle or power on
warmStart	1.3.6.1.2.1.11.1	read-only			System reload has been initialized without a power cycle
linkDown	1.3.6.1.2.1.11.2	read-only			Communication port link is down or went offline
linkUp	1.3.6.1.2.1.11.3	read-only			Communication port link is up or went online
authenticationFailure	1.3.6.1.2.1.11.4	read-only			SNMP request has failed due to improper authentication
egpNeighborLoss	1.3.6.1.2.1.11.5	read-only			Loss of peer relationship between sending neighbor

EUM2000 MIB Definitions

Table 31 EUM2000 WaveRider Enterprise MIBs

MIB Name	OID	Access	Value Type	Accepted Values	Description
serialNumber	1.3.6.1.4.1.2979.5.1.1	read-only	String		Hardware serial number
softwareVersion	1.3.6.1.4.1.2979.5.1.2	read-only	String		WaveRider firmware version of device
radioConfigVersion	1.3.6.1.4.1.2979.5.2.1	read-only	String		Radio firmware
radioConfigChannel	1.3.6.1.4.1.2979.5.2.2	read-write	Integer	1 to 14	Radio channel in use
radioConfigSpeed	1.3.6.1.4.1.2979.5.2.3	read-write	Integer	1-one 2 -two 3-five 4-eleven	Radio speed being used in MBps
radioConfigDomain	1.3.6.1.4.1.2979.5.2.4	read-only	Integer	0 - IEEE 1 - FCC	Current regulatory domain of radio
radioConfigIFS	1.3.6.1.4.1.2979.5.2.6	read-only	Integer	2,4,8,16,32,64,128	Interframe spacing of radio
radioEUMID	1.3.6.1.4.1.2979.5.2.7	read-write	Integer	1-16383	Unit ID of this EUM
radioCCUID	1.3.6.1.4.1.2979.5.2.8	read-write	Integer	1-16383	Unit ID of the CCU through which the EUM is communicating
radioStatsTransmitted	1.3.6.1.4.1.2979.5.4.1	read-only	Counter		Number of transmitted frames
radioStatsTxDelayed	1.3.6.1.4.1.2979.5.4.2	read-only	Counter		Number transmitted blocks that have been delayed
radioStatsRxPackets	1.3.6.1.4.1.2979.5.4.3	read-only	Counter		Number of received packets
radioStatsRxDataCRC Error	1.3.6.1.4.1.2979.5.4.4	read-only	Counter		Number of received data CRC errors

MIB Name	OID	Access	Value Type	Accepted Values	Description
radioStatsRxHeaderCRCError	1.3.6.1.4.1.2979.5.4.5	read-only	Counter		Number received MAC header CRC errors
radioStatsRxHeaderCRCFixed	1.3.6.1.4.1.2979.5.4.6	read-only	Counter		Number received MAC header CRC errors that have been fixed
radioStatsRxInvalidLen	1.3.6.1.4.1.2979.5.4.7	read-only	Counter		Number of invalid data lengths that have been received
radioStatsNICFailure	1.3.6.1.4.1.2979.5.4.8	read-only	Counter		Number of times the MAC has needed to be reloaded
radioStatsBroadCastDiscards	1.3.6.1.4.1.2979.5.4.9	read-only	Counter		Number of times a broadcast packet has been discarded

Table 32 EUM2000 RFC MIB-II Traps

MIB Name	OID	Access	Value Type	Accepted Values	Description
coldStart	1.3.6.1.2.1.11.0	read-only			Power cycle or power on
warmStart	1.3.6.1.2.1.11.1	read-only			System reload has been initialized without a power cycle
linkDown	1.3.6.1.2.1.11.2	read-only			Communication port link is down or went offline
linkUp	1.3.6.1.2.1.11.3	read-only			Communication port link is up or went online
authenticationFailure	1.3.6.1.2.1.11.4	read-only			SNMP request has failed due to improper authentication

MIB Name	OID	Access	Value Type	Accepted Values	Description
egpNeighborLoss	1.3.6.1.2.1.11.5	read-only			Loss of peer relationship between sending neighbor

Appendix E LMS2000 Specifications

NAP Specifications

The following tables list the technical specifications for the LMS2000 NAP (including the NMS Workstation).

Table 33 CAP-NAP Back Haul Interface Specifications

Maximum Number of CAP-NAP Links	15
Physical Interface	10/100BaseTx auto-sense Ethernet
Maximum Unidirectional Data Rate per Link	20 Mbps

Table 34 NAP-Internet Interface Specifications

Maximum Number of NAP-Internet Links	1
Physical Interface	10/100BaseTx auto-sense Ethernet, full or half-duplex
Maximum Aggregate Data Rate per Link	50 Mbps

Table 35 Power Supply Specifications

AC Input	110/230 \pm 15% VAC auto-sense, single phase
AC Input Frequency	50/60 \pm 3 Hz auto-sense
Maximum Input Power	1000 VA
Maximum UPS Operating Time at Full Load	10 minutes

Table 36 Environmental Specifications

Operating Temperature	+10° to +40° C indoor environment, 5% to 95% RH non-condensing
Storage Temperature	-20° to +70° C

Table 37 NAP Physical Specifications

NAP Height	42 in. (106.68 cm)
NAP Width	23 in. (58.42 cm)
NAP Depth	31.5 in. (80 cm)
NAP Weight	approximately 155 lb. (70 kg)

ABWM Specifications

The following table lists the specifications for the Advanced Bandwidth Manager (ABWM).

Table 38 iSurfRanger Environmental Specifications

Operating/Storage Temperature	0°C to +40°C ambient
Operating Humidity	0% to 85% non-condensing
Altitude	10,000 feet maximum operating
Power	100-240 volts AC, 50-60 Hz, 2 Amps

Table 39 iSurfRanger Physical Specifications

Controller Dimensions	3.5" x 19" x 17"
Module Dimensions	3" x 7.75" x 15"
Controller Weight	12 lbs (5.5 kg)
Module Weight	12 lbs (5.5 kg)

Table 40 Other iSurfRanger Specifications

Port Characteristics	<ul style="list-style-type: none"> • Two 802.3U, 10BaseT/100BaseTx, RJ-45 Ethernet ports, input and output • Two RS-232, RJ-11 console ports • Full duplex Fast Ethernet with wire speed throughput
Management	<ul style="list-style-type: none"> • Interface to HP OpenView • SNMP MIBs I and II • Enterprise MIB
Industry Standards Complied With	<ul style="list-style-type: none"> • FCC Part 15 Class A • CSA Approved • TUV GS Mark, EN 60950 • CE Mark, Ctick, and UL

CAP Specifications

The following tables list the technical specifications for the LMS2000 CAP.

Table 41 CAP Radio Specifications

Maximum Number of Operational CCUs and Orthogonal Channels	3
Maximum Number of Standby CCUs	1

Table 42 Ethernet Back Haul Interface Specifications

Physical Interface	10/100BaseTx auto-sense, full or half-duplex
Maximum Unidirectional Data Rate	20 Mbps

Table 43 Power Supply Specifications

AC Input	110/230 \pm 15% VAC auto-sense, single phase
AC Input Frequency	50/60 \pm 3 Hz auto-sense
Maximum Input Power	1700 VA (without air conditioning unit)
Maximum UPS Operation Time at Full Load	10 minutes

Table 44 Environmental Specifications

Operating Temperature	0° to +40° C with integral fan cooling; 0° to +55° C with optional air conditioning unit, 5% to 95% RH non-condensing
Storage Temperature	-20° to +70° C

Table 45 CAP Physical Specifications

CAP Height	42 in. (106.68 cm)
CAP Width	23 in. (58.42 cm)
CAP Depth	31.5 in. (80 cm)
CAP Weight	approximately 155 lb. (70 kg)

RFSM Specifications

The following table lists the technical specifications for the RFSM.

Table 46 RFSM Radio Specifications

Insertion Loss	< 1.0 dB
Port to Port Isolation	> 80 dB
RF Switching Time	< 50 ms
Return Loss	> 18 dB
Input Port Current Output (Biased)	~ 12 mA
Voltage Range on Unbiased Ports	50 Vdc max
Input Port Sensitivity (Unbiased Ports)	< 2 Vdc disconnect > 4 Vdc connect
Input Port Sensitivity (Biased Ports)	< 100 ohm connect > 5 kohm disconnect
Input Port Transient Response (Unbiased Ports)	5 ms deglitching of input signal
Output Port Range (25 deg C)	max 350 mA at 60 Vdc
Input Power	110/230 \pm 15% VAC single phase 60/50 Hz \pm 3 Hz 200 mA max

RF Connectors	Female SMA
RF Port Impedance	50 ohm
DB9 Debug Port	9600 baud, 8N1, DTE

Table 47 RFSM Ethernet Interface Specifications

Ether Port	10BaseT, RJ-45
------------	----------------

Table 48 RFSM Physical Specifications

Dimensions	19" rack mount 2U (3.5") height 12" depth
------------	---

CCU and EUM Specifications

The following tables list the technical specifications for the EUM and CCU configured for operation in the FCC/IC RF Regulatory Domain.

Table 49 CCU and EUM Radio Specifications

Minimum Channel Center Frequency	2.412 GHz
Maximum Channel Center Frequency	2.462 GHz
Channel Bandwidth	22 MHz
Center Frequency Spacing Increment	5 MHz
Minimum Separation Between Co-located Channels	25 MHz
Maximum Co-located Channels	3
Co-located Channel Set	1, 6, 11
Co-located Channel Set Center Frequencies	2.412 GHz, 2.437 GHz, 2.462 GHz
Modulation Scheme	CCK (Complementary Code Keying) DSSS (Direct Sequence Spread Spectrum)
Receiver Sensitivity for BER < 10 ⁻⁵	-72 dBm (EUM2000 and CCU2000) -82 dBm (EUM2000-A and CCU2000-A)
Maximum Over-the-Air, Raw Data Rate	11 Mbps

Table 50 Ethernet Interface Specifications

Physical Interface	10BaseTx half-duplex
--------------------	----------------------

Table 51 Power Supply Specifications

AC Input	110/230 \pm 15% VAC, single phase
AC Input Frequency	50/60 \pm 3 Hz
Maximum Input Current	1.5 A

Table 52 Environmental Specifications

Operating Temperature	0° to +55° C, indoor environment 5%-95% RH non-condensing
Storage Temperature	-20° to +70° C

Appendix F Acronyms and Glossary

Table 53 Acronyms and Abbreviations

Acronym or Abbreviation	Definition
ABWM	Advanced Bandwidth Manager
AC	Alternating Current
API	Application Programming Interface
ARP	Address Resolution Protocol
ARQ	Automatic Retry Request
ASCII	American Standard Code for Information Interchange
CAP	Communications Access Point
CCU	CAP Channel Unit
CIR	Committed Information Rate
CLI	Command Line Interface
CPU	Central Processing Unit
CSA	Canadian Standards Association
CTS	Clear To Send
dB	decibel
dBi	decibel—with respect to an isotropic radiator
DCE	Data Communication Equipment
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server, Domain Network Server
DPRAM	Dual Port Random-access Memory
DRAM	Dynamic Random-access Memory

Acronym or Abbreviation	Definition
DSR	Data Set Ready
DSSS	Direct-sequence Spread Spectrum
DTE	Data Terminal Equipment
ESN	Electronic Serial Number
ETSI	European Telecommunications Standards for Industry
EUM	End-user Modem
FCC	Federal Communications Commission (U.S.A.)
FRU	Field Replaceable Unit
FTP	File Transfer Protocol
GHz	GigaHertz
GMT	Greenwich Mean Time
IC	Industry Canada
ICMP	Internet Control Message Protocol
ID	Identifier, Identification
IP	Internet Protocol
ISM	Industrial, Scientific, and Medical (Unlicensed Radio Band)
ISP	Internet Service Provider
LAN	Local Area Network
LED	Light-emitting Diode
LMDS	Local Multipoint Distribution System
LMS	Last Mile Solution™
LOS	Line Of Sight
MAC	Media Access Control, Medium Access Controller
Mbps	Megabits per second
MBR	Maximum Burst Rate
MHz	MegaHertz
MIB	Management Information Base
MTU	Maximum Transmission Unit
n/a	not applicable
NAP	Network Access Point
NCL	Network Communication Link
NMS	LMS Network Management System
OAM	Operations, Administration and Maintenance
OID	Object Identifier

Acronym or Abbreviation	Definition
OS	Operating System
PC	Personal Computer
PHY	Physical Layer
RADIUS	Remote Access Dial-in User Service
RF	Radio Frequency
RIP	Routing Information Protocol
RMA	Returned Merchandise Authorization
RFSM	Radio Frequency Switching Matrix
RSSI	Receive Signal Strength Indicator
RTS	Request To Send
Rx	Receive
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SOHO	Small Office/Home Office
SRAM	Static Random Access Memory
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TDD	Time-Division Duplex (Modulation)
TDMA	Time-Division Multiple Access
Tx	Transmit
UL	Underwriters Laboratories
UPS	Uninterruptable Power Supply

Table 54 LMS Network Glossary

Term	Definition
Back Haul	Equipment used to provide the communication link between the NAP and CAP, or between the NAP and Internet/ISP (when direct connection is not possible).
Bandwidth Manager	The entity in the NAP that uses various algorithms to manage end-user access to the network interface bandwidth, based on subscribed level of service.
Broadcast (Message)	A message sent by one network device to all other devices connected to the network.

CAP RF Subsystem	The RF Equipment associated with a CAP, including CCUs, RFSM, antennas, and transmission lines.
Cell Size	The nominal radius of the geographic area served by a single CAP, within which EUMs can reliably receive service.
Channel	Generally, the medium through which information is communicated. In wireless communications, the channel is usually defined by the center frequency, modulation type, and occupied bandwidth.
CLI (Command Line Interface)	In contrast to a graphical user interface, a CLI is a configuration and control interface based on keyboard-entry commands and responses.
Console Port	Typically, the 9-pin RS 232 serial port on an LMS device to which a terminal or laptop computer is connected, for the purpose of configuring or controlling the device.
Configuration Terminal	In contrast to centralized control from the NMS, the configuration terminal is provided for the purpose of configuring or controlling a device directly through its console port.
DNS (Domain Name System)	A database system that translates domain names into IP addresses. For example, waverider.com is converted into 207.23.187.242.
DSSS (Direct-Sequence Spread Spectrum)	A form of spread-spectrum communications that uses a high-speed code sequence, along with the information being sent, to modulate the RF carrier.
Ethernet Switch	In the context of LMS, the devices that provide data link layer Ethernet connection between the router, NMS, UPS, and back-haul equipment at the NAP, and the CCUs, RFSM, back-haul equipment and UPS at the CAP.
Host Name	The common name given to network devices to make them more-easily identifiable by network operators and maintenance personnel.
Gateway	A device connecting two networks that use different communications technologies or protocols; for example, an IP/ Telephony Gateway provides a connection between an IP network and a telephone network.
IP (Internet Protocol)	The network-layer protocol in the TCP/IP stack (defined by RFC 791).
Line of Sight	The radio link between a transmitter and receiver is said to be line of sight if the direct path between the two is relatively free from physical obstruction.
MAC (Medium Access Control)	The mechanism of managing access, by multiple users, to a common transmission medium.
Multicast (Message)	A message sent by a network device to a limited set of network devices.

Orthogonal Channels	Communications channels that can operate over a common transmission medium without significantly interfering with each other. In the context of LMS, radio channels on appropriately spaced frequencies are considered to be orthogonal.
Point-to-Multipoint	A communications architecture in which a central station (CAP, for example) communicates with multiple remote stations (EUMs).
POTS (Plain Old Telephone Service)	The basic telephone service provided by the public switched telephone network (PSTN).
Radio Module	The device in the EUM (or CCU) that provides the wireless interface to the LMS network. The radio module performs signal spreading and modulation, channelization, up-conversion and amplification in the transmit direction, and signal amplification, down-conversion, channel selection, demodulation, de-spreading and data recovery in the receive direction.
Range	The maximum distance that a signal can be reliably transmitted between a CCU and EUM.
RFSM (RF Switch Matrix)	The CAP RFSM provides connectivity between multiple CCU's and antennas, under the control of the NMS, for the purpose of CCU redundancy. If an active CCU fails, the RFSM will switch out the failed CCU and switch in the standby CCU.
RIP (Routing Information Protocol)	A routing protocol in which network routers periodically broadcast their entire current routing database.
Router	A network device that routes IP messages from one physical port to another based on a table of routes that are manually entered by a crafts person (static routes) or generated by the router using a routing protocol such as RIP.
Routing	The process of finding a path to a destination host through an IP network.
Sectorization	An RF engineering technique whereby co-located transceivers are connected to separate antennas with different but geometrically arranged azimuths, for the purpose of optimizing radio channel reuse, extending range, and reducing interference. 120° sectorization is commonly applied in LMS systems.
SNMP (Simple Network Management Protocol)	A protocol used to manage nodes in an IP network.
SNMP Agent	An agent "resides" on an SNMP-managed device, and performs operations when requested to do so by an SNMP manager.

SNMP Community	A grouping of SNMP agents that can be managed by an SNMP manager. An SNMP manager can manage more than one SNMP community. The community name is used to authenticate the SNMP manager before allowing it access to the agent.
SNMP MIB (Management Information Base)	The information that an SNMP manager, such as the NMS, can request from an SNMP agent.
SNMP Trap	A message sent by an SNMP agent to an NMS, console, or terminal to indicate the occurrence of a significant event, such as a specified condition, or a defined threshold that was reached.
SNMP Trap Server	The server to which SNMP trap messages are forwarded.
Spread Spectrum	A communication technology in which the transmitted signal occupies a much greater bandwidth than the information bandwidth. The benefits of spread spectrum are generally lower spectral power density, and immunity to noise, interference and jamming.
Static Route	A route that is manually entered into a routing table by a crafts person or network operator.
Subscriber	In the context of LMS, it is the individual or entity associated with an EUM.
TCP (Transmission Control Protocol)	The connection-oriented transport layer protocol that provides reliable, full-duplex data transmission in TCP/IP networks.
Telnet	A terminal emulation program for TCP/IP networks.
Unicast	A message sent by one network device to another network device.
User Authentication	In LMS, the secure mechanism through which a user identification is verified.
User Authorization	The secure mechanism by which a user is approved to use LMS services. To illustrate, an EUM may be authenticated but denied service because of the delinquent payment of a bill.
VoIP (Voice over IP)	The ability to carry normal telephony-style voice over an IP-based internet, with POTS-like functionality, reliability and voice quality.

Index

A

accounts	
branch	27
deleting	269
disabling	267
report	231
advanced bandwidth manager	4
bandwidth controls	148
bandwidth sets	153
controller	143
iSurfRanger	130
priorities	153
redundancy	143
schedules	160
system security parameters	151
traffic policies	161
antenna subsystem	9

B

back haul	17
backhaul	9
Backup Exec	7
backups	
manual	191
properties	178
schedule	177, 193
SNMPc	184
bandwidth controls	148
bandwidth manager	55
bandwidth sets	153
battery disposal	264
buttons	31

C

CAP	7
configuration defaults	292
configuring	62
default configuration	14, 63
Ethernet switch	8, 67
testing connections	19
UPS	9
Castlerock SNMPc Server	7
CCU	8, 233
adding EUM	105
adding EUMs	73
connection to RFSM	118

enabling radio	75
Ethernet properties	73
ID	73
IP statistics	242
LED color on RFSM	212
monitoring with RFSM	211
network interface statistics	239
network IP address	75
password	72
radio channel	74
radio properties	73
radio transmission	75
replacing	215
routing table	76
SNMP	
communities	80
properties	78
trap servers	81
switching configurations	221
updating firmware	276
uploading configurations	83
cleaning	262
colors	32
command-line syntax	299
communities	39
CCU	80
configuration	
defaults	291
EUM configuration file	100
importing	88
RFSM	115
uploading CCU	83
uploading EUM	101
connection	
Internet	68
testing	19
connections	
CCU and RFSM	118
EUM	86
continuous receive test	170
continuous transmit test	168
controller	143

D

data flow	11
database	
synchronizing	275

default configuration		inventory branch	26
CAP	14, 63	IP address, CCU	75
NAP	18, 46	IP statistics	242
deleting	269	ISP interface	7
device configuration defaults	291	iSurfRanger	130
DHCP	96		
DNS server,EUM	99	L	
E		LMS2000 branch	25
Ethernet IP address,EUM	107	logs	
Ethernet properties		NMS application logs	246
CCU	73	NMS transaction	248
EUM	91	RADIUS logs	250
Ethernet switch	4, 8, 52, 67	RADIUS server error	251
EUM	10	RADIUS server user log	252
adding to CCU	105	SNMPc server event	258
connecting	86		
creating a record	87	M	
deploying	108	maintenance	
DHCP	96	cleaning	262
DNS server	99	humidity	261
Ethernet IP address	107	temperature	261
Ethernet properties	91	menus, shortcut	28
firmware report	233	Microsoft SQL Agent	7
importing configuration	88	Microsoft SQL Server	6
IP statistics	242	Microsoft Windows NT	5
network interface statistics	239		
passwords	89	N	
radio properties	91	NAP	2
removing	268	bandwidth manager	55
routing table	93	configuration defaults	291
saving configuration	100	configuring	45
service level	101	connecting to the Internet	68
SNMP properties	97	default configuration	18, 46
subscriber	101	Ethernet switch	4, 52
updating firmware	276	router	4, 53
upload configuration	101	testing connection	19
		UPS	4, 62
F		Network interface	7
firmware report	233	network interface statistics	239
firmware, updating	276, 279	network IP report	235
frequencies	297	network map	36
		NMS	5
H		application logs	246
hardware, replacing	280	client	5
humidity	261	repairing workstation	281
		server	4, 5
I		transaction logs	248
icons	32	workstation	21
RFSM	111		
RFSM switch control	213	O	
installing, RFSM	112	opening records	33
Internet, connecting to the NAP	68	operating channel frequencies	297

P		
passwords		
CCU	72	
EUM	89	
RFSM	117	
SNMPc Server	36	
ping test	174	
polling engine		
re-establishing polling	225	
RFSM	123, 214	
power failure	262	
priorities	153	
Properties screen	33	
R		
Radio	245	
radio		
CCU radio channel	74	
radio frequency subsystem	9	
radio properties		
CCU	73	
EUM	91	
radio transmission		
enabling on CCU	75	
radio, enabling on CCU	75	
RADIUS	6	
log parameters	250	
server error log	251	
server statistics	253	
server user log	252	
records		
creating EUM	87	
management	23	
opening	33	
recovering from power failure	262	
redundancy	143	
refreshing RFSM display	214	
removing an EUM	268	
repairing NMS workstation	281	
replacing		
CCU	215	
hardware components	280	
reports		
accounts	231	
CCU firmware	233	
EUM firmware	233	
network IP	235	
running	229	
service level	234	
SNMPc trend	237	
RFSM		
configuring	115	
connections to CCUs	118	
display refresh	214	
icons	111	
installing	112	
LED colors	212	
monitoring CCU status	211	
password	117	
polling engine	123, 214	
re-establishing polling	225	
service	121	
switch control icons	213	
switching configurations	221	
updating firmware	279	
RIP	95	
router	53	
routing		
CCU routing tables	76	
EUM routing tables	93	
static	76	
running reports	229	
S		
schedules	160	
backups	177, 193	
service level		
EUM	101	
service levels		
report	234	
services		
RFSM	121	
shortcut menus	28	
SNMP		
CCU properties	78	
communities	80	
EUM properties	97	
trap servers	81	
SNMPc		
backing up	184	
communities	39	
network map	36	
password	36	
Server	7	
server device management details	254	
server event logs	258	
trend report	237	
trend reports	40	
specifications	321	
SQL		
Agent	7	
Server	6	
static routing	76, 93	
statistics		
IP	242	
network interface	239	
RADIUS server	253	

subscribers	101, 269
disabling	267
switch control icons	213
switching CCU configurations	221
synchronizing database information . . .	275
system security parameters	151

T

temperature.	261
testing	
continuous receive.	170
continuous transmit	168
ping test	174
transmit/receive loopback.	172
traffic policy.	161
transmit/receive loopback test	172
trap servers	
CCU	81
trend reports	40
troubleshooting	283

U

updating	
EUM and CCU firmware.	276
RFSM firmware	279
upload configuration	
EUM.	101
UPS	4, 9, 62
battery	15

V

Veritas Backup Exec	7
Vircom VOP RADIUS.	6

W

Windows NT	5
----------------------	---

— This page is intentionally left blank —



Telephone: +1 416-502-3161
Fax: +1 416-502-2968
Email: techsupport@waverider.com
URL: www.waverider.com